SANS | GIAC CERTIFICATIONS

2025

Guide des carrières de la cybersécurité

Trouvez votre voie. Développez de nouvelles compétences. Prouvez votre expertise.

Zoom sur les nouvelles formations

- **ICS310 :** ICS Cybersecurity Foundations™
- **SEC406 :** Linux Security for InfoSec Professionals™
- **SEC480 :** AWS Secure Builder™
- **SEC495 :** Leveraging LLMs: Building and Securing RAG, Contextual RAG, and Agentic RAG™
- **SEC547 :** Defending Product Supply Chains™
- **SEC598 :** Security Automation for Offense, Defense, and Cloud™
- **LDR419 :** Performing A Cybersecurity Risk Assessment™
- **LDR519 :** Cybersecurity Risk Management and Compliance™
- **LDR520 :** Cloud Security for Leaders™
- **LDR553 :** Cyber Incident Management™
- **FOR577 :** Linux Incident Response and Threat Hunting™
- **FOR589 :** Cybercrime Intelligence™

+80 formations pratiques

+120 formateurs certifiés SANS Certified Instructor

+55 certifications GIAC

Découvrez nos
plus de 120
formateurs certifiés SANS Certified Instructor

Découvrez votre avenir dans la cybersécurité

Bienvenue dans le catalogue de formation SANS 2025. Depuis plus de 35 ans, notre mission est d'accompagner la montée en compétences des membres de la communauté cyber.

Ce guide, par une sélection de métiers, de parcours et de compétences essentielles, propose un référentiel complet pour accompagner votre développement professionnel à chaque étape. Il présente les formations recommandées pour des rôles spécifiques et des domaines clés, s'aligne sur le cadre NICE, et met en lumière certaines des carrières les plus passionnantes du secteur.

Nous espérons qu'il vous aidera, vous et votre équipe, à planifier votre avenir collectif. Quand vous serez prêts, SANS sera à vos côtés pour former, valider et certifier les compétences et connaissances afin de hisser votre expertise en cybersécurité au niveau supérieur.

À problèmes réels, experts réels

Apprenez la cybersécurité auprès d'instructeurs de terrain.

Bénéficiez des conseils avisés de nos instructeurs et auteurs de formation reconnus – 100 % d'entre eux sont en activité et s'échinent chaque jour à résoudre des problèmes de cybersécurité concrets et de premier plan.

Heather Barnhart
Enquêtrice chevronnée, elle est intervenue sur des affaires variées allant de l'exploitation des enfants aux médias d'Oussama Ben Laden en passant par des homicides.

David Hoelzer
Chercheur au centre de recherche Cybermedia Research, au centre Identity Theft and Financial Fraud Research Operations Center, et au laboratoire Internet Forensics Lab.

Robert M. Lee
Plusieurs fois auditionné par le Congrès américain pour son expertise des cybermenaces sur les infrastructures critiques.

Se former, se certifier, briller

Des formations, labos et certifications pointus pour monter sereinement en compétences.

Que vous soyez novice ou expérimenté en stratégies cyber, SANS vous propose plus de 80 formations pratiques et un accès à plus de 55 certifications GIAC. Notre objectif : vous fournir des compétences que vous pourrez déployer immédiatement, à tous les stades de votre carrière.

Apprendre en toute flexibilité

In-Person

- Formation en immersion, loin de toute distraction
- Réseautage auprès de spécialistes du même secteur
- Ateliers pratiques en bonus
- Événements exclusifs pour les stagiaires

Live Online

- Formation interactive à suivre du bureau ou depuis le confort de votre domicile
- Accès en temps réel aux équipes de formation, aux instructeurs et aux assistants
- Sessions bonus sur des thèmes d'actualité

OnDemand

- E-learning flexible à votre rythme
- Quatre mois d'accès aux supports de formation et labos, en tout lieu et à tout moment
- Accompagnement en direct par des experts techniques certifiés GIAC

Private

- Discussion sur mesure adaptée au secteur
- Lieu choisi pour réduire les frais de déplacement
- Calendrier flexible calé sur vos impératifs

Philip Hagen
Il a développé et maintient la distribution SOF-ELK, une appliance virtuelle préconfigurée avec la pile ELK.

Frank Kim
Ancien RSSI de SANS Institute, où il pilotait la fonction des risques informationnels au sein de la source de formation et de certification en cybersécurité la plus respectée au monde.

Sélectionnez les formations et certifications alignées avec votre plan de carrière

Sommaire

Se former, se certifier, briller	1
Apprendre en toute flexibilité	1
Trouvez votre formation – par axe	3
Trouvez votre formation – référentiel NICE	4
Trouvez votre formation – cadre ECSF	5
SANS Training Roadmap	6
New2Cyber – Fondamentaux de la cybersécurité et de l'IT	8
Offensive Operations	13
Cloud Security	29
Cyber Defense	39
Cybersecurity Leadership	54
Digital Forensics & Incident Response (DFIR) and Threat Hunting	69
Industrial Control Systems (ICS) Security	84
SANS Stay Sharp	92
Cyber Ranges – NetWars	93
SANS OnDemand	94
Formation intra-entreprise en cybersécurité	95
SANS Security Awareness	96
Certifications GIAC	98
SANS Executive Cyber Exercises	99
SANS Summits	100
Ressources gratuites en cybersécurité	101

Chez SANS, nous nous consacrons à la transmission et à la validation de compétences pratiques parce que, nous le savons, au sein de l'équipe de cybersécurité, chacun a un rôle à jouer pour dresser cette ligne de défense essentielle dans la bataille contre des adversaires en perpétuelle évolution.

Le catalogue comprend 80 formations et 55 certifications GIAC réparties en 7 axes afin de vous assurer de trouver et d'acquérir les compétences en phase avec vos intérêts et votre plan de carrière.

Quelle que soit la formation recherchée, avec son programme allant d'un socle de tactiques défensives à l'expertise hyperspécialisée comme l'analyse de logiciels malveillants et le développement d'exploits, SANS vous accompagne.

Nos formations et certifications aident les professionnels de la cybersécurité dans leur hétérogénéité à se développer et à valider leurs compétences.

Vous découvrez SANS ? Vous ne savez pas exactement quels thème ou niveau sélectionner pour votre prochaine formation ? Et si vous prévisualisiez sans frais une heure de formation sur la plateforme SANS OnDemand ?

Prévisualisez nos formations à **sans.org/demo**

Trouvez votre formation

Des formations ciblées en phase avec vos besoins et avec les pratiques du secteur.

Sept axes pointus pour les professionnels de la cybersécurité

Orientez-vous à l'aide des couleurs des cursus pour trouver votre formation idéale dans notre catalogue.

5 formations | 114 labos | 3 certifications

New2Cyber

New2Cyber sont des formations pratiques à la cybersécurité conçues pour que vous et vos équipes compreniez le mode de fonctionnement des attaquants, la mise en œuvre de la défense en profondeur et la réponse aux incidents afin de réduire les risques et de sécuriser correctement les systèmes.

Formations :

SEC275 SEC403 SEC406
SEC301 AIS247 SEC480
SEC401 ICS310
SEC402 SEC366

16 formations | 423 labos | 9 certifications

Offensive Operations

Les formations aux opérations offensives de SANS vont de l'introduction aux tests d'intrusion et au red teaming jusqu'aux compétences avancées, comme l'écriture de code d'exploitation et le développement d'infrastructure de commande et contrôle (C2) sur mesure. Nous proposons d'autres formations spécialisées, comme le fonctionnement en purple team, la sécurité des appareils mobiles ou sans fil, etc.

Formations :

SEC504 SEC575 SEC660
SEC535 SEC580 SEC670
SEC542 SEC588 SEC699
SEC556 SEC598 SEC760
SEC560 SEC599 SEC501
SEC565 SEC617

14 formations | 339 labos | 11 certifications

Digital Forensics and Incident Response

Notre cursus DFIR d'inforensique et de réponse aux incidents vous enseignera à détecter les systèmes compromis, à identifier quand et comment une intrusion a lieu, à comprendre ce que l'attaquant a volé ou modifié, et à contenir les incidents et y remédier.

Formations :

FOR498 FOR528 FOR589
FOR500 FOR572 FOR608
FOR508 FOR577 FOR610
FOR509 FOR578 FOR710
FOR518 FOR585 ICS515

15 formations | 193 labos | 7 certifications

Cybersecurity Leadership

Le cursus de leadership en sécurité de SANS forme les leaders cyber au profil pratique à constituer et à mener des équipes de sécurité, à communiquer avec les responsables techniques et métier, et à développer les capacités garantes du succès de leur organisation.

Formations :

AIS247 LDR514 LDR551
LDR414 LDR516 LDR553
LDR419 LDR519 SEC366
LDR433 LDR520 SEC405
LDR512 LDR521 SEC566

12 formations | 381 labos | 8 certifications

Cyber Defense

Le cursus intensif de cyberdéfense en immersion de SANS est conçu pour vous aider, vous et vos équipes, à maîtriser les étapes concrètes de défense des systèmes et des applications contre les menaces les plus dangereuses.

Formations :

SEC406 SEC530 SEC275
SEC450 SEC547 SEC301
SEC495 SEC555 SEC401
SEC501 SEC573 SEC497
SEC503 SEC595 SEC587
SEC511 SEC673

7 formations | 105 labos | 3 certifications

Industrial Control Systems

Le cursus sur la sécurité des systèmes de contrôle industriel de SANS propose des formations pratiques conçues pour faire acquérir des stratégies offensives et défensives afin de protéger les environnements des systèmes de contrôle industriel (ICS).

Formations :

ICS310 ICS456 ICS613
ICS410 ICS515
ICS418 ICS612

2 formations | 49 labos | 1 certification

Open-Source Intelligence

Les formations en renseignement de sources ouvertes viennent soutenir les efforts des professionnels pour les aider à déterminer les besoins de leurs clients, puis à collecter les données pertinentes à leurs investigations dans les sources ouvertes, surtout sur internet.

Formations :

SEC497
SEC587

8 formations | 172 labos | 6 certifications

Cloud Security

Le cursus de sécurité du cloud de SANS prépare les professionnels de la cybersécurité à concevoir, construire, déployer et gérer des infrastructures, plateformes et applications cloud afin de détecter, prévenir et contrer les menaces les plus préjudiciables au cloud.

Formations :

SEC480 SEC540 FOR509
SEC488 SEC541 LDR520
SEC510 SEC545 SEC588
SEC522 SEC549

Trouvez votre formation par fonction à l'aide du référentiel NICE

Le référentiel NICE (National Initiative for Cybersecurity Education) est un socle essentiel pour décrire et échanger les informations sur les métiers de la cybersécurité.

Il vous sert à identifier les formations et certifications pertinentes pour une fonction, la vôtre ou celle que vous visez.

Design and Development

Ces formations mènent des recherches, conceptualisent, conçoivent, développent et testent des systèmes techniques, notamment sur les réseaux cloud et du périmètre.

Formations :

LDR512 SEC510 SEC556
LDR516 SEC511 SEC560
SEC301 SEC522 SEC566
SEC401 SEC530 SEC573
SEC402 SEC540 SEC588
SEC403 SEC542 SEC673
SEC488 SEC549

Implementation and Operation

Ces formations servent à implémenter, administrer, configurer, opérer et assurer la maintenance des systèmes technologiques pour garantir des performances et une sécurité efficaces et efficientes.

Formations :

FOR578 SEC402 SEC566
LDR516 SEC403 SEC573
LDR551 SEC488 SEC595
SEC301 SEC504 SEC598
SEC401 SEC510 SEC673

Oversight and Governance

Ces formations servent à apporter leadership, gestion, direction et sensibilisation pour que l'organisation gère avec efficacité les risques à la cybersécurité de l'entreprise et mène des travaux de cybersécurité.

Formations :

ICS418 LDR519 SEC402
ICS456 LDR520 SEC403
LDR419 LDR521 SEC488
LDR433 LDR551 SEC504
LDR512 LDR553 SEC549
LDR514 SEC301
LDR516 SEC401

Protection and Defense

Ces formations servent à protéger les systèmes techniques et réseaux contre les risques, et à identifier et analyser ceux-ci. Elles comprennent l'investigation d'événements ou crimes cyber touchant des réseaux et des systèmes techniques.

Formations :

FOR508 ICS515 SEC556
FOR509 LDR516 SEC560
FOR518 LDR553 SEC565
FOR528 SEC401 SEC573
FOR572 SEC450 SEC588
FOR577 SEC503 SEC598
FOR578 SEC504 SEC599
FOR585 SEC510 SEC660
FOR589 SEC511 SEC670
FOR608 SEC522 SEC673
FOR610 SEC540 SEC699
FOR710 SEC541
ICS410 SEC542

Cyberspace Intelligence

Ces formations visent à collecter, traiter, analyser et communiquer les informations, issues de toutes les sources de renseignement, sur les acteurs étrangers – leurs programmes dans le cyberespace, leurs intentions, leurs capacités, leur recherche et développement, et leurs activités opérationnelles.

Formations :

FOR578 SEC541 SEC599
FOR589 SEC542 SEC660
ICS515 SEC560 SEC699
LDR553 SEC565 SEC760
SEC504

Cyberspace Effects

Ces formations servent à planifier, prendre en charge et exécuter des capacités dans le cyberespace avec pour premier objectif la défense externe ou la projection de forces dans le cyberespace ou au travers de celui-ci.

Formations :

FOR508 SEC504 SEC588
FOR528 SEC541 SEC599
FOR532 SEC542 SEC660
FOR572 SEC556 SEC673
FOR577 SEC560 SEC699
FOR578 SEC565
FOR589 SEC573

Investigation

Ces formations servent à mener des enquêtes sur des événements ou crimes cybernétiques ayant un lien avec les systèmes IT, le réseau et les preuves informatiques.

Formations :

FOR498 FOR572 FOR610
FOR500 FOR577 FOR710
FOR508 FOR578 SEC504
FOR509 FOR585 SEC573
FOR518 FOR589
FOR528 FOR608

Industrial Control Systems

Ces formations composent un référentiel de sécurité qui protège la technologie opérationnelle et les systèmes de contrôle industriel contre les risques intentionnels ou accidentels.

Formations :

ICS410 ICS456 ICS612
ICS418 ICS515 ICS613

Trouvez votre formation par fonction à l'aide du cadre ECSF

Trouvez le bon parcours de formation pour vous et pour votre organisation.

Le cadre européen des compétences en cybersécurité, dit ECSF (European Cybersecurity Skills Framework), fournit un outil pratique qui facilite l'identification et l'articulation des tâches, des aptitudes, des compétences et des connaissances associées aux métiers des professionnels européens de la cybersécurité. Il décrit 12 profils types de la cybersécurité, avec pour principal objectif de créer un langage commun entre les talents, les employeurs et les organismes de formations au sein de l'UE. SANS a corrélé ses propres formations aux 12 profils ECSF afin que vous trouviez celle qui vous convient selon votre fonction actuelle ou à venir.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Chief Information Security Officer (CISO)

LDR512 (GSLC)
LDR514 (GSTRT)
LDR520
LDR521
LDR551 (GSOM)

Cyber Incident Responder

SEC504 (GCIH)
FOR508 (GCFA)
FOR509 (GCFR)
FOR528
FOR572 (GNFA)
FOR608 (GEIR)
FOR710
LDR553 (GCIL)

Cyber Legal, Policy, and Compliance Officer

LDR514 (GSTRT)

Cyber Threat Intelligence Specialist

SEC504 (GCIH)
FOR509 (GCFR)
FOR528
FOR578 (GCTI)
FOR710

Cybersecurity Architect

SEC530 (GDSA)
SEC549 (GCAD)

Cybersecurity Educator

SEC275 (GFACT)
SEC401 (GSEC)
SEC403
SEC504 (GCIH)

Cybersecurity Implementer

SEC450 (GSOC)
SEC501 (GCED)
SEC504 (GCIH)
SEC511 (GMON)
SEC522 (GWEB)

Cybersecurity Researcher

SEC566 (GCCC)
LDR516

Cybersecurity Risk Manager

SEC301 (GISF)
LDR512 (GSLC)
LDR419

Digital Forensics Investigator

FOR498 (GBFA)
FOR500 (GCFE)
FOR508 (GCFA)
FOR528
FOR572 (GNFA)
FOR578 (GCTI)
FOR608 (GEIR)

Penetration Tester

SEC542 (GWAPT)
SEC560 (GPEN)
SEC588 (GCPN)
SEC660 (GXPN)

SANS Training Roadmap

Topic | Course Code | GIAC Certification

Essentials | ICS410 **ICS/SCADA Security Essentials™** | GICSP

Course Title

Baseline Skills

NEW TO CYBERSECURITY | COMPUTERS, TECHNOLOGY, AND SECURITY

COMPUTER & IT FUNDAMENTALS	SEC275 **Foundations: Computers, Technology & Security™** | GFACT
CYBERSECURITY FUNDAMENTALS	SEC301 **Introduction to Cyber Security™** | GISF

These entry-level courses cover a wide spectrum of security topics and are liberally sprinkled with real-life examples. A balanced mix of technical and managerial issues makes these course appealing to attendees who need to understand the salient facets of information security basics and the basics of risk management.

CORE TECHNIQUES | PREVENT, DEFEND, MAINTAIN

SECURITY ESSENTIALS	SEC401 **Security Essentials: Network, Endpoint, and Cloud™** | GSEC

Whether you are new to information security or a seasoned practitioner with a specialized focus, SEC401 will provide the essential information security skills and techniques you need to protect and secure your critical information and technology assets, whether on-premise or in the cloud.

LINUX SECURITY	SEC406 **Linux Security for InfoSec Professionals**
BLUE TEAM	SEC450 **Blue Team Fundamentals: Security Operations and Analysis™** | GSOC
ATTACKER TECHNIQUES	SEC504 **Hacker Tools, Techniques, and Incident Handling™** | GCIH

All professionals entrusted with hands-on cybersecurity work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense in depth, understand how attacks work, and manage incidents when they occur. To be secure, you should set a high bar for the baseline set of skills in your security organization.

ROLE-BASED TRAINING FROM SANS SECURITY AWARENESS

Security Essentials for IT Administrators

Role-based PCI DSS Compliance Training

Protecting against cyber threats require continuous investment in skills development. Short-form modular training provides various teams with a role-focused understanding of evolving security concepts.

FORENSICS ESSENTIALS

DIGITAL ACQUISITION AND RAPID TRIAGE	FOR498 **Digital Acquisition and Rapid Triage™** | GBFA

CLOUD SECURITY

ESSENTIALS	SEC488 **Cloud Security Essentials™** | GCLD

If you are new to cybersecurity or looking to up-skill, cloud security essentials is a requirement for today's organizations. This course provides the basic knowledge required to introduce students to the cloud security industry, as well as in-depth, hands-on practice in labs.

Cloud Security for Developers

AWS	SEC480 **AWS Secure Builder™** | AWS Secure Builder Micro-Credential by GIAC

Focused Job Roles

DESIGN, DETECTION, AND DEFENSIVE CONTROLS

Focused Cyber Defense Skills

ADVANCED GENERALIST	SEC501 **Advanced Security Essentials – Enterprise Defender™** | GCED
MONITORING & OPERATIONS	SEC511 **Cybersecurity Engineering: Advanced Threat Detection and Monitoring™** | GMON
SECURITY ARCHITECTURE	SEC530 **Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise™** | GDSA

The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and to interpret their output.

Open-Source Intelligence

OSINT	SEC497 **Practical Open-Source Intelligence (OSINT)™** | GOSI

OFFENSIVE OPERATIONS | PENETRATION TESTING, OFFENSIVE SECURITY

Every Offensive Professional Should Know

NETWORK PEN TESTING	SEC560 **Enterprise Penetration Testing™** | GPEN
WEB APPS	SEC542 **Web App Penetration Testing and Ethical Hacking™** | GWAPT

The professional who can find weakness is often a different breed than one focused exclusively on building defenses. A basic tenet of Red Team/Blue Team deployments is that finding vulnerabilities requires different ways of thinking and different tools. Offensive skills are essential for cybersecurity professionals to improve their defenses.

INCIDENT RESPONSE & THREAT HUNTING | HOST & NETWORK FORENSICS

ENDPOINT FORENSICS	FOR500 **Windows Forensic Analysis™** | GCFE FOR508 **Advanced Incident Response, Threat Hunting, and Digital Forensics™** | GCFA FOR608 **Enterprise-Class Incident Response & Threat Hunting™** | GEIR
NETWORK FORENSICS	FOR572 **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response™** | GNFA

Whether you're seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.

CORE CLOUD SECURITY

Preparation for More Focused Job Functions

PREVENTION	SEC510 **Cloud Security Controls and Mitigations™** | GPCS
AUTOMATION & DEVSECOPS	SEC540 **Cloud Native Security and DevSecOps Automation™** | GCSA

Specific Skills, Specialized Roles

ADVANCED CYBER DEFENSE | HARDEN SPECIFIC DEFENSES

Topic-Focused

TRAFFIC ANALYSIS	SEC503 **Network Monitoring and Threat Detection In-Depth™** | GCIA
SIEM	SEC555 **Detection Engineering and SIEM Analytics™** | GCDA
PYTHON CODING	SEC573 **Automating Information Security with Python™** | GPYC SEC673 **Advanced Information Security Automation with Python™**
DATA SCIENCE	SEC595 **Applied Data Science and AI/Machine Learning for Cybersecurity Professionals™** | GMLE

Open-Source Intelligence

OSINT	SEC587 **Advanced Open-Source Intelligence (OSINT) Gathering & Analysis™**

SPECIALIZED OFFENSIVE OPERATIONS | FOCUSED TECHNIQUES & AREAS

Network, Web, and Cloud

EXPLOIT DEVELOPMENT	SEC660 **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking™** | GXPN SEC760 **Advanced Exploit Development for Penetration Testers™**
CLOUD	SEC588 **Cloud Penetration Testing™** | GCPN

Specialized Penetration Testing

SOCIAL ENGINEERING	SEC467 **Social Engineering for Security Professionals™**
AI	SEC535 **Offensive AI – Attack Tools and Techniques™**
RED TEAM	SEC565 **Red Team Operations and Adversary Emulation™** | GRTP SEC670 **Red Teaming Tools – Developing Windows Implants, Shellcode, Command and Control™**
MOBILE	SEC575 **iOS and Android Application Security Analysis and Penetration Testing™** | GMOB
PEN TESTING	SEC580 **Metasploit for Enterprise Penetration Testing™**
WIRELESS & IoT	SEC556 **IoT Penetration Testing™** SEC617 **Wireless Penetration Testing and Ethical Hacking™** | GAWN

Purple Team

DETECTION ENGINEERING	SEC598 **Security Automation for Offense, Defense, and Cloud™** SEC599 **Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses™** | GDAT SEC699 **Advanced Purple Teaming – Adversary Emulation & Detection Engineering™**

DIGITAL FORENSICS, MALWARE ANALYSIS, & THREAT INTELLIGENCE | SPECIALIZED INVESTIGATIVE SKILLS

Specialization

CLOUD FORENSICS	FOR509 **Enterprise Cloud Forensics & Incident Response™** | GCFR
RANSOMWARE	FOR528 **Ransomware and Cyber Extortion™**

Training designed for non-security technical professionals to make a swift and significant impact on the security of AWS workloads.

ROLE-BASED TRAINING FROM SANS SECURITY AWARENESS

Developer Secure Code Training

Educate everyone involved in the software development process including developers, architects, managers, testers, business owners, and partners with role-focused training that ensures your team can properly build defensible applications from the start.

INDUSTRIAL CONTROL SYSTEMS SECURITY

FOUNDATIONS	ICS310 **ICS Cybersecurity Foundations™**
ESSENTIALS	ICS410 **ICS/SCADA Security Essentials™** | GICSP
MANAGEMENT	ICS418 **ICS Security Essentials for Leaders™**

FOUNDATIONAL LEADERSHIP

Every Cybersecurity Manager Should Know

CISSP® TRAINING	LDR414 **SANS Training Program for CISSP® Certification™** | GISP
SECURITY AWARENESS	LDR433 **Managing Human Risk™** | SSAP
RISK ASSESSMENT	LDR419 **Performing a Cybersecurity Risk Assessment™**
CIS IG1	SEC366 **CIS Implementation Group 1™**

With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those leaders will not necessarily perform hands-on work, but they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.

ROLE-BASED TRAINING FROM SANS SECURITY AWARENESS

EndUser Awareness Training

Engaging, modular, and multilingual end-user training focuses on the most pressing risk and compliance topics to address employee security behaviors and develop a culture of security across your organization.

CYBER RANGES

MULTI-SKILL MULTI-DISCIPLINE	BootUp CTF Core NetWars SANS Skills Quest by NetWars

SANS Cyber Ranges provide interactive hands-on exercises that cover a wide range of topics to solidify skills and create muscle memory.

ARTIFICIAL INTELLIGENCE

AI Security Essentials

LEADERSHIP	AIS247 **AI Security Essentials for Business Leaders™**
THREAT HUNTING & DEFENSE	SEC595 **Applied Data Science and AI/Machine Learning for Cybersecurity Professionals™** | GMLE
APPLICATION SECURITY	SEC495 **Leveraging LLMs: Building & Securing RAG, Contextual RAG, and Agentic RAG™** SEC545 **GenAI and LLM Application Security™**

ROLE-BASED TRAINING FROM SANS SECURITY AWARENESS

Workforce Risk Management Fundamentals for AI

Designed for employees across all roles—from marketing to developers—this training prepares your team to adopt and use AI technologies safely and effectively.

MONITORING & DETECTION	SEC541 **Cloud Security Threat Detection™** | GCTD
ARCHITECTURE	SEC549 **Cloud Security Architecture™** | GCAD

With the massive global shift to the cloud, it becomes more critical for every organization to have experts who understand the security risks and benefits that come with public cloud use, how to navigate and take full advantage of multicloud environments, and how to incorporate security from the start of all development projects.

INDUSTRIAL CONTROL SYSTEMS SECURITY

DEFENSE & RESPONSE	ICS515 **ICS Visibility, Detection, and Response™** | GRID
ADVANCED SECURITY	ICS612 **ICS Cybersecurity In-Depth™** ICS613 **ICS/OT Penetration Testing & Assessments™**
NERC Protection	
NERC SECURITY ESSENTIALS	ICS456 **Essentials for NERC Critical Infrastructure Protection™** | GCIP

Industrial systems run the world, and the need for cyber security professionals to defend them is critical. Learn the skills needed to safeguard critical infrastructure for the sake of operations, national security, and the safety of human life.

STRATEGIC LEADERSHIP FOR CISOs

Transformational Cybersecurity Leader

TECHNOLOGY LEADERSHIP	LDR512 **Security Leadership Essentials for Managers™** | GSLC
SECURITY STRATEGY	LDR514 **Security Strategic Planning, Policy, and Leadership™** | GSTRT
SECURITY CULTURE	LDR521 **Security Culture for Leaders™**

Operational Cybersecurity Executive

VULNERABILITY MANAGEMENT	LDR516 **Building and Leading Vulnerability Management Programs™**
SOC	LDR551 **Building and Leading Security Operations Centers™** | GSOM
CIS CONTROLS	SEC566 **Implementing and Auditing CIS Controls™** | GCCC

Cyber Risk Officer

TECHNOLOGY LEADERSHIP	LDR512 **Security Leadership Essentials for Managers™** | GSLC
RISK & COMPLIANCE	LDR519 **Cybersecurity Risk Management and Compliance™**
INCIDENT RESPONSE	LDR553 **Cyber Incident Management™** | GCIL

CYBER RANGES

Practice for Focused Job Functions

CYBER DEFENSE	Cyber Defense NetWars
DIGITAL FORENSICS & INCIDENT RESPONSE	DFIR NetWars DFIR NetWars Continuous
INDUSTRIAL CONTROL SYSTEMS	ICS NetWars
POWER GENERATION AND DISTRIBUTION	GRID NetWars

These interactive hands-on learning exercises cover specific job roles for in-depth practical application and assessment of cybersecurity subject matter to help advance your career in a specific field.

MALWARE ANALYSIS	FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques™** | GREM FOR710 **Reverse-Engineering Malware: Advanced Code Analysis™**

Threat Intelligence

CYBER THREAT INTELLIGENCE	FOR578 **Cyber Threat Intelligence™** | GCTI FOR589 **Cybercrime Investigations™**

Digital Forensics and Media Exploitation

SMARTPHONES	FOR585 **Smartphone Forensic Analysis In-Depth™** | GASF
MAC FORENSICS	FOR518 **Mac and iOS Forensic Analysis and Incident Response™** | GIME
LINUX FORENSICS	FOR577 **LINUX Incident Response and Threat Hunting™** | GLIR

SPECIALIZATION IN CLOUD SECURITY

Specialization for Advanced Skills and Roles

APPLICATION SECURITY	SEC522 **Application Security: Securing Web Apps, APIs, and Microservices™** | GWEB
AI APPLICATION SECURITY	SEC545 **GenAI and LLM Application Security™**
CLOUD PEN TEST	SEC588 **Cloud Penetration Testing™** | GCPN
CLOUD FORENSICS	FOR509 **Enterprise Cloud Forensics and Incident Response™** | GCFR
CLOUD DESIGN & IMPLEMENTATION	LDR520 **Cloud Security for Leaders™**

Learning how to convert traditional cybersecurity skills into the nuances of cloud security is a necessity for proper monitoring, detection, testing, and defense.

ROLE-BASED TRAINING FROM SANS SECURITY AWARENESS

ICS Cybersecurity Awareness Training

NERC CIP Compliance Training

Help protect critical systems by reinforcing the behavior your engineers, system operators and others who interact with operational technology environments require to prevent, identify and respond to cyber incidents.

LEADERSHIP SPECIALIZATIONS

Management Specialization

CLOUD DESIGN & IMPLEMENTATION	LDR520 **Cloud Security for Leaders™**
PROJECT MANAGEMENT	LDR525 **Managing Cybersecurity Initiatives & Effective Communication™** | GCPM

ROLE-BASED TRAINING FROM SANS SECURITY AWARENESS

Security Essentials for Business Leaders and Managers

Leadership-focused modules enable managers to efficiently build and sustain a secure digital environment crucial for business operations.

AXE DE FORMATION SANS

NEW2CYBER Fondamentaux de la cybersécurité et de l'IT

Tous les professionnels qui se voient confier des tâches pratiques de cybersécurité devraient acquérir un socle commun de compétences sur le fonctionnement des attaques, la mise en œuvre d'une défense en profondeur et la réponse aux incidents afin de réduire les risques et de sécuriser correctement les systèmes.

La sécurité dicte de placer haut la barre lorsque vous définissez ce socle de compétences dans votre organisation. À l'issue d'une formation New2Cyber de SANS, vous saurez :

- Adopter des techniques axées sur les problèmes de sécurité prioritaires dans votre organisation
- Établir un socle solide de politiques et pratiques fondamentales pour entraîner votre équipe de sécurité à la réponse aux incidents
- Déployer une panoplie de stratégies et techniques pour défendre une entreprise sous tous ses angles
- Identifier les vecteurs d'attaque les plus récents et mettre en œuvre des contrôles pour les prévenir et les détecter
- Utiliser des stratégies et des outils pour détecter les attaques
- Développer des indicateurs de sécurité pertinents formant la base d'un guide opérationnel à implémenter par l'équipe IT, à valider par les auditeurs et compréhensible par la direction
- Mettre en œuvre un programme exhaustif de sécurité axé sur la prévention et la détection des attaques et la réponse à y apporter
- Développer une feuille de route de sécurité interne évolutive pour répondre aux besoins d'aujourd'hui et de demain

« Cette formation dresse un panorama complet de la sécurité... Cette manne d'informations vous servira à déterminer des problèmes de sécurité que vous n'aviez même pas envisagés. »

— Frank Perrelli, **IESO**

Fonctions New2Cyber :

- Analyste sécurité
- Analyste inforensique
- Ingénieur sécurité
- Responsable technique
- Auditeur

SEC275: **Foundations: Computers, Technology & Security™**

GFACT
Foundational Cybersecurity Technologies
DoD 8140*
giac.org/gfact

4 jours	38 crédits CPE	80 labos

Vous apprendrez à...

- Connaître les principaux composants matériels et les notions de mémoire afférentes
- Comprendre les usages de la virtualisation et des conteneurs, leurs avantages et leurs inconvénients
- Vous familiariser avec l'anatomie des exploits courants, la méthodologie et les outils des attaquants
- Vous familiariser avec les outils d'investigation inforensique et leur fonction
- Utiliser vos connaissances acquises sur le contrôle d'accès, les autorisations et les commandes Linux les plus courantes
- Maîtriser les bases des notions réseau, des protocoles, des différents types de serveurs, et leurs utilisations
- Déterminer le résultat d'une opération logique élémentaire
- Appréhender la syntaxe de programmation, les constructs et les erreurs des principaux langages
- Reconnaître les différents systèmes de fichiers, les technologies web et les modèles de cloud computing
- Vous approprier les notions et la terminologie de la cryptographie
- Connaître les questions éthiques et juridiques en lien avec le piratage
- Comprendre les étapes d'une attaque, ainsi que les stratégies et concepts clés de défense
- Vous familiariser avec les principales commandes CLI, les permissions et le contrôle d'accès sous Windows

Public visé :

- Personnes en réorientation professionnelle
- Autodidactes en ligne en quête de nouvelles compétences
- Étudiants des premier et deuxième cycles
- Professionnels sans connaissances approfondies en cybersécurité
- Nouvelles recrues en IT/cybersécurité
- Personnes en reconversion

James Lyne
Auteur de la formation

*DoD 8140 APPROVED
sans.org/8140

SANS Foundations est la formation certifiée d'introduction à la cybersécurité la plus exhaustive du marché. Développée par les plus grands spécialistes, SEC275™ établit un socle de connaissances et de compétences en cybersécurité qui donne aux profils non techniques et sans expérience du secteur une maîtrise suffisante pour parler la même langue que les professionnels. Accompagné par des formateurs de renom, vous acquérez les notions fondamentales de sécurité et d'informatique et développez vos compétences de programmation dans un environnement pédagogique interactif, au travers de cours en vidéo et d'exercices et labos pratiques. SANS Foundations vous apporte des compétences pratiques, de terrain, qui vont bien plus loin que n'importe quelle autre formation aux bases de la cybersécurité.

Maîtrisez les fondamentaux de la cybersécurité

Bilan

- Vous réduisez le risque de lacunes en connaissances cyber fondamentales dans votre organisation.
- Vous réduisez les coûts du recrutement externe en faisant monter en compétences votre équipe IT actuelle.
- Vous assurez aux néophytes un socle solide qui portera leur réussite dans des formations avancées.
- Vous stimulez la croissance de l'entreprise en formant vos collaborateurs techniques au plus haut niveau.
- Vous justifiez l'investissement avec la certification GFACT, qui valide les acquis des collaborateurs.
- Vous concevez des schémas d'intégration efficaces pour vos collaborateurs, avec l'assurance que les bases de la cybersécurité seront connues.

« Je trouve que SANS Foundations est le meilleur point de départ, qu'on ait ou pas un profil IT. Les exemples sont nombreux, du niveau débutant à intermédiaire. »

— Sri Ayu Ningsih, **Aleph-Labs**

« Même si j'occupe un poste sénior dans la sécurité, SANS Foundations est un outil fantastique pour réviser les concepts importants et m'a aidé à mieux m'acquitter de mes responsabilités. »

— Noah Pack

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC275**

MODES DE FORMATION DE SEC275

OnDemand

SEC301: **Introduction to Cyber Security™**

GISF Information Security Fundamentals
giac.org/gisf
ANAB ACCREDITED ISO/IEC 17024 PERSONNEL CERTIFICATION BODY
DoD 8140*

5 jours	30 crédits CPE	14 labos

Vous apprendrez à...

- Communiquer avec confiance sur divers sujets concernant la sécurité de l'information, les termes et les concepts
- Comprendre et appliquer les principes de moindre privilège
- Comprendre et appliquer la triade CIA (confidentiality, integrity, availability) pour classer les ressources de sécurité critiques par priorité
- Construire des mots de passe plus sécurisés, et plus faciles à retenir
- Acquérir les principes de la cryptographie, les processus, procédures et applications
- Comprendre le fonctionnement d'un ordinateur

Public visé :

- Tout novice en sécurité des informations qui cherche à s'initier aux fondamentaux de la sécurité
- Toute personne démunie face à une avalanche de termes techniques complexes dont la signification lui échappe
- Les professionnels qui ont besoin de se familiariser avec les concepts, principes et jargons généraux, sans pour autant vouloir entrer dans les détails
- Les personnes en reconversion vers le marché porteur de la sécurité des informations en quête d'une formation ou d'une certification reconnues
- Les responsables qui refusent que leur entreprise fasse les gros titres comme la dernière victime en date d'un piratage massif

Fonctions du référentiel NICE

- Authorizing Official/Designating Representative (OPM 611)
- Knowledge Manager (OPM 431)
- Privacy Officer/Privacy Compliance Manager (OPM 732)
- Cyber Instructor (OPM 712)
- Communications Security (COMSEC) Manager (OPM 723)

Keith Palmgren
Auteur de la formation

*DoD 8140 APPROVED
sans.org/8140

Moyen le plus rapide de monter en compétences en sécurité des informations, cette introduction est conçue et enseignée par des vétérans chevronnés de la cybersécurité. Elle couvre un large spectre de thèmes de sécurité agrémentés d'exemples issus du terrain. Les termes et concepts sont expliqués en détail et les labos pratiques les consolident. Cette formation, qui vulgarise une sélection équilibrée de sujets techniques, intéressera les personnes qui doivent comprendre les grandes facettes de la cybersécurité. Si vous devez acquérir rapidement un socle en cybersécurité, les explications de SEC301 et ses 14 ateliers répondent précisément au cahier des charges !

Bilan

- Vous sécurisez les actifs de votre organisation avec les principes de moindre privilège.
- Vous comprenez les fondamentaux des technologies d'authentification, d'autorisation, de chiffrement et de défense comme les pare-feu.
- Vous communiquez sur une large gamme d'attaques : ingénierie sociale, téléchargements furtifs, attaques par point d'eau, déplacement latéral, réseaux zombies « botnets », dépassement de mémoire tampon, etc.
- Vous évitez de subir le prochain piratage massif qui fera l'ouverture du 20 heures.

Programme

SECTION 1 : Bases de la cybersécurité

SECTION 2 : Introduction à la cryptographie

SECTION 3 : Authentification, autorisation et réseau

SECTION 4 : Sécurité sans fil, attaques réseau et logiciels malveillants

SECTION 5 : Technologies de la cybersécurité et sécurité web

« SEC301 est excellente sur le fond, elle couvre un large spectre d'informations applicables tant professionnellement que dans la vie. Les labos sont extrêmement instructifs et consolident les acquis. »

— Jimmy T., **militaire**

« Très bonne formation pour acquérir un socle de connaissances. Particulièrement utile en ce qu'elle étoffe les notions de base. »

— Shruti Iyer, **DCS Corporation**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC301**

MODES DE FORMATION DE SEC301

In-Person **Live Online** **OnDemand**

SEC401: **Security Essentials – Network, Endpoint, and Cloud™**

GSEC Security Essentials: giac.org/gsec — CyberLive DoD 8140*

6 jours	46 crédits CPE	20 labos

Vous apprendrez à...

- Maîtriser les grands domaines de la cybersécurité et savoir créer un programme de sécurité sur la base du triptyque détection, réponse, prévention
- Appliquer les conseils pratiques axés sur la résolution des problèmes de sécurité prioritaires dans l'organisation et prendre les mesures qui mènent à des solutions de sécurité efficaces
- Comprendre comment les attaquants adaptent leurs tactiques et leurs techniques et moduler votre défense en conséquence
- Appréhender la nature des ransomwares et mieux vous en protéger
- Tirer parti d'une architecture réseau défendable (VLAN, NAC et 802.1x) sur la base d'indicateurs de compromission APT
- Comprendre et appliquer la méthodologie de gestion des identités et des accès (IAM), y compris les aspects d'authentification forte (authentification multifacteur)

Public visé :

- Professionnels de la sécurité
- Responsables
- Collaborateurs opérationnels
- Ingénieurs et responsables IT
- Administrateurs
- Spécialistes de l'inforensique, experts en tests d'intrusion et auditeurs
- Toute personne novice en sécurité informatique avec une expérience des systèmes d'information et des réseaux

Fonctions du référentiel NICE

- Security Control Assessor (OPM 612)
- Database Administrator (OPM 421)
- Data Analyst (OPM 422)
- Technical Support Specialist (OPM 411)
- Network Operations Specialist (OPM 441)
- System Administrator (OPM 451)
- Systems Security Analyst (OPM 461)
- Cyber Instructional Curriculum Developer (OPM 711)
- IT Investment/Portfolio Manager (OPM 804)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Infrastructure Support Specialist (OPM 521)

Bryan Simon
Auteur de la formation

* DoD 8140 APPROVED
sans.org/8140

Sous menace permanente, les organisations doivent impérativement se tenir prêtes à la compromission qui finira par se matérialiser. Aujourd'hui plus que jamais, l'essentiel est la rapidité de détection et de réponse. Plus l'attaquant reste dans votre environnement, plus les effets seront dévastateurs. Peut-être qu'aujourd'hui, la question la plus cruciale en sécurité des informations est : « En combien de temps peut-on détecter une attaque, y répondre et y remédier ? »

La sécurité des informations consiste à focaliser vos défenses sur les zones qui comptent vraiment, d'autant que celles-ci dépendent des particularités de votre organisation. La formation SEC401™ vous enseigne les bases du langage et des rouages de la sécurité des informations et de l'informatique, et vous apprend à appliquer efficacement vos nouveaux acquis à vos enjeux spécifiques. Vous y acquerrez les connaissances indispensables pour sécuriser sereinement les systèmes ou les organisations.

SEC401™ vous enseigne les mesures les plus efficaces pour prévenir les attaques et détecter les assaillants – vous acquérez ainsi des techniques exploitables applicables dès votre retour au bureau. Éclairages et informations pratiques vous prépareront à gagner la bataille incessante contre les cyberattaquants aux profils variés qui tentent d'infiltrer votre environnement.

Bilan

- Vous savez traiter les enjeux de sécurité prioritaires.
- Vous exploitez les points forts et les différences des principaux clouds en matière de sécurité.
- Vous cartographiez pour gagner en visibilité sur le réseau et valider la surface d'attaque.
- Vous réduisez votre surface d'attaque par le renforcement et la gestion de la configuration.

Programme

SECTION 1 : Bases de la sécurité réseau et cloud
SECTION 2 : Défense en profondeur
SECTION 3 : Gestion des vulnérabilités et réponse
SECTION 4 : Technologies de sécurité des données
SECTION 5 : Sécurité Windows et Azure
SECTION 6 : Sécurité des conteneurs, de Linux et de Mac

« SEC401 offre une excellente présentation des fondamentaux de la sécurité délivrée par des professionnels chevronnés du secteur. »
— Jason W., **agence fédérale américaine**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC401**

MODES DE FORMATION DE SEC401

In-Person **Live Online** **OnDemand**

SEC402: **Cybersecurity Writing: Hack the Reader™**

2 jours | 12 crédits CPE

Vous apprendrez à...

- Utiliser les cinq clés d'une communication écrite efficace dans vos rapports, vos briefings, vos emails et vos autres écrits professionnels autour de la sécurité
- Intégrer ces éléments à votre arsenal par des exercices pratiques scénarisés à partir de situations réelles courantes
- Déterminer les grands enjeux à prendre en compte dans vos rapports sur la sécurité et vos autres communications écrites
- Comprendre comment choisir les mots, la structure, la présentation et le ton adaptés
- Améliorer immédiatement vos compétences en repérant et corrigeant les faiblesses dans des extraits de communication en sécurité
- Vous servir de listes de contrôle pratiques pour rédiger clairement et efficacement du premier coup

Public visé :

- Manager ou simplement membre de l'équipe
- Consultant ou collaborateur sans contact externe
- Spécialiste ou débutant
- Défenseur ou attaquant
- Terrien ou alien

Fonctions du référentiel NICE

- Authorizing Official/Designating Representative (OPM 611)
- Systems Requirements Planner (OPM 641)
- System Testing and Evaluation Specialist (OPM 671)
- Knowledge Manager (OPM 431)
- Cyber Legal Advisor (OPM 731)
- Cyber Instructor (OPM 712)
- Security Awareness & Communications Manager (OPM 712)
- IT Program Auditor (OPM 805)

Lenny Zeltser
Auteur de la formation

Vous voulez améliorer vos écrits ? Apprenez à voler l'attention du lecteur ! Découvrez comment trouver un angle, déjouer les défenses de vos lecteurs et capturer leur attention pour délivrer votre message, même s'ils sont trop occupés ou peu intéressés par les communications des autres. Cette formation unique en son genre, conçue sur mesure pour les professionnels de la cybersécurité, va renforcer vos compétences rédactionnelles et booster votre carrière.

Bilan

- Vous sécurisez les actifs de votre organisation avec les principes de moindre privilège.
- Vous appréhendez les fondamentaux de la gestion des risques, de la politique de sécurité, et de l'authentification, de l'autorisation et de la redevabilité.
- Vous apprenez à communiquer sur une large gamme d'attaques : ingénierie sociale, téléchargements furtifs, attaques par point d'eau, déplacement latéral et bien plus encore.
- Vous évitez de subir le prochain piratage massif qui fera l'ouverture du 20 heures.

Programme

SECTION 1 : Communiquer en cybersécurité : voler l'attention du lecteur – jour 1

SECTION 2 : Communiquer en cybersécurité : voler l'attention du lecteur – jour 2

« Les compétences de rédaction appliquées à la cybersécurité sont indispensables pour évoluer professionnellement. »

— R. Wajda, **Secure Cloud LLC**

« J'ai suivi une formation intra-entreprise pour améliorer la communication écrite juste avant de venir. J'ai remarqué des similitudes, mais l'angle cybersécurité ici est extrêmement précieux ! »

— Andrew Walker, **Novant Health**

« Remarquable formation. Elle offre un cadre d'évaluation et un guide de rédaction pour tout écrit futur. »

— Jordan Whitley, **New York Life**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC402**

MODES DE FORMATION DE SEC402

OnDemand

AXE DE FORMATION SANS

Offensive Operations

Dans une organisation, les tactiques offensives servent à déceler et à comprendre les vulnérabilités d'un système afin de corriger les problèmes avant qu'une attaque ne survienne.

Les adversaires évoluent et les attaques se sophistiquent : les experts en intrusion et les red teams doivent reproduire les techniques d'attaque qui existent sur le terrain, découvrir les problèmes et formellement documenter leurs constatations pour apporter toute leur valeur à l'équipe sécurité.

À l'issue d'une formation aux opérations offensives de SANS, vous saurez :

- Reproduire les attaques actuelles les plus puissantes et les plus courantes
- Découvrir des vulnérabilités dans des systèmes cibles
- Exploiter ces vulnérabilités dans un environnement contrôlé
- Mettre en œuvre votre expertise technique pour déterminer et documenter les risques et leur impact commercial potentiel
- Mener des tests sûrs et dans les règles de l'art, conformément au périmètre et aux règles d'engagement précisément définis
- Aider une organisation à hiérarchiser ses ressources par priorité

« En une semaine, le formateur nous a fait passer de l'analyse classique des vulnérabilités à l'art véritable des tests d'intrusion. Merci SANS d'avoir renforcé mes capacités en sécurité de l'information et celles de mon entreprise ! »

— Mike Dozier, **Savannah River Nuclear Solutions**

Fonctions des opérations offensives :

- Expert en tests d'intrusion système/réseau
- Expert en tests d'intrusion applicatifs
- Chargé de réponse aux incidents
- Spécialiste dans la recherche de vulnérabilités
- Développeur d'exploits
- Membre de red team
- Responsable sécurité mobile

SEC504: **Hacker Tools, Techniques, and Incident Handling™**

GCIH Incident Handler
giac.org/gcih

CyberLive
DoD 8140*

6 jours	38 crédits CPE	+30 labos

Public visé :

- Chargés de réponse aux incidents
- Chef d'équipe de réponse aux incidents
- Administrateurs système en première ligne pour défendre leurs systèmes et répondre aux attaques
- Tout autre personnel de sécurité intervenant en premier lieu en cas d'attaque d'un système
- Professionnels de la sécurité générale et architectes sécurité souhaitant concevoir, élaborer et faire fonctionner leurs systèmes afin de prévenir, détecter et répondre aux attaques

Fonctions du référentiel NICE

- Technical Support Specialist (OPM 411)
- Systems Security Analyst (OPM 461)
- Privacy Officer/Privacy Compliance Manager (OPM 732)
- Cyber Instructional Curriculum Developer (OPM 711)
- Cyber Instructor (OPM 712)
- Security Awareness & Communications Manager (OPM 712)
- Information Systems Security Manager (OPM 722)
- IT Investment/Portfolio Manager (OPM 804)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Incident Responder (OPM 531)
- Adversary Emulation Specialist/Red Teamer (OPM 541)
- Threat/Warning Analyst (OPM 141)
- All-Source Analyst (OPM 111)
- Mission Assessment Specialist (OPM 112)
- Target Network Analyst (OPM 132)
- Cyber Intel Planner (OPM 331)

Joshua Wright
Auteur de la formation

* DoD 8140 APPROVED
sans.org/8140

Transformez vos compétences de réponse aux incidents et entrez dans la tête des pirates avec SEC504™.Les plus de 30 labos pratiques vous apprendront à enquêter sur les cyberincidents, à développer le renseignement d'intérêt cyber et à appliquer des stratégies de défense contre des menaces concrètes. Des attaques de mot de passe aux techniques de contournement de l'authentification multifacteur (MFA) des services cloud, cette formation vous entraîne au cœur des tactiques les plus récentes. Manipulez des outils sophistiqués et simulez des attaques en *live* pour affûter vos capacités défensives tout en préparant la certification GIAC GCIH. À l'issue de la formation, vous serez paré à défendre des environnements cloud et sur site contre les cybermenaces en évolution permanente.

Bilan

- Vous appliquez une approche dynamique à la réponse à incident.
- Vous identifiez les menaces par l'analyse des journaux, des réseaux et des hôtes.
- Vous apprenez les bonnes pratiques d'une réponse efficace aux incidents cloud.
- Vous exploitez PowerShell pour collecter les données et analyser les cybermenaces.
- Vous apprenez les processus de cyberenquête – analyse dynamique, analyse réseau et analyse mémoire.
- Vous apprenez les stratégies défensives pour protéger les actifs essentiels.
- Vous découvrez comment les assaillants exploitent les systèmes cloud contre les organisations.
- Vous appréhendez les techniques des attaquants pour échapper aux outils de détection des extrémités.
- Vous découvrez comment les assaillants exploitent les failles de sécurité complexes du cloud.
- Vous vous familiarisez avec les étapes de l'attaque – découverte du réseau interne et déplacement latéral après la compromission initiale.
- Vous apprenez comment les agresseurs exploitent les systèmes en accès public, notamment Microsoft 365.

Programme

SECTION 1 : Réponse aux incidents et cyberenquêtes
SECTION 2 : Analyse réseau et énumération d'utilisateurs
SECTION 3 : Attaques de mot de passe et infrastructures d'exploit
SECTION 4 : Attaques des applications web
SECTION 5 : Techniques d'évasion et de post-exploitation
SECTION 6 : Événement CTF

« La réponse aux incidents est l'aspect le plus méconnu par les petites entreprises. SEC504 nous donne les moyens d'aider la direction à en comprendre toute la valeur. »

— David Freedman, **Nationwide Payment Solutions**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC504**

MODES DE FORMATION DE SEC504

In-Person **Live Online** **OnDemand**

SEC542: **Web App Penetration Testing and Ethical Hacking™**

GWAPT Web Application Penetration Tester
giac.org/gwapt
CyberLive

6 jours | 36 crédits CPE | +30 labos

Vous apprendrez à...

- Appliquer la méthodologie de l'Open Source Foundation for Application Security aux tests d'intrusion dans les applications web afin de garantir que ceux-ci sont cohérents, répétables, rigoureux et sous contrôle qualité
- Analyser les résultats des outils d'automatisation des tests web pour éliminer les faux positifs, valider les résultats et déterminer leur impact sur l'activité
- Rechercher les principales failles dans les applications web
- Utiliser Python pour créer des scripts de test et d'exploitation lors d'un test d'intrusion
- Rechercher et exploiter les failles par injection SQL pour déterminer de façon réaliste les risques encourus
- Comprendre et exploiter les vulnérabilités de désérialisation non sécurisée avec ysoserial et d'autres outils similaires
- Créer des configurations et tester des charges dans d'autres attaques web
- Tester de façon aléatoire les entrées potentielles (fuzzing) pour détecter les attaques par injection avec ZAP, Burp Suite's Intruder et ffuf
- Expliquer l'impact opérationnel des failles logiques sur les applications web

Public visé :

- Professionnels de la sécurité en général
- Experts en tests d'intrusion
- Hackers éthiques
- Développeurs d'applications web
- Concepteurs, architectes et développeurs de sites web

Fonctions du référentiel NICE

- Security Control Assessor (OPM 612)
- Software Developer (OPM 621)
- Secure Software Assessor (OPM 622)
- System Testing and Evaluation Specialist (OPM 671)
- Information Systems Security Developer (OPM 631)
- Systems Developer (OPM 632)
- Vulnerability Assessment Analyst (OPM 541)
- Pen Tester (OPM 541)
- Exploitation Analyst (OPM 121)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)

Eric Conrad
Auteur
de la formation

Timothy McKenzie
Auteur
de la formation

Bojan Zdrnja
Auteur
de la formation

SEC542™ donne aux stagiaires les moyens d'évaluer et d'exposer rapidement les vulnérabilités dans les applications web, et met en lumière les répercussions potentielles de leur exploitation. Vous acquérez la maîtrise des outils et méthodes des attaquants et, partant, une expérience tangible de l'exploitation d'applications web dans votre entreprise. Par des exercices concrets, vous apprenez les bonnes pratiques des tests d'intrusion sur les applications web, réalisez une injection SQL dans des bases de données backend pour appréhender l'exfiltration des données sensibles, et utilisez l'injection de script intersite (xss) pour vous emparer de l'infrastructure cible.

Bilan

- Vous appliquez une méthodologie reproductible pour mener des tests d'intrusion à forte valeur ajoutée.
- Vous découvrez et exploitez les failles de sécurité des applications web clés.
- Vous savez expliquer les conséquences potentielles des failles de sécurité des applications web.
- Vous faites comprendre toute l'importance de la sécurité des applications web pour la posture de sécurité globale.
- Vous maniez plus efficacement les outils d'attaque des applications web.
- Vous rédigez les rapports de test d'intrusion sur application web.

Programme

SECTION 1 : Introduction et collecte d'informations

SECTION 2 : Test à données aléatoires (fuzzing), analyse de vulnérabilités, authentification et tests de sessions

SECTION 3 : Injection

SECTION 4 : XSS, SSRF et XXE

SECTION 5 : CSRF, failles de logique et outils avancés

SECTION 6 : Événement CTF

« Cette formation m'a appris à vraiment suivre la méthodologie lors d'un test d'intrusion. Pendant le CTF, j'ai réalisé tout le temps qu'on peut perdre si on ne respecte pas sa méthodologie. »

— Sean Rosado, **RavenEye**

« SEC542 expose à une kyrielle d'outils et de techniques extrêmement précieux dans le cadre de la reconnaissance d'un site cible. »

— Gareth Grindle, **QA Ltd.**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC542**

MODES DE FORMATION DE SEC542

In-Person | **Live Online** | **OnDemand**

SEC556: **IoT Penetration Testing™**

3 jours	18 crédits CPE	15 labos

Vous apprendrez à...

- Évaluer les contrôles IoT côté réseau, les applications web et les points de terminaison des API des IoT sous l'angle de l'IoT
- Étudier le matériel pour en connaître toute la fonctionnalité, et mettre au jour les points d'interaction par lesquels tirer des données du matériel
- Découvrir le microprogramme à partir du matériel ou d'autres manières, en explorer les secrets et les défauts d'implémentation
- Analyser, interagir avec et manipuler les technologies sans fil Wi-Fi, LoRa et Zigbee et comprendre les failles de sécurité dans la mise en œuvre
- Interagir avec Bluetooth basse consommation (BLE) pour manipuler des appareils
- Automatiser la récupération de protocoles radio inconnus pour réaliser des attaques par rejeu et d'autres analyses

Public visé :

- Experts en tests d'intrusion
- Développeurs de systèmes embarqués
- Analystes sécurité
- Architectes sécurité
- Ingénieurs sécurité produit
- Concepteurs de produits IoT
- Quiconque lance un objet IoT

Fonctions du référentiel NICE

- System Testing and Evaluation Specialist (OPM 671)
- Vulnerability Assessment Analyst (OPM 541)
- Pen Tester (OPM 541)
- Adversary Emulation Specialist/Red Teamer (OPM 541)
- Cyber Ops Planner (OPM 332)

Larry Pesce
Auteur de la formation

James Leyte-Vidal
Auteur de la formation

Une tendance va s'accentuant ces dernières années : toujours plus de petits appareils informatiques accèdent au réseau pour apporter une connectivité à des objets autrefois déconnectés. Si l'électroménager connecté a une utilité discutable, l'Internet des objets (IoT) est là pour rester. Il apporte une connectivité accrue vraiment utile à de nombreux appareils, avec des avantages non négligeables pour les consommateurs et les entreprises.

Malheureusement, dans la course à la surenchère technologique connectée, beaucoup de ces appareils omettent de prendre en compte la sécurité dans leur conception ou le font le moins possible. Ce n'est pas la première fois que nous constatons cette attitude lors de nos tests, mais l'IoT se distingue en ce qu'il regroupe de nombreuses piles technologiques hétérogènes comme des versions personnalisées de systèmes d'exploitation, des interfaces web et API, divers protocoles réseau (p. ex. Zigbee, LoRa, Bluetooth/BLE, Wi-Fi) et des réseaux sans fil propriétaires. Cette gamme étendue de technologies disparates et mal sécurisées en fait un point d'appui idéal pour rebondir dans les réseaux, et ouvre des perspectives de modification des données des utilisateurs, de manipulation du trafic réseau, etc.

La formation SEC556™ vous familiarise avec les interfaces courantes des objets connectés. Elle propose aussi une procédure et un cadre de tests d'attaque IoT, dit « Internet of Things Attack » (IoTA), pour évaluer ces appareils dans les nombreuses couches du modèle OSI (interconnexion de systèmes ouverts). Analyse des protocoles réseau et des firmwares, problèmes d'implémentation matérielle, failles dans les applications... : nous vous apportons les outils et les techniques pragmatiques pour évaluer la gamme des appareils IoT en constante évolution. L'approche pédagogique vous donne l'occasion d'étudier l'écosystème IoT dans de nombreuses verticales, du secteur automobile aux systèmes de contrôle industriel en passant par la santé et la fabrication. Dans tous les cas, si la méthodologie est immuable, le modèle de risque varie.

Programme

SECTION 1 : Introduction aux services web et au trafic réseau IoT

SECTION 2 : Exploiter les interfaces matérielles IoT et analyser les firmwares

SECTION 3 : Exploiter l'IoT sans fil : Wi-Fi, BLE, Zigbee, LoRa et SDR

« Les labos sont un excellent moyen de s'approprier et d'assimiler les concepts. Le travail de mise à l'échelle et de virtualisation pour reproduire les exercices est incroyable. »

— Lee Neely, **Lawrence Livermore National Laboratory**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC556**

MODES DE FORMATION DE SEC556

In-Person **Live Online** **OnDemand**

SEC560: **Enterprise Penetration Testing™**

GPEN Penetration Tester
giac.org/gpen
ANAB ACCREDITED ISO/IEC 17024 PERSONNEL CERTIFICATION BODY
CyberLive
DoD 8140*

6 jours	36 crédits CPE	+30 labos

Public visé :

- Personnel de sécurité chargé d'évaluer réseaux et systèmes pour en détecter et corriger les vulnérabilités
- Experts en tests d'intrusion
- Hackers éthiques
- Défenseurs soucieux de mieux comprendre les méthodologies, outils et techniques offensifs
- Auditeurs ayant besoin d'approfondir leurs compétences techniques
- Membres de red team
- Membres de blue team
- Spécialistes inforensiques soucieux de mieux comprendre les tactiques offensives
- Chargés de réponse aux cyberincidents qui cherchent à comprendre l'état d'esprit d'un attaquant

Fonctions du référentiel NICE

- Security Control Assessor (OPM 612)
- System Testing and Evaluation Specialist (OPM 671)
- Vulnerability Assessment Analyst (OPM 541)
- Pen Tester (OPM 541)
- Exploitation Analyst (OPM 121)
- Mission Assessment Specialist (OPM 112)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)
- Cyber Operator (OPM 321)

Jon Gorenflo
Auteur de la formation

Jeff McJunkin
Auteur de la formation

* DoD 8140 APPROVED
sans.org/8140

SEC560: Enterprise Penetration Testing™, la formation par excellence aux tests d'intrusion, vous arme pour évaluer et atténuer le risque cyber dans les entreprises complexes d'aujourd'hui. Au cours de labos d'entraînement, vous apprenez à planifier, à exécuter et à appliquer des tests d'intrusion avec les techniques et outils les plus récents. Experts en tests d'intrusion, administrateurs système et chargés de défense, la formation SEC560™ s'adresse à vous : en renforçant vos compétences et votre compréhension de la logique d'un assaillant, elle vous donne les moyens d'améliorer sans délai la sécurité opérationnelle. SEC560™ a été conçue pour vous préparer à mener des tests d'intrusion à haute valeur ajoutée et à grande échelle. Et c'est précisément ce que vous ferez en fin de formation. Vous commencerez par développer vos compétences grâce à des labos complets et stimulants avant d'attaquer le grand finale de la formation : un scénario concret de test d'intrusion. Vous mènerez ce test d'intrusion de bout en bout en appliquant les connaissances, les outils et les principes abordés tout au long de la formation, et ce afin de découvrir et d'exploiter les vulnérabilités d'une organisation cible réaliste.

Vous apprendrez à...

- Planifier et préparer correctement un test d'intrusion d'entreprise
- Effectuer une reconnaissance approfondie pour faciliter l'ingénierie sociale, l'hammeçonnage, le ciblage des données pertinentes et la démonstration d'objectifs appropriés
- Deviner des mots de passe efficacement et en toute sécurité pour prendre pied dans un environnement cible ou vous enfoncer dans le réseau
- Exploiter des systèmes cibles de diverses manières pour y accéder et mesurer le véritable risque commercial associé
- Piller systématiquement les systèmes exploités afin de collecter des informations et vous enfoncer dans le réseau jusqu'à vos objectifs
- Utiliser les techniques d'élévation de privilèges pour augmenter votre niveau d'accès aux systèmes Windows ou Linux, voire à l'Active Directory lui-même
- Exécuter un mouvement latéral, rebondir pour étendre l'accès obtenu à l'organisation et identifier les risques que les analyses de surface n'ont pas décelés
- Utiliser des frameworks de commande et de contrôle (C2, C&C) pour gérer et piller à distance les hôtes compromis
- Attaquer les domaines et forêts Active Directory que la plupart des organisations utilisent
- Exécuter plusieurs attaques Kerberos, notamment Kerberoasting, Golden Ticket et Silver Ticket
- Mener une reconnaissance Azure à distance, avec ou sans informations d'identification
- Exécuter des attaques par pulvérisation de mots de passe sur Entra ID

Programme

SECTION 1 : Tests d'intrusion de a à z : planification, périmètre, reconnaissance et balayage
SECTION 2 : Accès initial, charges utiles et appréciation de la situation
SECTION 3 : Attaques de mot de passe, persistance et élévation des privilèges
SECTION 4 : Déplacement latéral et reporting
SECTION 5 : Domination du domaine et annihilation d'Azure
SECTION 6 : Test d'intrusion et exercice CTF

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC560**

MODES DE FORMATION DE SEC560

In-Person | Live Online | OnDemand

SEC565: **Red Team Operations and Adversary Emulation™**

GRTP
Red Team Professional
giac.org/grtp

6 jours | 36 crédits CPE | +25 labos

Vous apprendrez à...

- Vous servir de renseignements d'intérêt cyber et planifier une mission de red team
- Configurer l'infrastructure nécessaire pour réussir l'opération compte tenu de la sécurité opérationnelle
- Créer vos armes pour infiltrer une organisation
- Lister et extraire les données de valeur à l'aide d'outils automatisés ou à la main pour atteindre vos objectifs
- Vous déplacer latéralement et vous implanter de manière persistante dans un réseau d'entreprise
- Élever vos privilèges en exploitant différents vecteurs d'attaque et problèmes de configuration que vous aurez d'abord appris à identifier
- Rédiger un bilan éloquent pour que votre client tire toute la valeur de l'exercice

Public visé :

- Professionnels de la sécurité
- Experts en tests d'intrusion
- Membres de red team
- Membres de blue team
- Auditeurs
- Chargés de la sécurité des systèmes d'information

Fonctions du référentiel NICE

- Adversary Emulation Specialist/Red Teamer (OPM 541)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)
- Partner Integration Planner (OPM 333)

Jean-François Maes
Auteur de la formation

David Mayer
Auteur de la formation

Efficaces pour dresser la liste des vulnérabilités, les tests d'intrusion le sont moins pour sensibiliser le personnel ou développer les processus en défense. Or, des équipes blue team ou de défense mal informées quant aux données offensives à améliorer en entrée risquent d'enfermer leurs organisations dans un processus cyclique axé exclusivement sur les vulnérabilités des systèmes, sans porter attention à l'accompagnement des défenseurs vers la détection et la réponse efficaces aux attaques.

Dans la formation SEC565™, les stagiaires apprennent à planifier et à exécuter des missions de red team complètes qui s'appuient sur l'émulation d'attaque : organisation de red team, exploitation de renseignements sur les menaces en lien avec les tactiques, techniques et procédures (TTP) de l'adversaire, émulation de ces TTP, restitution et analyse du bilan de mission de la red team et, au bout du compte, amélioration de la posture de sécurité globale de l'organisation. Dans ce cadre, les stagiaires émuleront l'attaque d'une organisation cible sur le modèle d'un environnement d'entreprise incluant notamment Active Directory, des courriers électroniques riches en renseignements, des serveurs de fichiers et des terminaux sous Windows.

Dans cette formation, vous apprendrez à :

- Utiliser le renseignement sur les menaces dans l'émulation
- Élaborer un plan d'émulation d'attaque
- Relier les actions au framework MITRE® ATT&CK™ pour faciliter la communication avec la blue team
- Établir une infrastructure C2 résiliente et avancée
- Maintenir la sécurité opérationnelle tout au long de la mission
- Valoriser l'accès initial pour élever vos privilèges et vous propager par le réseau
- Énumérer des comptes dans Active Directory et attaquer l'annuaire
- Collecter et exfiltrer sans risque des données sensibles
- Finaliser une mission, apporter de la valeur et planifier de nouveaux tests

Programme

SECTION 1 : Planifier l'émulation d'attaque et le renseignement
SECTION 2 : Infrastructure d'attaque et sécurité opérationnelle
SECTION 3 : S'introduire dans l'environnement et y rester
SECTION 4 : Attaques sur Active Directory et déplacement latéral
SECTION 5 : Atteindre l'objectif et créer un rapport
SECTION 6 : Événement CTF immersif pour red team

« Le contenu est absolument incroyable. Même si vous connaissez déjà un peu le sujet, la richesse des informations est telle que vous en approfondirez votre compréhension et renforcerez vos procédures ! »

— Kemmner Lankfurd, **NetPlas Neckarsulm**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC565**

MODES DE FORMATION DE SEC565

In-Person **Live Online** **OnDemand**

SEC575: **iOS and Android Application Security Analysis and Penetration Testing™**

GMOB
Mobile Device Security Analyst
giac.org/gmob

6 jours	36 crédits CPE	+20 labos

Public visé :

- Experts en tests d'intrusion
- Hackers éthiques
- Auditeurs ayant besoin d'approfondir leurs compétences techniques
- Personnel de sécurité chargé d'évaluer, de déployer ou de sécuriser des téléphones et tablettes mobiles
- Administrateurs système et réseau qui gèrent les téléphones et tablettes mobiles

Imaginez une surface d'attaque présente à l'échelle de votre organisation et entre les mains de tous les utilisateurs. Elle change régulièrement d'endroit, elle héberge des données extrêmement sensibles et stratégiques, et elle est dotée de nombreuses technologies sans fil, toutes mûres pour une attaque. Malheureusement, ce type de surface existe : ce sont les appareils mobiles. Ils forment la plus grande surface d'attaque dans la plupart des organisations. Et pourtant, ces dernières ont rarement les compétences nécessaires pour évaluer les risques concomitants.

La formation SEC575: iOS and Android Application Security Analysis and Penetration Testing™ est conçue pour vous apporter les compétences nécessaires à la compréhension des forces et des faiblesses des appareils fonctionnant sous Apple iOS et Android, y compris Android 14 et iOS 17. Les appareils mobiles ne sont plus seulement une technologie de confort, mais des outils essentiels, que tout le monde ou presque emporte avec lui et qui remplacent souvent l'ordinateur traditionnel dans les échanges de données professionnelles au quotidien. Cette tendance s'observe dans les entreprises, les hôpitaux, les banques, les écoles et les commerces partout dans le monde. Les utilisateurs ne se sont jamais autant servis des appareils mobiles ; nous en sommes conscients et les acteurs malveillants aussi. La formation SEC575™ propose un tour d'horizon de ces appareils.

Programme

SECTION 1 : iOS

SECTION 2 : Android

SECTION 3 : Analyse statique des applications

SECTION 4 : Analyse dynamique et manipulation des applications mobiles

SECTION 5 : Tests d'intrusion

SECTION 6 : Événement CTF de mise en pratique

« On croit connaître la cybersécurité, et puis on suit SEC575 de SANS et boum ! On comprend qu'il nous reste encore beaucoup à apprendre ! »

— Steve M.

« SEC575 est une formation utile immédiatement, aussi bien pour les experts en tests d'intrusion que pour les développeurs. »

— Roy Cabaniss, **LGS**

« Très bien organisé, réellement intéressant et ludique. Un moyen très efficace d'apprendre à analyser des applis et de se prendre au jeu. »

— Myriam Leggieri, **Google**

Jeroen Beckers
Auteur de la formation

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC575**

MODES DE FORMATION DE SEC575

In-Person **Live Online** **OnDemand**

SEC580: **Metasploit for Enterprise Penetration Testing™**

2 jours	12 crédits CPE	+20 labos

Public visé :

- Ingénieurs sécurité IT
- Experts en tests d'intrusion
- Consultants en sécurité
- Personnel chargé de l'évaluation des vulnérabilités
- Personnel chargé la gestion des vulnérabilités
- Analystes de la sécurité des réseaux
- Auditeurs
- Ingénieurs sécurité généralistes
- Chercheurs en sécurité

Un mot des auteurs

« Metasploit est l'outil d'exploitation gratuit le plus répandu aujourd'hui. Tout le monde l'utilise : experts en tests d'intrusion, personnes chargées d'évaluer les vulnérabilités, auditeurs et acteurs malveillants. Toutefois, la plupart n'utilisent et ne comprennent qu'environ 10 pour cent de sa fonctionnalité et passent à côté d'autres fonctions extrêmement utiles. Ici, les stagiaires achèvent de maîtriser les 10 pour cent déjà connus, mais plus en détail et en mettant l'accent sur la sécurité, et découvrent les 90 pour cent restants à appliquer ensuite pour renforcer l'efficacité de leurs tests. À l'issue de la formation, les stagiaires sauront tirer d'un outil gratuit une puissance comparable à celle de nombreux outils commerciaux bien plus chers. »

— Jeff McJunkin

Jeff McJunkin
Auteur de la formation

Nombre d'entreprises doivent aujourd'hui respecter des normes légales et sectorielles qui les obligent à mener régulièrement des tests d'intrusion et des évaluations des vulnérabilités. Les outils et services commerciaux qui le permettent s'avèrent souvent onéreux. S'il existe des outils gratuits et robustes, comme Metasploit, peu de testeurs en maîtrisent l'ensemble des fonctionnalités et savent les appliquer dans le cadre d'une méthodologie de test professionnelle. Metasploit a été conçu pour aider les testeurs à confirmer des vulnérabilités grâce à une plateforme open source simple d'utilisation. Dans cette formation, vous apprendrez à en tirer tout le potentiel.

Dans SEC580™, vous découvrirez comment appliquer les incroyables capacités de Metasploit Framework dans un protocole complet de tests d'intrusion et d'évaluation des vulnérabilités employant une méthodologie de tests exhaustive et efficace. À l'issue de la formation, vous aurez acquis une compréhension solide de Metasploit et de l'intérêt de l'intégrer au quotidien à vos activités d'évaluation et à vos tests d'intrusion. Vous y gagnerez une compréhension approfondie de Metasploit Framework, qui dépasse largement la simple présentation de l'exploitation d'un système à distance. Vous découvrirez l'exploitation, la reconnaissance post-exploitation, les techniques d'évasion d'antivirus, les attaques par hameçonnage ciblé (spear-phishing) et le vaste jeu de fonctionnalités de Meterpreter, un environnement shell personnalisé créé spécialement pour l'exploitation et l'analyse des failles de sécurité.

La formation couvrira également les nombreux pièges qu'un testeur peut rencontrer lorsqu'il utilise Metasploit Framework, ainsi que la manière de les éviter ou de les contourner, pour des tests plus sûrs et plus efficaces.

Programme

SECTION 1 : Metasploit pour les tests d'intrusion d'entreprise – partie 1

SECTION 2 : Metasploit pour les tests d'intrusion d'entreprise – partie 2

« SEC580 est la meilleure formation au monde pour connaître Metasploit en profondeur. »

— Tom Reeves, **Northrup Grumman**

« Les supports de la formation SEC580 vous enseignent pas à pas les fondamentaux de Metasploit. »

— Scott Tirapelle, **Franchise Tax Board**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC580**

MODES DE FORMATION DE SEC580

In-Person **Live Online**

SEC588: **Cloud Penetration Testing™**

GCPN
Cloud Penetration Tester
giac.org/gcpn

6 jours	36 crédits CPE	27 labos

Vous apprendrez à...

- Mener des tests d'intrusion cloud
- Évaluer les environnements cloud et dégager de la valeur en localisant les vulnérabilités
- Appréhender de visu la construction des environnements cloud et l'insertion de facteurs d'échelle dans la collecte de preuves
- Évaluer les risques de sécurité dans les environnements AWS et Microsoft Azure, les deux principales plateformes actuelles
- Appliquer immédiatement vos nouvelles connaissances dans votre travail

Public visé :

- Professionnels de la sécurité, en attaque comme en défense, pour acquérir une compréhension approfondie des vulnérabilités, des configurations peu sécurisées et du risque associé que leur organisation court
- Experts en tests d'intrusion
- Analystes vulnérabilité
- Auditeurs risque
- Ingénieurs DevOps
- Ingénieurs de fiabilité de site (SRE)

Fonctions du référentiel NICE

- Security Control Assessor (OPM 612)
- System Testing and Evaluation Specialist (OPM 671)
- Vulnerability Assessment Analyst (OPM 541)
- Pen Tester (OPM 541)
- Cyber Ops Planner (OPM 332)

« Minutieusement conçue, la formation SEC588 contrebalance un contenu théorique dense avec des labos pratiques pour répondre aux enjeux centraux de la sécurité cloud. Elle est indispensable à tout professionnel de la sécurité en quête de connaissances pointues. »

— Armin Iraqi, **Fortum**

Aaron Cure
Auteur de la formation

Moses Frost
Auteur de la formation

SEC588™ vous arme des techniques d'intrusion cloud les plus modernes et vous montre comment évaluer les environnements cloud. Cette formation plonge dans des sujets comme les microservices cloud, les datastores en mémoire, les fonctionnalités sans serveur, les maillages Kubernetes et les conteneurs. Elle aborde également l'identification et les tests d'applications cloud (cloud-first et cloud native). Vous y découvrirez aussi des tactiques d'intrusion propres à Azure et AWS, d'autant plus importantes que les deux fournisseurs se partagent plus de la moitié du marché. Il ne suffit pas d'évaluer et de sécuriser le datacenter : il faut aussi savoir évaluer et communiquer les risques auxquels l'entreprise devrait faire face si ses services cloud n'étaient pas sécurisés.

Bilan

- Vous apprenez à évaluer et tester les environnements cloud lors de labos cloud en conditions réelles.
- Vous comprenez les différences entre les infrastructures natives cloud, multicloud et hybrides.
- Vous menez des tests d'intrusion sur des microservices de production.
- Vous apprenez comment les acteurs malveillants exploitent les conteneurs et les pipelines CI/CD.
- Vous savez attaquer Kubernetes, les fonctions sans serveur et les conteneurs Windows.
- Vous appréhendez le fonctionnement des systèmes d'identité et les moyens de les attaquer.

Programme

SECTION 1 : Architecture, découverte et reconnaissance à grande échelle

SECTION 2 : Attaquer les systèmes de gestion des identités

SECTION 3 : Attaquer et exploiter frauduleusement les services cloud

SECTION 4 : Vulnérabilités dans les applications cloud natives

SECTION 5 : Attaques sur les infrastructures et exercices de red team

SECTION 6 : Projet final

« La formation SEC588 m'a appris bien plus que ce que j'en attendais. Elle définit le cadre des tests d'intrusion cloud, indispensable face à l'essor des nouvelles technologies des prestataires cloud. »

— Jonus Gerrits, **Phillips66**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC588**

MODES DE FORMATION DE SEC588

In-Person **Live Online** **OnDemand**

ZOOM NOUVELLE FORMATION

SEC598: **Security Automation for Offense, Defense, and Cloud™**

6 jours	36 crédits CPE	+15 labos

Compétences acquises

- Comprendre les problèmes de sécurité que rencontrent la plupart des organisations aujourd'hui
- Diviser les problèmes de sécurité en plusieurs sous-éléments, définir des solutions automatisées pour ceux-ci, puis enchaîner totalement des fonctions capables de traiter automatiquement plusieurs problèmes
- Vous servir d'outils comme Terraform, Ansible, CHEF Puppet et bien d'autres pour automatiser en local des configurations sécurisées, fixer une configuration de l'état souhaité (DSC), déployer l'infrastructure programmable (IaC) dans divers environnements, et automatiquement détecter les incidents de sécurité et y répondre
- Évaluer des scénarios issus du monde réel dans une combinaison d'environnements cloud et sur site à l'aide d'un cadre de référence utilisable et déployable immédiatement dans votre organisation

Public visé :

- Architectes sécurité
- Ingénieurs automaticiens
- Ingénieurs sécurité
- Ingénieurs spécialistes de la détection
- Chargés de réponse aux cyberincidents
- Analystes de risques d'entreprise
- Hackers éthiques
- Experts en tests d'intrusion
- Techniciens red team
- Membres de blue team
- Membres de purple team
- Analystes de centre des opérations de sécurité (SOC)
- Ingénieurs cloud

Fonctions du référentiel NICE

- Data Analysis (OPM 422)
- Cybersecurity Architecture (OPM 652)
- Systems Testing and Evaluation (OPM 671)
- Technology Research and Development (OPM 661)
- Defensive Cybersecurity (OPM 511)
- Incident Response (OPM 531)
- Infrastructure Support (OPM 521)
- All-Source Analysis (OPM 111)
- Cyberspace Operations (OPM 321)

Jason Ostrom
Auteur de la formation

Jeroen Vandeleur
Auteur de la formation

Les machines ne prennent pas le pouvoir, mais vous, si !

Maîtriser les workflows d'automatisation décuple les forces des équipes de sécurité. Alors que leur périmètre d'intervention augmente en volume et en complexité dans l'entreprise moderne, les équipes de sécurité s'évertuent à prévenir, détecter et émuler les menaces contre leur organisation et à y répondre.

Dans ce combat acharné, l'élite des équipes de sécurité a appris à libérer toute la puissance de l'automatisation. Les ingénieurs extrêmement compétents en sécurité et en automatisation savent déployer des solutions qui soulagent les équipes de sécurité de nombreuses tâches non prioritaires pour les laisser se focaliser sur les initiatives haute priorité et critiques.

Dans cette formation, l'organisation fictive (mais réaliste) GLOBEX sert de cadre aux plus de 15 exercices de labo et au projet final axés sur des cas d'usage d'automatisation de la sécurité, à emporter ensuite avec vous et implémentables au sein de votre organisation.

Vous apprendrez à...

- Convertir des activités reproductibles en tâches automatisées
- Automatiser les fonctionnalités de prévention et de détection de certaines techniques d'attaque qu'assaillants et red teams utilisent sur le terrain, et les réponses à apporter
- Améliorer l'efficacité de votre SOC en mettant au jour des possibilités d'optimisations dans les responsabilités de niveau 1 et 2
- Utiliser Terraform pour ses fonctions avancées, les modules d'infrastructure programmable (IaC), et la mise en place d'une infrastructure dynamique de tests d'intrusion et de red team
- Configurer une émulation d'attaque cloud et exploiter des outils cloud natifs pour mesurer vos capacités de détection et votre implémentation de réponse automatisée
- Exploiter les outils d'IaC pour mettre en place des workflows automatisés de recherche de compromission, de confinement, d'acquisition, de mise en quarantaine, et de réponse aux incidents
- Exploiter l'IaC pour déployer des capacités automatisées d'entraînement cyber – sur site, cloud natives et hybrides – afin d'améliorer vos programmes de sécurité et votre compréhension des outils offensifs et des contrôles défensifs

Programme

SECTION 1 : Notions d'automatisation en sécurité
SECTION 2 : Ingénierie d'automatisation de la sécurité
SECTION 3 : Automatisation de la sécurité dans le cloud
SECTION 4 : Automatisation de la sécurité offensive
SECTION 5 : Automatisation de la sécurité défensive
SECTION 6 : Projet final d'automatisation de la sécurité

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC598**

MODES DE FORMATION DE SEC598

In-Person **Live Online**

SEC599: **Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses™**

GDAT
Defending Advanced Threats
giac.org/gdat

6 jours	36 crédits CPE	+20 labos

Vous apprendrez à...

- Comprendre le déroulement d'attaques récentes de haut niveau et les moyens de les arrêter
- Mettre en œuvre des contrôles de sécurité aux différentes phases des modèles Cyber Kill Chain et MITRE ATT&CK pour prévenir, détecter et lutter contre les attaques

Public visé :

- Architectes sécurité et ingénieurs sécurité
- Experts en tests d'intrusion et red team
- Responsables sécurité technique
- Directeurs, ingénieurs et analystes des centres des opérations de sécurité
- Quiconque cherche à mieux comprendre le fonctionnement des attaques persistantes et les mesures à prendre dans l'environnement IT pour mieux prévenir, détecter et lutter contre les incidents

Fonctions du référentiel NICE

- Adversary Emulation Specialist/Red Teamer (OPM 541)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)
- Partner Integration Planner (OPM 333)

« Les labos de SEC599 sont fantastiques, tout comme le décorticage des techniques offensives et des options de défense actuelles. J'apprécie que les thèmes abordent une large base d'environnements, pour des niveaux de maturité en sécurité des plus élémentaires aux plus avancés. »

— Michael Ebrahimi, **Accenture**

Erik Van Buggenhout
Auteur de la formation

Stephen Sims
Auteur de la formation

Les cybermenaces sont en plein essor : les attaques par ransomware touchent tout type d'entreprises sans distinction de taille, pendant que les adversaires étatiques tentent de s'ouvrir un accès à vos actifs les plus précieux. SEC599™ vous apporte les connaissances et l'expertise nécessaires pour venir à bout des menaces actuelles. Comme les stratégies préventives ne suffisent pas, nous présentons des contrôles de sécurité pour détecter et arrêter les adversaires et intervenir.

Les auteurs de la formation, Stephen Sims et Erik Van Buggenhout, certifiés GIAC Security Expert, sont des professionnels aguerris. Ils ont acquis une compréhension approfondie des cyberattaques et de leurs modes opératoires par les tests d'intrusion et la réponse aux incidents. Dans leurs formations sur les tests d'intrusion, une question revient : « Comment prévenir ou détecter ce type d'attaque ? » La formation SEC599™, qui donne aux stagiaires des exemples réels de prévention d'attaques, est leur réponse : outre les 20 labos inclus, une journée entière est consacrée à un exercice de défense du drapeau, où les stagiaires défendent notre entreprise virtuelle contre plusieurs vagues d'attaques différentes ciblant son environnement.

Bilan

- Vous comprenez le déroulement d'attaques récentes de haut niveau et les moyens de les arrêter.
- Vous mettez en œuvre des contrôles de sécurité à chaque étape des modèles Cyber Kill Chain et MITRE ATT&CK pour prévenir, détecter et lutter contre les attaques.

Programme

SECTION 1 : Introduction et reconnaissance

SECTION 2 : Livraison et détonation de charge utile

SECTION 3 : Exploitation, persistance, et commande et contrôle

SECTION 4 : Déplacement latéral

SECTION 5 : Passage à l'action sur les objectifs, recherche de compromission et réponse aux incidents

SECTION 6 : Projet final : exercice de défense contre une attaque APT

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC599**

MODES DE FORMATION DE SEC599

In-Person **Live Online** **OnDemand**

SEC617: **Wireless Penetration Testing and Ethical Hacking™**

GAWN
Assessing and Auditing Wireless Networks
giac.org/gawn

6 jours | 36 crédits CPE | +20 labos

Vous apprendrez à...

- Identifier et localiser les points d'accès des hackers malveillants en utilisant des outils gratuits ou peu coûteux
- Mener un test d'intrusion sur les technologies sans fil à faible consommation pour identifier des systèmes de contrôle et les vulnérabilités qui leur sont associées
- Identifier des vulnérabilités et contourner les mécanismes d'authentification des réseaux Bluetooth
- Implémenter un test d'intrusion WPA2-Enterprise afin d'exploiter les systèmes client sans fil vulnérables pour en récolter les données d'authentification
- Utiliser Scapy pour forcer les paquets personnalisés afin de manipuler autrement les réseaux sans fil, en développant rapidement des outils d'attaque personnalisés qui répondent aux exigences des tests d'intrusion
- Identifier les attaques Wi-Fi en utilisant le suivi de paquets réseau capturés et les outils d'analyse gratuits
- Identifier et exploiter les défauts de sécurité des systèmes de badges d'accès sans contact
- Décoder les signaux radio propriétaires issus de radios logicielles
- Élaborer des tests d'intrusion pour de nombreuses technologies sans fil propriétaires ou basées sur les normes

Public visé :

- Hackers éthiques et experts en tests d'intrusion
- Personnel de sécurité réseau
- Administrateurs système et réseau
- Équipes de réponse aux incidents
- Décideurs des politiques de sécurité des systèmes d'information
- Auditeurs de sécurité
- Consultants en SSI
- Ingénieurs systèmes sans fil
- Développeurs de systèmes sans fil embarqués

Larry Pesce
Auteur de la formation

James Leyte-Vidal
Auteur de la formation

Cette formation s'adresse aux professionnels qui cherchent à acquérir une expertise technique complète pour comprendre, analyser et défendre les différentes technologies sans fil, omniprésentes dans nos environnements et véritables points d'entrée pour les attaquants.

Les auteurs de SEC617™, experts en tests d'intrusion, savent que les organisations ne considèrent bien souvent pas les appareils sans fil comme une surface d'attaque et ne déploient pas les défenses et la supervision requises. Et cela en dépit du fait que les technologies sans fil sont largement déployées dans les suites exécutives des hôtels, les services financiers, les administrations publiques, les chaînes de fabrication, les réseaux de vente au détail, les dispositifs médicaux et les systèmes de contrôle du trafic aérien. Dans le contexte établi des technologies sans fil, peu sécurisées et faisant l'objet d'attaques, la formation SEC617™ a été conçue pour aider les stagiaires à développer les compétences indispensables pour identifier, évaluer et estimer les menaces, et s'en prémunir. Ces compétences sont incontournables pour les organisations de sécurité exigeantes.

Programme

SECTION 1 : Collecte et analyse de données Wi-Fi

SECTION 2 : Attaques et techniques d'exploitation Wi-Fi

SECTION 3 : Attaques de Wi-Fi d'entreprise et Zigbee

SECTION 4 : Attaques par Bluetooth et radio logicielle

SECTION 5 : Piratage RFID, de cartes à puce et NFC

SECTION 6 : Événement CTF

« Les explications cryptographiques détaillées de SEC617 facilitent la compréhension du fonctionnement de différents algorithmes de chiffrement, ce qui est une première pour moi ! »

— Jonathan Wilhoit, **Fluor**

« SEC617 vous fait acquérir une compréhension élémentaire des menaces et vulnérabilités des réseaux sans fil, mais peut aussi vous emmener beaucoup plus loin, selon les questions que vous posez. »

— Daniel Mayernik, **Integrity Applications Incorporated**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC617**

MODES DE FORMATION DE SEC617

In-Person | **Live Online** | **OnDemand**

SEC660: **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking™**

GXPN
Exploit Researcher and Advanced Penetration Tester
giac.org/gxpn
CyberLive

6 jours	46 crédits CPE	+30 labos

Vous apprendrez à...

- Réaliser des tests de fuzzing pour améliorer votre processus de cycle de développement logiciel sécurisé
- Exploiter les dispositifs réseau et évaluer les protocoles d'applications réseau
- Échapper aux environnements restrictifs sur Linux et Windows
- Tester les implémentations cryptographiques
- Modéliser les techniques utilisées par les assaillants pour découvrir les vulnérabilités de type zero-day et développer des exploits
- Développer des appréciations quantitatives et qualitatives des risques plus précises grâce à la validation
- Démontrer la nécessité et les effets des techniques récentes d'atténuation des exploits

Public visé :

- Experts en tests d'intrusion réseau et système
- Chargés de réponse aux incidents
- Développeurs d'application
- Ingénieurs sécurité IDS

Fonctions du référentiel NICE

- Vulnerability Assessment Analyst (OPM 541)
- Pen Tester (OPM 541)
- Adversary Emulation Specialist/Red Teamer (OPM 541)
- Exploitation Analyst (OPM 121)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)
- Cyber Operator (OPM 321)

« La qualité des labos et des devoirs de SEC660 atteste de la valeur des formations de SANS par rapport à ses concurrents. Une formation à la fois excellente, stimulante et gratifiante. »

— Michael R., **militaire**

James Shewmaker
Auteur de la formation

Stephen Sims
Auteur de la formation

SEC660™ se veut la suite logique de SEC560: Enterprise Penetration Testing, mais elle s'adresse aussi aux personnes qui ont une première expérience en tests d'intrusion. Les stagiaires ayant démontré les connaissances préalables nécessaires analyseront des dizaines d'attaques réelles qu'utilisent les experts en tests d'intrusion les plus accomplis. La méthodologie de chaque attaque sera abordée, puis suivie d'exercices dans un labo concret pour renforcer l'acquisition des concepts avancés et savoir appliquer les techniques apprises dès le retour au travail. Chaque journée de formation comprend un entraînement supplémentaire de deux heures en soirée pour parfaire la maîtrise des techniques étudiées. Parmi les thèmes abordés, on trouve les attaques contre les contrôles d'accès réseau (NAC) et la manipulation des réseaux locaux virtuels (VLAN), l'exploitation d'appareils réseau, la capacité à s'enfoncer au-delà des environnements restreints de Linux et de Windows, IPv6, l'élévation des privilèges Linux et l'écriture d'exploit, le test des chiffrements en place, les tests à données aléatoires (fuzzing), le contournement des contrôles OS modernes comme les mécanismes de distribution aléatoire de l'espace d'adressage (ASLR) et la prévention de l'exécution des données (DEP), la programmation orientée retour (ROP), l'écriture d'exploit Windows et bien d'autres encore !

Bilan

- Vous menez en toute sécurité des tests d'intrusion sur des matériels réseau, routeurs, commutateurs et implémentations de contrôle d'accès au réseau (NAC).
- Vous savez tester les implémentations cryptographiques.
- Vous aidez votre organisation à se prémunir contre la prolifération des identités et la dette technique par la centralisation.
- Vous exploitez un point d'ancrage sans privilège dans un cadre de post-exploitation et d'élévation de privilèges.
- Vous utilisez les tests à données aléatoires (fuzzing) pour le réseau et des applications autonomes.
- Vous écrivez des exploits visant des applications Linux et Windows.
- Vous contournez les tentatives d'atténuation d'exploits comme ASLR, DEP et les protections « stack canaries ».

Programme

SECTION 1 : Attaques réseau pour experts en tests d'intrusion

SECTION 2 : Crypto et post-exploitation

SECTION 3 : Tests de sécurité de produits, test à données aléatoires (fuzzing) et techniques de couverture de code

SECTION 4 : Exploiter Linux pour experts en tests d'intrusion

SECTION 5 : Exploiter Windows pour experts en tests d'intrusion

SECTION 6 : Événement CTF

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC660**

MODES DE FORMATION DE SEC660

In-Person · Live Online · OnDemand

SEC670: **Red Teaming Tools – Developing Windows Implants, Shellcode, Command and Control™**

6 jours	46 crédits CPE	+22 labos

Vous apprendrez à...

- Créer des implants Windows à compilation personnalisée
- Collecter des informations sur une cible
- Cacher les processus aux outils en mode utilisateur
- Accrocher et décrocher du code avec des fonctions *hook* et contourner les antivirus
- Créer et exécuter du shellcode personnalisé
- Élever les privilèges du niveau d'intégrité moyen à élevé (NT AUTHORITY\SYSTEM)
- Rester persistant malgré les redémarrages
- Envoyer un signal à l'infrastructure C2 configurée

Public visé :

- Techniciens red team
- Développeurs d'exploits
- Experts en tests d'intrusion
- Développeurs CNO Linux
- Développeurs Windows
- Développeurs AV/EDR

Fonctions du référentiel NICE

- Adversary Emulation Specialist/Red Teamer (OPM 541)

Jonathan Reiter
Auteur de la formation

Aucune école ni université n'enseigne à développer des outils à compilation personnalisée pour Windows. De là, le secteur de la cybersécurité souffre d'un déficit aigu de compétences, qui limite les capacités globales des opérations de red team. Les prestataires de défense et les secteurs en quête de développeurs d'outils Windows font face à une pénurie de talents et n'arrivent pas à affûter leurs défenses.

SEC670™ est la première formation de son genre à offrir une expérience concrète en labo de création de programmes à compilation personnalisée, spécialement conçus pour Windows en C/C++. En créant leurs propres outils exploitant les API Windows, les stagiaires y apprennent les rouages internes des outils offensifs existants qui offrent des fonctions d'élévation de privilèges, de persistance et de collecte. Les défenses de Windows, désormais plus robustes, et les solutions d'antivirus connectées au cloud compliquent les opérations furtives. Dans ce cadre, la formation présente aux stagiaires les techniques que les acteurs étatiques malveillants mettent en œuvre actuellement dans leurs implants.

Dans cette formation, vous apprendrez à :

- Définir de nouvelles conventions d'appel et des types de données propres à Windows
- Comprendre le fonctionnement interne des processus, threads et services Windows
- Injecter subrepticement par des API Windows du shellcode dans d'autre processus
- Créer un service caché persistant
- Vous cacher des outils en mode utilisateur comme Task Manager
- Créer et exécuter du shellcode sans être détecté
- Contourner les hooks de l'espace utilisateur et implémenter les vôtres
- Contrôler votre implant depuis votre serveur C2

Programme

SECTION 1 : Développement d'outil Windows

SECTION 2 : Apprendre à connaître votre cible

SECTION 3 : Actions opérationnelles

SECTION 4 : Persistance : Meurs un autre jour

SECTION 5 : Améliorer votre implant : shellcode, évasion et C2

SECTION 6 : Événement CTF

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC670**

MODES DE FORMATION DE SEC670

In-Person **Live Online** **OnDemand**

SEC699: **Advanced Purple Teaming – Adversary Emulation and Detection Engineering™**

5 jours	36 crédits CPE	29 labos

Bilan

- Élaborez des plans d'émulation d'attaque réalistes pour mieux protéger l'organisation
- Lancez des attaques avancées notamment par contournement de liste blanche applicative, par attaque interforêts (abus de délégation) et stratégies de persistance furtive
- Élaborez des règles SIGMA de détection de techniques d'attaque avancée

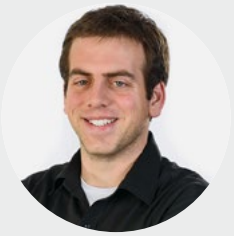
Public visé :

- Experts en tests d'intrusion
- Hackers éthiques
- Défenseurs soucieux de mieux comprendre les méthodologies, outils et techniques offensifs
- Membres de red team
- Membres de blue team
- Membres de purple team
- Spécialistes inforensiques soucieux de mieux comprendre les tactiques offensives

Fonctions du référentiel NICE

- Adversary Emulation Specialist/Red Teamer (OPM 541)
- Target Developer (OPM 131)
- Cyber Ops Planner (OPM 332)
- Partner Integration Planner (OPM 333)

Jean-François Maes
Auteur de la formation



Erik Van Buggenhout
Auteur de la formation

Dans cette formation pointue, les stagiaires purple team sont plongés dans le monde de l'émulation d'attaques pour fortifier les défenses contre les violations de données. Dans l'univers des auteurs de menaces, les expériences de terrain qu'ils découvrent au sein d'un environnement dynamique d'entreprise les aident à maîtriser la détection et l'émulation des techniques d'attaque. Soixante pour cent du temps de formation est consacré aux labos, et les activités comprennent :

- Une partie sur les stratégies classiques d'automatisation comme Ansible, Docker et Terraform qui servent notamment à déployer un environnement d'entreprise multidomaine pour émuler les attaques en quelques clics.
- L'élaboration d'un véritable processus, de l'outillage et de la planification pour le fonctionnement en purple team.
- L'élaboration de plans d'émulation d'attaques à la manière d'acteurs réels comme APT-28, APT-34 et Turla avec des outils comme Covenant et Caldera.
- L'étude en profondeur de techniques comme les attaques par délégation Kerberos, les contournements de réduction de la surface d'attaque/Applocker, les contournements d'EDR, l'interface AMSI (Anti-Malware Scan Interface), l'injection de processus, et le détournement d'objet COM.
- L'ingénierie de détection et l'analyse de la télémétrie pour repérer les techniques ci-dessus.
- Un projet final rythmé qui met à rude épreuve vos compétences d'émulation d'attaque.

SEC699™ est la suite logique de SEC599™. Tous deux certifiés GIAC Security Experts, les auteurs Erik Van Buggenhout, principal auteur de SEC599™, et Jean-François Maes, principal auteur de SEC565™, sont des professionnels chevronnés que leurs activités tant en red team qu'en blue team ont dotés d'une compréhension approfondie des rouages des cyberattaques. Dans la formation SEC699™, ils unissent leurs forces pour enseigner des méthodes d'émulation d'attaque dans le but de détecter et prévenir les atteintes aux données.

Programme

SECTION 1 : Introduction et outils essentiels

SECTION 2 : Émulation et détection des stratégies d'intrusion initiale

SECTION 3 : Émulation et détection d'élévation de privilèges et de déplacement latéral

SECTION 4 : Émulation et détection de persistance

SECTION 5 : Plans d'émulation (accès extensif à CTF Range)

« SEC699 est dans l'ensemble la meilleure formation que j'ai suivie comme chargé de réponse aux incidents et analyste SOC. Elle simule par de nombreuses techniques les véritables attaques et options de défense du terrain. Elle m'a apporté un cadre structuré pour faire évoluer nos fonctions SOC actuelles. »

— Maurice von Wintersdorff, **Philips**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC699**

MODES DE FORMATION DE SEC699

In-Person **Live Online** **OnDemand**

SEC760: **Advanced Exploit Development for Penetration Testers™**

6 jours	46 crédits CPE	+30 labos

Vous apprendrez à...

- Découvrir les vulnérabilités zero-day des programmes qui fonctionnent sur les systèmes d'exploitation récents et patchés
- Utiliser les fonctionnalités avancées d'IDA Pro et rédiger des scripts IDAPython
- Déboguer à distance les applications Linux et Windows
- Comprendre et exploiter les dépassements de tas Linux
- Mener des tests à données aléatoires (fuzzing) sur applications propriétaires
- Décompresser et examiner des packages de mise à jour Windows
- Comparer les correctifs (patch diffing) des programmes, des bibliothèques et des pilotes pour identifier les vulnérabilités corrigées
- Réaliser le débogage de noyau Windows jusqu'à Windows 10 64 bits build 1903
- Rétroconcevoir et exploiter des pilotes du noyau Windows

Public visé :

- Experts séniors en tests d'intrusions réseau et système sachant développer des exploits
- Développeurs d'applications sécurisées (C et C++)
- Professionnels de la rétro-ingénierie de systèmes
- Gestionnaires d'incidents séniors sachant développer des exploits
- Analystes des menaces séniors sachant développer des exploits
- Spécialistes dans la recherche de vulnérabilités
- Chercheurs en sécurité

Fonctions du référentiel NICE

- Adversary Emulation Specialist / Red Teamer (OPM 541)
- Exploitation Analyst(OPM 121)
- Target Developer (OPM 131)

Jaime Geiger
Auteur de la formation

Stephen Sims
Auteur de la formation

Les vulnérabilités des systèmes d'exploitation prédominants, tels que Microsoft Windows 10 et 11 et les distributions Linux les plus récentes, sont souvent très complexes et subtiles. Mais quand des attaquants accomplis les exploitent, ces vulnérabilités sapent les défenses d'une organisation, qu'elles exposent à des dégâts considérables. Peu de professionnels de la sécurité ont les compétences requises pour découvrir pourquoi une vulnérabilité complexe existe et comment écrire un exploit pour la compromettre. Paradoxalement, les assaillants doivent entretenir ces compétences, quel que soit le degré de complexité. SANS SEC760: Advanced Exploit Development for Penetration Testers™ enseigne les compétences requises pour trouver des vulnérabilités applicatives par rétroconception, déboguer à distance des noyaux et des applications utilisateur, chercher des exploits 1-day dans les correctifs, mener des tests à données aléatoires (fuzzing), et écrire des exploits complexes ciblant par exemple le noyau Windows et le tas Linux moderne, tout en contournant les mesures sophistiquées d'atténuation des exploits.

Vous apprendrez à...

- Écrire des exploits modernes ciblant les systèmes d'exploitation Windows 10 et 11
- Suivre des techniques de développement d'exploit comme le fuzzing avancé, l'exploitation du noyau et de pilotes, l'exploitation 1-day au moyen de l'analyse de correctifs, les dépassements de tas Linux et autres attaques avancées
- Utiliser efficacement divers débogueurs et plug-ins pour améliorer et accélérer la recherche de vulnérabilités
- Gérer des techniques récentes d'atténuation des exploits visant à faire échouer ceux-ci

Programme

SECTION 1 : Atténuations des exploits et rétroconception avec IDA

SECTION 2 : Exploitation avancée pour Linux

SECTION 3 : Tests à données aléatoires, dits « fuzzing », avancés

SECTION 4 : Comparaison de correctifs ou « patch diffing », exploits 1-day et noyaux Windows

SECTION 5 : Débogage de noyau Windows et exploitation

SECTION 6 : Défi CTF

« J'ai suivi de nombreux autres cours de développement d'exploit avancé et aucun ne décortique les exploits comme cette formation. »

— Adam Logue, **SecureWorks**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC760**

MODES DE FORMATION DE SEC760

In-Person **Live Online** **OnDemand**

AXE DE FORMATION SANS

Cloud Security

La technologie du cloud computing s'avère la plus porteuse de transformations de notre ère. La sécurité du cloud jouera un rôle déterminant dans son adoption. Il s'agit d'anticiper l'évolution du cloud, plutôt que de se focaliser sur son fonctionnement actuel. Nous aurons besoin à l'avenir de compétences techniques approfondies sur le cloud combinées à la connaissance des fonctionnalités des services et de la sécurité de chaque grand cloudiste. Osez franchir le pas pour vous transformer en as de la cybersécurité du cloud.

Issu d'un processus de consensus dans notre secteur d'activité, notre programme à l'approche globale et pragmatique traite de la sécurité du cloud public, notamment les scénarios multicloud et de cloud hybride pour l'entreprise comme pour les organisations en croissance. Découvrez comment les différents fournisseurs cloud interagissent l'un avec l'autre et les nuances entre eux, ne vous contentez pas de connaître les rouages d'une seule plateforme.

En formation à la sécurité du cloud, vous apprendrez par la pratique à :

- Durcir et configurer les services de Cloud public d'AWS, de Microsoft Azure et de Google Cloud Platform (GCP)
- Automatiser les bonnes pratiques de sécurité et de conformité
- Utiliser des services cloud pour construire et déployer des systèmes et applications de manière sécurisée
- Insérer fluidement la sécurité dans votre chaîne d'outils DevOps
- Construire, déployer et gérer les conteneurs et Kubernetes en sécurité
- Mettre au jour les vulnérabilités et les faiblesses de vos environnements cloud
- Déceler l'activité des attaquants dans les journaux de vos clouds

« Le monde a pris le tournant du cloud et nous, professionnels de la sécurité, devons faire de même. »

— Daniel Harrison, **Capital One**

Fonctions de sécurité du cloud :

- Analyste en sécurité cloud
- Ingénieur sécurité cloud
- Architecte sécurité cloud
- Responsable sécurité cloud
- Professionnel DevOps

ZOOM NOUVELLE FORMATION

SEC480: **AWS Secure Builder™**

AWS SECURE BUILDER MICRO-CREDENTIAL BY GIAC

AWS Secure Builder
giac.org/micro-credentials/aws-secure-builder

2 jours	12 crédits CPE	8 labos

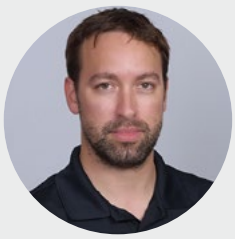
Vous apprendrez à...

- Mettre en œuvre les bonnes pratiques de sécurité du secteur dans les charges de travail AWS
- Maîtriser la gestion des identités et des accès (IAM) d'AWS, notamment les rôles, les politiques et les permissions pour le contrôle des accès sécurisés
- Étudier et évaluer les services AWS en fonction de la documentation sur la sécurité, des contrôles, et des risques relevés par les audits
- Surveiller les incidents de sécurité et y répondre à l'aide des outils AWS de détection, de réponse et de protection
- Automatiser les processus de sécurité à l'aide de services AWS comme AWS Lambda et AWS GuardDuty
- Identifier les lacunes de sécurité dans les pipelines d'intégration et de livraison continues (CI/CD) et repérer les écarts dans les pratiques actuelles de sécurité cloud
- Sécuriser les données en transit et au repos à l'aide du chiffrement et d'autres mesures de protection
- Mener des audits et des évaluations de sécurité complets à des fins de conformité et d'identification des risques
- Assurer que les déploiements AWS respectent les normes sectorielles et les obligations réglementaires
- Développer et mettre en œuvre des plans de réponse à incident adaptés aux environnements AWS
- Optimiser en permanence votre posture de sécurité à l'aide de revues et d'actualisations régulières

Public visé :

Spécialistes d'implémentation AWS :

- Développeurs d'applications web
- Responsables d'équipe cloud
- Ingénieurs cloud
- Architectes cloud
- Administrateurs cloud
- Tout profil technique appelé à construire des environnements cloud AWS, à y évoluer, à les configurer ou à les gérer



Serge Borso
Auteur de la formation

Intégrer la sécurité dès le début

Les violations de données d'une infrastructure cloud découlent souvent d'erreurs de configuration commises involontaires par du personnel extérieur à l'équipe sécurité. Développeurs, ingénieurs, architectes et autres rôles voisins dans le cloud doivent être formés sur leur plateforme pour privilégier efficacement la sécurité et réduire la probabilité de violations préjudiciables. La formation SEC480: AWS Secure Builder™ remplit cette fonction en dotant les personnels techniques des compétences nécessaires pour intégrer dès le départ les principes de sécurité aux charges de travail AWS. Elle comprend huit modules complets, chacun disposant de son labo pratique qui assure que les stagiaires acquièrent l'expérience concrète de la construction d'environnements AWS sécurisés.

Bilan

- Vous facilitez la mise en œuvre de solutions de sécurité évolutives dans toute votre organisation.
- Vous augmentez la confiance et la satisfaction de vos clients.
- Vous consolidez la posture de sécurité de l'organisation.
- Vous renforcez la confiance des employés et leurs compétences en développement AWS sécurisé.
- Vous améliorez la conformité avec les règles de sécurité cloud.
- Vous favorisez l'agilité de votre activité grâce aux pratiques sécurisées dans le cloud.
- Vous allégez la charge de travail et le stress de l'équipe sécurité.

Programme

MODULE 1 : Responsabilité en sécurité : envers qui, pour quoi et de quoi

MODULE 2 : Identification et autorisation

MODULE 3 : Intégration et livraison continues (CI/CD)

MODULE 4 : Sécurisation renforcée des charges de travail et des services

MODULE 5 : Supervision de la sécurité

MODULE 6 : Exposition et vecteurs d'attaque

MODULE 7 : Réponse aux incidents

MODULE 8 : Confiance, contrôle et supply chain

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC480**

MODES DE FORMATION DE SEC480

OnDemand

SEC488: **Cloud Security Essentials™** MISE À JOUR MAJEURE

GCLD Cloud Security Essentials giac.org/gcld — ANAB ACCREDITED — DoD 8140*

6 jours | 36 crédits CPE | 40 labos (à double parcours)

Vous apprendrez à...

- **Mettre au jour les faiblesses de sécurité cloud :** acquérez l'expertise pour repérer les écarts dans la posture de sécurité cloud de votre organisation.
- **Maîtriser la communication de la sécurité cloud :** échangez sans crainte sur les concepts de sécurité du cloud avec des experts techniques et la direction.
- **Ouvrir un chemin dans les défis du cloud :** guidez votre organisation avec adresse parmi les nombreux enjeux et possibilités dynamiques de la sécurité du cloud.
- **Identifier les risques des services cloud :** repérez et évaluez les risques associés aux offres des différents fournisseurs de services cloud.
- **Choisir des contrôles de sécurité efficaces :** sélectionnez les bonnes mesures de sécurité selon les différentes architectures de sécurité réseau et cloud.
- **Évaluer les fournisseurs cloud avec recul :** d'après leur documentation, leurs contrôles de sécurité et leurs rapports d'audit.
- **Rentabilisez les services des grands fournisseurs cloud :** utilisez avec confiance les services de grands cloudistes comme AWS, Azure et GCP.

Public visé :

- Ingénieurs sécurité cloud
- Analystes en sécurité cloud
- Administrateurs système
- Gestionnaires de risques
- Responsables sécurité
- Auditeurs de sécurité cloud
- Professionnels de sécurité cloud
- Architectes cloud
- Professionnels de l'informatique
- Développeurs en environnement cloud
- Agents de conformité chargés de la sécurité du cloud
- Ingénieurs réseau en évolution vers des rôles en sécurité du cloud

Fonctions du référentiel NICE

- Security Architect (OPM 652)
- Systems Security Analyst (OPM 461)
- Information Systems Security Manager (OPM 722)

Ryan Nicholson
Auteur de la formation

* DoD 8140 APPROVED
sans.org/8140

Les fondamentaux d'un environnement cloud sécurisé

Même si votre organisation excelle à sécuriser les environnements sur site, la transition vers le cloud présente ses propres défis, auxquels vous n'êtes pas nécessairement prêts. Les organisations adoptent rapidement les technologies cloud à travers le monde, sans appréhender totalement les principaux problèmes de sécurité comme la configuration des environnements dans le triple objectif de protéger les données sensibles, de maintenir la conformité réglementaire, et de détecter les accès non autorisés. De nombreuses formations se révèlent insuffisantes à trop se concentrer sur la théorie. SEC488: Cloud Security Essentials™ répond à ces défis en 20 labos pratiques, un grand projet final CTF, et des contenus haut de gamme qui vous aident à bâtir un socle cloud sécurisé.

Bilan

- **Risque cloud minimisé :** sécurisez vos environnements cloud pour réduire drastiquement vos vulnérabilités.
- **Protection des ressources informatiques :** gardez tout votre budget en protégeant votre puissance de calcul.
- **Conformité renforcée :** améliorez la conformité de votre sécurité cloud en respectant les normes réglementaires et en allant au-delà.
- **Efficacité boostée :** exploitez l'automatisation pour rationaliser les opérations et augmenter la productivité globale.
- **Rétention des collaborateurs :** renforcez la sécurité organisationnelle, et améliorez ainsi la satisfaction et la fidélité de vos effectifs.
- **Notoriété :** protégez et améliorez la notoriété de votre organisation en sécurisant vos opérations dans le cloud.
- **Confiance client :** augmentez la confiance de votre clientèle par des mesures de sécurité cloud robustes et fiables.

Programme

SECTION 1 : Gestion des identités et des accès (IAM)
SECTION 2 : Gestion de la configuration et de la puissance de traitement
SECTION 3 : Protection des données
SECTION 4 : Réseau et détection
SECTION 5 : Conformité, réponse aux incidents et tests d'intrusion
SECTION 6 : CloudWars

« J'ai beaucoup appris, je suis allée bien plus loin que ce à quoi je m'attendais, et je n'ai vraiment pas l'impression d'avoir perdu mon temps. Les instructeurs et leurs assistants sont de premier ordre et ont fait de cette formation une expérience excellente. »

— Marni Reemer, **AWS**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC488**

MODES DE FORMATION DE SEC488

In-Person | Live Online | OnDemand

SEC510: **Cloud Security Controls and Mitigations™** MISE À JOUR MAJEURE

GPCS
Public Cloud Security
giac.org/gpcs

5 jours | 38 crédits CPE | +20 labos

Vous apprendrez à...

- Prendre des décisions avisées pour les 3 grands fournisseurs de services cloud en comprenant les rouages internes des offres de plateforme et d'infrastructure à la demande (PaaS et IaaS) de chacun
- Mettre en œuvre la gestion sécurisée des identités et des accès (IAM) avec plusieurs couches de défense en profondeur
- Construire et sécuriser des réseaux multicloud avec segmentation et contrôle des accès
- Chiffrer les données au repos et en transit dans l'ensemble de chaque cloud
- Contrôler la confidentialité, l'intégrité et la disponibilité des données pour chaque service de stockage cloud
- Prendre en charge d'autres plateformes informatiques comme des services applicatifs ou l'informatique sans serveur (FaaS)
- Intégrer mutuellement les fournisseurs cloud sans recourir à des identifiants persistants
- Automatiser la sécurité et les vérifications de conformité à l'aide de plateformes cloud natives
- Accompagner les équipes d'ingénieurs dans l'application de contrôles de sécurité à l'aide de Terraform et de l'infrastructure programmable (IaC)

Public visé :

- Analystes sécurité
- Ingénieurs sécurité
- Chercheurs en sécurité
- Ingénieurs cloud, ingénieurs DevOps
- Auditeurs sécurité
- Administrateurs système
- Collaborateurs opérationnels

Fonctions du référentiel NICE

- Security Control Assessor (OPM 612)
- Enterprise Architect (OPM 651)
- Security Architect (OPM 652)
- Research & Development Specialist (OPM 661)
- Information Systems Security Developer (OPM 631)

Brandon Evans
Auteur de la formation

Eric Johnson
Auteur de la formation

Prévenir les attaques avec des contrôles déterminants

Aujourd'hui, les organisations dépendent d'environnements multicloud complexes qui doivent prendre en charge des centaines de services différents sur plusieurs clouds. Ces services sont rarement sécurisés par défaut. Les services comparables des autres fournisseurs de services cloud doivent être protégés, mais les méthodes sont très différentes. Les équipes de sécurité doivent posséder une compréhension approfondie des services AWS, Azure et Google Cloud pour bien les verrouiller. Cocher les critères de conformité ne suffit pas à protéger la confidentialité, l'intégrité et la disponibilité des données de votre organisation et n'empêchera pas non plus les assaillants de faire tomber vos systèmes critiques. Avec les contrôles adéquats, les organisations peuvent réduire leur surface d'attaque et éviter que les incidents de sécurité se transforment en violation. L'erreur est humaine. Il faut limiter l'impact de ce qui est inévitable.

Bilan

- Vous réduisez la surface d'attaque des environnements cloud de votre organisation.
- Vous évitez que des incidents ne se muent en violation grâce à une défense en profondeur.
- Vous contrôlez la confidentialité, l'intégrité et la disponibilité des données chez les trios grands fournisseurs cloud.
- Vous renforcez l'automatisation sécurisée pour rester en phase avec l'environnement des affaires actuel.
- Vous empêchez les accès involontaires aux actifs cloud sensibles.
- Vous réduisez le risque de ransomware affectant les données cloud de l'organisation.

Programme

SECTION 1 : Gestion des identités et des accès dans le cloud
SECTION 2 : Réseaux virtuels cloud
SECTION 3 : Sécurité des données dans le cloud
SECTION 4 : Services des applications cloud et sécurité des utilisateurs
SECTION 5 : Multicloud et services de gestion de la posture de sécurité cloud (CSPM)

« Une formation incroyablement bien conçue. De nouvelles informations exploitables à chaque page. »

— Jordan N., **administration fédérale américaine**

« C'est incroyable de pouvoir échanger avec les trois cloudistes en même temps pendant le labo. Impressionnant. »

— Christopher Hearn, **comté de Harris, Texas**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC510**

MODES DE FORMATION DE SEC510

In-Person | **Live Online** | **OnDemand**

SEC522: **Application Security: Securing Web Applications, APIs, and Microservices™**

GWEB
Web Application Defender
giac.org/gweb

6 jours	36 crédits CPE	+20 labos

Vous apprendrez à...

- Vous défendre contre les attaques du Top 10 OWASP
- Implémenter la sécurité des infrastructures et la gestion de la configuration
- Intégrer dans la sécurité les composants cloud à une application web
- Mettre en œuvre les mécanismes d'authentification et d'autorisation, notamment les schémas SSO
- Assurer la sécurité des requêtes web cross-domain
- Définir des en-têtes HTTP qui jouent un rôle protecteur
- Défendre les API SOAP, REST et GraphQL
- Implémenter en toute sécurité une architecture de microservices
- Vous défendre contre des défauts liés aux entrées comme l'injection SQL, XSS et CSRF

Public visé :

- Développeurs d'application
- Analystes ou responsables de la sécurité des applications
- Architectes d'applications
- Experts en tests d'intrusion curieux des stratégies défensives
- Professionnels de la sécurité curieux d'en savoir plus sur la sécurité des applications web
- Auditeurs qui doivent comprendre les mécanismes défensifs des applications web
- Personnel d'organisations certifiées PCI qui doit se former au respect de ces normes

Fonctions du référentiel NICE

- Software Developer (OPM 621)
- Secure Software Assessor (OPM 622)
- Research & Development Specialist (OPM 661)
- Information Systems Security Developer (OPM 631)
- Systems Developer (OPM 632)

Jason Lam
Auteur de la formation

Dr Johannes Ullrich
Auteur de la formation

La question n'est pas de savoir « si », mais « quand ». Préparez-vous à une attaque web. Nous vous accompagnons.

Les logiciels des systèmes de comptabilité, de surveillance de la sécurité et de contrôle industriel ont ceci de commun que ce sont tous des applications web basées sur des interfaces de programmation d'application (API). Il est donc essentiel de bien comprendre les vulnérabilités web pour protéger une organisation, sur site ou en cloud. SEC522 forme les professionnels de la sécurité aux compétences nécessaires pour identifier et atténuer les vulnérabilités courantes des applications web, des services cloud natifs et des API, ainsi qu'à l'intégration des bonnes pratiques aux processus de développement. Cette formation comprend 20 labos pratiques et un exercice de défense CTF en sixième partie.

Bilan

- Respect des critères des normes PCI DSS et d'autres obligations de conformité.
- Réduction des risques globaux de sécurité applicative, protection de la réputation de l'entreprise.
- Acculturation à l'état d'esprit « shift left », qui vise à traiter rapidement et précocement les problèmes de sécurité, ce qui évite des reprises coûteuses.
- Capacité à adopter des applications modernes dotées d'API et de microservices de manière sécurisée.
- Préparation des stagiaires à la certification GWEB.

Programme

SECTION 1 : Fondamentaux du web et configurations sécurisées

SECTION 2 : Défenses liées aux entrées

SECTION 3 : Authentification et autorisation

SECTION 4 : Services web et sécurité frontale

SECTION 5 : Sécurité des API et des microservices

SECTION 6 : DevSecOps et exercice de défense du drapeau

« Bien pensés et faciles à suivre, les labos font acquérir de bonnes compétences pratiques. »

— Barbara Boone, **CDC**

« SEC522 enseigne les défenses pour sécuriser les applications web, et montre aussi que la fréquence et la simplicité de ces attaques obligent à sécuriser les applications. »

— Brandon Hardin, **ITC**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC522**

MODES DE FORMATION DE SEC522

In-Person **Live Online** **OnDemand**

SEC540: **Cloud Native Security and DevSecOps Automation™**

GCSA Cloud Security Automation
giac.org/gcsa
ANAB ACCREDITED ISO/IEC 17024 PERSONNEL CERTIFICATION BODY
DoD 8140*

5 jours	38 crédits CPE	+35 labos

Vous apprendrez à...

- Comprendre l'approche DevOps et identifier les clés du succès
- Intégrer l'exploration des vulnérabilités aux workflows et aux pipelines CI/CD
- Décomposer les résultats de l'analyse des vulnérabilités et afficher les données sur les tableaux de bord CI/CD
- Gérer les secrets des serveurs CI/CD et des applications cloud natives
- Automatiser la gestion des configurations avec l'infrastructure programmable (IaC)
- Construire, durcir et publier des images maîtres de machines virtuelles à l'aide de workflows CI/CD
- Exploiter et sécuriser les technologies de conteneurs avec Docker et Kubernetes
- Durcir les clusters Kubernetes avec l'identité de charge de travail et le contrôle d'admission

Public visé :

- Quiconque travaille dans un environnement cloud public/DevOps ou s'y prépare
- Quiconque cherche à savoir placer des contrôles, tests de sécurité et autres sur le cloud et sur des projets DevOps à livraison continue
- Quiconque souhaite apprendre à migrer des charges de travail DevOps vers le cloud, notamment vers AWS et Microsoft Azure
- Quiconque souhaite savoir exploiter les services de sécurité applicative cloud proposés par AWS ou Azure
- Développeurs
- Architectes logiciels
- Ingénieurs opérationnels
- Administrateurs système
- Analystes sécurité
- Ingénieurs sécurité
- Auditeurs
- Gestionnaires de risques
- Consultants en sécurité

Fonctions du référentiel NICE

- Software Developer (OPM 621)
- Secure Software Assessor (OPM 622)
- Enterprise Architect (OPM 651)
- Research & Development Specialist (OPM 661)
- Information Systems Security Developer (OPM 631)
- Systems Developer (OPM 632)

Frank Kim
Auteur de la formation

Eric Johnson
Auteur de la formation

Ben Allen
Auteur de la formation

*DoD 8140 APPROVED
sans.org/8140

Sécurisez vos systèmes à la vitesse du cloud

Les organisations passent au cloud pour faciliter la transformation numérique et récolter les bénéfices de l'informatique dans le cloud. Toutefois, les équipes de sécurité peinent à comprendre la chaîne d'outils DevOps et comment mettre en place des contrôles de sécurité dans leurs pipelines automatisés qui délivrent les modifications au système cloud. Sans contrôle de sécurité efficace dans les pipelines, les équipes de sécurité perdent en visibilité sur les changements publiés dans les environnements de production. SEC540™ leur apporte les connaissances nécessaires pour automatiser les garde-fous et les politiques de sécurité dans les pipelines DevOps, l'infrastructure cloud, les orchestrateurs des conteneurs et les environnements de microservices de leur organisation. À l'issue de cette formation, les stagiaires se seront approprié la culture DevOps et auront acquis une expérience pratique, prêts à élaborer le programme de sécurité cloud et DevSecOps de leur organisation.

Bilan

- Vous constituez une équipe de sécurité moderne formée à la sécurité cloud native et aux workflows DevSecOps.
- Vous associez les équipes DevOps et ingénierie pour intégrer la sécurité dans vos pipelines automatisés et en amont dans le processus de développement.
- Vous exploitez les services cloud natifs pour déployer, durcir et surveiller les produits logiciels.
- Vous vous assurez que votre organisation est prête à remanier, revoir et reconstruire les produits pendant la migration vers le cloud.
- Vous utilisez la surveillance du cloud et l'automatisation déclenchée par les événements pour améliorer les fonctionnalités de sécurité et répondre efficacement aux risques.

Programme

SECTION 1 : Automatisation de la sécurité DevOps
SECTION 2 : Sécurité de l'infrastructure cloud
SECTION 3 : Opérations de sécurité cloud natives
SECTION 4 : Sécurité des microservices et sans serveur
SECTION 5 : Conformité et protection continues

« La MEILLEURE formation que j'ai jamais suivie chez SANS. Quand je me connecte en télétravail après la journée de formation, je peux l'appliquer immédiatement à mes tâches et responsabilités quotidiennes. Je suis déjà allé dire à mon équipe sur Slack qu'il fallait absolument que ce soit leur prochaine formation. »

— Brian Esperanza, **Teradata**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC540**

MODES DE FORMATION DE SEC540

In-Person | Live Online | OnDemand

SEC541: **Cloud Security Threat Detection™** MISE À JOUR MAJEURE

GCTD
Cloud Threat Detection
giac.org/gctd

5 jours	30 crédits CPE	21 labos

Vous apprendrez à...

- Utiliser frauduleusement les identités dans les environnements cloud
- Surveiller les auteurs de menaces à l'aide d'outils de journalisation cloud natifs
- Définir et comprendre les ressources informatiques comme les machines virtuelles (VM) et les conteneurs
- Détecter et traiter les pivots d'attaque au sein de votre infrastructure cloud
- Mettre en œuvre des stratégies de détection efficaces à l'aide des outils du fournisseur cloud
- Enquêter sur les instances dans vos ressources informatiques et les analyser pour y détecter les activités suspectes
- Mener la détection et l'analyse détaillée des menaces dans les environnements Microsoft 365 et Azure
- Remonter d'une source de journal à l'autre pour mettre au jour tout le déroulé d'une attaque
- Construire des workflows d'automatisation pour alléger les tâches de sécurité répétitives
- Centraliser et normaliser les données issues de différentes sources pour améliorer la détection des menaces et l'analyse

Public visé :

- Analystes en sécurité cloud
- Ingénieurs spécialistes de la détection des menaces
- Membres du centre des opérations de sécurité (SOC)
- Chargés de réponse aux incidents de sécurité
- Architectes sécurité cloud
- Experts en tests d'intrusion
- Responsables SOC
- Membres de blue team
- Analystes inforensiques
- Professionnels de la sécurité offensive cherchant à comprendre les techniques défensives
- Professionnels de l'informatique en évolution vers des rôles en sécurité du cloud
- Quiconque chargé de sécuriser les environnements cloud dans tout secteur

Fonctions du référentiel NICE

- Security Architect (OPM 652)
- Systems Security Analyst (OPM 461)
- Information Systems Security Manager (OPM 722)

Shaun McCullough
Auteur de la formation

Ryan Nicholson
Auteur de la formation

Les attaquants peuvent s'enfuir, mais pas se cacher. Notre radar repère toutes les menaces.

Si le passage à l'infrastructure cloud apporte de nombreux avantages, il expose aussi les organisations à des menaces nouvelles et en constante évolution. Beaucoup d'organisations ne se rendent pas compte des différences essentielles entre les environnements sur site et cloud, ce qui rend difficile l'appréhension des données à journaliser et des moyens pour détecter efficacement les menaces. À la différence d'autres formations surtout théoriques, SEC541™ propose une expérience pratique, mains sur le clavier, au travers de 21 labos concrets qui couvrent AWS, Azure et Microsoft 365. Elle donne les moyens à votre équipe de maîtriser la journalisation, la détection des menaces et la surveillance cloud natives, en résolvant des problèmes cachés triviaux à haut ROI. Avec SEC541™, dotez votre équipe des compétences pour améliorer la posture de sécurité cloud de votre organisation et garder une longueur d'avance sur les violations potentielles.

Bilan

- **Temps de détection et de réponse réduits :** identifiez rapidement les menaces cloud critiques et réagissez-y.
- **Meilleure visibilité :** avec un éclairage multifacette sur votre environnement cloud.
- **Meilleure posture de sécurité :** mettez en œuvre des stratégies efficaces de détection des menaces cloud.
- **Gestion proactive des menaces :** traitez précocement les menaces et contribuez à la résolution rapide des incidents.
- **Efficacité et automatisation :** gagnez en efficacité grâce à l'automatisation des workflows de détection et de réponse.
- **Réduction des coûts :** évitez les conséquences financières en sécurisant en amont votre environnement cloud.
- **Montée en compétences :** armez votre équipe des technologies et connaissances de pointe en sécurité cloud pour se défendre contre les menaces sophistiquées.

Programme

SECTION 1 : Plan de management et attaques réseau
SECTION 2 : Calcul et attaques des applications
SECTION 3 : Services de sécurité et découverte de données
SECTION 4 : L'écosystème Microsoft
SECTION 5 : Échange de données « data shipping », automatisation et exercice CloudWars

« C'est une formation très bien conçue. Shaun et Ryan ont bien travaillé. Le contenu est excellent, il y a beaucoup à apprendre. »

— Scott Perry

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC541**

MODES DE FORMATION DE SEC541

In-Person **Live Online** **OnDemand**

ZOOM NOUVELLE FORMATION

SEC545: **GenAI and LLM Application Security™**

3 jours	18 crédits CPE	11 labos

Vous apprendrez à...

- **Comprendre les notions et termes clés :** appréhendez en profondeur l'intelligence artificielle générative (GenAI), les architectures des grands modèles de langage (LLM) et leur application dans les scénarios de terrain.
- **Explorer différents modèles et outils :** étudiez les types de modèles et d'outils pour bâtir et déployer des applications de GenAI.
- **Ajuster finement et personnaliser :** apprenez à affiner et à adapter les modèles à des cas d'utilisation précis.
- **Évaluer les risques et leurs stratégies d'atténuation :** identifiez les risques propres aux applications de GenAI et explorez les techniques efficaces de réduction des risques.
- **Sécuriser la génération augmentée de récupération (RAG), les plongements et les bases de données vectorielles :** comprenez ces notions et la configuration sécurisée des différents éléments.
- **Explorer les opérations et les contrôles de sécurité :** approfondissez les aspects opérationnels de la construction et du déploiement d'applications de GenAI et les contrôles de sécurité pertinents.
- **Comparer les options d'hébergement :** comprenez les possibilités d'hébergement de la GenAI et leurs différences du point de vue de la sécurité.
- **Exploiter les contrôles de sécurité du cloud :** découvrez les contrôles proposés par les cloudistes dans leurs offres d'hébergement de LLM.
- **Explorer les technologies voisines de la GenAI :** étudiez par ex. LangChain et les agents et comprenez les risques de sécurité induits.
- **Intégrer la GenAI aux cadres de sécurité :** apprenez à bâtir ou à intégrer les pratiques de sécurité de la GenAI aux frameworks de sécurité existants dans votre organisation.

Public visé :

- Ingénieurs sécurité des applications
- Ingénieurs sécurité cloud
- Analystes SOC, chargés de réponse à incident et spécialistes du renseignement d'intérêt cyber
- Professionnels de la sécurité
- Auditeurs sécurité, responsables de la conformité et gestionnaires de risques

Ahmed Abugharbia
Auteur de la formation

La nouveauté du secteur explique l'absence de standardisation actuelle des pratiques de sécurité de l'IA générative (GenAI). Cette formation veut contribuer au développement des bonnes pratiques sécuritaires de la GenAI, en proposant au secteur des clés issues de la recherche en cours et un cursus évolutif.

La formation SEC545 explore en profondeur les technologies d'IA générative, à commencer par ses principes essentiels et les technologies sous-jacentes. Pour évaluer les risques de sécurité, elle s'attache à identifier et à analyser les menaces en production qui impactent les applications de GenAI. À mesure qu'ils progressent, les stagiaires apprennent à établir de bonnes pratiques de sécurité en explorant différentes mesures pour sécuriser dans les faits les applications d'IA générative.

La formation commence par une introduction aux fondamentaux de l'IA générative, qui couvre les notions et termes clés comme les grands modèles de langage (LLM), les plongements et la génération augmentée de récupération (RAG). Elle s'intéresse ensuite aux risques de sécurité associés à cette GenAI, notamment les attaques par injection de prompts, les modèles malveillants et les vulnérabilités de la chaîne logicielle. Puis elle plonge dans les éléments essentiels de la construction d'une application d'IA générative, en traitant notamment les bases de données vectorielles, le framework LangChain et les agents d'IA. La formation se conclut sur une présentation complète des applications d'hébergement de GenAI, avec des discussions sur les tenants et aboutissants des options de déploiement local, des solutions cloud et des plateformes comme AWS Bedrock.

Bilan

- Compréhension des applications d'IA générative.
- Identification des risques associés aux applications d'IA générative.
- Atténuation efficace des risques de l'IA générative.

Programme

SECTION 1 : IA générative, grands modèles de langage et risques de sécurité

SECTION 2 : Sécuriser les applications d'IA générative

SECTION 3 : MLSecOps et sécurisation du cycle de vie des applications d'IA générative

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC545**

MODES DE FORMATION DE SEC545

In-Person **Live Online**

SEC549: **Cloud Security Architecture™**

MISE À JOUR MAJEURE

GCAD
Cloud Security Architecture and Design
giac.org/gcad

5 jours	30 crédits CPE	+20 labos

Vous apprendrez à...

- Faciliter l'activité par des conceptions d'architecture de sécurité cloud pour l'entreprise
- Faire le lien entre les conceptions d'architecture cloud et les solutions du marché
- Établir une base sécurisée et évolutive des identités dans le cloud
- Centraliser les identités des effectifs de votre organisation pour éviter la prolifération
- Construire des réseaux microsegmentés à l'aide de modèles en étoile
- Configurer des pare-feu réseau centralisés pour inspecter le trafic nord-sud et est-ouest
- Incorporer des contrôles réseau et identité
- Créer des périmètres de données pour les référentiels de données dans le cloud
- Centraliser et partager les ressources d'un service de gestion de clés (KMS) dans toute une organisation
- Activer les opérations de sécurité et la réponse aux incidents dans le cloud
- Appréhender la télémétrie et la journalisation disponibles dans les différents modèles de services (IaaS, PaaS et SaaS)
- Concevoir des architectures de journalisation en mode « push and pull » pour centraliser l'agrégation des journaux
- Prévoir des processus de récupération cloud en utilisant plusieurs couches de comptes de secours

Public visé :

- Architectes solutions
- Auditeurs sécurité
- Architectes cloud
- Ingénieurs sécurité
- Architecte sécurité
- Ingénieurs cloud
- Ingénieurs DevOps
- Administrateurs système
- Operations
- Toute personne chargée de :
  - faciliter l'activité par une architecture cloud sécurisée
  - évaluer et adopter de nouvelles offres cloud
  - planifier des migrations vers le cloud
  - mettre en œuvre ou gérer les identités et les accès dans le cloud
  - gérer un réseau virtuel cloud

Eric Johnson
Auteur de la formation

David Hazar
Auteur de la formation

Gregory Leonard
Auteur de la formation

Les organisations transfèrent leurs infrastructures et leurs applications vers le cloud à un rythme enlevé. À mesure qu'avancent les migrations, les architectes sécurité peinent à concevoir des solutions hybrides et cloud natives conformes aux critères de sécurité de leur organisation. Le passage au cloud exige de comprendre en profondeur les menaces qu'induit une telle migration et la manière dont l'architecture de référence « well-architected framework » de chaque fournisseur atténue ces menaces.

SEC549™ enseigne aux professionnels à concevoir une organisation cloud évolutive adaptée aux besoins de l'entreprise. Au fil de presque 20 labos pratiques, les stagiaires apprennent à concevoir des solutions cloud pour leur organisation, quel que soit son stade de transition vers le cloud – planification de la première charge de travail, gestion des environnements existants complexes, ou en activité dans un écosystème cloud natif évolué.

Bilan

- Vous atténuez les risques qu'introduisent les technologies cloud et leur adoption rapide.
- Vous réduisez le risque lié aux migrations vers le cloud avec la planification d'une approche progressive.
- Vous prévenez la prolifération des identités et la dette technique par la centralisation.
- Vous stimulez la croissance de l'entreprise à l'aide de garde-fous de haut niveau.
- Vous empêchez la multiplication des mauvais patrons de conception « antipattern » aux conséquences coûteuses dans l'organisation cloud.
- Vous appliquez les schémas d'accès acquis pour faciliter la progression de votre organisation vers le zero trust.
- Vous concevez des stratégies efficaces d'accès conditionnel et apprenez à placer des garde-fous autour des exceptions dictées par l'activité.

Programme

SECTION 1 : Fondamentaux de l'identité et de la gestion des comptes dans le cloud
SECTION 2 : Mettre en œuvre un périmètre des identités dans le cloud
SECTION 3 : Opérations de sécurité cloud natives
SECTION 4 : Périmètres d'accès aux données dans le cloud
SECTION 5 : Le SOC axé sur le cloud

« Les labos sont la simulation la plus réaliste que j'aie jamais vue de la vie d'un architecte sécurité. Pour les aspirants architectes, c'est un excellent exemple de ce qui se passe au quotidien dans une architecture. »

— Maciej Bak, **Standard Chartered**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC549**

MODES DE FORMATION DE SEC549

In-Person **Live Online** **OnDemand**

Formation SANS désormais disponible sur AWS Marketplace

Renforcez la sécurité cloud tout en maximisant vos avantages AWS EDP.

Dotez vos équipes de l'expertise nécessaire à la protection de votre infrastructure cloud. Accédez aux formations SANS Cloud Security par AWS Marketplace et créez des packages d'apprentissage évolutifs, flexibles et efficaces selon les besoins de votre organisation.

Adaptez l'apprentissage à vos conditions :

Formations sur mesure
Choisissez la formation la plus récente, **SEC480: AWS Secure Builder** et une sélection exhaustive de formations allant des configurations IAM et de la gestion des autorisations aux bonnes pratiques de la sécurité du cloud.

Partout, à tout moment
Formations à la demande pour que vos équipes apprennent à leur rythme, où qu'elles se trouvent – perturbations minimales de l'activité et participation élargie.

Animées par des spécialistes et en correspondance avec GIAC
Anticipez les menaces émergentes avec des formations de pointe, conçues et délivrées par des leaders de la cybersécurité, et alignées sur les crédits GIAC réputés dans le secteur.

Achat simplifié
Rationalisez votre processus d'achat et optimisez votre budget AWS Enterprise Discount Program (EDP).

Explorez l'offre de formation de SANS sur AWS Marketplace.

Scannez ce code pour élaborer votre plan de formation sur mesure.

AXE DE FORMATION SANS

Cyber Defense

Mettant l'accent strictement sur la cybersécurité, un chargé de défense se concentre sur la protection de l'organisation contre les cyberattaques. Mise en œuvre de contrôles de sécurité, validation de l'efficacité des contrôles, amélioration et surveillance continues... les cyberdéfenseurs renforcent les capacités de leur organisation à résister aux attaques.

Les formations en cyberdéfense vous apprendront à :

- Déployer les outils et techniques nécessaires pour défendre vos réseaux avec clairvoyance et discernement
- Implémenter une conception moderne de la sécurité afin de protéger vos actifs et de vous défendre face aux menaces
- Établir et maintenir une approche globale et multicouche de la sécurité
- Détecter les intrusions et analyser le trafic réseau
- Appliquer une approche proactive de la supervision de sécurité réseau (NSM), des diagnostics et atténuations en continu (CDM), et de la supervision continue de la sécurité (CSM)
- Utiliser des méthodes et des processus pour améliorer les solutions de journalisation
- Appliquer des principes et des contrôles de sécurité technique dans le cloud

« Les techniques acquises dans cette formation me permettent d'améliorer immédiatement nos capacités de détection et de journalisation. »

— Kendon Emmons, **Dart Container**

Fonctions de cyberdéfense :

- Responsable/analyste SOC
- Spécialiste en détection des intrusions et en recherche de compromissions
- Ingénieur et architecte réseau et sécurité
- Analyste OSINT, enquêteur
- Administrateur système de serveur/d'extrémité
- DevSecOps et automatisation
- Chargé de réponse aux cyberincidents
- Analyste en renseignement d'intérêt cyber (CTI)

SEC406: **Linux Security for InfoSec Professionals™**

5 jours	30 crédits CPE	40 labos

Vous apprendrez à...

- Appréhender avec assurance la ligne de commande Linux et sécuriser efficacement les systèmes Linux à l'aide de bonnes pratiques et de techniques de durcissement
- Configurer et gérer l'authentification des utilisateurs, les contrôles d'accès et les autorisations
- Auditer les systèmes Linux et analyser les journaux de sécurité pour y détecter les menaces
- Gérer les processus système, surveiller les performances et optimiser l'utilisation des ressources
- Implémenter les techniques de réponse à incident pour les événements de sécurité Linux
- Administrer à distance en sécurité en vous servant de SSH, SCP et OpenSSL Configurer des pare-feu et sécuriser les communications réseau Linux
- Installer, actualiser et gérer les logiciels Linux en toute sécurité avec la gestion des packages

Public visé :

- Toute personne chargée de la gestion de serveurs Linux et de leur sécurité
- Quiconque déploie et gère des applications sur solutions cloud Linux
- Professionnels de la sécurité souhaitant connaître les bonnes pratiques de sécurité Linux et les mettre en œuvre dans leur organisation
- Professionnels IT qui veulent mieux comprendre les concepts de sécurité Linux et améliorer leurs compétences en sécurité des systèmes Linux
- Quiconque veut en savoir plus sur la sécurité Linux et protéger les systèmes et données de son organisation contre les cybermenaces

Mark Baggett
Auteur
de la formation

Charles Goldner
Auteur
de la formation

Sécuriser, commander, protéger : formation pratique à la sécurité pour Linux

La plupart des professionnels novices de l'InfoSec connaissent mieux Windows que Linux, alors que dans les fonctions offensives, défensives, ICS et inforensiques, nombre d'outils indispensables exigent une compréhension solide de Linux. Cela pose un sérieux défi pour qui manque de l'expérience requise, car ces systèmes sont souvent utilisés dans les environnements fortement exposés, comme les zones démilitarisées et le cloud. Il est ironique de constater qu'aujourd'hui, nos plateformes de sécurité des informations créent elles-mêmes de nouveaux risques de sécurité. La formation à la sécurité pour Linux résout le problème avec de nombreux exercices concrets, au cours desquels les stagiaires développent rapidement les compétences Linux nécessaires et se muent en un atout pour leur future équipe de sécurité des informations.

Cette formation à la sécurité pour Linux s'intéresse aux aspects fondamentaux de l'administration Linux, qui vont de la configuration d'un système sécurisé Linux à la gestion des utilisateurs et des permissions, en passant par l'utilisation de la ligne de commande. Elle met aussi l'accent sur les aspects sécuritaires de ces compétences et enseigne ainsi aux stagiaires à sécuriser leur système Linux et à le défendre contre des attaques. Vous apprendrez comment une erreur de configuration engendre une vulnérabilité, comment attaquer celle-ci et comment atténuer ces risques. À l'issue de la formation, les stagiaires disposeront des connaissances et compétences requises pour sécuriser les systèmes Linux, identifier les menaces pour la sécurité et mettre en œuvre les mesures de prévention appropriées. L'expérience que vous aurez acquise vous transformera en un utilisateur de Linux compétent et fiable, un véritable atout pour votre employeur et non un risque.

Programme

SECTION 1 : Ligne de commande Linux

SECTION 2 : Syntaxe Shell et gestion des comptes

SECTION 3 : Contrôle d'accès des fichiers et des utilisateurs

SECTION 4 : Gestion des processus et des journaux

SECTION 5 : Gestion des paquets, SSH et du réseau

« Même si j'utilise Linux depuis un moment, j'ai appris et compris beaucoup de choses, et maintenant, tout s'éclaire. »

— John R., **militaire**

« J'ai vraiment aimé le déroulé de la formation – un bon déroulé, facile à suivre. »

— Christopher Hannon, **stagiaire SEC406**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC406**

MODES DE FORMATION DE SEC406

Live Online **OnDemand**

SEC450: **SOC Analyst Training – Applied Skills for Cyber Defense Operations™**

GSOC
Security Operations
giac.org/gsoc

6 jours	36 crédits CPE	16 labos

Vous apprendrez à...

- Exploiter au mieux la télémétrie de sécurité, notamment celle issue des capteurs des terminaux, du réseau et cloud
- Identifier les meilleures possibilités d'utilisation de la plateforme SOAR ou autres outils d'automatisation de script
- Conserver la maîtrise de vos opérations de sécurité, grâce aux discussions approfondies sur les tâches à accomplir d'étape en étape par l'équipe SOC ou SecOps – de la création des données à la détection, au triage et à l'analyse des incidents et la réponse à apporter
- Identifier et distinguer sans délai les alertes généralistes des attaques sophistiquées à haut risque et fort impact, et mener une analyse exhaustive des incidents de sécurité sans biais cognitif
- Expliquer en détail les processus et techniques afin de réduire au maximum les faux positifs
- Trier rapidement et correctement les incidents de sécurité à l'aide de techniques d'enrichissement et de corrélation de données qui démêlent immédiatement les vrais des faux positifs
- Créer, pour les activités courantes du SOC, des workflows d'automatisation qui soulagent les analystes des tâches ennuyeuses et dégagent du temps pour la recherche de compromission et l'ingénierie de détection

Public visé :

- Analystes sécurité
- Spécialistes en investigation d'incident
- Ingénieurs et architectes sécurité
- Responsables sécurité technique
- Responsables de centre des opérations de sécurité (SOC) qui cherchent à acquérir une perspective technique pour améliorer la qualité de leur analyse, réduire le taux de renouvellement du personnel et diriger un SOC efficace
- Quiconque aspirant à une carrière en défense (blue team)

Fonctions du référentiel NICE

- Cyber Defense Analyst (OPM 511)
- Cyber Defense Infrastructure Support Specialist (OPM 521)

John Hubbard
Auteur de la formation

Le guide vers l'excellence de l'analyse SOC

SEC450™ est conçue de a à z comme la formation la plus exhaustive du marché à l'analyse SOC. Vous êtes un opérationnel de la cyberdéfense ? Vous bâtissez un SOC ou cherchez de meilleures données, workflows et techniques d'analyse pour le vôtre ? SEC450™ s'adresse à vous ! Cette formation, parce qu'elle explique en détail la mission et l'état d'esprit d'une opération de cyberdéfense moderne, arme et fait monter en puissance la prochaine génération d'individus qui rejoindront les blue teams. Six jours de formation, six manuels, vingt labos pratiques, et en projet final, une journée entière consacrée à une compétition de défense du drapeau... aucune autre offre du marché n'est aussi complète que la formation SEC450™ pour SOC et analystes sécurité.

Bilan

- Une solution prête à l'emploi – qui répond aux besoins de formation des analystes SOC et leur apporte les compétences nécessaires à la compréhension des outils, des données et des priorités défensives indispensables pour protéger votre réseau contre les cyberattaques dévastatrices.
- Vous déduisez des priorités stratégiques claires pour l'équipe des opérations de sécurité.
- Vous montrez que vous savez valoriser la télémétrie de sécurité, notamment celle issue des capteurs des terminaux, du réseau et cloud.
- Une méthode éprouvée qui réduit au maximum les faux positifs.
- Des techniques de tri des incidents de sécurité rapide et sans erreur.
- Des méthodes qui améliorent l'efficacité, les performances et l'impact de votre SOC.

Programme

SECTION 1 : Présentation des équipes, des outils et de la mission des équipes des opérations de sécurité

SECTION 2 : Analyse du trafic réseau

SECTION 3 : Présentation de la défense des terminaux, de la journalisation pour la sécurité et de l'identification des programmes malveillants

SECTION 4 : Trier les alertes et analyser les emails avec efficacité

SECTION 5 : Amélioration en continu, analytique et automatisation

SECTION 6 : Projet final de défense du drapeau

« Jusqu'ici, SEC450 répond à mes attentes, et même plus. Il y a juste un an, je suis passé chef d'équipe SOC. Cette formation me fait monter en compétences et structure mon approche et ma vision de ce que mon SOC doit être. »

— Radek Ochrymowicz, **Frontex**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC450**

MODES DE FORMATION DE SEC450

In-Person **Live Online** **OnDemand**

SEC495: **Leveraging LLMs: Building & Securing RAG, Contextual RAG, and Agentic RAG™**

1 jour | 5 crédits CPE

Vous apprendrez à...

- Bâtir une solution backend de génération augmentée de récupération (RAG) de bout en bout
- Étendre une RAG pour implémenter des solutions de RAG contextuelles
- Comprendre et mettre en œuvre des agents IA dans un contexte de LLM à des fins de supervision RAG
- Mettre en œuvre des contrôles de sécurité restreignant la divulgation d'informations par un LLM
- Prévenir les attaques par injection de prompt et s'en défendre

Public visé :

- Quiconque chargé de mettre en œuvre une solution d'IA générative pour la recherche d'informations
- Stagiaires ayant validé SEC595 et souhaitent en savoir plus sur les LLM
- Professionnels qui veulent comprendre comment exploiter les LLM à des fins d'extraction d'information par des publics internes ou par des clients

Bilan

- Les stagiaires comprennent comment travailler avec les bases de données vectorielles et les exploiter.
- Les stagiaires savent mettre en œuvre en interne des solutions de type chatbot ou similaires.
- Les stagiaires savent construire des solutions d'IA et de LLM sans divulguer d'informations internes sensibles à des tiers ou à l'aide d'une API publique ou commerciale.
- Les stagiaires comprennent comment construire des solutions RAG contextuelles de pointe.
- Les stagiaires comprennent comment mettre en œuvre des solutions d'IA basées sur des agents liées à des LLM.

David Hoelzer
Auteur de la formation

Les directions de nombreuses organisations ont enjoint d'être à l'écoute des possibilités d'exploiter l'IA dans leurs activités. Beaucoup sont confrontées au même problème : le manque d'articulation claire quant à la vision de l'IA de l'entreprise.

Si SEC595™ vous enseigne tout ce qu'il faut savoir pour bâtir des solutions d'IA et d'apprentissage automatique de pointe pour aider à résoudre les problèmes de cybersécurité du monde réel, SEC495™ a un tout autre but. Or la plupart des équipes de gestion désireuses d'intégrer l'IA réagissent aux informations sur les grands modèles de langage (LLM), qui figurent en bonne place dans les médias grand public ces dernières années. Au cours de SEC495™, vous travaillerez avec votre instructeur à construire un système de génération augmentée de récupération (RAG), entièrement autohébergé et exploitant un LLM. Vous apprendrez en outre à mettre en œuvre des contrôles de sécurité pour défendre le modèle contre l'injection de prompts, ainsi que des contrôles de sensibilité des informations pour restreindre les réponses du LLM en fonction des droits de l'utilisateur.

Si vous devez bâtir une solution LLM pour répondre à des questions, extraire des informations d'une base documentaire ou réaliser des tâches similaires, cette formation vous rendra rapidement opérationnel.

Un mot de l'auteur

« La direction nous sollicite de plus en plus souvent pour valoriser l'IA dans l'entreprise. Comment y arriver ? À quoi cela ressemble-t-il ? S'il n'y a pas de réponse unique, SEC595™ en apporte de très claires dans le domaine de la surveillance et de la recherche de compromission, et SEC495™ vous inculque tout ce qu'il faut pour vous lancer dans la construction de solutions à base de LLM. Si les solutions dans SEC595™ sont extrêmement utiles et pointues, la formation SEC495, axée sur la construction de solutions RAG à base de LLM, est bien mieux appréhendée par les équipes de direction, qui voient et comprennent instantanément l'utilité de la solution.

Si nous nous focalisons sur la valorisation et la sécurisation des RAG à des fins de recherche documentaire, d'autres magnifiques extensions naturelles existent, comme l'identification de la conformité à des critères définis par des politiques, la création automatique de rapports, etc. Mieux encore, dans SEC495™, tout est réalisé avec des conteneurs sur site. Vous pouvez héberger ceux-ci dans le cloud, passer à grande échelle ou utiliser à la place des API commerciales, mais vous apprendrez à implémenter tous les éléments sans jamais envoyer d'informations sensibles à un tiers. Un gros atout ! »

— Dave Hoelzer

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC495**

MODES DE FORMATION DE SEC495

OnDemand

SEC497: **Practical Open-Source Intelligence (OSINT)™**

GOSI
Open-Source Intelligence
giac.org/gosi

6 jours	36 crédits CPE	+29 labos

Vous apprendrez à...

- Mener différents types d'enquêtes OSINT dans un cadre de sécurité opérationnelle
- Créer des comptes leurres
- Localiser des informations sur Internet, notamment quand elles sont supprimées et difficiles à trouver
- Localiser des individus en ligne et analyser leur présence en ligne
- Comprendre le dark web et y effectuer des recherches efficacement
- Rendre compte de l'infrastructure selon différents axes critiques – cyberdéfense, analyse de fusion et acquisition, tests d'intrusion...
- Utiliser des méthodes souvent révélatrices du propriétaire d'un site web et des autres sites qu'il possède ou exploite
- Comprendre les différents types de données compromises disponibles et leur utilisation à des fins offensives et défensives
- Collecter et utiliser efficacement les données des réseaux sociaux

Public visé :

- Enquêteurs OSINT
- Analystes en renseignement d'intérêt cyber (CTI)
- Services de renseignement
- Forces de l'ordre
- Experts en tests d'intrusion/membres de red team
- Cyberdéfenseurs
- Cabinets de recrutement
- Journalistes
- Enquêteurs
- Enquêteurs inforensiques
- Personnel des ressources humaines

Fonctions du référentiel NICE

- Data Analyst (OPM 422)
- Threat/Warning Analyst (OPM 141)
- All-Source Analyst (OPM 111)
- Target Network Analyst (OPM 132)
- All Source-Collection Manager (OPM 311)
- All Source-Collection Requirements Manager (OPM 312)
- Cyber Intel Planner (OPM 331)
- Cyber Ops Planner (OPM 332)

Matt Edmondson
Auteur de la formation

Apprendre à maîtriser le renseignement de sources ouvertes

SEC497™ est une formation complète sur le renseignement de sources ouvertes (OSINT) conçue par un professionnel riche de plus de 20 ans d'expérience. Elle vise à vous enseigner les compétences, outils et méthodes les plus importants dont vous aurez besoin pour développer ou affiner vos capacités à enquêter. SEC497™ fournit des informations exploitables aux stagiaires de tout l'écosystème OSINT, notamment les analystes du renseignement, les agents des forces de l'ordre, les analystes en renseignement d'intérêt cyber et les cyberdéfenseurs, les experts en tests d'intrusion, les enquêteurs et quiconque veut améliorer ses compétences de renseignement de sources ouvertes. Du néophyte au praticien chevronné, chacun y trouvera son compte.

SEC497™ s'intéresse aux techniques concrètes et utiles au quotidien. Pensée pour être accessible aux novices de l'OSINT, la formation apporte aux plus expérimentés des outils robustes et éprouvés à ajouter à leur arsenal pour résoudre les problèmes dans leur environnement réel. Elle met l'accent sur la compréhension du fonctionnement des systèmes pour éclairer la prise de décision et comprend des exercices pratiques issus de scénarios réels des secteurs public et privé. Nous ne nous contentons pas de discuter de la recherche de pointe et de détection des valeurs aberrantes : nous pratiquons ! Plongez-vous dans le programme de la formation pour connaître les sujets couverts.

Bilan

Avec cette formation, votre organisation va :

- Améliorer sa veille stratégique grâce aux techniques de l'OSINT
- Améliorer sa gestion des risques par l'identification des vulnérabilités
- Renforcer sa réponse à incident avec la collecte rapide d'informations
- Identifier et atténuer les menaces grâce aux données publiques
- Simplifier les processus de collecte et d'analyse des données pour une meilleure efficacité opérationnelle

Programme

SECTION 1 : Fondamentaux de l'OSINT et de l'OPSEC

SECTION 2 : Compétences essentielles de l'OSINT

SECTION 3 : Enquêter sur des individus

SECTION 4 : Enquêter sur des sites et infrastructures web

SECTION 5 : Automatisation, dark web, et grands ensembles de données

SECTION 6 : Projet final : Événement CTF

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC497**

MODES DE FORMATION DE SEC497

In-Person **Live Online** **OnDemand**

SEC501: **Advanced Security Essentials – Enterprise Defender™**

GCED
Enterprise Defender
giac.org/gced

6	38	25
jours	crédits CPE	labos

Vous apprendrez à...

- Identifier les menaces de sécurité réseau visant l'infrastructure, et concevoir des réseaux sécurisés qui minimisent l'impact des attaques grâce à l'analyse des configurations des équipements réseau et à la simulation d'attaques
- Décoder et analyser des paquets en utilisant divers outils pour identifier des anomalies et améliorer les défenses du réseau
- Comprendre les méthodes de l'adversaire pour compromettre les systèmes, et répondre aux attaques selon le processus de gestion des incidents en six étapes
- Effectuer des tests d'intrusion contre une entreprise afin de déterminer ses vulnérabilités et ses points de compromission
- Comprendre et utiliser des techniques de défense active
- Collecter des artefacts forensiques révélant l'activité système antérieure dans ses détails, extraire par carving des données supprimées de périphériques de stockage, analyser les chronologies super-timeline, et mener des analyses d'inforensique réseau
- Utiliser divers outils pour identifier et analyser les logiciels malveillants dans toute l'entreprise

Public visé :

- Profils techniques chevronnés en voie de reconversion ou de montée en compétences en cybersécurité
- Personnels du CERT/CSIRT qui ont besoin d'une large expérience transversale de nombreuses sous-disciplines de la cybersécurité
- Professionnels de l'InfoSec
- Professionnels de l'informatique
- Ingénieurs logiciels
- Analystes et ingénieurs des centres opérationnels
- Professionnels de la sécurité touche-à-tout et multicasquette

Fonctions du référentiel NICE

- Network Operations Specialist (OPM 441)
- Cyber Instructor (OPM 712)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Infrastructure Support Specialist (OPM 521)

Ross Bergman
Auteur de la formation

La reconversion et la montée en compétences cyber sont des sujets sensibles dans les entreprises, petites ou grandes. Les profils techniques doivent posséder un large éventail de connaissances et certaines compétences élémentaires dans plusieurs domaines. Tous les membres de l'équipe sécurité, de plus en plus souvent élargie à l'IT et au DevOps, doivent se tenir prêts à garantir la résilience aux attaques de n'importe quel système, logiciel ou infrastructure codé, construit et déployé. Ils doivent disposer des connaissances nécessaires pour repérer l'ennemi caché parmi eux, ce qui demande de maîtriser les tactiques, techniques et procédures de l'adversaire et d'être à l'aise avec les outils de terrain qui révèlent ces activités au sein de l'entreprise. L'intrus doit être contenu dès sa découverte – contrôler son déplacement latéral et restreindre l'étendue de son infiltration réduit au maximum les risques de divulgation, d'altération et de destruction des données critiques de l'entreprise. Pour éradiquer l'indésirable, tout le monde doit s'activer à remédier les systèmes compromis et à récupérer les actifs perdus. Prévenir. Détecter. Répondre.

Bilan

- Reconversion et montée en compétences des profils techniques pour qu'ils contribuent substantiellement à la cybersécurité de l'entreprise.
- Amélioration de l'efficacité, des performances et de la réussite des initiatives de cybersécurité.
- Des réseaux défendables pour réduire l'impact des attaques.
- Identification des points d'exposition pour hiérarchiser et corriger les vulnérabilités, et donc améliorer la sécurité globale de l'organisation.
- Détection de l'attaquant sur site et dans le cloud grâce à la surveillance et à l'analyse de l'activité réseau, et à la corrélation de l'activité dans les systèmes.
- Compréhension des méthodes d'attaque contre les systèmes, les périphériques réseau et les applications web.

Programme

SECTION 1 : Architecture réseau défendable

SECTION 2 : Tests d'intrusion

SECTION 3 : Bases des opérations de sécurité

SECTION 4 : Inforensique et réponse aux incidents (DFIR)

SECTION 5 : Analyse de logiciels malveillants

SECTION 6 : Projet final de défense de l'entreprise

« C'est la meilleure formation technique que j'ai jamais suivie. SEC501 m'a fait connaître de nombreux outils et concepts précieux, et la solide introduction à ces outils m'assure de pouvoir continuer à me perfectionner en solo. »

— Curt Smith, **Hildago Medical Services**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC501**

MODES DE FORMATION DE SEC501

In-Person **Live Online** **OnDemand**

SEC503: **Network Monitoring and Threat Detection In-Depth™**

GCIA Intrusion Analyst
giac.org/gcia
CyberLive
DoD 8140*

6 jours	46 crédits CPE	+37 labos

Vous apprendrez à...

- Configurer et exécuter Snort et Suricata
- Créer et écrire des règles efficaces et performantes pour Snort, Suricata et FirePOWER
- Configurer et exécuter l'IDS open source Zeek pour fournir un cadre d'analyse du trafic hybride
- Créer des scripts automatiques de corrélation des menaces avec Zeek
- Comprendre les composants des couches TCP/IP pour identifier le trafic normal et anormal afin d'y repérer les menaces
- Utiliser les outils d'analyse de trafic pour repérer les signaux de compromission ou de menace active
- Mener des analyses inforensiques réseau pour repérer les TTP dans le trafic et y débusquer des menaces actives
- Utiliser la méthode de carving pour extraire du trafic réseau des fichiers et autres types de contenus afin de reconstruire les événements
- Créer des filtres BPF pour examiner de près un caractère particulier du trafic
- Créer des paquets avec Scapy
- Utiliser des outils NetFlow/IPFIX pour trouver des anomalies de comportement et des menaces sur le réseau
- Utiliser votre connaissance de l'architecture et du matériel réseau pour personnaliser l'emplacement des capteurs de surveillance du réseau et analyser le trafic

Public visé :

- Analystes de surveillance réseau, système, sécurité et de centre des opérations de sécurité
- Ingénieurs/administrateurs réseau
- Responsables sécurité opérationnelle

Fonctions du référentiel NICE

- Cyber Defense Analyst (OPM 511)

David Hoelzer
Auteur de la formation

* DoD 8140 APPROVED
sans.org/8140

Détecter, analyser, protéger : maîtriser la détection proactive des menaces réseau

SEC503 est la formation la plus importante de toute votre carrière en sécurité des informations. Les anciens stagiaires la décrivent comme la plus difficile jamais entreprise, mais aussi la plus gratifiante. Vous voulez détecter efficacement les activités zero-day qui ont lieu sur votre réseau avant qu'elles ne soient publiques ? Cette formation s'adresse à vous. SEC503 ne concerne pas ceux qui cherchent à comprendre les alertes issues d'un outil de surveillance du réseau clé en main. Elle vise plutôt ceux qui veulent acquérir une compréhension approfondie de ce qui se passe en ce moment sur leur réseau, et qui soupçonnent qu'il s'y passe des choses graves qu'aucun de leurs outils ne détecte.

La formation SEC503 se distingue de toutes les autres par son approche pédagogique de la surveillance réseau et de l'inforensique réseau qui, partant du particulier pour aller vers le général, se traduit naturellement par un gain d'efficacité dans la recherche des compromissions. Au lieu de s'intéresser à un outil pour vous montrer comment vous en servir selon la situation, elle vous apprend le fonctionnement des protocoles TCP/IP et leur logique. Après deux parties initiales sur les « paquets langue étrangère », nous abordons les protocoles courants de la couche application et une approche générale pour étudier et comprendre les nouveaux protocoles. Pendant tous les échanges, l'application directe des connaissances sert à identifier les menaces connues comme zero-day.

Bilan

- Vous évitez à votre organisation de faire les gros titres.
- Vous augmentez la détection dans les environnements réseau traditionnels, hybrides et cloud.
- Vous augmentez l'efficacité de la modélisation des menaces pour les activités réseau.
- Vous réduisez la durée de présence d'un attaquant.

Programme

SECTION 1 : Surveillance et analyse du réseau : Partie I
SECTION 2 : Surveillance et analyse du réseau : Partie II
SECTION 3 : Détection des menaces selon la signature et réponse
SECTION 4 : Construire des systèmes de détection des menaces zero-day
SECTION 5 : Détection, inforensique et analytique des menaces à grande échelle
SECTION 6 : Projet final de surveillance avancée du réseau et de détection des menaces

« J'avais une grande expérience en analyse post-incident sur les hôtes, mais une connaissance limitée de l'analyse et de l'inforensique réseau ; j'ai pu combler nombre des lacunes de mon parcours avec SEC503. »

— Jared H., **militaire**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC503**

MODES DE FORMATION DE SEC503

In-Person **Live Online** **OnDemand**

SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring™ MISE À JOUR MAJEURE

GMON Continuous Monitoring
giac.org/gmon
DoD 8140*

6 jours | 46 crédits CPE | 23 labos

Vous apprendrez à...

- Mener des évaluations exhaustives de l'état actuel afin de concevoir des défenses modernes et d'en définir les priorités
- Appliquer des référentiels de défense comme MITRE ATT&CK et le zero trust
- Rechercher les compromissions potentielles à l'aide de techniques et d'outils avancés
- Procurer une visibilité dans toute l'infrastructure décentralisée moderne et hybride
- Explorer le paysage moderne du système de noms de domaine et du chiffrement TLS pour allier les considérations de protection, de détection et de confidentialité
- Appréhender la pile et les outils de sécurité du cloud – plateforme de protection d'applications natives cloud, gestion de la posture de sécurité cloud, gestion des droits d'utilisation sur l'infrastructure cloud, et plateforme de protection de la charge de travail du cloud pour une solide protection du cloud
- Mettre en œuvre la sécurité des terminaux par le contrôle d'application et une plateforme de protection EPP
- Défendre les applications d'IA et des grands modèles de langage et sécuriser la supply chain IA/logicielle

Public visé :

- Architectes sécurité
- Ingénieurs sécurité séniors
- Responsables sécurité technique
- Directeurs, ingénieurs et analystes des centres des opérations de sécurité
- Analystes en défense des réseaux
- Quiconque impliqué dans l'implémentation des diagnostics et atténuations en continu, ou la supervision continue de la sécurité ou de la sécurité réseau

Fonctions du référentiel NICE

- Security Architect (OPM 652)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Infrastructure Support Specialist (OPM 521)

Eric Conrad
Auteur de la formation

Seth Misenar
Auteur de la formation

*DoD 8140 APPROVED
sans.org/8140

Surveiller, détecter, protéger : maîtriser la détection de menaces avancées pour le cloud, le réseau et les terminaux

Dans un panorama de menaces en constante évolution, les mesures de cybersécurité classiques ne suffisent plus. Cette formation avancée relève le défi et équipe les stagiaires de compétences pointues en ingénierie de cybersécurité et en détection des menaces avancées dans les environnements cloud, réseau et des terminaux. Avec ses 18 labos pratiques, un projet final sous forme de projet, et des défis gamifiés d'entraînement intensif, elle vous plonge dans des scénarios de production. Maîtrisez la détection et la réponse réseau (NDR) et terminaux (EDR) et le référentiel MITRE ATT&CK pour bâtir un SOC robuste aux défenses fondées sur les menaces. Grâce à cette formation complète, développez votre expertise et gardez une longueur d'avance sur les attaquants.

Bilan

Avec cette formation, votre organisation va :

- Impulser des stratégies de détection et de protection efficaces pour le cloud, le réseau et les terminaux
- Concevoir une architecture de sécurité défendable et des opérations adaptées à l'entreprise hybride moderne
- Améliorer substantiellement les capacités opérationnelles sécuritaires de votre organisation
- Identifier les lacunes de protection et de détection dans l'ensemble de l'infrastructure hybride
- Maximiser les capacités de l'infrastructure et des actifs actuels
- Interpréter les données pour détecter rapidement les intrusions potentielles ou les actions non autorisées

Programme

SECTION 1 : Principes de la défense fondée sur les menaces : référentiels, recherche, et évaluation de l'état actuel

SECTION 2 : Cloud, périphérie et réseau : visibilité et protection

SECTION 3 : Recherche de compromissions avec les outils de détection et de réponse réseau (NDR)

SECTION 4 : Sécurité de l'entreprise hybride : détection et protection des utilisateurs et des terminaux

SECTION 5 : Défense des applications d'IA générative, automatisation, protection de la chaîne logicielle et SOC

SECTION 6 : Projet final : concevoir, détecter, défendre

« Les séances en labo apportent une expérience pratique indispensable, qui vient consolider les acquis théoriques. »

— Olivia M., **BAH**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC511**

MODES DE FORMATION DE SEC511

In-Person | Live Online | OnDemand

SEC530: **Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise™**

GDSA
Defensible Security Architecture | DoD 8140*
giac.org/gdsa

6 jours	36 crédits CPE	19 labos

Vous apprendrez à...

- Analyser une architecture de sécurité pour mettre au jour les failles
- Découvrir les données, les applications, les actifs et les services, et évaluer l'état de conformité
- Implémenter des technologies aux fonctions de prévention, de détection et de réponse améliorées
- Comprendre les solutions de sécurité, leurs lacunes, mais aussi leurs réglages fins et leur exploitation
- Comprendre les conséquences des stratégies de chiffrement à tout va
- Appliquer les principes appris en formation pour concevoir une architecture de sécurité défendable
- Déterminer les besoins précis en supervision de la sécurité pour des organisations de toutes tailles
- Valoriser les investissements en architecture de sécurité en reconfigurant les technologies
- Déterminer les capacités requises pour prendre en charge la supervision continue des principaux contrôles de sécurité critiques
- Configurer la journalisation (log) et la supervision appropriées pour soutenir le centre des opérations de sécurité et le programme de supervision continue

Public visé :

- Architectes sécurité
- Ingénieurs réseau
- Architectes réseau
- Analystes sécurité
- Ingénieurs sécurité séniors
- Administrateurs système
- Responsables sécurité technique
- Analystes défense réseau CND
- Spécialistes en supervision de la sécurité
- Spécialistes en investigation numérique

Fonctions du référentiel NICE

- Enterprise Architect (OPM 651)
- Security Architect (OPM 652)

Ismael Valenzuela
Auteur de la formation

* DoD 8140 APPROVED
sans.org/8140

Sécurité dès la conception : le zero trust pour les réseaux hybrides modernes

Cette formation vous aide à bâtir et à maintenir une architecture de sécurité vraiment défendable par la mise en œuvre des principes, piliers et fonctionnalités du zero trust et avec la volonté de valoriser les investissements et l'infrastructure actuels. Vous apprendrez à évaluer, reconfigurer et valider l'existant afin d'améliorer significativement les capacités de prévention, de détection et de réponse de votre organisation, d'augmenter sa visibilité, de réduire sa surface d'attaque et même de trouver des moyens innovants d'anticiper les attaques. La formation explorera aussi en profondeur certaines technologies récentes et leurs capacités, leurs forces et leurs faiblesses. Vous en retirerez de précieuses recommandations et suggestions pour élaborer, dans le cadre de votre démarche zero trust, une infrastructure de sécurité robuste, couche par couche, efficace à travers les environnements hybrides.

Bilan

- Vous savez identifier et comprendre les lacunes des solutions de sécurité.
- Vous concevez et implémentez des stratégies zero trust qui valorisent vos technologies et investissements.
- Vous optimisez les investissements en architecture de sécurité en reconfigurant vos technologies.
- Vous combinez des couches de défense qui augmentent la durée de la protection et la probabilité de la détection.
- Vous améliorez les capacités de prévention, de détection et de réponse.
- Vous réduisez la surface d'attaque.

Programme

SECTION 1 : Ingénierie et architecture de sécurité défendable : vers le zero trust

SECTION 2 : Ingénierie et architecture de sécurité réseau

SECTION 3 : Architecture de sécurité applicative centrée sur le réseau

SECTION 4 : Architecture de sécurité applicative centrée sur les données

SECTION 5 : Architecture zero trust : traiter les adversaires déjà présents dans nos réseaux

SECTION 6 : Défi pratique de sécurisation du drapeau

« Cette formation montre comment améliorer la posture de sécurité globale d'une organisation. Elle aide à faire le lien entre les différents domaines au sein de l'infrastructure de sécurité. »

— Farruk Ali, **UPS**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC530**

MODES DE FORMATION DE SEC530

In-Person **Live Online** **OnDemand**

ZOOM NOUVELLE FORMATION

SEC547: **Defending Product Supply Chains™**

3 jours	18 crédits CPE	13 labos

Vous apprendrez à...

- Créer des nomenclatures logicielles à partir du code source
- Créer des pipelines d'attestation
- Comprendre la publication des vulnérabilités
- Valider les composants vulnérables
- Repérer les composants contrefaits
- Construire un programme de sécurité de la supply chain
- Comprendre comment les assaillants étrangers manipulent les supply chains
- Utiliser des outils open source de sécurité de la supply chain
- Collaborer avec les développeurs pour insérer la sécurité dans votre processus de développement de produits
- Réagir plus efficacement aux menaces sur la supply chain
- Utiliser des techniques efficaces pour répondre à la prochaine grande vulnérabilité sur la supply chain

Public visé :

- Gestionnaires de risques de la supply chain
- Équipes de sécurité produit et de réponse aux incidents de sécurité produit (PSIRT)
- Propriétaires d'actifs et opérateurs chargés de la sécurité
- Analystes sécurité et chargés de réponse aux incidents
- Responsables de la sécurité produit

Fonctions du référentiel NICE

- Incident Response (OPM 531)
- Infrastructure Support (OPM 521)
- Cyber Operations Planning (OPM 332)

Tony Turner
Auteur de la formation

Des achats au produit : sécurisez votre supply chain

Le panorama de la menace a changé. Il ne suffit plus d'ériger un périmètre robuste pour tenir les adversaires à distance. Les attaques sur la supply chain sont un des nombreux moyens efficaces de contourner les contrôles classiques du périmètre. Lors de ces attaques difficiles à repérer, les organisations laissent à leur insu l'adversaire entrer par le biais de technologies « de confiance », ce qui entraîne une autocompromission. SEC547: Defending Product Supply Chains™ apprend à réduire au maximum le risque d'attaque sur la supply chain par le biais de stratégies et tactiques approfondies de gestion du risque de la chaîne d'approvisionnement. La formation couvre le panorama des menaces. Elle apporte des compétences critiques aux défenseurs au cours de 13 labos sur mesure, et illustre par des exemples réels le fonctionnement de ces attaques et les moyens d'empêcher que cela vous arrive. À l'issue de cette formation, vous disposerez des bonnes pratiques pour injecter sécurité et assurance dans vos achats technologiques.

Bilan

- Vous augmentez la résilience de votre organisation face aux menaces d'attaque.
- Vous réduisez le coût de votre programme de sécurité en atténuant les risques.
- Vous menez des évaluations de vos fournisseurs et de la supply chain de vos produits.
- Vous diminuez l'impact des attaques sur la supply chain au sein de votre organisation.
- Vous hiérarchisez les risques au sein de votre programme d'approvisionnement.
- Vous repérez les fuites de secrets commerciaux et industriels.
- Vous identifiez les risques de présence étrangère dans votre supply chain.
- Vous coordonnez les échanges avec les parties prenantes sur la sécurité de la supply chain.

Programme

SECTION 1 : Fournisseurs et produits
SECTION 2 : Nomenclature matérielle et logicielle
SECTION 3 : Transparence logicielle et réponse

« Cette formation m'a aidée à identifier des éléments clés, des procédures, des outils pertinents et des conseils utiles pour élaborer une méthode en phase avec la stratégie, systématique et efficace pour traiter les points noirs dans le processus de la supply chain. »

— Liana Torres, **Savannah River Nuclear Solutions**

« J'ai adoré cette formation. Elle regorge d'informations utiles que je prévois d'incorporer dans mes projets internes ! »

— Rossano Ferraris, **Accenture**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC547**

MODES DE FORMATION DE SEC547

Live Online **OnDemand**

SEC555: **Detection Engineering and SIEM Analytics™**

GCDA
Detection Analyst
giac.org/gcda

5 jours	30 crédits CPE	18 labos

Vous apprendrez à...

- Créer un labo de détection
- Créer des règles de détection d'adversaire
- Optimiser votre architecture SIEM
- Utiliser des outils pour mener une émulation d'attaque afin d'analyser les journaux d'activité y afférents
- Utiliser les données des journaux pour déterminer l'efficacité des contrôles de sécurité
- Simplifier le traitement et le filtrage des gros volumes de données engendrés par les différents appareils
- Exploiter les outils SIEM cloud et sur site et les sources de journalisation
- Obtenir des informations de MITRE ATT&CK et acquérir la capacité à relier les détections à des tactiques et techniques particulières
- Enregistrer et surveiller les capacités de détection dans de nombreuses sources de données
- Comprendre comment l'optimisation SOAR peut améliorer considérablement l'ingénierie de détection et le temps de réponse
- Établir des bases de référence, identifier les tendances et découvrir les valeurs aberrantes afin de déceler une activité hostile

Public visé :

- Spécialiste en détection des intrusions
- Analyste en détection
- Analyste sécurité
- Ingénieur sécurité
- Spécialiste en recherche des menaces
- Chargé de réponse aux incidents
- Architecte sécurité
- Spécialiste en supervision de la sécurité
- Spécialiste en investigation numérique
- Expert en tests d'intrusion

Fonctions du référentiel NICE

- Data Analyst (OPM 422)
- Cybersecurity Defender (OPM 511)
- Incident Responder (OPM 531)
- Threat Analyst (OPM 141)

Nick Mitropoulos
Auteur de la formation

L'ingénierie de détection et l'analyse SIEM au service de l'art de la cyberdéfense

Dans un monde où les cybermenaces se sophistiquent toujours plus, les organisations ont besoin de défenseurs qualifiés qui peuvent garder une longueur d'avance. Cette formation ouvre la voie à la maîtrise de l'ingénierie de détection – l'art de créer des défenses proactives – et le SIEM, le pilier de la détection des menaces et de la réponse modernes. Que vous soyez nouvel analyste en détection ou analyste sécurité qui monte en compétences, vous acquerrez l'expertise pratique pour déceler les attaques et enquêter dessus. SEC555™ apporte aux stagiaires la formation, les méthodes et des processus qui permettent d'améliorer les solutions de journalisation et promeut la création de règles de détection saines dans l'optique d'une surveillance proactive.

Bilan

- Réduction du risque commercial par l'identification et l'atténuation des menaces en quasi-temps réel
- Mise en place d'un processus valide d'évaluation des fournisseurs pour guider le choix de partenaires de sécurité appropriés
- Hiérarchisation des menaces selon l'impact sur l'entreprise et la criticité des actifs
- Compilation d'une base de données d'actifs pour aider à surveiller les actifs critiques
- Appréciation du lien entre l'ingénierie de détection et les objectifs plus larges de l'organisation, comme la conformité réglementaire et l'efficacité opérationnelle
- Meilleure connaissance de l'importance de la précision de la détection pour éviter l'accoutumance aux alertes et les inefficacités opérationnelles
- Exploration du soutien de l'ingénierie de détection à la collaboration transversale avec des équipes comme l'IT, la sécurité et la conformité
- Évaluation et gestion efficace des risques en exploitant les données de détection pour éclairer les décisions stratégiques
- Adoption d'une stratégie favorable à l'évolutivité du système

Programme

SECTION 1 : Ingénierie de détection et architecture SIEM

SECTION 2 : Analyse du réseau et des points de terminaison

SECTION 3 : Découverte des actifs, référentiels et UEBA

SECTION 4 : Journalisation et surveillance du cloud

SECTION 5 : Alerte et détection pour les pipelines d'ingénierie

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC555**

MODES DE FORMATION DE SEC555

In-Person **Live Online**

SEC573: **Automating Information Security with Python™**

GPYC
Python Coder
giac.org/gpyc

6	36	+128
jours	crédits CPE	labos

Vous apprendrez à...

- Utiliser Python pour réaliser rapidement et efficacement des tâches de routine
- Automatiser l'analyse de journaux et de paquets à l'aide d'opérations sur les fichiers, d'expressions régulières et de modules d'analyse pour débusquer l'ennemi
- Développer des outils d'inforensique pour extraire données binaires et nouveaux artefacts
- Lire les données dans les bases de données et dans le registre Windows
- Interagir avec les sites web pour collecter des renseignements
- Développer des applications client-serveur UDP et TCP
- Automatiser les processus système et traiter leur sortie

Public visé :

- Professionnels de la sécurité que l'automatisation de tâches de routine laisserait se concentrer sur l'important
- Analystes inforensiques las d'attendre un hypothétique outil commercial pour l'analyse des artefacts
- Défenseurs du réseau qui passent au crible d'énormes volumes de journaux et de paquets pour repérer les intrus dans leurs réseaux
- Chargés de tests d'intrusion prêts à passer de la simple utilisation de scripts tout faits aux opérations informatiques offensives professionnelles
- Professionnels de la sécurité qui veulent passer de simple consommateur d'outils de sécurité à fournisseur de solutions de sécurité

Fonctions du référentiel NICE

- Secure Software Assessor (OPM 622)
- Research & Development Specialist (OPM 661)
- Data Analyst (OPM 422)
- Cyber Defense Analyst (OPM 511)
- Cyber Operator (OPM 321)
- Law Enforcement/CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

Mark Baggett
Auteur de la formation

Polyvalent, reproductible et efficace, Python automatise les tâches de sécurité

Comme les défis ne cessent d'évoluer en sécurité, la demande de profils aptes à comprendre un problème technologique et à développer rapidement une solution s'intensifie. S'il vous faut attendre qu'un tiers développe un outil pour récupérer un artefact forensique, ou pour corriger ou exploiter une nouvelle vulnérabilité, vous resterez à la traîne. Les employeurs qui ont la sécurité des informations à cœur n'ont plus le choix : ils doivent pouvoir développer rapidement leurs outils en interne. Cette formation vous apprend à élaborer des solutions pour que votre organisation reste dans la course face à l'adversaire. SEC573™ est une formation immersive, en autonomie et pratique, aux nombreux labos. Elle commence par les bases nécessaires pour les novices du code, puis elle présente aux stagiaires des défis inforensiques défensifs et offensifs, inspirés du terrain. Vous développerez un programme injecteur pour une opération offensive ; vous apprendrez à fouiller vos journaux pour y déceler les dernières attaques ; vous programmerez du code pour extraire des artefacts numériques de mémoires, de disques durs et de paquets ; vous automatiserez l'interaction avec l'API d'un site web ; et vous écrirez un analyseur personnalisé de paquets. Les labos ludiques et passionnants vous apprendront à développer des outils et à acquérir des compétences essentielles, qui feront de vous le fleuron de votre équipe de sécurité des informations.

Bilan

Avec cette formation, votre organisation va :

- Automatiser les processus système et traiter les entrées avec célérité et efficacité
- Créer des programmes qui améliorent l'efficacité et la productivité
- Développer des outils pour fournir les défenses vitales dont nos organisations ont besoin

Programme

SECTION 1 : Ateliers essentiels et défis pyWar
SECTION 2 : Ateliers essentiels et ENCORE des défis pyWar
SECTION 3 : Python en défense
SECTION 4 : Python pour l'analyse post-incident
SECTION 5 : Python pour les opérations offensives
SECTION 6 : Défi CTF

« Python est un outil indispensable dans le monde de l'InfoSec, et SEC573 m'a permis de m'outiller. »

— Ben Weber, **Raymond James**

« Très bien agencé. Cela fait des années que j'ai peur d'apprendre à coder. En l'équivalent de quelques jours d'étude, j'ai été rassuré. »

— Blake Thompson, **Merrick Bank**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC573**

MODES DE FORMATION DE SEC573

In-Person **Live Online** **OnDemand**

SEC587: **Advanced Open-Source Intelligence (OSINT) Gathering and Analysis™** MISE À JOUR MAJEURE

6 jours	36 crédits CPE	20 labos

Vous apprendrez à...

- Collecter et analyser les données publiques pour les transformer en renseignements exploitables à l'aide d'outils et de techniques avancées d'OSINT
- Rationaliser le processus d'OSINT à l'aide de systèmes automatisés et augmenter ainsi l'efficacité et l'exactitude de la collecte de renseignements
- Identifier et atténuer les menaces grâce à votre maîtrise de l'OSINT pour prévoir et prévenir d'éventuelles vulnérabilités
- Appréhender les aspects éthiques et légaux de la collecte de renseignements pour assurer le respect des obligations et des règles
- Tirer un avantage concurrentiel de l'OSINT en l'appliquant à la surveillance et à l'analyse des tendances du marché et du secteur en vue de nourrir la stratégie commerciale
- Améliorer les processus décisionnels par des éclairages factuels et en temps réel issus de différentes sources accessibles, ouvertes et publiques
- Mettre en œuvre des solutions technologiques pour gérer et analyser efficacement de grands jeux de données issus de sources disparates et prendre des décisions avisées

Public visé :

- Analystes du renseignement en sources ouvertes et autres sources
- Enquêteurs judiciaires
- Enquêteurs militaires
- Enquêteurs privés
- Enquêteurs d'assurance
- Analystes du renseignement
- Analystes géopolitiques
- Journalistes
- Chercheurs
- Ingénieurs sociaux
- Chargés de recherche dans les secteurs de l'information et de la politique
- Chargés de réponse aux cyberincidents
- Analystes inforensiques DFIR
- Spécialistes du renseignement d'intérêt cyber (CTI)

Matt Edmondson
Auteur de la formation

Au-delà de l'essentiel : techniques avancées d'OSINT

La plupart des grandes enquêtes de l'ère numérique se nourrissent du renseignement de sources ouvertes (OSINT) : il était urgent d'organiser une formation avancée sur ce thème. À chaque nouvelle enquête, la collecte, l'exploitation et l'analyse des données OSINT se compliquent. Dans le monde entier, les professionnels du renseignement de sources ouvertes ont besoin de monter en puissance, et ils requièrent les moyens et les méthodes pour valider la fiabilité de leur analyse et en rendre compte dans des rapports solides et impartiaux. Dans la formation SEC587™, vous apprendrez les techniques avancées de collecte et d'analyse de renseignement de sources ouvertes. Vous développerez aussi votre compréhension des langages de programmation courants, tels que JSON et Python, et de leurs usages. Vous vous intéresserez également au darknet et aux aspects financiers (cryptomonnaie) ainsi qu'à la désinformation et à l'analyse d'images et de vidéos en sources ouvertes. Cette formation avancée intensive apportera aux enquêteurs aguerris de nouvelles techniques et méthodologies, et aux analystes novices cette profondeur supplémentaire pour trouver, collecter et analyser des sources de données du monde entier.

Bilan

- Vous améliorez la prise de décision par des éclairages factuels issus de données publiques.
- Vous identifiez en amont les risques à l'aide de techniques avancées d'OSINT.
- Vous gagnez en efficacité par la collecte automatisée de renseignements.
- Vous gardez une longueur d'avance sur la concurrence en surveillant les tendances du secteur et du marché.
- Vous assurez la conformité légale et éthique de la collecte du renseignement.

Programme

SECTION 1 : Désinformation, analyse du renseignement, renseignement de sources ouvertes russes et chinoises

SECTION 2 : Python pour le renseignement de sources ouvertes (OSINT)

SECTION 3 : Analyse de vidéos, d'images et de sons ; IA et OSINT ; énumération avancée et gaming

SECTION 4 : Leurres « sock puppets », sécurité des opérations, darknet, cryptomonnaies, et le monde du sans-fil

SECTION 5 : Surveillance automatisée, pistage de véhicules, et fichiers protégés par mot de passe

SECTION 6 : Projet final

« Couvrir de nombreux aspects de l'OSINT est vraiment utile pour bien ancrer les fondamentaux et comprendre les différentes applications des compétences en investigation des sources ouvertes. »

— Dan Black

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC587**

MODES DE FORMATION DE SEC587

In-Person **Live Online** **OnDemand**

SEC595: **Applied Data Science and AI/Machine Learning for Cybersecurity Professionals™**

GMLE
Machine Learning Engineer
giac.org/gmle

6 jours	36 crédits CPE	30 labos

Vous apprendrez à...

- Appliquer des modèles statistiques à des problèmes réels avec pertinence
- Créer des visualisations de vos données
- Exploiter les méthodes mathématiques pour rechercher d'éventuelles compromissions sur votre réseau
- Convertir les données en votre possession en représentations auxquelles vous pourrez appliquer des techniques d'IA et d'apprentissage automatique
- Comprendre et appliquer des méthodes d'apprentissage et de classification non supervisés
- Construire des réseaux neuronaux d'apprentissage profond
- Construire et comprendre les réseaux neuronaux convolutifs
- Comprendre comment construire des données synthétiques fidèles
- Comprendre et construire des algorithmes génétiques de recherche
- Comprendre les fondamentaux du déploiement conteneurisé

Public visé :

- Professionnels de l'InfoSec qui veulent comprendre l'apprentissage automatique
- Professionnels qui veulent appliquer les principes de la science des données à des problèmes concrets
- Quiconque s'est intéressé aux fondamentaux sans réussir à présenter son problème de manière à le traiter par apprentissage automatique
- Membres de centres des opérations de sécurité (SOC) et de blue team qui veulent identifier les anomalies et personnaliser la recherche de compromission

Fonctions du référentiel NICE

- Data Analyst (OPM 422)

David Hoelzer
Auteur de la formation

Mobiliser la science des données et l'IA au service de solutions avancées de recherche de compromission

Intensive et pratique, la formation SEC595™ pose les bases de la science des données, des statistiques, des probabilités, de l'apprentissage automatique et de l'IA. Elle s'articule autour de brèves discussions et de labos pratiques rigoureux, au cours desquels les stagiaires acquièrent une compréhension intuitive et pertinente des concepts, des liens qu'ils entretiennent et de leur utilisation pour résoudre des problèmes de terrain. La logique est la même qu'en apprentissage, l'objectif étant de vous faire passer de débutant à vétéran de l'IA et des domaines voisins. Si vous voulez exploiter ces techniques d'IA, mais que vous ne connaissez encore rien à la science des données ou à l'apprentissage automatique, cette formation est faite pour vous !

Bilan

- Vous créez des tableaux de bord de visualisation.
- Vous résolvez des problèmes à l'aide de réseaux neuronaux.
- Vous améliorez l'efficacité et les performances des initiatives de cybersécurité et en assurez le succès.
- Vous construisez des solutions d'apprentissage automatique adaptées aux besoins de votre organisation.
- Vous vous préparez à la certification GMLE.

Programme

SECTION 1 : Acquisition, nettoyage et manipulation de données
SECTION 2 : Exploration des données et statistiques
SECTION 3 : Les bases de l'apprentissage automatique : arbres, forêts et k-moyennes
SECTION 4 : Les bases de l'apprentissage automatique : apprentissage profond
SECTION 5 : Les bases de l'apprentissage automatique : auto-encodeurs
SECTION 6 : Les bases de l'apprentissage automatique : modèles fonctionnels et déploiement

« L'IA et l'apprentissage automatique appliqués à la cybersécurité sont mal compris et leur image est souvent faussée. Cette formation offre un équilibre entre le bagage nécessaire à un responsable pour développer sa compréhension de ces technologies et l'expérience pratique. »

— Thomas L., **militaire**

« J'apprécie vraiment que cette formation parte de l'expérience plutôt que d'un manuel. Les anecdotes illustrant l'histoire de certaines notions m'ont vraiment aidé à assembler les pièces du puzzle. »

— Brian Morris, **Ville d'Austin**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC595**

MODES DE FORMATION DE SEC595

In-Person **Live Online** **OnDemand**

ZOOM NOUVELLE FORMATION

SEC673: **Advanced Information Security Automation with Python™**

6 jours	36 crédits CPE	27 labos

Vous apprendrez à...

- Rendre vos packages installables avec PIP (Package Installer for Python) pour faciliter leur distribution et leur mise à jour
- Établir une structure de données adaptée à votre application pour accélérer son développement
- Utiliser des fonctionnalités avancées comme les décorateurs, les générateurs et les gestionnaires de contexte afin de simplifier le code
- Accélérer l'exécution de programmes grâce au multithread et au multitâche
- Éliminer les erreurs en cascade par l'implémentation de tests unitaires de sorte que les changements minimes ne deviennent pas d'énormes erreurs
- Créer et gérer des journaux adéquats dans les applications Python afin de détecter ce qui fonctionne pour vous, mais crée des erreurs pour les autres
- Mettre en œuvre l'automatisation et l'interaction applicatives pour pouvoir vous consacrer à des tâches plus importantes

Public visé :

- Professionnels de la sécurité qui savent coder en Python et sont prêts à passer au niveau supérieur
- Développeurs d'outils qui veulent savoir publier des packages Python installables et faciles à utiliser
- Défenseurs de réseau souhaitant apprendre à étendre la fonctionnalité des packages Python courants afin de créer de nouvelles capacités de détection
- Professionnels de la sécurité qui ont besoin d'accélérer leurs outils par l'ajout de capacités multithread et multitâche

Mark Baggett
Auteur de la formation

Évolutive, fiable, optimisée : automatisation avancée de la sécurité avec Python

Quand un problème lui résiste, l'équipe de sécurité se tourne vers vous. Vous savez coder et vous pouvez développer les outils qui comblent les lacunes des technologies installées. Mais même si vous savez écrire un script correct pour obtenir les résultats voulus, la maintenance de ce code vous pèse parfois. À chaque nouvelle fonction, vous avez l'impression de repartir de rien. Vous avez besoin que votre code s'exécute plus rapidement et répartisse sa charge sur plusieurs threads, voire plusieurs processeurs. Quand un utilisateur subit une erreur, vous ne pouvez que conjecturer sur ce qui s'est passé, car votre application ne remonte pas assez d'informations. Vous rêvez que vos applications aient les fonctionnalités ainsi que la facilité de maintenance et d'utilisation des projets de cybersécurité open source les plus courants. Vous vous inquiétez de laisser des failles de sécurité dans le programme que vous développez. Et si ce n'est pas le cas, vous devriez peut-être y regarder de plus près. Une chose est claire : vous êtes prêt à monter en compétences de codage. La formation SEC673™ est faite pour vous !

SEC673™ se veut la suite logique de SEC573: Automating Information Security with Python™, mais elle s'adresse aussi aux personnes maîtrisant les bases de la programmation Python. Elle passe tout de suite aux concepts avancés. Elle s'intéresse aux techniques de codage des packages courants de sécurité de l'information open source et à leur application dans nos projets de cybersécurité en Python. En nous inspirant des meilleures techniques, nous consacrerons la semaine à rendre la sécurité des informations de notre projet, SPF100, aussi facile à développer et maintenir que celle des grands projets de cybersécurité. Vous apprendrez à organiser votre code et à vous servir de concepts de programmation avancée pour que celui-ci gagne en rapidité, en efficacité et en facilité de maintenance.

Programme

SECTION 1 : Les fondamentaux des packages Python

SECTION 2 : Les objets Python

SECTION 3 : Les objets Python (suite)

SECTION 4 : Concepts avancés

SECTION 5 : Concepts avancés (suite)

SECTION 6 : Défi CTF

« Le contenu pédagogique [de SEC673] est excellent ! J'aime l'accent mis sur l'optimisation et l'efficacité dans l'apprentissage de Python. La formation en prend une tout autre dimension. »

— Samuel Cosentino, **CISCO**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC673**

MODES DE FORMATION DE SEC673

In-Person **Live Online** **OnDemand**

AXE DE FORMATION SANS

Cybersecurity Leadership

Dans un monde où le paysage des menaces ne cesse d'évoluer, la cybersécurité s'avère plus précieuse que jamais en entreprise. Les acteurs économiques comprennent désormais l'importance de sécuriser les actifs informationnels de valeur et les risques non négligeables que font courir les atteintes ou les attaques.

Les organisations ont besoin de directeurs et de responsables cyber sachant allier leurs connaissances techniques aux indispensables compétences managériales, pour mener efficacement leurs projets, équipes et initiatives en soutien des objectifs de l'entreprise.

L'axe Cybersecurity Leadership propose des approches pratiques et concrètes de gestion du risque cyber. Cette séquence de formations interactives et pratiques aide les managers actuels ou en devenir à mettre leurs compétences managériales au niveau de leurs connaissances techniques.

À l'issue d'une formation au leadership en cybersécurité de SANS, vous saurez :

- Développer vos compétences en gestion et en leadership
- Comprendre et analyser le risque
- Créer une stratégie efficace de cybersécurité
- Élaborer un programme de gestion des vulnérabilités
- Développer des plans stratégiques de sécurité en fonction des objectifs opérationnels et organisationnels
- Interagir et communiquer efficacement avec les principaux intéressés en responsabilité
- Mesurer les effets de votre programme de sécurité
- Établir une culture de la sécurité et l'entretenir
- Protéger les environnements cloud et entreprise et donner le cap

« Cette formation et cette stratégie d'apprentissage font un travail remarquable en apportant du sens, de l'orientation et de la motivation pour favoriser le changement par l'éducation ! »

— Jeremy R., **U.S. Military**

Fonctions de leadership en cybersécurité :

- Responsable/analyste SOC
- Spécialiste en détection des intrusions et en recherche de compromissions
- Ingénieur et architecte réseau et sécurité
- Analyste OSINT, enquêteur
- Administrateur système de serveur/d'extrémité
- DevSecOps et automatisation
- Chargé de réponse aux cyberincidents
- Analyste en renseignement d'intérêt cyber (CTI)

AIS247: **AI Security Essentials for Business Leaders™**

1/2 journée | 2 crédits CPE

Vous apprendrez à...

- Comprendre comment fonctionne l'IA générative et comment son utilisation peut augmenter la productivité
- Comprendre la rédaction de prompts pour optimiser les interactions et les sorties des systèmes d'IA génératives, en assurant clarté et pertinence
- Traiter et atténuer les risques associés à l'IA, notamment les biais, la dépendance excessive à l'IA et la sécurité des données
- Apprécier l'essentiel de ce qui se passe à l'intersection de l'IA et de la cybersécurité et comment gérer les risques associés
- Obtenir des éclairages sur les considérations éthiques et les bonnes pratiques pour utiliser l'IA
- Acquérir les compétences de base pour évaluer les initiatives d'IA et façonner des stratégies d'IA performantes

Public visé :

- RSSI, DSI, directeurs techniques et des opérations, directeurs marketing
- Responsables métiers, chefs d'unité, cadres
- Professionnels séniors juridiques, RH, marketing, commerciaux et financiers
- Officiers de sécurité des systèmes d'information
- Responsables, superviseurs et chefs d'équipe IT
- Directeurs, responsables et ingénieurs sécurité
- Responsables produits, chefs de produits
- Ingénieurs, développeurs de logiciels et analystes impliqués dans adoption de l'IA

Dan deBeaubien
Auteur de la formation

AIS247: AI Security Essentials for Business Leaders™ est une formation indispensable pour les professionnels qui évoluent dans l'environnement dynamique de l'intelligence artificielle du monde de l'entreprise. Cette formation propose une exploration complète de l'IA générative (GenAI), à commencer par la compréhension essentielle des facteurs qui en font un élément stratégique dans plusieurs secteurs. Elle plonge dans les mécanismes de l'IA générative et aborde des sujets comme la rédaction de prompts et les complexités des grands modèles de langage. Les stagiaires acquièrent de précieuses connaissances qui viennent éclairer les risques courants liés à l'utilisation de la GenAI, notamment sur les stratégies et tactiques d'atténuation du risque.

Un des fils rouges de la formation AIS247 est la gestion du cyber-risque lié à l'IA et le développement de politiques d'IA. Les stagiaires se dotent ainsi des connaissances pour gérer les innovations de l'intelligence artificielle en responsabilité et en sécurité. La formation est conçue pour répondre aux besoins d'une large part des professionnels impliqués dans la mise en œuvre de l'IA, des décisionnaires sur les sujets d'IA aux techniciens et utilisateurs finaux, afin de peindre un tableau exhaustif du rôle de la GenAI tant dans la sphère personnelle que professionnelle.

Elle met en avant l'application pratique de l'IA au travail en insistant sur les gains de productivité, la réduction des coûts et l'amélioration de la qualité du travail. Applications et cas d'usage types sont fournis dans la formation et couvrent divers points forts de la GenAI, notamment la création de contenus, l'analyse de données, l'ingénierie logicielle, l'assistance client et la cybersécurité. Par ces exemples pratiques, les stagiaires comprennent l'engouement des entreprises à utiliser l'IA dans leur environnement et à trouver le juste équilibre entre gain de productivité et gestion des risques.

AIS247™ traite des enjeux de la mise en œuvre de l'IA, avec des discussions portant sur l'utilisation éthique et sécurisée des technologies d'IA, l'importance de la transparence et de la redevabilité, et le besoin et la procédure d'élaboration de politiques d'IA conformes aux objectifs de l'entreprise. À l'issue de la formation, les stagiaires comprendront les aspects technologiques de l'IA, pourquoi il s'agit d'une force transformatrice dans l'entreprise, et comment appliquer ces outils efficacement, éthiquement et en toute sécurité.

Bilan

- Compréhension claire de l'imminence et des motifs de l'adoption de la GenAI, et de l'importance de gérer les risques associés.
- Éclairages sur le rôle de l'IA dans l'entreprise et sa valorisation pour accroître la productivité.
- Meilleure capacité à traiter directement les risques primaires issus de la mise en œuvre de l'intégration et de l'usage quotidien de l'IA.
- Appréhension des contenus, des équipes et des processus nécessaires à la mise en œuvre efficace des politiques sur l'IA dans votre organisation.
- Compréhension de la nécessité d'un usage éthique et transparent de l'IA sur le lieu de travail en lien avec les enjeux de pression, de risque humain et cyber, d'atténuation des risques, et des stratégies politiques.

Consultez le descriptif détaillé de la formation sur **SANS.ORG/AIS247**

MODES DE FORMATION DE AIS247

OnDemand

LDR414: **SANS Training Program for the CISSP®** Certification™

GISP
Information Security Professional
giac.org/gisp

6 jours | 52 crédits CPE

Vous apprendrez à...

- Comprendre les huit domaines de connaissance compris dans l'examen CISSP®
- Analyser les questions posées au cours de l'examen et sélectionner les bonnes réponses
- Appliquer les connaissances et les compétences de test acquises pour réussir l'examen CISSP®
- Comprendre et expliquer tous les concepts couverts par les huit domaines de connaissance
- Appliquer les compétences acquises dans les huit domaines pour résoudre des problèmes de sécurité dès votre retour sur le terrain

Public visé :

- Professionnels de la sécurité qui veulent comprendre les concepts couverts par l'examen CISSP® comme définis par (ISC)²
- Responsables qui cherchent à connaître les domaines critiques de la sécurité de l'information
- Administrateurs système, sécurité et réseau désireux de comprendre les applications pratiques des domaines de connaissance CISSP® sur leurs activités
- Professionnels et responsables sécurité qui cherchent des moyens pratiques pour appliquer les huit domaines de connaissances dans leurs activités

« Cette formation se concentre sur les concepts clés à maîtriser pour l'examen CISSP®. Ne vous battez pas avec des manuels de mille pages. Laissez-vous guider par ce cours ! »

— Carl Williams, **Harris Corporation**

Eric Conrad
Auteur de la formation

Seth Misenar
Auteur de la formation

Vous voulez vous former à l'examen CISSP® ?

SANS LDR414: SANS Training Program for the CISSP®™ Certification accompagne les candidats dans la préparation de la certification en sécurité des systèmes d'information CISSP®.

La formation se concentre exclusivement sur la révision des huit principaux domaines de connaissance identifiés par (ISC)² et sur lesquels porte l'examen CISSP®. Chaque domaine de connaissance est décomposé pour étudier la relation des composants entre eux et avec d'autres domaines de la sécurité des systèmes d'information.

Un mot des auteurs

« La certification CISSP® existe depuis presque 25 ans. L'examen est conçu pour vérifier votre compréhension du Common Body of Knowledge, à envisager comme le langage commun des professionnels de la sécurité des informations. On dit souvent que ce socle est très vaste et peu approfondi. L'examen CISSP® couvre beaucoup d'informations théoriques qu'un professionnel de la sécurité doit absolument comprendre. Ce contenu est parfois ardu et les stagiaires, qui n'en saisissent pas toujours l'application directe dans leur rôle, s'ennuient. L'objectif de notre formation est de rendre concrets les huit domaines de connaissance de CISSP®. Pour que ces informations prennent corps, les thèmes importants sont abordés par le biais d'études de cas, d'exemples et d'anecdotes. Nous prenons le pari que, si vous suivez la formation de SANS au CISSP®, vous vous passionnerez pour les huit domaines de connaissance ! »
— Eric Conrad et Seth Misenar

Programme

SECTION 1 : Introduction, sécurité et gestion des risques

SECTION 2 : Sécurité des actifs et ingénierie de sécurité (partie 1)

SECTION 3 : Ingénierie de sécurité (partie 2) : sécurité des communications et du réseau

SECTION 4 : Gestion des identités et des accès (IAM)

SECTION 5 : Évaluation de la sécurité et tests ; opérations de sécurité

SECTION 6 : Sécurité du développement logiciel

« Cette formation segmente les énormes manuels du CISSP® en subdivisions gérables et m'a aidé à me focaliser et à identifier mes points faibles. Les connaissances et les compétences pédagogiques du formateur sont excellentes. »

— Jeff Jones, **Constellation Energy Group**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/LDR414**

MODES DE FORMATION DE LDR414

In-Person | **Live Online** | **OnDemand**

LDR419: **Performing A Cybersecurity Risk Assessment**

2 jours	12 crédits CPE	7 labos

Vous apprendrez à...

- Appréhender le contexte commercial pour un programme de gestion des risques
- Créer la charte d'un programme de cybersécurité
- Comprendre les éléments fondamentaux du risque
- Choisir les mesures de cyberprotection appropriées
- Mener des évaluations de risques de tiers
- Mener une évaluation des risques de cybersécurité
- Évaluer la documentation de cybersécurité
- Examiner la mise en œuvre des mesures de cyberprotection
- Rendre minutieusement compte du risque aux parties prenantes métier
- Rendre efficacement compte du risque aux parties prenantes techniques
- Répondre productivement au risque identifié lors d'une évaluation

Public visé :

- Professionnels en gestion des risques
- Professionnels de la gouvernance, du risque et de la conformité
- Chargés d'audit informatique
- Directeurs de la conformité aux normes de sécurité
- Gestion de l'assurance de l'information
- Administrateurs/ingénieurs système

Fonctions du référentiel NICE

- Risk Management (SP-RSK-001)
- Risk Management (SP-RSK-002)
- Test and Evaluation (SP-TST-001)

« On acquiert une bonne compréhension de l'historique des évaluations de risques et des audits, y compris des questions politiques sous-jacentes. »

— Kevin Shivers, **université du Maryland**

James Tarala
Auteur de la formation

La législation récente oblige les organisations à mener une évaluation du risque cyber à des fins de conformité et d'audit. Toutefois, nombreuses sont celles qui s'exécutent sans stratégie particulière, ce qui se traduit par des défenses aléatoires, des programmes inefficaces et des pertes financières. Dans cette introduction, la compréhension du contexte économique pour évaluer le cyber-risque aide à bien définir le risque commercial pour s'en prémunir. Au-delà de la théorie, apprenez à vous préparer correctement aux évaluations de risques vraiment utiles et à les mener à bien – sachez quels risques rechercher selon votre contexte organisationnel, comment les faire émerger efficacement et présenter à la direction des résultats exploitables. LDR419™ enseigne aux stagiaires les connaissances fondamentales et les compétences pratiques nécessaires pour mener des évaluations des risques.

Formation pratique à l'évaluation des risques en cybersécurité

Chaque étude de cas a pour cadre une entreprise technologique fictive, Initech Systems, qui cherche à développer un programme de cybersécurité plus mature. Les stagiaires ont l'occasion d'explorer les stratégies de cybersécurité et les plans tactiques propres à Initech, mais issus d'exemples du terrain. Pour dérouler ces études de cas, ils participent au jeu de simulation sur table Cyber42 et s'immergent dans des scénarios de production qui déclenchent des discussions et incitent à la réflexion sur des situations auxquelles les stagiaires seront confrontés au bureau.

- Évaluation du modèle de gouvernance d'une organisation
- Évaluation des objectifs d'un programme de cybersécurité afin de procéder à l'inventaire des mesures de cyberprotection
- Création d'un plan exhaustif d'évaluation des risques pour l'interne et des tiers
- Évaluation d'une politique de cybersécurité
- Évaluation des mesures techniques de protection de la cybersécurité
- Création d'une note sur les risques à l'intention de la direction
- Rédaction d'un plan d'action personnel

Bilan

- Justification d'une évaluation des cyber-risques du point de vue économique
- Préparation d'une évaluation des risques pertinente pour l'activité
- Conformité avec les obligations réglementaires et plus
- Transmission efficace des résultats d'une évaluation des risques aux principales parties prenantes
- Création d'une stratégie pour répondre aux cyber-risques identifiés

Programme

SECTION 1 : Préparer une évaluation des risques de cybersécurité

SECTION 2 : Mener une évaluation des risques de cybersécurité

Consultez le descriptif détaillé de la formation sur **SANS.ORG/LDR419**

MODES DE FORMATION DE LDR419

In-Person **Live Online** **OnDemand**

LDR433: **Managing Human Risk™**

SSAP
SANS Security Awareness Professional
sans.org/ssap

3 jours | 18 crédits CPE

Vous apprendrez à...

- Comparer et évaluer de manière exhaustive la maturité de votre programme par rapport à ceux de vos pairs
- Comprendre le modèle de maturité de la sensibilisation à la sécurité et comment l'utiliser pour guider votre programme
- Assurer la conformité avec les principales normes et réglementations
- Mettre en œuvre les modèles des théories de l'apprentissage, de changement comportemental et de culture d'entreprise
- Définir le risque humain et expliquer ses trois variables constitutives
- Expliquer les processus d'évaluation des risques
- Expliquer et exploiter les avancées les plus récentes de l'intelligence artificielle pour augmenter exponentiellement votre impact
- Utiliser les nouveautés du renseignement d'intérêt cyber (CTI) et décrire les tactiques, les techniques et les procédures (TTP) les plus courantes des attaques exploitant le facteur humain
- Identifier, mesurer et hiérarchiser les risques humains et définir les comportements pour gérer ces risques
- Identifier les rôles à haut risque et les formations spécialisées dont ils ont besoin

Public visé :

- Chargés de la sensibilisation, de la formation, de la mobilisation ou de la culture en matière de sécurité
- Agents chargés de la gestion de la sécurité
- Auditeurs sécurité, et responsables juridiques, de la gouvernance, de la protection des données personnelles, de la mise en conformité
- Personnels de formation, des ressources humaines et de communication
- Représentants d'organisations réglementées par secteur – HIPAA, RGPD, FISMA, FERPA, PCI-DSS, ISO/IEC 27001, SOX, NERC ou toute autre norme de conformité
- Toute personne impliquée dans la planification, le déploiement ou le maintien d'un programme d'éducation, de formation, d'influence ou de communication en faveur de la sécurité

Fonctions du référentiel NICE

- Cyber Instructional Curriculum Developer (OPM 711)
- Security Awareness & Communications Manager (OP 712)

Lance Spitzner
Auteur de la formation

La cybersécurité n'est plus seulement un défi technique, mais humain : les personnes jouent un rôle dans 80 % des violations. Pour la plupart des organisations, le plus gros enjeu est désormais la gestion du risque humain. Cette formation donne aux professionnels de la sécurité les moyens de bâtir, de gérer et de mesurer efficacement le risque humain en modifiant et en sécurisant les comportements en interne. Les stagiaires se voient fournir une feuille de route structurée avec une stratégie détaillée pour mobiliser et sécuriser leurs effectifs. La formation inclut sept labos très interactifs en équipe et les supports téléchargeables « Digital Download Package ». Il s'agit de la seule formation courte SANS sanctionnée par un titre de compétences reconnu dans le secteur, SSAP.

Bilan

- Vous alignez votre programme de sensibilisation avec les priorités stratégiques de l'entreprise en sécurité.
- Vous identifiez, hiérarchisez et gérez les principaux risques humains au sein de l'entreprise.
- Vous intégrez plus rigoureusement les efforts de sensibilisation de votre équipe au cadre plus global de la gestion des risques.
- Vous rentabilisez votre investissement en pérennisant le programme pour, au-delà de changer les comportements, intégrer une culture forte de la sécurité.
- Vous communiquez et montrez la valeur du changement dans la langue de l'entreprise à la haute direction.

Programme

SECTION 1 : Fondamentaux et identification/hiérarchisation du risque humain

SECTION 2 : Identifier et changer les comportements

SECTION 3 : Culture de la sécurité et mesure du changement

« Pertinent, actuel et présenté avec une application concrète claire. »

— Rhys Arnold, **Bridewill**

« Excellentes connaissances que toute organisation devrait avoir. »

— Mtinawa Banda, **Uk CAA**

« Toutes les entreprises ont besoin d'une telle formation. »

— Nelson Estrada, **GoodFarms**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/LDR433**

MODES DE FORMATION DE LDR433

In-Person **Live Online** **OnDemand**

LDR512: **Security Leadership Essentials for Managers™**

GSLC Security Leadership
giac.org/gslc
ANAB ACCREDITED ISO/IEC 17024 PERSONNEL CERTIFICATION BODY
DoD 8140*

5 jours | 30 crédits CPE | 23 labos

Vous apprendrez à...

- Comprendre les différents référentiels de cybersécurité
- Comprendre et analyser le risque
- Comprendre les avantages et les inconvénients des différents rapports hiérarchiques
- Gérer et prendre le leadership des projets et des équipes techniques
- Élaborer un programme de gestion des vulnérabilités
- Sécuriser les workflows DevOps évolués
- Exploiter stratégiquement un système de gestion des informations et des événements de sécurité (SIEM)
- Prendre la tête d'un SOC
- Faire évoluer les comportements et développer une culture de la sécurité
- Gérer les projets de sécurité de manière efficace
- Favoriser les architectures de sécurité récentes et le cloud
- Construire des capacités d'ingénierie de sécurité par l'automatisation et l'infrastructure programmable (IaC)

Public visé :

- RSSI
- Officiers de sécurité des systèmes d'information
- Directeurs sécurité
- Responsables sécurité
- Futurs chefs sécurité
- Personnel de sécurité ayant des responsabilités d'équipe ou de gestion
- Quiconque veut aller au-delà des compétences techniques
- Profils techniques qui veulent apprendre à communiquer avec les dirigeants dans leur langue

Fonctions du référentiel NICE

- Information Systems Security Manager (OPM 722)
- Cyber Workforce Developer and Manager (OPM 751)
- Cyber Policy and Strategy Planner (OPM 752)
- Executive Cyber Leadership (OPM 901)
- Program Manager (OPM 801)
- IT Project Manager (OPM 802)

Frank Kim
Auteur de la formation

*DoD 8140 APPROVED
sans.org/8140

Mener des initiatives de sécurité pour gérer le risque informationnel

Les responsables de la sécurité doivent allier connaissances techniques et compétences de leadership pour gagner le respect et comprendre les tâches de l'équipe technique, mais aussi pour planifier et gérer correctement les projets et les initiatives de sécurité. Cette formation enseigne aux leaders les éléments clés de tout programme de sécurité moderne. Vous apprendrez à appréhender rapidement la terminologie et les questions critiques touchant à la sécurité des informations, notamment les référentiels de sécurité, l'architecture de sécurité, l'ingénierie cybersécurité, la sécurité informatique et réseau, la gestion des vulnérabilités, la cryptographie, la protection des données, la sensibilité à la sécurité, la sécurité des applications, le DevSecOps, la sécurité cloud et les opérations de sécurité. Il ne s'agit pas d'une simple formation à la sécurité. Vous apprendrez à piloter des équipes de sécurité et à gérer des programmes au cours des 23 activités ludiques Cyber42 de 60 à 80 minutes chacune.

Bilan

- Formation de cadres qui savent construire un programme moderne de sécurité
- Anticipation des capacités de sécurité à mettre en œuvre pour dynamiser l'activité et atténuer les menaces
- Formation d'équipes de sécurité plus performantes

Programme

SECTION 1 : Construire votre programme de sécurité

SECTION 2 : Architecture de sécurité technique

SECTION 3 : Ingénierie de la sécurité

SECTION 4 : Leadership et management de la sécurité

SECTION 5 : Détection des attaques et réponse

« J'aime beaucoup l'alternance entre les cours et le jeu Cyber42. »

— Jamil A., **administration américaine**

« La formation est géniale. Tant d'informations précieuses dans une excellente formation intensive au leadership en sécurité. »

— Ian D., **administration américaine**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/LDR512**

MODES DE FORMATION DE LDR512

In-Person | **Live Online** | **OnDemand**

LDR514: **Security Strategic Planning, Policy, and Leadership™**

GSTRT
Strategic Planning, Policy, and Leadership
giac.org/gstrt
DoD 8140*

5 jours | 30 crédits CPE | 15 labos

Vous apprendrez à...

- Développer des plans de sécurité stratégiques
- Créer une politique de sécurité de l'information efficace
- Comprendre les différentes phases du processus de planification stratégique
- Appliquer vos connaissances approfondies des grands outils de planification
- Cultiver les compétences fondamentales pour créer des plans stratégiques qui protègent votre entreprise
- Stimuler les innovations clés
- Fluidifier la collaboration avec vos partenaires au sein de l'entreprise
- Élaborer des plans stratégiques de sécurité en fonction des objectifs opérationnels et organisationnels

Public visé :

- RSSI
- Officiers de sécurité des systèmes d'information
- Directeurs sécurité
- Responsables sécurité
- Futurs chefs sécurité
- Personnel de sécurité ayant des responsabilités d'équipe ou de gestion
- Quiconque veut aller au-delà des compétences techniques
- Profils techniques qui veulent apprendre à communiquer avec les dirigeants dans leur langue

Fonctions du référentiel NICE

- Information Systems Security Manager (OPM 722)
- Cyber Workforce Developer and Manager (OPM 751)
- Cyber Policy and Strategy Planner (OPM 752)
- Executive Cyber Leadership (OPM 901)
- Program Manager (OPM 801)
- IT Project Manager (OPM 802)

Frank Kim
Auteur de la formation

*DoD 8140 APPROVED
sans.org/8140

Aligner les initiatives de sécurité sur la stratégie

La nouvelle génération de responsables de la sécurité doit combler le fossé qui sépare le personnel de sécurité des hauts dirigeants en planifiant stratégiquement la façon de construire et de gérer des programmes de sécurité efficaces. Toutefois, nous, professionnels de la sécurité et de l'IT, peinons à créer une stratégie de sécurité et à exécuter un plan alliant politique rigoureuse et leadership fort, car nous passons le plus clair de notre temps à répondre et à réagir. La planification stratégique ne fait presque jamais partie de nos attributions avant que nous n'accédions à un poste supérieur et, lorsque cela arrive, nous ne disposons pas des compétences indispensables pour rejoindre le peloton. Cette formation à la sécurité des informations vous fournit les outils pour bâtir un plan stratégique de cybersécurité et une politique de sécurité informatique complète et guider vos équipes dans l'exécution de votre plan et de votre politique. À l'issue de la formation, vous aurez préparé un exposé pour la direction, lu trois études de cas, traité les questions qui se posent à quatre entreprises fictives, analysé neuf scénarios, et répondu à vingt événements Cyber42.

Bilan

- Création d'un plan de sécurité qui trouve un écho auprès de vos clients
- Développement de leaders qui savent aligner la cybersécurité sur les objectifs de l'entreprise
- Formation d'équipes de sécurité plus performantes

Programme

SECTION 1 : Bases de la planification stratégique
SECTION 2 : Développement d'une feuille de route stratégique
SECTION 3 : Développement et évaluation de politique de sécurité
SECTION 4 : Compétences de gestion et de leadership
SECTION 5 : Atelier de planification stratégique

« J'ai apprécié Cyber42. J'ai particulièrement aimé passer en revue les différentes réponses pour discuter de leurs effets sur les scores de chacun. »

— Alexander Walker, **TechVets**

« J'aurais eu besoin de cette formation il y a 10 ans, quand j'ai pris mes fonctions de RSSI. Les discussions du groupe de travail, les outils et la théorie sont ancrés dans le concret et applicables dans mon quotidien professionnel. »

— Mark Potter, **NewWave**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/LDR514**

MODES DE FORMATION DE LDR514

In-Person | **Live Online** | **OnDemand**

LDR516: **Strategic Vulnerability and Threat Management™**

5 jours | 30 crédits CPE | 16 labos

Vous apprendrez à...

- Créer, implémenter et faire mûrir votre programme de gestion des vulnérabilités et obtenir l'adhésion des parties intéressées
- Implémenter des techniques pour dresser et mettre à jour la liste précise et pertinente des actifs informatiques au sein de l'entreprise et du cloud
- Identifier les processus et les technologies efficaces dans l'infrastructure et les applications et bien les configurer
- Reconnaître les faux positifs et les faux négatifs courants dans votre arsenal d'identification
- Hiérarchiser les vulnérabilités non comblées à traiter avec diverses techniques
- Communiquer et restituer efficacement les informations sur les vulnérabilités au sein de l'organisation
- Identifier et expliquer le risque associé aux vulnérabilités non comblées dont la remédiation n'est pas actuellement prioritaire

Public visé :

- Responsables de programmes sur les vulnérabilités et analystes chargés de gérer les vulnérabilités en entreprise ou dans le cloud
- Directeurs, responsables et officiers de sécurité des systèmes d'information
- Futurs responsables en sécurité de l'information
- Professionnels en gestion des risques, continuité d'activité et reprise d'activité
- Administrateurs et gestionnaires des opérations informatiques
- RSSI
- Responsables, administrateurs, intégrateurs, développeurs et intermédiaires (broker) cloud
- Gestionnaires des risques et de la sécurité cloud
- Professionnels de l'informatique du service public chargés de la gestion des vulnérabilités de l'environnement entreprise ou cloud (FedRAMP, NIST CSF)

Fonctions du référentiel NICE

- Security Control Assessor (OPM 612)
- Vulnerability Assessment Analyst (OPM 541)

Jonathan Risto
Auteur de la formation

David Hazar
Auteur de la formation

Arrêtez de traiter les symptômes. Attaquez-vous aux causes.

La gestion des vulnérabilités, des correctifs et de la configuration ne date pas d'hier. C'est même un des rôles historiques de la sécurité. Pourtant, la gestion efficace de ces fonctions reste rare. Le nombre de vulnérabilités non traitées est impressionnant dans la plupart des grandes organisations, qui toutes luttent pour rester au fait du flux ininterrompu de nouvelles failles de sécurité affectant leur infrastructure et leurs applications. Si on ajoute à cela le cloud et la vitesse toujours plus grande à laquelle les organisations doivent fournir systèmes, applications et fonctionnalités à leurs clients internes comme externes, la sécurité semble un objectif inaccessible. Cette formation vous expose comment développer efficacement la maturité de votre programme de gestion des vulnérabilités et non plus seulement identifier les vulnérabilités, mais les résorber.

Bilan

Avec cette formation, votre organisation va :

- Comprendre les avantages et les inconvénients des programmes modernes de gestion des vulnérabilités
- Anticiper et planifier les conséquences liées aux environnements en cloud
- Réaliser l'importance du contexte et comprendre comment collecter, stocker, maintenir et utiliser efficacement les informations contextuelles
- Communiquer utilement et efficacement les informations sur les vulnérabilités et le risque associé aux principales parties intéressées
- Déterminer comment regrouper les vulnérabilités pour identifier les obstacles ou déficiences actuels
- Identifier les métriques porteuses d'adoption et de changement dans l'organisation
- Comprendre quelles capacités de remédiation sont disponibles aux équipes de technologie en amont ou pour résoudre les vulnérabilités

Programme

SECTION 1 : Planification et conception de la gestion des vulnérabilités

SECTION 2 : Identification des vulnérabilités

SECTION 3 : Analyse des vulnérabilités, métriques et communication afférentes

SECTION 4 : Piloter la remédiation et l'automatisation

SECTION 5 : Collaboration et amélioration continue

« Cette formation devrait être obligatoire pour tout membre d'une équipe VM. Les informations fournies sont immédiatement utiles dans n'importe quelle organisation. »

— Brandi Loveday-Chesley

Consultez le descriptif détaillé de la formation sur **SANS.ORG/LDR516**

MODES DE FORMATION DE LDR516

In-Person | **Live Online** | **OnDemand**

ZOOM NOUVELLE FORMATION

LDR519: **Cybersecurity Risk Management and Compliance™**

5 jours | 30 crédits CPE

Vous apprendrez à...

- Identifier et gérer les cyber-risques par des méthodologies structurées de modélisation et d'évaluation des menaces
- Hiérarchiser et allouer les ressources efficacement grâce à votre compréhension de la criticité de diverses menaces et vulnérabilités cyber
- Développer votre maîtrise des référentiels du secteur, notamment RMF (Risk Management Framework) du NIST et FAIR, pour améliorer la posture de cybersécurité de votre organisation
- Appliquer des exercices pratiques et des études de cas issus du terrain pour renforcer vos acquis théoriques et valider vos stratégies de cybersécurité
- Maîtriser la conduite des évaluations et des audits exhaustifs des cyber-risques afin d'assurer la conformité aux normes réglementaires
- Améliorer vos capacités décisionnelles par des éclairages factuels et des simulations qui vous prépareront aux enjeux cyber en production

Public visé :

- Professionnels en gestion des risques
- Professionnels de la gouvernance, du risque et de la conformité
- Chargés d'audit informatique
- Directeurs de la conformité aux normes de sécurité
- Gestion de l'assurance de l'information
- Administrateurs/ingénieurs système

Fonctions du référentiel NICE

- Risk Management (RSK) SP-RSK-001
- Risk Management (RSK) SP-RSK-002
- Test and Evaluation (TST) SP-TST-001

James Tarala
Auteur de la formation

LDR519™ traite une question non négligeable dans le domaine de la cybersécurité : gérer et atténuer efficacement les cyber-risques tout en assurant la conformité réglementaire. Cette question s'avère chaque jour plus pertinente de par la nature évolutive et complexe des cybermenaces, aux conséquences potentiellement considérables sur l'exploitation, la sécurité des données et la continuité globale de l'activité. Cette formation complète plonge dans la modélisation des menaces, les référentiels de protection et l'analytique des risques pour vous doter des compétences nécessaires à la gestion efficace des risques de cybersécurité. Apprenez à hiérarchiser les menaces, à sélectionner les dispositifs de protection appropriés et à assurer la conformité réglementaire. Tirez des informations pratiques de nombreuses études de cas, issus du monde réel, et des simulations SANS Cyber42, qui renforcent votre appréhension de la gouvernance de la cybersécurité et de la gestion de programme. Rejoignez-nous pour maîtriser l'art de la gestion du risque et de la conformité et sécuriser le futur numérique de votre organisation.

Bilan

- Vous dotez vos effectifs de compétences avancées pour identifier, évaluer et atténuer les cyber-risques, et améliorez ainsi la sécurité organisationnelle.
- Vous alignez les efforts de cybersécurité sur les objectifs commerciaux dans le cadre d'une approche structurée de la gestion des risques et de la conformité.
- Vous améliorez vos capacités décisionnelles en intégrant la modélisation des menaces et l'analytique des risques à la planification stratégique.
- Vous renforcez la résilience organisationnelle aux cybermenaces changeantes par des stratégies proactives de gestion des risques.
- Vous assurez la conformité aux normes sectorielles et aux obligations réglementaires, réduisant dans le même temps le risque de répercussions juridiques et financières.
- Vous mettez en œuvre des mesures de cyberprotection robustes et adaptées au profil de risque propre à votre entreprise.
- Vous encouragez une culture de sensibilité à la sécurité et d'esprit critique parmi les membres de l'équipe afin d'améliorer la posture de sécurité globale.

Programme

SECTION 1 : Stratégie de gestion du risque cyber

SECTION 2 : Modélisation de la menace cyber

SECTION 3 : Référentiel de cybersécurité

SECTION 4 : Validation des mesures de protection et gestion des risques tiers (TPRM)

SECTION 5 : Analytique des cyber-risques et réponse

Consultez le descriptif détaillé de la formation sur **SANS.ORG/LDR519**

MODES DE FORMATION DE LDR519

In-Person **Live Online**

LDR520: **Cloud Security for Leaders™**

5 jours	30 crédits CPE	+12 labos

Vous apprendrez à...

- Définir une stratégie de sécurisation de charge de travail dans le cloud capable de prendre en charge les objectifs des petites ou grandes entreprises
- Établir à partir de la stratégie de sécurité une feuille de route adaptée au rythme soutenu de l'adoption du cloud et de la migration tout en maintenant une garantie de sécurité élevée
- Comprendre les fondamentaux de la sécurité en environnement cloud chez les différents cloudistes, et expliquer et motiver les décisions stratégiques pertinentes auprès des parties intéressées
- Élaborer un plan efficace d'évolution de la posture de sécurité au fil du temps vers plus de maturité, en exploitant les fonctions de sécurité des fournisseurs de cloud pour l'optimiser
- Expliquer la vision de la sécurité de l'organisation dans le domaine cloud à la direction, collaborer avec vos collègues et mobiliser vos équipes pour amener le changement de culture de la sécurité imposé par la transformation cloud

Public visé :

- Cette formation s'adresse prioritairement aux cadres et à la direction en position de piloter ou de prendre des décisions impactantes sur la transition de l'informatique vers les environnements cloud.

Fonctions du référentiel NICE

- Information Systems Security Manager (OPM 722)
- Program Manager (OPM 801)
- IT Project Manager (OPM 802)

Jason Lam
Auteur de la formation

Cette formation à la stratégie de sécurité appliquée au cloud se focalise sur ce que les cadres, directeurs et responsables sécurité doivent savoir pour élaborer leur plan ou feuille de route au moment de gérer les fonctions de mise en œuvre de la sécurité dans le cloud. Pour protéger les investissements et l'environnement cloud de l'organisation, une équipe de gestion compétente doit s'engager dans une planification et une gouvernance approfondies. Nous mettons l'accent sur les connaissances indispensables pour élaborer une feuille de route de sécurité du cloud et implémenter efficacement les fonctionnalités de sécurité correspondantes. Prendre des décisions éclairées sur la sécurité lors de du passage au cloud implique de comprendre la technologie, les processus et les personnes en lien avec ce type d'environnement.

Bilan

- Vous établissez un programme de sécurité du cloud adapté au rythme enlevé de la transformation de l'entreprise.
- Vous comprenez le niveau de maturité actuel et futur de la sécurité du cloud par rapport aux points de référence du secteur.
- Vous prenez des décisions éclairées sur les programmes de sécurité du cloud.
- Vous anticipez les fonctionnalités de sécurité et les garde-fous à ériger pour sécuriser l'environnement cloud.
- Vous protégez les données de l'entreprise pendant la migration des charges de travail vers le cloud.

Programme

SECTION 1 : Fondamentaux de la sécurité du cloud et gestion des identités

SECTION 2 : Architecture et protection de l'environnement de sécurité du cloud

SECTION 3 : Protection des données, détection et réponse, et gouvernance de la sécurité cloud

SECTION 4 : Sécurisation des charges de travail et garantie de sécurité

SECTION 5 : Projet final multicloud

« Les formations de ce type, abordant la sécurité du cloud sous l'angle managérial, sont rares et la qualité de celle-ci est proprement incroyable. »

— Benoit Ramillon, **UEFA**

« Excellente formation, très riche en informations, mais qui montre surtout le modèle à suivre pour renforcer la sécurité dans les environnements cloud d'entreprise. »

— Jesus Fernandez, **FEMSA**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/LDR520**

MODES DE FORMATION DE LDR520

In-Person **Live Online** **OnDemand**

LDR521: **Security Culture for Leaders™**

5 jours	30 crédits CPE	+12 labos

Vous apprendrez à...

- Expliciter la culture et son importance en cybersécurité, inventorier et mesurer les indicateurs de la culture globale de l'organisation et de celle de la sécurité
- Définir les indicateurs d'une culture robuste de la sécurité, vous aligner dessus, et les intégrer à la culture actuelle de votre organisation
- Fournir un cadre et des principes directeurs à votre équipe de sécurité pour jeter les bases d'une forte culture de la sécurité
- Communiquer efficacement la valeur commerciale de la sécurité à la direction générale et au conseil d'administration pour obtenir leur soutien et leur implication
- Mobiliser et motiver vos équipes pour qu'elles fassent de la cybersécurité leur priorité
- Simplifier la sécurité et supprimer les barrières, et ainsi potentiellement faciliter l'intégration de la sécurité dans les actions quotidiennes de tous

Public visé :

- Responsables de la sécurité des systèmes d'information
- Responsables de réponse aux risques et managers de gestion des risques
- Responsables de la sensibilisation, de la mobilisation ou de la culture en matière de sécurité
- Responsables sécurité confirmés qui mènent des initiatives de sécurité à grande échelle
- Directeurs, responsables et officiers de sécurité des systèmes d'information
- Architectes et consultants en sécurité de l'information
- Futurs responsables en sécurité de l'information
- Responsables de la continuité et de la reprise d'activité
- Délégués à la protection des données/vie privée

Fonctions du référentiel NICE

- Cyber Instructional Curriculum Developer (OPM 711)
- Security Awareness and Communications Manager (OPM 712)
- Information Systems Security Manager (OPM 722)
- Cyber Workforce Developer and Manager (OPM 751)
- Cyber Policy and Strategy Planner (OPM 752)
- Executive Cyber Leadership (OPM 901)
- Program Manager (OPM 801)
- IT Project Manager (OPM 802)

Lance Spitzner
Auteur de la formation

Russell Eubanks
Auteur de la formation

S'inspirant de situations réelles du monde entier, la formation LDR521™ de SANS vous apprend à façonner une culture dans laquelle la direction comme les effectifs donnent du crédit à la cybersécurité et en font leur priorité. Dans cette formation pratique, incluant une série d'exercices et de labos interactifs, vous appliquez ces concepts à différentes initiatives de sécurité issues du terrain. Vous apprenez aussi rapidement à transformer votre équipe de sécurité et à intégrer la sécurité à la culture de votre entreprise à tous les échelons, à commencer au plus haut. Vous appliquez les conclusions des travaux de recherche de Daniel Kahneman, qui lui ont valu le prix Nobel, de la théorie du coup de pouce ou « nudge » de Thayler et Sunstein, du modèle ADKAR, et du Golden Circle de Simon Sinek. Découvrez en quoi Monsieur Spock, Homer Simpson, la métaphore de l'éléphant et de son cornac, et la malédiction de la connaissance jouent un rôle essentiel pour renforcer la culture de sécurité.

Bilan

- **Sécurité à grande échelle :** facilitez-vous le travail en passant votre équipe et vous-même à l'échelle. Réduisez le risque de burnout dans l'équipe de sécurité que vous avez le privilège d'encadrer.
- **Sécurité dès le départ :** intégrez la sécurité dès le début de tout projet ou initiative de chaque division dans votre organisation.
- **Soutien de la direction :** obtenez l'appui dont vous avez besoin auprès de la haute hiérarchie pour vos projets les plus importants.
- **Protection des effectifs :** les collaborateurs adopteront les comportements que vous voulez sans qu'on leur dise quoi faire et ne pas faire au travail.
- **Initiatives réussies :** augmentez le taux de succès de vos initiatives sécuritaires en emportant l'adhésion de services clés comme l'IT, l'ingénierie, et le métier.
- **Ambassadeurs :** transformez votre équipe de sécurité en hérauts de la sécurité qui mobilisent, motivent et arment vos effectifs pour mieux se protéger.

Programme

SECTION 1 : Fondamentaux de la culture organisationnelle et sécuritaire

SECTION 2 : Mobiliser pour la culture de la sécurité

SECTION 3 : Susciter et mesurer une culture de la sécurité

SECTION 4 : Impliquer la direction

SECTION 5 : Atelier final

« Je suis ravie de cette formation axée sur l'intégration des valeurs sécurité dans notre culture internationale, c'est exactement l'aide dont ma société a besoin MAINTENANT. »

— Laura M., **KPMG LLP**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/LDR521**

MODES DE FORMATION DE LDR521

In-Person **Live Online** **OnDemand**

LDR551: **Building and Leading Security Operations Centers™**

GSOM
Security Operations Manager
giac.org/gsom

5 jours | 30 crédits CPE | +17 labos

Vous apprendrez à...

- Établir un SOC aux bases solides avec une mission claire, une charte et des objectifs organisationnels
- Collecter les journaux et données réseau les plus importants
- Constituer, former et encapaciter une équipe hétérogène
- Créer des playbooks et gérer des cas d'usage de détection
- Exploiter le renseignement sur les menaces pour axer vos efforts de détection sur les véritables priorités
- Appliquer des stratégies de défense active et de recherche de compromission
- Implémenter un workflow efficace de tri des alertes et d'enquête
- Mettre en œuvre la planification et l'exécution efficaces de la réponse aux incidents
- Choisir les indicateurs et une stratégie à long terme pour améliorer le SOC
- Former et retenir vos effectifs, et prévenir l'épuisement professionnel
- Mener une évaluation du SOC à l'aide de planification de capacité, de tests purple team et de l'émulation d'attaque

Public visé :

Cette formation s'adresse à qui cherche à construire un centre des opérations de sécurité (SOC) pour la première fois ou à améliorer celui déjà en exploitation dans son organisation.

Elle cible notamment les profils de stagiaires suivants :

- Responsables ou managers de centre des opérations de sécurité (SOC)
- Directeurs sécurité
- Nouveaux membres de l'équipe des opérations de sécurité
- Analystes SOC séniors/principaux
- Profils techniques de RSSI et de directeurs sécurité

Fonctions du référentiel NICE

- Information Systems Security Manager (OV-MGT-001)
- Cyber Policy and Strategy Planner (OV-SSP-002)
- Executive Cyber Leadership (OV-EXL-001)
- Program Manager (OV-PMA-001)
- Cyber Defense Incident Responder (PR-CIR-001)
- OT SOC Operator (ZZ-ICS-004)

John Hubbard
Auteur de la formation

Mark Orlando
Auteur de la formation

Prévenir – Détecter – Répondre | Personnes – Processus – Technologie

Si vous êtes un responsable ou manager d'un centre des opérations de sécurité (SOC) qui cherche à libérer toute la puissance d'une cyberdéfense proactive alimentée par le renseignement, alors LDR551™ est la formation faite pour vous ! Dans un monde où les environnements informatiques et les auteurs de menace évoluent à un rythme que peu d'équipes parviennent à suivre, donnez à votre SOC les moyens de se défendre contre des acteurs malveillants fortement motivés. Les environnements modernes extrêmement dynamiques exigent une capacité de cyberdéfense mêlant anticipation, réactivité et renseignement. Cette formation de manager de SOC vous accompagne dans ces activités critiques, du début à la fin, et vous apprend à concevoir des défenses adaptées au profil de risque unique de votre organisation. À son issue, vous saurez aligner les activités de votre SOC sur les objectifs organisationnels.

Bilan

- Mise en œuvre des stratégies alignant la cyberdéfense sur les objectifs organisationnels.
- Abaissement du profil de risque grâce à de meilleurs outils et techniques de validation de la sécurité.
- Méthodologies de recrutement interne ou temporaire, de formation et de rétention des cyberdéfenseurs compétents.
- Collaboration et coordination transverses efficaces.
- Optimisation immédiate de la sécurité avec les actifs existants.
- Baisse des dépenses due à la plus grande fluidité des opérations de cybersécurité.

Programme

SECTION 1 : Conception du SOC et planification opérationnelle
SECTION 2 : Télémétrie et analyse au SOC
SECTION 3 : Détection, recherche et tri des attaques
SECTION 4 : Réponse aux incidents
SECTION 5 : Métriques, automatisation et amélioration continue

« Cette formation étend immédiatement votre kit de ressources à la résolution de problèmes de gestion de l'exploitation de NOSC. »

— Ron L., **administration américaine**

« Le contenu est génial ! Il couvre de nombreux sujets et m'a exposé à de nombreux nouveaux concepts et idées, et fait le lien avec des exemples actuellement en production. »

— Prasanth Chatti, **Campbells Soup Company**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/LDR551**

MODES DE FORMATION DE LDR551

In-Person | **Live Online** | **OnDemand**

LDR553: **Cyber Incident Management™**

GCIL
Cyber Incident Leader
giac.org/gcil

5	30	+26
jours	crédits CPE	labos

Vous apprendrez à...

- Catégoriser et définir correctement les limites des incidents et les objectifs consécutifs de l'équipe de gestion des incidents
- Concevoir, préparer, corriger, publier et contrôler toutes les communications dans le cadre de la gestion d'un incident grave
- Gérer une équipe soumise à une pression intense, et reconnaître les réactions naturelles qui se manifesteront et leur signification
- Encadrer l'équipe, gagner la confiance de la direction, et dépasser les attentes de toutes les personnes impliquées
- Calculer, coordonner et exécuter des activités pour contrer la compromission tant côté système que données
- Réfléchir aux stratégies et réagir aux incidents de ransomware, notamment développer des exercices et des formations autour de telles attaques dévastatrices
- Structurer, gérer et présenter un briefing à votre équipe, à la direction ou au conseil d'administration
- Organiser le passage de la phase d'incident actif au retour à la normale et exécuter ce plan
- Préparer, mettre en place et mener des exercices de gestion de cyberincident

Public visé :

- Responsables sécurité
- Professionnels de la sécurité
- Responsables
- Personnels juridiques, RH et communications

Fonctions du référentiel NICE

- Knowledge Manager (OM-KMG-001)
- Cyber Legal Advisor (OV-LGA-001)
- Privacy Officer/Privacy Compliance Manager (OV-LGA-002)
- Information Systems Security Manager (OV-MGT-001)
- Communications Security (COMSEC) Manager (OV-MGT-002)
- Cyber Policy and Strategy Planner (OV-SPP-002)
- Executive Cyber Leadership (OV-EXL-001)

Steve Armstrong-Godwin
Auteur de la formation

Ouvrir en cas d'urgence

Si mener la charge contre un cyberincident ou y contribuer vous inquiète, alors cette formation est faite pour vous. LDR553: Cyber Incident Management™ se focalise sur les enjeux non techniques auxquels les leaders sont confrontés en période de crise. Vous avez probablement une équipe technique complète prête à chercher, comprendre et mettre fin à l'attaque, mais elle a besoin d'informations, d'encadrement, de soutien, d'écoute et de clarté pour optimiser son temps et son efficacité. Nous nous focalisons sur la formation d'une équipe pour remédier à l'incident, l'encadrement de l'équipe, la communication des données critiques à des fins de briefing, et l'exposé de ce briefing. Nous nous intéressons à la communication à tous les niveaux – équipes de terrain, direction et conseil d'administration, journalistes d'investigation, et même attaquants. Cette formation contient neuf études de cas pour acquérir les connaissances par la pratique.

Bilan

- Des collaborateurs incités à encadrer des équipes de gestion des cyberincidents ou à y apporter leur contribution.
- Processus de gestion des incidents simplifiés pour des résolutions plus rapides.
- Identification et correction des écarts entre les plans de gestion des incidents de sécurité et les stratégies de réponse.
- Performances des équipes des incidents de sécurité accrues pour répondre aux enjeux en mutation.
- Planification stratégique et appréhension d'attaques à forts enjeux, comme la fraude au virement et les ransomwares, afin de façonner un cadre de réponse résilient.
- Fluidité accrue de la collaboration entre les équipes techniques et non techniques pendant la réponse à incident, pour une approche plus intégrée.
- Instillation d'une culture de l'amélioration continue, en affinant les prochaines stratégies de réponse grâce aux enseignements tirés des incidents.
- Intégration proactive du renseignement d'intérêt cyber afin d'anticiper et d'atténuer les menaces avant qu'elles ne dégénèrent.

Programme

SECTION 1 : Compréhension de l'incident et communication afférente

SECTION 2 : Évaluer l'étendue des dégâts, planifier la remédiation et exécuter le plan

SECTION 3 : Formation, valorisation du renseignement d'intérêt cyber (CTI), et bug bounties

SECTION 4 : Incidents cloud, fraude au virement, vol d'informations d'identification, et métriques des incidents

SECTION 5 : IA appliquée aux incidents, extorsion de fonds, ransomware, et exercice final

« C'est une formation parfaite pour qui encadre les cyberincidents. Je n'ai rien trouvé de comparable, de loin. »

— Lee Taylor, **police du Leicestershire**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/LDR553**

MODES DE FORMATION DE LDR553

In-Person **Live Online** **OnDemand**

SEC405: **Business Finance Essentials™** MISE À JOUR MAJEURE

1 jour | 6 crédits CPE

Vous apprendrez à...

- Améliorer votre connaissance des sujets financiers en entreprise
- Améliorer votre compréhension et appréhension de la santé financière de l'entreprise
- Vous préparer à collaborer avec le service financier de votre entreprise
- Développer les compétences et connaissances pour agir en conseil financier avisé dans votre organisation

Public visé :

- Directeurs de la sécurité des systèmes d'information
- Chargés de la sécurité des systèmes d'information
- Chefs de la sécurité des systèmes d'information
- Quiconque aspirant à devenir un responsable efficace en sécurité de l'information

Bilan

- Vous communiquez efficacement avec votre DAF et le service financier, car vous parlez leur langue.
- Vous présentez vos idées et initiatives adossées à de solides données financières – l'assurance de justifier les investissements et de susciter l'adhésion de la direction.
- Vous appliquez une méthode financière en huit étapes pour communiquer plus efficacement les sujets financiers.
- Vous connaissez les objectifs financiers de l'organisation et les interprétez correctement.
- Vous alignez mieux le programme de cybersécurité sur les priorités stratégiques de votre organisation.
- Vous améliorez votre compréhension des décisions et compromis commerciaux de l'entreprise.
- Vous renforcez votre collaboration avec les acteurs clés en montrant votre sens des affaires et votre réflexion stratégique.

Russell Eubanks
Auteur de la formation

Et si vous aviez l'assurance pour appréhender les enjeux financiers de votre organisation avant de vous plonger une heure de plus dans vos projets de cybersécurité – ou pour négocier chaque euro supplémentaire de votre budget cyber ? Comprendre la gestion financière responsable n'est pas qu'une question de budget – il s'agit de prendre des décisions stratégiques éclairées, sources de sécurité et de réussite commerciale.

Dans cette formation aux bases de la finance d'entreprise, vous ne vous contenterez pas d'apprendre la théorie, vous l'appliquerez. Par des exercices concrets, vous monterez un business case convaincant pour l'investissement en cybersécurité et élaborerez un budget pluriannuel. Ces modèles pratiques guideront votre prise de décision sur le terrain – en vous donnant les moyens de plaider en faveur de la cybersécurité à tous les niveaux de votre organisation.

La formation vous dote du bagage financier et des compétences décisionnelles pour communiquer efficacement la valeur de la cybersécurité, justifier les investissements critiques et aligner les initiatives sur les priorités commerciales. Les connaissances et les outils acquis avec SEC405™ vont non seulement renforcer votre leadership, mais aussi dynamiser votre équipe et consolider la posture financière et de sécurité de votre organisation.

Qu'est-ce que la culture financière en entreprise ?

Il s'agit de la capacité à comprendre et à appliquer les principes de la gestion financière pour prendre des décisions commerciales saines. Pour les professionnels de la cybersécurité, il est crucial d'acquérir ce bagage pour aligner les initiatives de sécurité sur les objectifs de l'entreprise, s'assurer les budgets nécessaires et communiquer efficacement avec la direction. Cette acculturation présente des avantages pour les professionnels et, appliquées, ces connaissances ne manqueront pas d'attirer l'attention de la direction générale.

Business case concret et formation à la planification budgétaire

Les exercices pratiques inclus visent à développer votre capacité à justifier les investissements en cybersécurité, à affecter efficacement des ressources et à faire correspondre les initiatives de sécurité aux objectifs commerciaux. Vous créerez un business case clair, aux investissements structurés et rationalisés de façon à soutenir les priorités de l'entreprise et ses objectifs financiers. Cet entraînement vous prépare à répliquer efficacement le processus dans votre cadre professionnel.

En outre, vous élaborerez un budget pluriannuel, ce qui vous apportera un éclairage précieux sur la planification stratégique et les étapes nécessaires pour vous assurer un financement à long terme de vos projets cyber critiques. En plus de renforcer les principales notions, ces exercices apportent des modèles et des compétences immédiatement opérationnelles qui vous aident à :

- Collaborer efficacement avec l'équipe financière
- Démontrer votre gestion financière responsable
- Endosser le rôle de conseil financier fiable dans votre organisation

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC405**

MODES DE FORMATION DE SEC405

OnDemand

SEC566: **Implementing and Auditing CIS Controls™**

GCCC
Critical Controls
giac.org/gccc

5 jours	30 crédits CPE	+17 labos

Vous apprendrez à...

- Appliquer des contrôles de sécurité issus de menaces réelles, qui sont mesurables, évolutifs et fiables pour faire obstacle aux attaques connues et protéger les informations et systèmes importants de votre organisation
- Comprendre l'importance de chaque contrôle et le risque de compromission en cas d'omission
- Expliquer les objectifs défensifs qui offrent des retours rapides et améliorent la visibilité sur le réseau et les systèmes
- Identifier et utiliser des outils pour la mise en œuvre automatique de ces contrôles
- Créer des outils de notation pour mesurer l'efficacité de chaque contrôle
- Utiliser des métriques spécifiques pour établir un référentiel et mesurer l'efficacité des contrôles
- Relier avec compétence les contrôles CIS aux obligations et normes de conformité comme PCI-DSS, le CSF du NIST, ISO 27000, etc.
- Réaliser un audit de chaque contrôle CIS avec des modèles, des checklists et des scripts, spécifiques et éprouvés, fournis pour faciliter le processus

Public visé :

- Chargés d'audit de l'assurance de l'information
- Chargés de mise en œuvre ou administrateurs système
- Analystes de la conformité réglementaire
- Administrateurs IT
- Personnels et prestataires du ministère de la Défense
- Agences fédérales ou clients
- Organisations du secteur privé qui cherchent à améliorer leurs processus d'assurance de l'information et à sécuriser leurs systèmes
- Fournisseurs et consultants en sécurité qui cherchent à rester à jour en matière de cadres de travail pour l'assurance de l'information

Fonctions du référentiel NICE

- Security Control Assessor (SP-RSK-002)

Brian Ventura
Auteur de la formation

Les attaques informatiques médiatisées montrent que les actions offensives prennent l'avantage sur les mesures défensives. En cybersécurité, ingénieurs, auditeurs, et membres des équipes de conformité et de protection des données personnelles se demandent comment protéger et défendre concrètement leurs systèmes et données, et comment mettre en œuvre une liste prioritaire de contrôles de cyberhygiène. Dans SEC566™ de SANS, les stagiaires découvrent comment une organisation peut défendre ses informations au moyen d'une norme validée de contrôles de cybersécurité. Ils apprennent notamment à mettre en œuvre, à gérer et à évaluer les règles des contrôles de sécurité définies dans les CIS Controls. Ils acquièrent une connaissance de première main des contrôles CIS et de l'écosystème d'outils pour les implémenter dans l'ensemble des réseaux complexes des organisations, notamment dans les actifs cloud.

Bilan

- Réduction efficace des risques cyber les plus importants.
- Critères de conformité alignés sur les solutions et objectifs commerciaux et sécuritaires.
- Statut des efforts défensifs de cybersécurité présenté à la direction en termes managériaux clairs.
- Assurance que l'entreprise a une stratégie complète de défense et de conformité.

Programme

SECTION 1 : Introduction et présentation des CIS Critical Controls

SECTION 2 : Protection des données, identification et authentification, gestion du contrôle d'accès, gestion des journaux d'audit

SECTION 3 : Protections des serveurs, des postes de travail, des périphériques réseau (partie 1)

SECTION 4 : Protections des serveurs, des postes de travail, des périphériques réseau (partie 2)

SECTION 5 : Gouvernance et sécurité opérationnelle

« SEC566 m'a été très précieuse. Je pensais connaître les contrôles de sécurité, mais la formation m'a fait comprendre que je n'en maîtrisais que les bases. J'ai acquis des connaissances approfondies dans ce domaine. »

— Keri Powell, **Textron**

« À l'issue de cette formation, j'ai une envie renouvelée de retourner au travail, d'ajuster mes scans de vulnérabilités et de les faire tourner. »

— Jason Hinojosa, **Rush Enterprises**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/SEC566**

MODES DE FORMATION DE SEC566

In-Person **Live Online** **OnDemand**

AXE DE FORMATION SANS

Digital Forensics & Incident Response (DFIR) and Threat Hunting

Quelle que soit sa taille, une organisation a besoin de personnel qui maîtrise les techniques de réponse aux incidents pour identifier les systèmes compromis, circonscrire efficacement la violation et remédier rapidement à l'incident.

De même, les organismes publics et les forces de l'ordre sont en demande de collaborateurs compétents pour exploiter les supports informatiques et récupérer les éléments de preuve sur les appareils et systèmes ennemis. Une formation SANS Incident Response, Threat Hunting and Digital Forensics vous apprend à :

- Traquer l'adversaire avant et pendant un incident dans toute l'entreprise
- Acquérir des connaissances inforensiques approfondies sur les systèmes d'exploitation Microsoft Windows, Linux et Apple OSX
- Examiner smartphones et dispositifs mobiles pour y repérer les logiciels malveillants et les artefacts forensiques
- Intégrer l'inforensique réseau à vos enquêtes pour obtenir plus rapidement de meilleurs résultats
- Ne négliger aucun détail en intégrant l'analyse des mémoires dans vos enquêtes
- Trier, conserver, configurer et examiner de nouvelles sources de preuve propres au cloud et les intégrer dans vos enquêtes
- Comprendre les capacités des logiciels malveillants pour en tirer des renseignements sur les menaces, réagir aux incidents de cybersécurité et fortifier les défenses
- Identifier, extraire, hiérarchiser et exploiter le renseignement d'intérêt cyber provenant d'intrusions persistantes et avancées (APT)
- Apprécier qu'un chargé de réponse aux incidents bien formé puisse s'avérer le seul rempart de l'entreprise en cas de compromission
- Identifier, collecter, préserver les données et répondre à un incident sur une large gamme de dispositifs de stockage en garantissant l'intégrité incontestable des éléments de preuves
- Vous confronter aux spécificités des ransomwares pour vous y préparer, les détecter, les débusquer, y répondre et gérer l'après
- Rechercher des renseignements sur les menaces dans les bas-fonds de la cyberdélinquance à l'aide de techniques de collecte de renseignement d'origine humaine (ROHUM) et d'outils d'analyse de blockchain pour remonter les transactions criminelles en cryptomonnaies

« Cette formation est indispensable ! Les outils et les compétences qu'on y acquiert sont vraiment excellents ! »

— James Tayler, **Context Information Security**

Fonctions de recherche de compromission et réponse aux incidents :

- Threat hunter
- Analyste inforensique
- Analyste de logiciels malveillants
- Analyste en sécurité cloud
- Chargé de réponse aux incidents
- Analyste spécialiste de l'exploitation des médias
- Analyste du renseignement sur les menaces
- Professionnel des forces de l'ordre

FOR498: **Digital Acquisition and Rapid Triage™**

GBFA
Battlefield Forensics and Acquisition
giac.org/gbfa

6 jours	36 crédits CPE	34 labos

Vous apprendrez à...

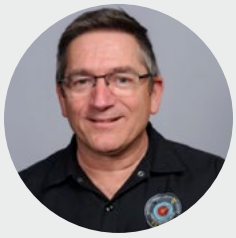
- Maîtriser les outils, techniques et procédures de localisation, d'identification et de collecte efficaces des données, où qu'elles se trouvent
- Gérer et traiter une scène de crime pour préserver l'intégrité de la preuve
- Réaliser les acquisitions de données sur des stockages au repos, notamment des disques mécaniques et à semiconducteurs (SSD)
- Identifier les nombreux emplacements susceptibles d'accueillir les données d'une enquête
- Mener une analyse inforensique de terrain en partant de la saisie des éléments de preuve jusqu'à l'exploitation des renseignements en 90 minutes ou moins
- Participer à la préparation de la documentation nécessaire à la communication avec des entités en ligne telles que Google, Facebook, Microsoft, etc.
- Comprendre les concepts et l'usage des technologies de stockage de grand volume, notamment les stockages JBOD ou RAID, les dispositifs NAS et d'autres stockages réseau adressables
- Identifier et collecter des données utilisateur dans des environnements de grande entreprise où les accès se font par le protocole SMB
- Recueillir les données volatiles comme la mémoire vive d'un système informatique
- Récupérer et conserver dans les règles de l'art les preuves numériques sur les appareils portables, cellulaires et autres

Public visé :

- Agents fédéraux et des forces de l'ordre
- Premiers intervenants
- Analystes inforensiques
- Professionnels de la cybersécurité
- Équipes de réponse aux incidents
- Analystes spécialistes de l'exploitation des médias
- Personnels du ministère de la Défense et professionnels du renseignement
- Tout profil système d'information, sécurité des informations ou informatique souhaitant acquérir une compréhension de la conservation des systèmes dans les règles de l'art

Fonctions du référentiel NICE

- Cyber Crime Investigator (OPM 221)
- Cyber Defense Forensics Analyst (OPM 212)



Kevin Ripa
Auteur de la formation

Eric Zimmerman
Auteur de la formation

L'heure tourne. Vous devez classer par priorité les preuves les plus précieuses pour traitement. Nous vous montrons comment faire !

FOR498™, formation à l'acquisition de données inforensiques, vous apporte les compétences nécessaires pour identifier les supports de stockage nombreux et variés utilisés actuellement, et pour collecter et conserver les données selon les règles de l'informatique légale, quels que soient le mode et l'emplacement de stockage. Elle couvre l'acquisition numérique à partir d'ordinateurs, de dispositifs portables, de réseaux et du cloud. Elle apprend aux stagiaires à trier rapidement, l'art et la manière de repérer et d'extraire rapidement des renseignements exploitables sur un disque dur, en moins de 90 minutes.

À l'issue de FOR498, vous saurez :

- Acquérir avec efficacité les données des sources suivantes :
  - ordinateurs PC, Microsoft Surface et Tablet PC
  - appareils Apple, Mac et MacBook
  - mémoire vive (RAM)
  - smartphones et appareils mobiles portables
  - stockage et services cloud
  - stockages réseau
  - environnements de machines virtuelles
- Produire des renseignements exploitables en 90 minutes ou moins

Programme

SECTION 1 : Préparation et gestion de la scène d'infraction, et interfaces de stockage
SECTION 2 : Appareils portables et processus d'acquisition
SECTION 3 : Tri et acquisition de données
SECTION 4 : Acquisition non traditionnelle et cloud
SECTION 5 : Acquisition pour Apple et l'internet des objets
SECTION 6 : Plongée au-delà des outils forensiques

« FOR498 fournit des bases solides d'acquisition et de tri des preuves à l'analyste inforensique débutant ! Les labos apportent des occasions nombreuses et variées de s'attaquer à des scénarios d'acquisition de données, du plus simple au plus complexe. »

— Chris G., **administration fédérale américaine**

« Dans le domaine DFIR, les choses se passent rarement comme prévu. Cette formation nous enseigne les approches pour garder le contrôle quand les choses prennent une tournure inattendue. »

— J-Michael Roberts, **Corvus Forensics**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR498**

MODES DE FORMATION DE FOR498

In-Person **Live Online** **OnDemand**

FOR500: **Windows Forensic Analysis™**

MISE À JOUR MAJEURE

GCFE Forensic Examiner
giac.org/gcfe

ANAB ACCREDITED ISO/IEC 17024 PERSONNEL CERTIFICATION BODY
CyberLive
DoD 8140*

6 jours	36 crédits CPE	22 labos

Vous apprendrez à...

- Mener une analyse post-incident poussée des systèmes d'exploitation Windows et de l'exploitation des médias
- Identifier les emplacements des artefacts forensiques et des preuves pour répondre aux questions cruciales
- Développer vos capacités d'analyse indépendamment des outils
- Extraire les constatations critiques et développer une capacité inforensique interne
- Établir des techniques analytiques structurées pour remplir aux mieux les missions des postes en sécurité

Public visé :

- Professionnels de la sécurité des informations qui veulent s'approprier les concepts des enquêtes d'informatique légale pour Windows
- Équipes de réponse aux incidents qui doivent utiliser des techniques pointues d'inforensique pour traiter leurs dossiers d'intrusion et de fuite de données dans les environnements Windows, évaluer les dégâts et développer des indicateurs de compromission
- Agents des forces de l'ordre, de l'administration fédérale et enquêteurs qui souhaitent acquérir une expertise d'enquête sur l'inforensique des systèmes d'exploitation Windows
- Analystes spécialistes de l'exploitation des médias qui doivent maîtriser l'exploitation tactique et celles des documents et supports (DOMEX)
- Tout profil système d'information, sécurité des informations ou informatique souhaitant acquérir une compréhension approfondie de l'inforensique pour Windows

Fonctions du référentiel NICE

- Cyber Crime Investigator (OPM 221)
- Cyber Defense Forensics Analyst (OPM 212)
- Law Enforcement/Counter Intelligence Forensics Analyst (OPM211)

Heather Barnhart
Conceptrice de la formation

Rob Lee
Auteur de la formation

Mattia Epifani
Auteur de la formation

Ovie Carroll
Auteur de la formation

* DoD 8140 APPROVED
sans.org/8140

Maîtrisez l'inforensique pour Windows – on ne protège bien que ce que l'on connaît

FOR500: Windows Forensic Analysis™ vise à inculquer une connaissance inforensique approfondie des systèmes d'exploitation Microsoft Windows. On ne protège bien que ce que l'on connaît. De ce fait, la compréhension des capacités et des artefacts inforensiques disponibles est une composante essentielle de la sécurité de l'information. Les stagiaires apprennent à récupérer, analyser et authentifier des données d'inforensique sur les systèmes Windows, à suivre les activités d'un utilisateur sur un réseau et à restituer leurs observations pour une utilisation future telle que gestion des réponses aux incidents, enquêtes internes, investigations sur un vol de propriété intellectuelle et contentieux civil ou criminel. Ils sauront valider les outils de sécurité, améliorer les évaluations des vulnérabilités, identifier les menaces internes, suivre les hackers et améliorer leurs politiques de sécurité. Vous l'ignorez peut-être, mais Windows enregistre discrètement une quantité incroyable de données sur les utilisateurs. FOR500™ vous apprend à exploiter cette source de données et à l'utiliser pour vos propres desseins.

Bilan

- Vous bâtissez une capacité d'informatique légale en interne pour répondre rapidement aux questions métier importantes et enquêter.
- Vous utilisez des techniques pointues d'inforensique pour traiter les dossiers de violation de données dans les environnements Windows.
- Vous comprenez toute la richesse de la télémétrie disponible sous Windows Enterprise.
- Vous savez repérer les emplacements des artefacts forensiques et des preuves pour répondre aux questions cruciales.
- Vous disposez d'une installation de labo inforensique préfabriquée à l'aide d'une palette d'outils gratuits, open source et commerciaux.
- Vous construisez des capacités d'enquête indépendantes des outils, car axées sur les techniques d'analyse.

Programme

SECTION 1 : Inforensique et tri avancé des données
SECTION 2 : Analyse du registre, exécution d'applications et inforensique du stockage cloud
SECTION 3 : Éléments d'interpréteur de commandes et profilage d'appareils amovibles
SECTION 4 : Analyse des emails, recherche Windows, surveillance de l'utilisation des ressources système (SRUM) et journaux d'événements
SECTION 5 : Analyse inforensique de navigateurs web
SECTION 6 : Défi d'inforensique Windows

« C'est une formation particulièrement intense au contenu pédagogique totalement actuel et, d'après mon expérience, introuvable ailleurs. »

— Alexander Applegate, **université d'Auburn**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR500**

MODES DE FORMATION DE FOR500

In-Person **Live Online** **OnDemand**

FOR508: **Advanced Incident Response, Threat Hunting, and Digital Forensics™** MISE À JOUR MAJEURE

GCFA Forensic Analyst giac.org/gcfa — CyberLive DoD 8140*

6 jours	36 crédits CPE	+35 labos

Vous apprendrez à...

- Maîtriser les outils et techniques de détection, de confinement et de remédiation des attaques
- Détecter des malwares actifs, dormants et personnalisés dans l'ensemble des systèmes Windows d'entreprise
- Traquer les menaces et répondre aux incidents à grande échelle
- Identifier le signal sortant *beaconing* de malwares, le mouvement latéral et l'activité C2 grâce à l'analyse de mémoire et à l'inforensique d'hôtes Windows
- Analyser les violations pour en déterminer la cause première, les vecteurs d'attaque et les mécanismes de persistance
- Contrer les techniques antiforensiques, récupérer les données effacées et suivre l'activité de l'attaquant
- Utiliser des outils forensiques pour éliminer les menaces et sécuriser l'entreprise

Public visé :

- Équipes de réponse aux incidents
- Threat hunters
- Analystes de centre des opérations de sécurité (SOC)
- Analystes inforensiques séniors
- Professionnels de la cybersécurité
- Agents fédéraux et des forces de l'ordre
- Membres de red team, experts en tests d'intrusion, développeurs d'exploits
- Stagiaires ayant réussi FOR500 et SEC504 et qui veulent monter en compétences

Fonctions du référentiel NICE

- Cyber Defense Incident Responder (OPM 531)
- All Source-Collection Manager (OPM 311)
- All Source-Collection Requirements Manager (OPM 312)
- Cyber Operator (OPM 321)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement/CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

Steve Anson
Auteur de la formation

Mike Pilkington
Auteur de la formation

*DoD 8140 APPROVED
sans.org/8140

Les tactiques et procédures de recherche de compromission et de réponse aux incidents ne cessent d'évoluer. Votre équipe ne peut plus se contenter d'anciennes techniques qui identifient mal les systèmes compromis, qui confinent mal la violation et qui, finalement, n'arrivent pas à remédier rapidement à l'incident ou à contenir la propagation du ransomware. Essentielles pour identifier et observer les signaux de présence de logiciels malveillants et les schémas d'activité, ces équipes de réponse aux incidents et de threat hunting alimentent le renseignement d'intérêt cyber, qui sert ensuite à détecter les intrusions en cours et à venir. Notre formation approfondie de réponse aux incidents et de recherche de compromission accompagne leur montée en compétences pour qu'elles sachent traquer, identifier et contrer un large spectre de menaces à l'intérieur des réseaux d'entreprise (incluant des APT d'adversaires étatiques, de syndicats du crime organisé, de groupes de ransomware ou de militants hacktivistes) et y répondre.

Bilan

- Compréhension du « métier » de pirate pour mener des évaluations de compromission en amont.
- Mise à niveau des capacités de détection.
- Développement du renseignement sur les menaces pour remonter la piste des adversaires cibles et se préparer aux prochains événements d'intrusion.
- Acquisition de compétences forensiques avancées visant à contrer les tactiques antiforensiques.

Programme

SECTION 1 : Recherche de compromission et réponse aux incidents avancées

SECTION 2 : Analyse d'intrusion

SECTION 3 : Analyse inforensique de mémoire dans la réponse aux incidents et la recherche de compromission

SECTION 4 : Analyse de la chronologie

SECTION 5 : Réponse aux incidents et recherche de compromission dans toute l'entreprise | Détection avancée des adversaires et des tactiques antiforensiques

SECTION 6 : Défi de réponse à incident d'un groupe APT

« Quelle richesse de contenu ! Je peux enfin aller au bout des choses et en comprendre d'autres, mystérieuses depuis longtemps. La formation FOR508 rend facile à comprendre ce qui est compliqué, mais en laisse encore davantage à explorer. Je l'adore. »

— Zachary T., **administration fédérale américaine**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR508**

MODES DE FORMATION DE FOR508

In-Person **Live Online** **OnDemand**

FOR509: **Enterprise Cloud Forensics and Incident Response™** MISE À JOUR MAJEURE

GCFR Cloud Forensics Responder
giac.org/gcfr
CyberLive

6 jours	36 crédits CPE	22 labos

Vous apprendrez à...

- Comprendre les données d'inforensique disponibles uniquement dans le cloud
- Mettre en œuvre les bonnes pratiques de journalisation du cloud pour les DFIR
- Collecter des preuves avec les ressources Microsoft Azure, AWS et Google Cloud Platform
- Comprendre les journaux que les analystes doivent examiner dans Microsoft 365 et Google Workspace
- Migrer vos processus inforensiques dans le cloud pour traiter plus rapidement les données

Public visé :

- Équipes de réponse aux incidents
- Threat hunters
- Analystes SOC
- Analystes inforensiques séniors
- Professionnels de la cybersécurité
- Agents fédéraux et des forces de l'ordre
- Stagiaires ayant validé FOR500, FOR508, SEC541 et SEC504 qui cherchent à ajouter l'inforensique cloud à leurs compétences

Fonctions du référentiel NICE

- Cyber Defense Incident Responder (OPM 531)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement/CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

David Cowen
Auteur de la formation

Pierre Lidome
Auteur de la formation

Josh Lemon
Auteur de la formation

Megan Roddie-Fonseca
Conceptrice de la formation

De l'orage dans le cloud

Le monde évolue et, avec lui, les données nécessaires aux investigations. Dans les plateformes cloud, le stockage des données et l'accès à celles-ci sont différents : les enquêteurs n'ont plus la possibilité d'accéder directement aux données ni d'extraire celles-ci par des méthodes classiques. Malheureusement, beaucoup essaient encore d'imposer aux hébergements cloud les méthodes traditionnelles d'analyse sur site. Au lieu de résister au changement, ils doivent apprendre à envisager les nouvelles opportunités qui se présentent à eux sous forme de nouvelles sources de preuve. FOR509: Enterprise Cloud Forensics and Incident Response™ répond au besoin actuel de montée en compétence vis-à-vis des environnements cloud d'entreprise à l'évolution rapide en faisant émerger des sources de preuve propres au cloud.

Bilan

- Appréhension de l'inforensique et de la réponse aux incidents dans le cloud.
- Identification des activités malveillantes dans le cloud.
- Recours économique aux outils et services cloud natifs du DFIR.
- Assurance d'une préparation adéquate des métiers à la réponse aux incidents cloud.
- Réduction de la durée de présence d'un adversaire dans les déploiements cloud compromis.

Programme

SECTION 1 : Microsoft 365 et Graph API

SECTION 2 : Microsoft Azure

SECTION 3 : Amazon Web Services (AWS)

SECTION 4 : Google Workspace

SECTION 5 : Google Cloud

SECTION 6 : Défi d'intrusion multicloud

« Cette formation est une excellente introduction très dense aux différents fournisseurs de services cloud et aux possibilités forensiques. »

—Marc Stroebel, **HvS-Consulting AG**

« FOR509 est absolument fantastique ! La somme de connaissances est sans pareil. À mon avis, cette formation va devenir très demandée. »

— Terrie Myerchin, **AT&T**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR509**

MODES DE FORMATION DE FOR509

In-Person **Live Online** **OnDemand**

FOR518: **Mac and iOS Forensic Analysis and Incident Response™** MISE À JOUR MAJEURE

GIME
iOS and macOS Examiner
giac.org/gime

6 jours | 36 crédits CPE | 23 labos

Vous apprendrez à...

- Comprendre les nuances entre les appareils macOS et iOS
- Plonger dans les secrets de la symbiose Apple entre les appareils et l'intérêt de ce fonctionnement dans les enquêtes
- Déterminer l'importance de chaque domaine de système de fichiers et de l'organisation des données
- Mener une analyse temporelle sur un système en corrélant les fichiers de données et les analyses de journeaux (log)
- Profiler l'utilisation des systèmes par des individus : fréquence d'utilisation, applications utilisées, préférences système personnelles, etc.
- Identifier les sauvegardes de données locales ou à distance, les images disque et les autres appareils rattachés
- Trouver les conteneurs chiffrés et des volumes FileVault, comprendre les données des trousseaux et contourner les mots de passe Mac
- Analyser et comprendre les métadonnées macOS et leur importance dans la base de données Spotlight, Time Machine et les attributs étendus
- Développer une connaissance approfondie du navigateur Safari, d'Apple Mail et de nombreuses autres applications en vous intéressant aux bases de données internes

Public visé :

- Analystes inforensiques séniors
- Représentants des forces de l'ordre, agents fédéraux et enquêteurs
- Analystes spécialistes de l'exploitation des médias
- Équipes de réponse aux incidents
- Professionnels de la cybersécurité
- Stagiaires ayant validé FOR500, FOR508, FOR526, FOR585 et FOR610 qui souhaitent parfaire leur expertise numérique

Fonctions du référentiel NICE

- Cyber Defense Incident Responder (OPM 531)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement /CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

Sarah Edwards
Conceptrice de la formation

FOR518™ est la première formation indépendante à l'inforensique et à la réponse à incident dans les environnements Mac et iOS. Elle propose aux stagiaires de s'intéresser aux données brutes, à l'analyse détaillée et en profondeur, et aux moyens de valoriser au maximum leurs incidents Mac ou iOS. Les compétences pratiques et approfondies en expertise numérique et en réponse à incident enseignées ici permettent aux analystes d'élargir leurs capacités, et de gagner la confiance et les connaissances pour analyser sans difficulté les systèmes Mac ou iOS.

Bilan

- Des employés armés pour enquêter sur différents délits comme l'utilisation abusive de l'informatique, les intrusions malveillantes sur les appareils, l'espionnage commercial, les menaces internes, et la fraude.
- Connaissance des modes de stockage des différentes données Apple et des méthodes d'analyse agnostiques sans recours à de coûteux outils inforensiques commerciaux.
- Identification des différents artefacts inforensiques et des nuances entre les plateformes Apple (macOS et iOS).
- Compréhension de la richesse des informations sur les utilisateurs qui indiquent l'utilisation normale ou frauduleuse d'un appareil.
- Connaissance des différences entre l'inforensique et les évaluations de sécurité en cas d'implication d'appareil Apple par rapport aux autres systèmes d'exploitation.

Programme

SECTION 1 : Fondamentaux iOS et Mac

SECTION 2 : Analyse de journaux, données des utilisateurs et configuration système

SECTION 3 : Système de fichiers et artefacts afférents

SECTION 4 : Analyse des données d'applications

SECTION 5 : Sujets d'analyse avancée

SECTION 6 : Défi d'inforensique et de réponse aux incidents en environnement Mac

« C'est très intéressant d'apprendre que si certains outils forensiques signalent les données comme chiffrées, il reste néanmoins possible de récupérer d'autres informations. »

— Gary Titus, **Stroz Friedberg LLC**

« C'est la formation Mac la plus complète que j'aie jamais suivie. »

— Daniel M., **agence fédérale américaine**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR518**

MODES DE FORMATION DE FOR518

In-Person | **Live Online** | **OnDemand**

ZOOM NOUVELLE FORMATION

FOR528: **Ransomware and Cyber Extortion™**

4 jours	24 crédits CPE	13 labos

Vous saurez

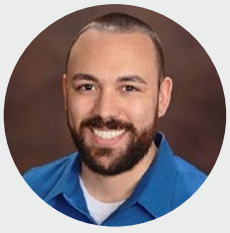
- Comment le ransomware est devenu une industrie majeure
- Comment les opérateurs de ransomwares pilotés (HumOR) se sont mués en équipes d'attaque bien huilées
- Qui et quelles organisations risquent le plus de subir une attaque par ransomware
- Comment les opérateurs de ransomware pénètrent dans l'environnement de leur victime
- Comment réagir quand un ransomware est actif dans votre environnement
- Quelles mesures prendre à la suite d'une attaque par ransomware
- Comment préparer au mieux votre organisation aux menaces HumOR
- Comment repérer les outils courants des opérateurs HumOR pour s'introduire dans un système et mener leurs activités de post-exploitation
- Quelles sont les différences entre des campagnes de ransomware et de cyberextorsion
- Comment traquer les opérateurs de ransomware sur votre réseau
- Comment repérer l'accès aux données et l'exfiltration de celles-ci

Public visé :

- Professionnels de la cybersécurité
- Équipes de réponse aux incidents
- Analystes de tri d'incidents
- Analystes de prestataire d'infogérance (MSP) ou de fournisseur de services de sécurité gérés (MSSP)
- Représentants des forces de l'ordre, agents fédéraux et enquêteurs
- Équipes IT de la santé et de l'hôtellerie
- Toute personne souhaitant approfondir sa compréhension de la réponse aux incidents de ransomware

Fonctions du référentiel NICE

- Cyber Defense Incident Responder (OPM 531)
- Cyber Operator (OPM 321)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement /CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)



Ryan Chapman
Auteur de la formation

Apprenez à déjouer les menaces d'un ransomware piloté par l'attaquant !

FOR528™ dispense une formation pratique indispensable à qui pourrait avoir à répondre à des incidents de ransomware. Dit aussi « rançongiciel », ce terme ne fait plus uniquement référence à un simple dispositif de chiffrement qui séquestre les ressources. L'avènement du ransomware piloté (HumOR) et sur abonnement (RaaS) a créé tout un écosystème prospère de campagnes d'attaques bien planifiées qu'il suffit de guider au clavier. Notre formation s'appuie sur d'ingénieuses attaques réelles et leurs traces, les artefacts inforensiques, pour donner à l'analyste que vous êtes tout ce qu'il vous faut pour réagir quand la menace devient réalité.

Bilan

- Des défenses renforcées grâce à des mesures de prévention visant à empêcher que des attaquants par ransomware n'accèdent à votre organisation.
- Détection rapide d'une attaque par ransomware qui parvient à accéder à votre environnement et qui exploite les outils courants des pirates.
- Compréhension de l'aspect que revêtent les attaques par ransomware pour nourrir un plan de réponse après détection sur le réseau.
- Réponse rapide grâce à la compréhension des priorités propres à votre environnement.
- Identification des sauvegardes à restaurer pour assurer la réussite de la procédure et éviter de réinstaurer un environnement où la menace conserverait son accès.
- Mise au jour des liens d'affiliation d'un acteur identifié dans votre environnement avec un groupe de ransomware.
- Identification des données susceptibles d'avoir été affectées, des modes d'accès et de la temporalité.
- Identification des données potentiellement exfiltrées par l'attaquant.
- Cette formation vous prépare à la certification GWEB, qui satisfait les critères DoD8140 IAT niveau 2.

Programme

SECTION 1 : Les bases de la réponse à incident de ransomware

SECTION 2 : Mode opératoire des ransomwares

SECTION 3 : Concepts avancés des ransomwares

SECTION 4 : Défi de la réponse à incident de ransomware

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR528**

MODES DE FORMATION DE FOR528

In-Person **Live Online** **OnDemand**

FOR572: **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response™** MISE À JOUR MAJEURE

GNFA Network Forensic Analyst | CyberLive
giac.org/gnfa

6 jours	36 crédits CPE	18 labos

Vous apprendrez à...

- Extraire des fichiers à partir de paquets réseau capturés et de fichiers de cache proxy pour procéder à l'analyse subséquente des malwares ou établir la perte de données définitive
- Utiliser les données historiques de NetFlow pour identifier les occurrences de réseau antérieures pertinentes et mesurer précisément la portée de l'incident
- Effectuer la rétro-ingénierie des protocoles réseau personnalisés pour identifier les capacités et les actions de commande et de contrôle d'un attaquant
- Déchiffrer le trafic SSL/TLS capturé pour identifier les actions des attaquants et les données dérobées à la victime
- Utiliser les données des protocoles de réseau typiques pour augmenter la fidélité des résultats de l'enquête
- Identifier les opportunités de collecte de preuves supplémentaires en fonction des systèmes et plateformes d'une architecture de réseau
- Examiner le trafic en utilisant des protocoles de réseau courants pour identifier des formes d'activité ou des actions spécifiques justifiant une enquête plus approfondie
- Intégrer les données de journalisation à un processus d'analyse complète pour combler des lacunes qui peuvent dater
- Mettre au jour comment les pirates utilisent des outils d'interception lors de communications apparemment sécurisées

Public visé :

- Équipes de réponse aux incidents
- Membres d'une *Hunt Team*
- Représentants des forces de l'ordre, agents fédéraux et enquêteurs
- Professionnels de la cybersécurité et personnel de centre des opérations de sécurité (SOC)
- Défenseurs de réseau
- Chargés de la sécurité des systèmes d'information
- Ingénieurs réseau
- Professionnels des technologies de l'information

Fonctions du référentiel NICE

- Cyber Defense Incident Responder (OPM 531)
- Cyber Operator (OPM 321)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement /CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

Philip Hagen
Auteur de la formation

Appliquez vos connaissances en inforensique système au réseau. Intégrez des preuves issues du réseau dans vos enquêtes, produisez de meilleures conclusions et effectuez le travail plus rapidement.

Que vous preniez en charge un incident d'intrusion, un vol de données, une utilisation à mauvais escient par les employés ou que vous participiez à une découverte proactive d'adversaires, le réseau offre souvent une vision sans pareille de l'incident. La formation FOR572™ de SANS couvre les outils, la technologie et les processus nécessaires à l'intégration des sources de preuves réseau dans vos enquêtes afin d'améliorer vos constatations et d'accélérer le travail.

Elle se concentre sur les connaissances nécessaires à l'examen et à la caractérisation des communications passées ou toujours d'actualité. Même si l'attaquant distant le plus qualifié parvient à compromettre un système avec un exploit indétectable, ce système doit encore communiquer sur le réseau. Sans canaux de commande et de contrôle et d'extraction de données, la valeur d'un système informatique compromis est presque nulle. Autrement dit, les adversaires parlent, et nous vous apprendrons à écouter.

Bilan

- Des investigations complétées des perspectives réseau propres à tous les environnements.
- Des bases de référence utilisables pour identifier par anticipation une activité malveillante, peu après la compromission et avant tout dégât à grande échelle.
- Valorisation supplémentaire des données réseau collectées et déjà utilisées pour des besoins opérationnels.
- Assurance que les observations critiques issues du réseau ne sont pas omises dans la recherche proactive de compromission ou les actions de réponse post-incident.

Programme

SECTION 1 : Du disque au câble

SECTION 2 : Principaux protocoles et agrégation/analyse des journaux

SECTION 3 : NetFlow et protocoles d'accès aux fichiers

SECTION 4 : Outils commerciaux, réseau sans fil, et recherche dans l'ensemble des paquets réseau

SECTION 5 : Chiffrement, rétro-ingénierie de protocole, sécurité opérationnelle, et renseignement

SECTION 6 : Défi final d'inforensique réseau

« Phil est probablement un des meilleurs instructeurs qu'il m'ait été donné de suivre. Compétent, intelligent, avec une connaissance riche et pertinente du secteur dans laquelle il sait piocher pour ses cours, et qui sait susciter l'intérêt pour le sujet. »

— Ronald B.

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR572**

MODES DE FORMATION DE FOR572

In-Person | **Live Online** | **OnDemand**

ZOOM NOUVELLE FORMATION

FOR577: **Linux Incident Response and Threat Hunting™**

GLIR
Linux Incident Responder
giac.org/glir

6	36	26
jours	crédits CPE	labos

Vous apprendrez à...

- Utiliser les outils, techniques et procédures nécessaires pour traquer, détecter et contenir toute une variété d'adversaires et pour répondre à des incidents
- Traquer les incidents à travers les systèmes Linux et y répondre à l'aide de la station de travail SIFT
- Identifier et suivre le signal sortant *beaconing* des logiciels malveillants vers leur canal de commande et de contrôle (C2) grâce à des techniques d'analyse
- Déterminer le déroulement d'une brèche en identifiant la pointe de l'attaque et les mécanismes d'hameçonnage ciblé (spear-phishing)
- Suivre l'activité de l'utilisateur et de l'attaquant à la seconde sur le système que vous analysez grâce à l'analyse chronologique approfondie et super-timeline
- Identifier les déplacements latéraux et les rebonds dans votre entreprise et mettre en lumière le passage d'un système à l'autre par les intrus sans vous faire repérer
- Suivre les mouvements des données à mesure que les attaquants collectent les données critiques et les acheminent vers des points de collecte pour exfiltration
- Récupérer et analyser des archives et des fichiers d'archives (.rar, .tar, etc.) utilisés par des attaquants de type APT pour exfiltrer les données sensibles depuis le réseau de l'entreprise
- Utiliser les données collectées pour mener une remédiation efficace sur l'ensemble de l'entreprise

Public visé :

- Équipes de réponse aux incidents
- Threat hunters
- Analystes inforensiques séniors
- Analystes chevronnés de centre des opérations de sécurité (SOC)
- Professionnels de la cybersécurité
- Agents fédéraux et des forces de l'ordre
- Membres de red team
- Experts en tests d'intrusion
- Développeurs d'exploits
- Stagiaires ayant validé SEC401, SEC450, SEC504 et SEC500 qui veulent monter en compétences
- Stagiaires ayant validé SEC508 qui veulent adapter leurs compétences à un autre système d'exploitation

Tarot (Taz) Wake
Auteur de la formation

La formation FOR577™ permet aux équipes de réponse aux incidents et de recherche de compromission de monter en compétences pour traquer, identifier et contrer un large spectre de menaces à l'intérieur des réseaux d'entreprise – des menaces persistantes et avancées (APT) d'États-nations hostiles aux syndicats du crime organisé et d'hacktivistes – et mener la reprise d'activité. Constamment mise à jour, elle fournit, pour répondre aux incidents d'aujourd'hui et rechercher les compromissions, des tactiques et techniques pratiques que l'élite des professionnels utilise quotidiennement dans sa lutte contre les violations sur le terrain.

Avec FOR577™, vous acquérez les compétences pour identifier et analyser les attaques et y répondre sur les plateformes Linux, mais aussi pour utiliser des techniques de recherche de compromission pour débusquer les pirates furtifs susceptibles de contourner les contrôles existants. Les notions abordées s'ancrent dans un socle commun – collecte de preuves, analyse, et prise de décision sur la base de celle-ci –, tout en se focalisant sur les caractéristiques propres à la plateforme Linux. En s'appuyant sur les outils de la station de travail SIFT de SANS, la formation apporte une solution intégrale qui permet aux chargés de réponse à incident de réagir vite et avec efficacité aux intrusions sophistiquées.

Bilan

- Compréhension du « métier » de pirate pour mener des évaluations de compromission en amont.
- Améliorations notables des capacités de détection grâce à une meilleure compréhension des nouvelles techniques d'attaque et des artefacts forensiques disponibles, et grâce à une approche axée sur les chemins d'attaque critiques.
- Développement du renseignement sur les menaces pour remonter la piste des adversaires cibles et se préparer aux prochains événements d'intrusion.
- Acquisition de compétences forensiques avancées visant à contrer les tactiques antiforensiques et l'escamotage des données aux yeux des experts techniques dans le cadre d'enquêtes internes ou externes.

Programme

SECTION 1 : Réponse aux incidents sous Linux et analyse

SECTION 2 : Analyse de disques et collecte de preuves

SECTION 3 : Journalisation Linux et analyse des journaux

SECTION 4 : Réponse en direct et données volatiles

SECTION 5 : Techniques avancées de réponse aux incidents

SECTION 6 : Défi de réponse à incident d'un groupe APT

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR577**

MODES DE FORMATION DE FOR577

In-Person **Live Online** **OnDemand**

FOR578: **Cyber Threat Intelligence™**

GCTI Cyber Threat Intelligence giac.org/gcti — DoD 8140*

6 jours	36 crédits CPE	24 labos

Vous apprendrez à...

- Développer des compétences d'analyse pour mieux appréhender, synthétiser et exploiter des scénarios complexes
- Identifier et créer des critères de renseignement grâce à des pratiques comme la modélisation de menace
- Maîtriser et développer des compétences en renseignement sur les menaces aux niveaux tactiques, opérationnels et stratégiques
- Générer des renseignements pour détecter des menaces précises, y répondre et les contrecarrer
- Identifier les différentes sources pour collecter les données sur l'adversaire et les exploiter à votre avantage
- Valider des informations de provenance extérieure pour réduire les dépenses liées aux mauvais renseignements

Public visé :

- Professionnels de la sécurité
- Équipes de réponse aux incidents
- Threat hunters
- Professionnels de la cybersécurité et personnel de centre des opérations de sécurité
- Analystes inforensiques et de logiciels malveillants
- Agents fédéraux et des forces de l'ordre
- Responsables techniques

Fonctions du référentiel NICE

- Data Analyst (OPM 422)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Incident Responder (OPM 531)
- Threat/Warning Analyst (OPM 141)
- All-Source Analyst (OPM 111)
- Mission Assessment Specialist (OPM 112)
- Target Network Analyst (OPM 132)
- All Source-Collection Manager (OPM 311)
- All Source-Collection Requirements Manager (OPM 312)
- Cyber Intel Planner (OPM 331)
- Partner Integration Planner (OPM 333)
- Cyber Operator (OPM 321)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement /CounterIntelligence Forensics Analyst (OPM 211)

Robert M. Lee
Auteur de la formation

Rebekah Brown
Conceptrice de la formation

*DoD 8140 APPROVED
sans.org/8140

Le meilleur professeur est l'attaquant lui-même !

Le renseignement d'intérêt cyber constitue un atout majeur pour les organisations qui cherchent à actualiser leurs programmes de réponse et de détection dans un monde où les menaces persistantes et avancées sont toujours plus sophistiquées. Les logiciels malveillants ne sont que des outils : la vraie menace est humaine. Le renseignement d'intérêt cyber cherche en priorité à contrer cette menace humaine, à la fois persistante et flexible, en lui opposant des défenseurs humains outillés et entraînés. En cas d'attaque ciblée, une organisation doit disposer d'équipe de threat hunting ou de réponse aux incidents de premier ordre. Cette équipe doit en outre disposer des renseignements nécessaires pour comprendre le fonctionnement des attaquants et leur faire obstacle. FOR578™ vous permettra, à vous et à votre équipe, de développer des compétences et techniques tactiques, opérationnelles et stratégiques en renseignement d'intérêt cyber pour mieux armer vos équipes, améliorer la précision de la recherche de compromission, optimiser votre réponse aux incidents. Vous serez en outre mieux à même de sensibiliser les organisations à l'évolution des menaces.

Bilan

- Compréhension de la nature dynamique du panorama des cybermenaces et conséquences pour votre organisation.
- Mise en pratique de techniques d'analyse pour informer les dirigeants clés de la meilleure façon de se défendre, eux-mêmes et leur organisation, contre certaines menaces.
- Identification de moyens d'exploiter à moindre coût les communs numériques et outils open source en renseignement sur les menaces, et prise en main de certains des outils commerciaux disponibles à fort impact.
- Communication efficace du renseignement sur les menaces aux niveaux tactique, opérationnel et stratégique.
- Tremplin pour les autres fonctions métiers clés, notamment les opérations de sécurité, la réponse à incident et l'exploitation commerciale.

Programme

SECTION 1 : Exigences et renseignement d'intérêt cyber
SECTION 2 : Socle de compétences : analyse d'intrusion
SECTION 3 : Sources de collecte
SECTION 4 : Analyse et production du renseignement
SECTION 5 : Diffusion et attribution
SECTION 6 : Projet final

« Le renseignement d'intérêt cyber est une discipline en soi, pas seulement un flux d'informations. Cette formation est une voie rapide vers la compréhension de ce domaine d'études, qui se développe rapidement. »

— Bertha Marasky, **Verizon**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR578**

MODES DE FORMATION DE FOR578

In-Person — Live Online — OnDemand

FOR585: **Smartphone Forensic Analysis In-Depth™** MISE À JOUR MAJEURE

GASF
Advanced Smartphone Forensics
giac.org/gasf

6 jours	36 crédits CPE	22 labos

Vous apprendrez à...

- Sélectionner les outils, techniques et procédures d'inforensique les plus efficaces pour analyser efficacement les données d'un smartphone
- Reconstruire des événements relatifs à une infraction en utilisant les informations des smartphones, notamment la reconstitution chronologique et l'analyse des liens (par exemple, qui communique avec qui, où et comment)
- Comprendre comment les systèmes de fichiers d'un smartphone enregistrent les données, comment elles se distinguent et comment les preuves sont conservées sur chaque dispositif
- Interpréter les systèmes de fichiers des smartphones et localiser les informations qui ne sont généralement pas accessibles aux utilisateurs
- Repérer comment les preuves sont arrivées sur l'appareil mobile – lorsque vous saurez dire si les données ont été créées par l'utilisateur, par l'IA ou par synchronisation, vous ne commettrez plus l'erreur de signaler de faux positifs remontés par les outils
- Incorporer des techniques de décodage manuelles pour récupérer des données de smartphones non analysées
- Lier un utilisateur et un smartphone à une date ou à une heure précises et à divers endroits
- Récupérer les communications masquées ou brouillées des applications du smartphone

Public visé :

- Analystes inforensiques chevronnés
- Analystes spécialistes de l'exploitation des médias
- Professionnels de la cybersécurité
- Équipes de réponse aux incidents
- Représentants des forces de l'ordre, agents fédéraux et enquêteurs
- Accidentologues
- Chargés d'audit informatique
- Stagiaires ayant validé SEC575, FOR308, FOR498, FOR563, FOR500, FOR508, FOR572, FOR526, FOR610 ou FOR518 de SANS qui souhaitent monter en compétences

Fonctions du référentiel NICE

- Cyber Crime Investigator (OPM 221)
- Cyber Defense Forensics Analyst (OPM 212)

Heather Barnhart
Conceptrice de la formation

Domenica Crognale
Conceptrice de la formation

Dans la formation FOR585™, les enquêteurs et analystes acquièrent les compétences pour détecter, décoder, déchiffrer et interpréter correctement les preuves récupérées sur des dispositifs mobiles. Elle est actualisée en permanence pour tenir compte des nouveautés – formats de fichiers, logiciels malveillants, systèmes d'exploitation de smartphones, applications tierces, insuffisances d'acquisition, techniques d'exploitation (comment obtenir l'accès physique ou à tout le système de fichiers), et chiffrement. Elle arme les stagiaires des connaissances inforensiques les plus récentes et à nulle autre pareilles sur les dispositifs mobiles, qu'ils pourront immédiatement appliquer dans leurs missions.

Bilan

- Compréhension des artefacts Android et iOS utiles dans les enquêtes.
- Compréhension des artefacts applicatifs des appareils iOS et Android.
- Valorisation de l'utilisation des smartphones pour géolocaliser les appareils quand quelque chose se produit.
- Informations sur les utilisations d'un appareil – connexion en voiture, synchronisation des données, mains libres, montres, etc.
- Baisse du potentiel d'infection des dispositifs mobiles par des logiciels malveillants grâce à la compréhension des modes d'infection et des moyens d'enquêter sur les malwares qui les ciblent.
- Compréhension en profondeur des bases de données SQLite et de la présence d'un tas de données sur les smartphones.
- Meilleure appréhension des outils commerciaux que votre entreprise utilise et recours aux scripts gratuits fournis en formation pour combler leurs éventuelles lacunes.
- Pratique de la création de requêtes SQLite et de scripts Python à des fins d'analyse forensique.
- Prise en compte des évolutions de la technologie mobile et des tendances d'investigation grâce au groupe des anciens de la formation SANS FOR585 Alumni Community Group.

Programme

SECTION 1 : Généralités sur les smartphones, bases de l'analyse, et inforensique SQLite

SECTION 2 : Inforensique Android

SECTION 3 : Inforensique des appareils iOS

SECTION 4 : Sauvegardes et données cloud, inforensique des logiciels malveillants et espions, et détection de la destruction de preuves

SECTION 5 : Analyse d'applications tierces

SECTION 6 : Projet final d'inforensique sur smartphone

« FOR585 est une formation au contenu extrêmement pertinent, qui guide les analystes vers les artefacts cruciaux dans le cadre d'enquêtes et de validation. Elle présente les détails clés pour chaque défi inforensique. »

— Quinn L., **agence fédérale américaine**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR585**

MODES DE FORMATION DE FOR585

In-Person **Live Online** **OnDemand**

ZOOM NOUVELLE FORMATION

FOR589: **Cybercrime Investigations™**

5 jours	30 crédits CPE	20 labos

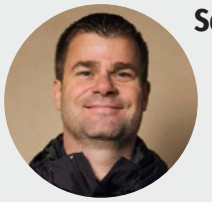
Vous apprendrez à...

- Comprendre comment les disciplines classiques de collecte de renseignements se sont adaptées aux réalités modernes axées cyber et à séparer ce qui exploitable du bruit
- Déceler, dans le cadre de vos besoins prioritaires de renseignement, les risques menaçant vos actifs et composants et liés aux auteurs et aux vecteurs des menaces
- Traduire les besoins de renseignement guidé par le risque en plans de collecte et tâches opérationnelles fondés sur les menaces
- Traiter les risques cybercriminels en fondant vos décisions sur les menaces, et déterminer ainsi vos défenses et vos réponses, et décider de protéger votre organisation ou de lancer des mesures de contre-offensive coûteuses pour les criminels
- Démystifier le monde interlope de la cybermenace pour accéder à des communautés, places de marché, sites de rançon, violations de données, journaux de malwares, etc. et les surveiller

Fonctions du référentiel NICE

- All Source-Collection Manager (OPM 311)
- All Source-Collection Requirements Manager (OPM 312)
- All-Source Analyst (OPM 111)
- Cyber Crime Investigator (OPM 221)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Forensics Analyst (OPM 212)
- Cyber Defense Incident Responder (OPM 531)
- Cyber Intel Planner (OPM 331)
- Cyber Operator (OPM 331)
- Cyber Ops Planner (OPM 332)
- Cyber Policy and Strategy Planner (OPM 752)
- Data Analyst (OPM 422)
- Exploitation Analyst (OPM 121)
- Law Enforcement/Counterintelligence Forensics Analyst (OPM 211)
- Mission Assessment Specialist (OPM 112)
- Partner Integration Planner (OPM 333)

Sean O'Connor
Auteur de la formation



Conan Beach
Auteur de la formation

Will Thomas
Auteur de la formation

Les enquêtes cybercriminelles sont indispensables à toute organisation souhaitant détecter une activité malveillante, y répondre et en attribuer la paternité, ainsi qu'aux forces de l'ordre et aux organismes publics chargés de retrouver, d'arrêter et de poursuivre les cybercriminels. FOR589: Cybercrime Investigations™ explore en profondeur le monde clandestin de la cybercriminalité mondiale, révélant les tactiques et techniques qu'utilisent les auteurs de menace pour exploiter les systèmes et rentabiliser les attaques. Cette formation mêle savoir-faire de l'enquêteur et pratiques de cybersécurité modernes pour améliorer les opérations. Que vous soyez membre de l'équipe de sécurité d'une entreprise, enquêteur des services de l'État ou juste quelqu'un qui souhaite acquérir des compétences pour pister et comprendre la cybercriminalité organisée et les menaces guettant votre organisation, cette formation va doper vos capacités.

Bilan

- Vous comblez les lacunes de connaissances en cyber- et en cryptocriminalité de vos équipes d'enquête.
- Vous consolidez vos capacités d'investigation des fraudes, de réponse aux incidents et de renseignement d'intérêt cyber (CTI) grâce à l'expertise acquise en cybercriminalité.
- Vous identifiez et réduisez les menaces cybercriminelles émergentes en enquêtant sur les auteurs avant que l'attaque s'aggrave.
- Vous bâtissez des mécanismes proactifs de détection et d'alerte en fonction de comportements délictueux.
- Vous enquêtez sur l'accès initial, le déploiement de malwares et les partenariats dans le milieu clandestin.
- Vous hiérarchisez vos pistes d'investigation selon les tendances du milieu et les mouvements des acteurs malveillants.
- Vous suivez méthodiquement les activités criminelles du début à la fin.

Public visé :

- Analystes en renseignement d'intérêt cyber (CTI)
- Professionnels du renseignement cyber
- Enquêteurs criminels
- Enquêteurs financiers
- Threat hunters
- Chargés de réponse aux cyberincidents
- Analystes inforensiques
- Professionnels de l'InfoSec
- Agents fédéraux et des forces de l'ordre
- Anciens stagiaires SANS qui veulent monter en compétences

Programme

SECTION 1 : Renseignement cybercriminel
SECTION 2 : Enquêtes sur les cryptomonnaies
SECTION 3 : Le milieu cybercriminel
SECTION 4 : Opérations sous couverture
SECTION 5 : Projet final

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR589**

MODES DE FORMATION DE FOR589

In-Person **Live Online**

FOR608: **Enterprise-Class Incident Response & Threat Hunting™**

GEIR
Enterprise Incident Responder
giac.org/geir

6 jours	36 crédits CPE	24 labos

Vous apprendrez à...

- Comprendre quand la réponse à incident doit inclure une interrogation approfondie des hôtes ou une collecte massive mais superficielle
- Déployer des plateformes de collaboration et d'analyse pour que les équipes coopèrent en même temps d'un pays, d'une région ou d'une salle à l'autre
- Collecter les données inforensiques des clouds et des hôtes dans les grands environnements
- Débattre des bonnes pratiques de réponse aux incidents sur les plateformes cloud Azure, M365 et AWS
- Utiliser les techniques d'analyse pour répondre aux incidents sur les systèmes d'exploitation Linux et Mac
- Analyser les microservices conteneurisés comme les conteneurs Docker
- Corréler et analyser les données issues de multiples machines et types de données à l'aide d'une myriade de techniques d'analyse
- Réaliser une analyse de données structurées et non structurées pour déduire un comportement d'attaquant
- Enrichir les données collectées pour repérer d'autres indicateurs de compromission (IoC)

Public visé :

Cette formation s'adresse aux professionnels de l'inforensique, de la réponse aux incidents, de la détection d'intrusion et de la recherche de compromission au sein d'entreprises moyennes à grandes, qui assurent la défense à l'échelle de l'entreprise avec toutes les complexités que cela implique.

FOR608 est une formation avancée qui fait l'impasse sur les bases élémentaires de l'inforensique réseau et des hôtes Windows et la réponse aux incidents. Si la formation n'est pas nécessairement plus technique que celles de niveau master, les bases en sont supposées acquises : ces thèmes et notions ne seront pas révisés.

Fonctions du référentiel NICE

- Cyber Defense Incident Responder (OPM 531)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement /CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

Mathias Fuchs
Auteur de la formation

Mike Pilkington
Auteur de la formation

Tarot (Taz) Wake
Auteur de la formation

FOR608™ s'intéresse à l'identification et à la réponse aux incidents trop étendus pour se focaliser sur les machines individuelles. À l'aide d'outils types de classe entreprise, les stagiaires apprennent les techniques pour collecter les données utiles à la recherche de compromission et à la réponse aux incidents. Ils s'attachent ensuite à approfondir les méthodologies d'analyse, à s'approprier diverses approches pour appréhender les déplacements et l'activité d'un assaillant sur des hôtes aux systèmes d'exploitation et fonctions hétérogènes en s'appuyant sur une gamme de techniques d'analyse.

Bilan

- Réduction de l'impact financier et réputationnel d'une violation par une gestion de la réponse plus efficace et précise.
- Techniques de gestion de réponse à incident qui optimisent l'utilisation des ressources pendant une enquête.
- Déploiement de plateformes de collaboration et d'analyse pour que les équipes coopèrent en même temps d'un pays, d'une région ou d'un service à l'autre.
- Compréhension et recherche des techniques utilisées par les attaquants pour échapper aux outils EDR et de contrôle des applications dans les systèmes Windows.
- Acquisitions des techniques d'analyse pour répondre aux incidents sur les systèmes d'exploitation Linux et macOS.
- Capacité à répondre et à analyser les microservices conteneurisés comme les conteneurs Docker.
- Discussion des bonnes pratiques de réponse pour les environnements cloud les plus courants, à savoir Microsoft365/AzureAD et AWS.

Programme

SECTION 1 : Détection proactive et réponse précoce
SECTION 2 : Dimensionnement de la réponse et analyse
SECTION 3 : Attaques modernes contre Windows, et inforensique et réponse aux incidents Linux
SECTION 4 : Analyser macOS et les conteneurs Docker
SECTION 5 : Attaques et réponse dans le cloud
SECTION 6 : Projet final : défi de réponse aux incidents de niveau entreprise

« Le traitement d'Elastic est impressionnant. Je l'utilise depuis plusieurs années, mais j'ai appris de nouvelles façons d'ingérer des données qui auraient pu m'épargner beaucoup de travail. »

— Simon H., **CyberCX**

« La formation couvre de nombreux sujets importants sur la détection et la réponse. J'ai apprécié les parties sur le renseignement axé sur les menaces et TimeSketch pour retracer la chronologie d'un incident. »

— Reggie M., **Amazon**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR608**

MODES DE FORMATION DE FOR608

In-Person **Live Online**

FOR610: **Reverse-Engineering Malware: Malware Analysis Tools & Techniques™**

GREM Reverse Engineering Malware
giac.org/grem
CyberLive
DoD 8140*

6 jours	36 crédits CPE	52 labos

Vous apprendrez à...

- Construire un environnement de laboratoire isolé et contrôlé pour analyser le code et le comportement des programmes malveillants
- Utiliser des outils de supervision du réseau et du système pour examiner la manière dont les logiciels malveillants interagissent avec le système de fichiers, le registre, le réseau et d'autres processus dans un environnement Windows
- Analyser les scripts JavaScript et PowerShell malveillants – souvent obfusqués – et fréquents dans les chaînes d'attaque
- Contrôler les aspects pertinents du comportement du programme malveillant grâce à l'interception du trafic réseau et au code patching pour effectuer une analyse efficace des malwares
- Utiliser un désassembleur et un débogueur pour examiner le fonctionnement interne des exécutables Windows malveillants
- Contourner différents outils de compression d'exécutables ou packers et d'autres mécanismes défensifs conçus par des auteurs de logiciels malveillants pour détourner l'attention de l'analyste, le tromper et le ralentir
- Reconnaître et comprendre des schémas courants au niveau de l'assembly du code malveillant, par exemple une injection de code, les interactions C2, les techniques d'injecteur et de téléchargeur, et les mesures empêchant les analyses

Public visé :

- Personnes qui traitent des incidents impliquant des malwares et souhaitent comprendre les principaux aspects des programmes malveillants
- Techniciens ayant expérimenté de manière informelle des aspects de l'analyse des malwares et cherchant à formaliser et étendre leur expertise dans ce domaine
- Analystes inforensiques et responsables IT cherchant à élargir leurs compétences pour assurer un rôle central dans le processus de réponse aux incidents

Fonctions du référentiel NICE

- Cyber Defense Incident Responder (OPM 531)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement/CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

Anuj Soni
Auteur de la formation

Lenny Zeltser
Auteur de la formation

* DoD 8140 APPROVED
sans.org/8140

Apprenez à examiner les logiciels malveillants sous toutes les coutures ! Particulièrement appréciée, cette formation aborde en profondeur les outils et techniques d'analyse de logiciels malveillants. FOR610™ permet aux enquêteurs spécialisés en inforensique, aux chargés de réponse aux incidents, aux ingénieurs sécurité et aux administrateurs informatiques de développer des compétences pratiques nécessaires pour analyser les programmes malveillants qui ciblent et infectent les systèmes Windows.

Connaître le potentiel des logiciels malveillants est un enjeu majeur pour en tirer des renseignements d'intérêt cyber, réagir aux incidents de cybersécurité et renforcer les défenses de l'entreprise. Cette formation vous permet d'acquérir des bases solides en rétro-ingénierie appliquée aux logiciels malveillants en vous familiarisant avec divers utilitaires de supervision système et réseau, un désassembleur, un débogueur et de nombreux autres outils disponibles gratuitement.

Bilan

- Des équipes capables de mener leurs analyses en interne sans recourir à une expertise externe
- Extension des capacités d'analyse de votre équipe pour augmenter la valeur offerte à vos parties prenantes internes et externes
- Meilleure efficacité des tâches d'analyse vous permettant de produire de précieux éclairages plus rapidement
- Réduction maximale du périmètre et du coût d'une éventuelle intrusion par une réponse précoce aux incidents de sécurité

Programme

SECTION 1 : Fondamentaux de l'analyse de logiciels malveillants

SECTION 2 : Rétroconception de code malveillant

SECTION 3 : Au-delà des exécutables classiques

SECTION 4 : Analyse en profondeur de logiciels malveillants

SECTION 5 : Étude de logiciels malveillants capables de s'autodéfendre

SECTION 6 : Tournoi d'analyse de logiciels malveillants

« J'ai acquis de nombreuses informations précieuses dans la formation FOR610, notamment les domaines à maîtriser pour faire mon travail. L'exercice pratique CTF m'a fait prendre conscience de l'ampleur de ce que je ne savais pas, alors : merci ! »

— Urban M., **CNF Technologies**

« Cette formation m'a permis d'affiner mes connaissances sur les techniques de malware, de comprendre comment mieux protéger les actifs et mener à bien toutes les étapes d'éradication. »

— Eric B., **Nestlé**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR610**

MODES DE FORMATION DE FOR610

In-Person **Live Online** **OnDemand**

FOR710: **Reverse-Engineering Malware: Advanced Code Analysis™**

5 jours	36 crédits CPE	12 labos

Vous apprendrez à...

- Gérer les techniques d'obfuscation, notamment la stéganographie, qui gênent l'analyse statique du code
- Identifier les principaux composants de l'exécution d'un programme pour analyser les malwares multiphases en mémoire
- Localiser et extraire le shellcode désobfusqué pendant l'exécution du programme
- Développer votre familiarité avec des formats de fichiers non exécutables pendant l'analyse de malwares
- Sonder les structures et champs associés à un en-tête PE
- Utiliser WinDbg Preview pour le débogage et l'évaluation des principales structures de données des processus en mémoire
- Repérer dans les ransomwares les algorithmes de chiffrement qui servent à chiffrer les fichiers et à protéger les clés
- Reconnaître les API Windows qui servent à chiffrer, et comprendre leur objet
- Enquêter sur l'obfuscation des données dans les logiciels malveillants, localiser précisément les implémentations d'algorithme, et décoder le contenu sous-jacent
- Écrire des scripts Python pour automatiser l'extraction et le déchiffrement de données
- Établir des règles pour identifier la fonctionnalité des malwares
- Utiliser des frameworks d'instrumentation de binaires dynamique (DBI) pour automatiser les workflows de rétro-ingénierie courants
- Écrire des scripts Python dans Ghidra pour accélérer l'analyse de code

Public visé :

- Professionnels de la cybersécurité qui veulent améliorer leurs compétences de niveau intermédiaire en rétroconception
- Ingénieurs en rétroconception qui doivent améliorer leur analyse de code obfusqués, évaluer les capacités de chiffrement dans les malwares et automatiser les tâches d'analyse

Fonctions du référentiel NICE

- Cyber Defense Incident Responder (OPM 531)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement/Counter Intelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

Anuj Soni
Auteur de la formation

Pendant qu'en défense, les professionnels affinent leurs compétences d'analyse et leurs capacités de détection automatique de malwares, les auteurs de maliciels vont toujours plus loin pour exécuter leurs programmes dans l'entreprise. C'est ainsi qu'on voit désormais des logiciels malveillants plus modulaires, avec plusieurs couches de code obfusqués qui s'exécute en mémoire pour empêcher la détection et gêner l'analyse. Les analystes doivent savoir traiter ces fonctionnalités avancées et recourir dès que possible à l'automatisation pour prendre en charge le volume, la diversité et la complexité du flot ininterrompu de malwares ciblant l'entreprise.

FOR710™, suite de la formation FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques™, aide les stagiaires de niveau intermédiaire en analyse de logiciels malveillants à franchir un cap en rétro-ingénierie. Écrite par Anuj Soni, SANS Certified Instructor, elle prépare les spécialistes des malwares à disséquer les exécutables Windows sophistiqués, ceux-là mêmes qui font la une des journaux et inquiètent les équipes de réponse aux incidents du monde entier.

Les compétences de rétro-ingénierie avancées ne s'acquièrent que par une pratique régulière. En plus des références utiles et de l'accompagnement du formateur, les stagiaires trouveront dans cette formation de nombreuses occasions de se confronter aux scénarios de rétro-ingénierie issus du terrain.

Programme

SECTION 1 : Désobfuscation et exécution de code

SECTION 2 : Chiffrement de logiciels malveillants

SECTION 3 : Automatisation de l'analyse de logiciels malveillants

SECTION 4 : Automatisation de l'analyse de logiciels malveillants (suite)

SECTION 5 : Tournois d'analyse avancée de logiciels malveillants (accès étendu)

« Les labos et les exercices d'automatisation sont excellents et montrent très clairement ce qu'il faut pour automatiser la rétroconception. »

— Daniel T., **ministère de la Justice**

« J'ai vraiment apprécié cette formation. J'ai trouvé que c'était la suite logique et adaptée de FOR610. Le contenu est dense et pertinent par rapport à ce que je vois tous les jours au travail. »

— Daniel R., **CrowdStrike**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/FOR710**

MODES DE FORMATION DE FOR710

In-Person **Live Online** **OnDemand**

AXE DE FORMATION SANS

Industrial Control Systems (ICS) Security

Le paysage actuel présente un ensemble chaotique et complexe de menaces planant sur les propriétaires et les opérateurs de systèmes de contrôle industriel.

Il ne s'agit plus de théorie ni de spéculation : les attaques causent des dommages matériels et affectent des processus physiques. Nous sommes témoins d'incidents où des intrusions malveillantes endommagent les systèmes et perturbent les opérations grâce à des malwares adaptés aux ICS. Nous devons nous tenir prêts à défendre nos systèmes de contrôle contre des adversaires toujours plus sophistiqués.

À l'issue d'une formation à la sécurité des systèmes de contrôle industriel (ICS) de SANS, vous saurez :

- Reconnaître les systèmes de contrôle industriel, leurs finalités, leurs déploiements, leurs enjeux et leurs contraintes
- Identifier les actifs des systèmes de contrôle industriel, analyser les topologies réseau, et superviser les points chauds critiques pour y détecter anomalies et menaces
- Comprendre les architectures et techniques de défense des réseaux et des systèmes
- Mener une réponse à incident ICS axée sur les opérations de sécurité, avec la sûreté et la fiabilité des opérations pour priorité
- Mettre en œuvre efficacement des contrôles d'accès physiques et numériques

« Après une introduction théorique, la formation se focalise rapidement et pleinement sur la pratique avec les différents éléments. Une expérience rare. »

— Bassem Hemida, **Deloitte**

Fonctions de sécurité des systèmes de contrôle industriel (ICS) et des technologies opérationnelles (OT) :

- Consultant en évaluation de la sécurité ICS et OT
- Ingénieur sécurité ICS
- Analyste sécurité ICS
- Ingénieur de systèmes de contrôle
- Ingénieur sécurité ICS
- Responsable sécurité ICS et OT

ZOOM NOUVELLE FORMATION

ICS310: **ICS Cybersecurity Foundations™**

1 jour	6 crédits CPE	3 labos

Vous apprendrez à...

- Maîtriser les principales mesures de sécurité pour protéger les systèmes industriels
- Connaître les référentiels IEC 62443, NIST 800-82, NIS2 et NERC CIP
- Reconnaître les termes spécialisés courants, les composants système et les différences entre opérations numériques et analogiques
- Comprendre les tendances clés, les bases des appareils, et les entrées/sorties des environnements OT (technologie opérationnelle)
- Analyser des études de cas pour voir comment les principes de l'ICS s'appliquent aux enjeux industriels réels

Bilan

- Dotez vos collaborateurs des connaissances pour identifier les composants ICS courants et implémenter des mesures de cybersécurité efficaces dans toutes vos opérations.
- Préparez vos effectifs à contrer les tactiques d'attaque en exploitant les informations des études de cas internationales et des stratégies de défense éprouvées.
- Donnez à votre équipe les moyens d'implémenter des contrôles ICS *ad hoc* qui répondent aux enjeux réglementaires et sectoriels et améliorent ainsi la résilience globale.

Public visé :

- Stagiaires novices de l'ICS
- Futurs stagiaires du cursus ICS
- Professionnels de la sécurité OT des secteurs réglementés et d'infrastructure critique
- Professionnels de la sécurité OT de secteurs non réglementés
- Professionnels côté fournisseur/intégrateur
- Quiconque travaille dans les industries d'infrastructure critique ou des ressources clés (électricité, eau, nucléaire, télécom, pétrole, gaz naturel, fabrication, chimie, chemin de fer, transports, etc.) et spécifiquement les environnements de technologie opérationnelle de ces organisations
- Personnel des armées intéressé par les environnements opérationnels, et qui utilise des actifs physiques ou fournit une assistance pour ceux-ci

Tim Conway
Auteur de la formation

Robert M. Lee
Auteur de la formation

Jeffrey Shearer
Auteur de la formation

Dans cette formation, les stagiaires commencent par développer leur compréhension des systèmes opérationnels et mécaniques, qui servira ensuite de socle pour mieux appréhender comment les opérateurs et propriétaires d'actifs ont automatisé ces environnements. Différents secteurs sont étudiés pour souligner les similitudes entre les environnements opérationnels de divers domaines et industries. Comprendre les briques et critères opérationnels communs à de nombreux secteurs permet d'éclairer les défenseurs quant aux domaines essentiels sur lesquels cibler en priorité les actions de cybersécurité basées sur le risque et qui soutiennent la mission opérationnelle plus globale.

Nous nous intéresserons à des études de cas de plusieurs secteurs et du monde entier qui montrent des événements cyber dans lesquels toute une variété de tactiques antagonistes ont été employées pour atteindre les objectifs. Ces études couvrent des attaques informatiques qui ont affecté les opérations, d'autres à base d'actions malveillantes manuelles sur des cibles opérationnelles, et d'autres encore qui visaient l'exploitation de malwares pour ICS. Leur analyse mettra au jour des leçons et des recommandations pour améliorer vos stratégies de défense, notamment des actions de défense à mener et à poursuivre en priorité.

Des secteurs sont confrontés selon leur pays à des obligations réglementaires et des normes propres, là où d'autres manquent d'accompagnement. Les praticiens et leaders en quête de contrôles de sécurité pertinents découvriront les cinq contrôles critiques ICS à adapter et à mettre en œuvre, quel que soit l'environnement.

Programme

SECTION 1 : Présentation du cursus ICS et de la place qu'ICS310 y trouve

SECTION 2 : Sujets sur les ICS et l'automatisation

SECTION 3 : Tendances et menaces ICS

SECTION 4 : Études de cas ICS et événements mondiaux

SECTION 5 : Normes et principes directeurs de cybersécurité pour les ICS

SECTION 6 : Les cinq contrôles critiques de l'ICS

Consultez le descriptif détaillé de la formation sur **SANS.ORG/ICS310**

MODES DE FORMATION DE ICS310

OnDemand

ICS410: **ICS/SCADA Security Essentials™**

GICSP
Global Industrial Cyber Security Professional
giac.org/gicsp

ANAB ACCREDITED ISO/IEC 17024 PERSONNEL CERTIFICATION BODY
CyberLive
DoD 8140*

6 jours	36 crédits CPE	15 labos

Vous apprendrez à...

- Comprendre divers systèmes de contrôle industriel, leurs finalités, leur usage, leur fonction et leur corrélation avec les IP de réseau ainsi qu'avec les communications industrielles
- Utiliser la conception des infrastructures des réseaux de contrôle (concepts d'architecture de réseau tels que la topologie, les protocoles et les composants) et faire le lien avec la norme CEI 62443 et le modèle Purdue
- Exécuter des outils de ligne de commande Windows pour repérer les éléments à risque élevé dans le système
- Exécuter des outils de ligne de commande (ps, ls, netscat, etc.) et du script basique Linux pour automatiser le fonctionnement de programmes afin de superviser en continu divers outils
- Travailler avec des systèmes d'exploitation (concepts d'administration de systèmes Unix/Linux et/ou Windows)
- Comprendre le cycle de vie de la sécurité des systèmes
- Comprendre les principes de l'assurance de l'information (confidentialité, intégrité, disponibilité, authentification, non-répudiation)
- Utiliser vos compétences en défense des réseaux pour détecter les intrusions sur les hôtes et par le réseau à l'aide d'outils de détection d'intrusion
- Implémenter les méthodologies de traitement et de réponse aux incidents
- Faire le lien entre différentes technologies, attaques et défenses d'ICS et des normes de cybersécurité comme le référentiel de cybersécurité du NIST, ISA/CEI 62443, ISO/CEI 27001, NIST SP 800-53, les contrôles de sécurité Critical Security Controls du CIS et le cadre COBIT 5

Public visé :

Formation conçue pour tout professionnel travaillant dans des environnements ICS, interagissant avec eux ou susceptible de les affecter (propriétaires d'actifs, fournisseurs, intégrateurs et toute autre tierce partie). Ils sont surtout issus de quatre domaines :

- IT (y compris l'assistance OT)
- Sécurité IT (y compris la sécurité OT)
- Ingénierie
- Normes professionnelles pour l'industrie et l'entreprise

Fonctions du référentiel NICE

- Process Control Engineer/Instrument & Control Engineer (ZZ-ICS-001)
- ICS/SCADA Security Engineer (ZZ-ICS-002)
- ICS/OT Systems Engineer (ZZ-ICS-003)
- OT SOC Operator (ZZ-ICS-004)

Justin Searle
Auteur de la formation

* DoD 8140 APPROVED
sans.org/8140

Les environnements de technologie opérationnelle (OT) sont confrontés à une déferlante de cybermenaces sophistiquées. Pourtant, beaucoup d'organisations s'appuient sur des mesures de sécurité IT mal adaptées aux enjeux distincts des systèmes de contrôle industriel (ICS) et de contrôle et d'acquisition de données en temps réel (SCADA). L'absence de connaissances spécialisées et d'expertise pratique en cybersécurité ICS expose l'infrastructure critique : le risque de perturbation opérationnelle, de perte financière et d'incidents de sécurité en est renforcé. Cette formation s'appuie sur les principes fondamentaux de la cybersécurité ICS pour faire acquérir aux professionnels des secteurs industriels les compétences avancées nécessaires à la sécurisation efficace des environnements OT. En s'intéressant aux exigences uniques des systèmes industriels, elle arme les professionnels de la cybersécurité IT et OT pour traiter les menaces émergentes, et assurer la sûreté, la sécurité et la résilience de l'infrastructure critique avec un impact opérationnel minimal.

Les secteurs de l'infrastructure critique et des ressources stratégiques sont confrontés à un panorama de menaces extrêmement dynamique où les cyberattaques peuvent désorganiser des services essentiels, compromettre la sûreté, et entraîner des dégâts économiques et opérationnels significatifs. Les professionnels qui opèrent, gèrent, conçoivent, mettent en œuvre, surveillent et défendent les systèmes de contrôle sont aux avant-postes de cette bataille. La formation est conçue spécifiquement pour ces professionnels : elle leur inculque les compétences et connaissances essentielles à la sécurisation et à la prise en charge des systèmes de contrôle dans les environnements à fort enjeu. Elle les arme pour répondre aux besoins de sécurité quotidiens de l'infrastructure critique afin d'assurer sa résilience, sa sûreté et sa continuité opérationnelle.

Programme

SECTION 1 : Généralités sur les systèmes de contrôle industriel
SECTION 2 : Architectures et processus
SECTION 3 : Communications et protocoles
SECTION 4 : Systèmes de supervision
SECTION 5 : Gouvernance de la sécurité ICS
SECTION 6 : Projet final CTF

« Cette formation est inestimable, parce que les exemples pratiques sont vraiment issus du terrain, et l'instructeur maîtrise clairement son sujet. »

— Theresa H., **Booz Allen Hamilton**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/ICS410**

MODES DE FORMATION DE ICS410

In-Person | Live Online | OnDemand

ICS418: **ICS Security Essentials for Leaders™**

2 jours	12 crédits CPE	11 labos

Vous apprendrez à...

- Exposer la valeur de la sécurité des ICS et lier les décisions sur le risque cyber à celles sur le risque global
- Repérer les tendances technologiques actuelles et à venir pour répondre aux besoins métiers
- Mesurer les réussites dans la gestion des risques cyber industriels, avec métriques pour la direction
- Utiliser les bonnes pratiques pour donner à vos équipes les moyens de détecter les incidents de sécurité ICS et d'y répondre
- Exploiter les informations externes, notamment le renseignement sur les menaces, pour dessiner les orientations de votre programme de sécurité ICS
- Fournir gouvernance, supervision, exécution et soutien dans l'ensemble des installations industrielles pour les initiatives et projets de sécurité ICS
- Appliquer à bon escient les principes de la sécurité de l'IT et des ICS pour un programme efficace de cybersécurité des systèmes de contrôle
- Développer vos effectifs en sécurité pour compenser les faiblesses en recrutement, en formation et en rétention
- Appliquer des techniques avancées pour façonner et réorienter la culture de sécurité de l'organisation

Public visé :

ICS418 s'adresse aux leaders responsables de sécuriser au quotidien des environnements ICS/OT, notamment les systèmes numériques de contrôle-commande (SNCC) et d'acquisition de données en temps réel (SCADA). Leurs profils peuvent varier :

- Profils managériaux à fort leadership et aux connaissances techniques limitées
- Profils techniques promus leaders avec peu de compétences managériales formelles
- Leaders en sécurité qui supervisent les environnements OT et ICS dans l'ensemble de l'organisation
- Chefs d'équipe chargés de mettre en œuvre des stratégies de cybersécurité dans des environnements industriels

Fonctions du référentiel NICE

- ICS/SCADA Security Engineer
- ICS/OT Systems Engineer
- OT SOC Operator

Jason Christopher
Auteur de la formation

Dean Parsons
Auteur de la formation

Le domaine de la sécurité des systèmes de contrôle industriel (ICS) est toujours dynamique. Les professionnels doivent en permanence adapter leurs stratégies défensives aux nouveaux enjeux et menaces. Pour compliquer encore la situation, toute modification apportée à la sécurité doit passer par des tests drastiques pour assurer la sûreté et la fiabilité des opérations industrielles.

Au niveau mondial, les « infrastructures critiques » et les « opérateurs de services essentiels » représentent des centaines de milliers voire des millions d'organisations industrielles. Certains constituent les artères vitales de notre société – l'eau, l'énergie, l'agroalimentaire et les industries de transformation critiques. Mais toute installation industrielle doit pouvoir compter sur un fonctionnement sûr et sécurisé. Devant l'aggravation des menaces, les nouvelles tendances technologiques et les exigences en évolution des personnels, il est vital que les leaders sécurité en technologie opérationnelle (OT) se forment aux techniques pour défendre leurs installations et leurs équipes.

La formation ICS418 de deux jours vient combler les lacunes identifiées chez les managers qui évoluent dans des environnements d'infrastructure vitale et OT. Elle arme les leaders, nouveaux ou anciens, pour prendre en charge les OT/ICS ou la cybersécurité IT/OT en voie de fusion. Ces responsables acquièrent ainsi l'expérience et les outils que le secteur exige désormais pour gérer le risque cyber au service de l'activité et assurer la sûreté et la fiabilité des opérations. À l'issue de cette formation, ils auront une solide connaissance des facteurs et contraintes de ces environnements qui allient les dimensions cyber et physiques. Ils comprendront aussi toutes les nuances de la gestion des personnes, des processus et des technologies dans l'ensemble de leurs organisations.

Programme

SECTION 1 : Responsable sécurité ICS – socle de développement et responsabilités

SECTION 2 : Développement de l'équipe de sécurité ICS

« Grâce aux enseignements de cette formation, je me suis préparé à approcher la haute direction au sujet des cyberdéfenses à mettre en œuvre sur les réseaux OT. »

— Vickram R., **Eastern Generating Company**

« Je monte depuis trois ans un programme et une équipe de sécurité des systèmes industriels et le contenu de cette formation capture vraiment tous les concepts ou presque de ce qu'il faut incorporer. »

— David B., **Pernod-Ricard**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/ICS418**

MODES DE FORMATION D'ICS418

In-Person **Live Online** **OnDemand**

ICS456: **Essentials for NERC Critical Infrastructure Protection™** MISE À JOUR MAJEURE

GCIP
Critical Infrastructure Protection
giac.org/gcip

5 jours | 31 crédits CPE | 23 labos

Vous apprendrez à...

- Comprendre les objectifs de cybersécurité des normes NERC CIP
- Comprendre le cadre réglementaire NERC, la source de son autorité et la procédure d'élaboration des normes CIP, ainsi que leur lien avec les autres normes de fiabilité BES
- Maîtriser le jargon NERC CIP, appréhender les termes apparemment semblables aux sens très différents avec les conséquences sur votre programme de conformité
- Décomplexifier pour mieux identifier et catégoriser les systèmes et les actifs électroniques BES
- Élaborer de meilleurs contrôles de gestion de la sécurité sur la base des éléments constitutifs de procédures et politiques efficaces en cybersécurité
- Comprendre les contrôles physiques et logiques et les règles de supervision
- Appréhender les critères de gestion des systèmes CIP-007 et leur lien aux critères de gestion de la configuration CIP-010 ; comprendre la différence des chronologies d'évaluation et de remédiation des vulnérabilités
- Déterminer les ingrédients d'un programme adapté d'évaluation des risques et de formation du personnel

Public visé :

- Cybersécurité IT et OT (ICS)
- Personnel technique opérationnel
- Personnel du centre des opérations de sécurité (SOC)
- Équipes de réponse aux incidents
- Équipe conformité
- Responsables d'équipe
- Personnes impliquées dans la gouvernance
- Fournisseurs/intégrateurs
- Auditeurs

Fonctions du référentiel NICE

- Privacy Officer/Privacy Compliance Manager (OPM 732)
- Process Control Engineer/Instrument & Control Engineer (ZZ-ICS-001)
- ICS/SCADA Security Engineer (ZZ-ICS-002)
- ICS/OT Systems Engineer (ZZ-ICS-003)
- OT SOC Operator (ZZ-ICS-004)
- ICS/SCADA Security Engineer
- ICS/OT Systems Engineer
- OT SOC Operator

Tim Conway
Auteur de la formation

Ted Gutierrez
Auteur de la formation

Stephen Sims
Auteur de la formation

L'environnement changeant des menaces et la pression réglementaire ont fait de la conformité aux normes américaines de fiabilité du réseau électrique NERC et de protection de l'infrastructure essentielle CIP un exercice complexe et à forts enjeux pour les opérateurs de systèmes électroniques BES. ICS456™ met les choses au clair par des conseils pratiques qui traduisent en action la politique réglementaire. Ciblant un public de professionnels des opérations, de la sécurité IT/OT et de la conformité, cette formation démystifie les exigences NERC CIP, les relie aux environnements de systèmes de contrôle industriel (ICS) de terrain, et arme les équipes pour gérer les risques, éviter les violations et bâtir une culture de cyberrésilience. Si votre mission est d'anticiper les audits tout en défendant votre infrastructure critique, ICS456™ vous dote des connaissances et des outils pour la mener avec assurance.

Au-delà des seuls fondamentaux de NERC CIP, ICS456™ fournit des stratégies exploitables de conformité et de sécurité. Vous y acquerrez une compréhension approfondie du rôle de la FERC (Federal Energy Regulatory Commission), de la NERC (North American Electric Reliability Corporation) et des organisations régionales dans l'application des normes de fiabilité. Elle aborde plusieurs approches d'identification et de catégorisation des systèmes électroniques BES (Bulk Electric System, l'infrastructure énergétique) pour s'assurer que les propriétaires d'actifs électroniques peuvent déterminer le périmètre et les critères applicables en fonction de leur environnement propre. Plus qu'une formation à la conformité, ICS456™ fait le lien entre les obligations réglementaires et l'implémentation de la sécurité sur le terrain. Vous explorerez des stratégies pratiques pour sécuriser les systèmes de contrôle industriel (ICS) et la technologie opérationnelle (OT), en appréciant les bonnes pratiques de cybersécurité à l'aulne des réalités de la conformité.

Programme

SECTION 1 : Identification et gouvernance d'actifs
SECTION 2 : Contrôle et surveillance des accès
SECTION 3 : Gestion des systèmes
SECTION 4 : Protection des informations et réponse à incident
SECTION 5 : Processus CIP

« ICS456 est indispensable pour réussir sa carrière dans un environnement CIP. »
— Tope Odubanjo, **NB Power**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/ICS456**

MODES DE FORMATION DE ICS456

In-Person | **Live Online** | **OnDemand**

ICS515: **ICS Visibility, Detection, and Response™**

GRID
Response and Industrial Defense
giac.org/grid
DoD 8140*

6 jours	36 crédits CPE	22 labos

Vous apprendrez à...

- Analyser les réseaux ICS et identifier les actifs et leurs flux de données pour comprendre les informations réseau nécessaires pour identifier les menaces avancées
- Utiliser les concepts de défense active (consommation de renseignement sur les menaces, supervision de la sécurité des réseaux, analyses de logiciels malveillants et réponse aux incidents, par exemple) pour assurer la sécurité du système ICS
- Concevoir un automate de programme industriel (PLC) personnalisé avec le kit SANS ICS515 Student Kit, que vous conserverez après la formation
- Acquérir des connaissances approfondies sur les menaces ciblant les ICS et sur les logiciels malveillants, notamment STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, TRISIS/TRITON, FROSTYGOOP, EKANS et PIPEDREAM
- Utiliser des outils techniques comme Shodan, Wireshark, Zeek, Suricata, Volatility, FTK Imager, des analyseurs de PDF, des logiciels de programmation d'automates programmables industriels et d'autres
- Créer des indicateurs de compromission dans YARA
- Exploiter des modèles (Sliding Scale of Cybersecurity, Active Cyber Defense Cycle, Collection Management Framework, ICS Cyber Kill Chain) afin d'extraire les informations des menaces et les utiliser pour conforter la sécurité des réseaux ICS à long terme

Public visé :

- Responsables et membres d'équipes de réponse aux incidents ICS
- Personnel des services de sécurité OT et ICS
- Professionnels de la sécurité IT
- Responsables d'équipes et analystes de centre des opérations de sécurité (SOC)
- Experts en tests d'intrusion et red team ICS
- Chargés de défense active

Fonctions du référentiel NICE

- Cyber Defense Incident Responder (OPM 531)
- ICS/SCADA Security Engineer
- ICS/OT Systems Engineer
- OT SOC Operator

Robert M. Lee
Auteur de la formation

*DoD 8140 APPROVED
sans.org/8140

Dans la formation ICS515, vous acquérez une meilleure visibilité et connaissance des actifs sur vos réseaux ICS (systèmes de contrôle industriel) et OT (technologies opérationnelles). Vous améliorez vos capacités de surveillance et de détection des cybermenaces, vous apprenez à disséquer les cyberattaques sur les ICS pour en tirer des leçons, et à répondre aux incidents. Enfin, la découverte d'une approche basée sur le renseignement pour l'exécution d'un programme de cybersécurité ICS ambitieux vous permet de garantir la sûreté et la fiabilité des opérations.

Les stagiaires apprennent également à comprendre l'environnement de leurs systèmes de contrôle industriel en réseau, à surveiller les menaces qui affectent ces ICS et à gérer les incidents en fonction des menaces identifiées. L'exploitation des interactions avec l'adversaire leur permet, grâce aux enseignements retirés, d'améliorer la sécurité des réseaux. Cette approche essentielle apprend à contrer des menaces aussi sophistiquées que les malwares STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, TRISIS/TRITON et les ransomwares. Indispensable à la compréhension et à l'exploitation d'un environnement d'automatisation moderne complexe, cette démarche permet aussi d'analyser les causes profondes d'événements hors du cadre cyber qui se manifestent sur le réseau. À l'issue de la formation, les stagiaires auront acquis les compétences fondamentales nécessaires à tout programme de cybersécurité des systèmes de contrôle industriel.

L'approche pratique choisie exploite de nombreux jeux de données techniques provenant d'entraînements et d'équipements ICS, avec des scénarios d'attaque et de déploiement de logiciels malveillants issus du terrain. L'objectif : proposer une expérience de détection et de réponse aux menaces la plus réaliste possible. Les stagiaires interagissent ainsi avec un automate programmable industriel (en anglais, PLC) qu'ils pourront conserver ensuite, avec un kit physique d'émulation des opérations de système électrique au niveau de la génération, de la transmission et de la distribution, et avec une machine virtuelle paramétrée comme une interface homme-machine (IHM) et une station de travail d'ingénierie (EWS).

Programme

SECTION 1 : Renseignement ICS d'intérêt cyber
SECTION 2 : Visibilité et identification des actifs
SECTION 3 : Détection des menaces ICS
SECTION 4 : Réponse aux incidents
SECTION 5 : Menace et manipulation de l'environnement
SECTION 6 : Journée d'exercice final : attaque en cours !

« Cette formation est un tremplin. J'y ai affiné mes connaissances sur les menaces qui pèsent sur les environnements ICS et acquis un cadre structurant pour me défendre activement, mais elle m'a aussi incité à me documenter davantage. »

— Srinath Kannan, **Accenture**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/ICS515**

MODES DE FORMATION DE ICS515

In-Person **Live Online** **OnDemand**

ICS612: **ICS Cybersecurity In-Depth™**

5 jours	30 crédits CPE	31 labos

Vous apprendrez à...

- Maîtriser des méthodes passives et actives de collecte sécurisée des informations dans un environnement ICS
- Identifier les vulnérabilités dans les environnements ICS
- Déterminer les modes opératoires frauduleux qui visent à interrompre et prendre le contrôle des processus, et bâtir les défenses pour les contrer
- Déployer en amont des mesures pour prévenir, détecter, ralentir ou arrêter les attaques
- Comprendre les opérations ICS et leur aspect « normal »
- Construire des points de passage obligés dans une architecture, déterminer les moyens de les utiliser dans la détection des incidents de sécurité et la réponse à leur apporter
- Gérer les environnements ICS complexes ; développer la capacité de détecter les événements de sécurité ICS et d'y répondre

Public visé :

- Anciens stagiaires d'ICS410 – ceux qui ont validé la formation ICS410: ICS/SCADA Security Essentials auront acquis les connaissances préalables nécessaires.
- Ingénieurs en contrôle industriel
- Ingénieurs des systèmes ou de la sûreté des systèmes
- Chargés de défense active en ICS
- Quiconque doté d'une expérience significative des systèmes de contrôle souhaitant comprendre les méthodes et procédures de mise en sûreté d'un environnement ICS

Fonctions du référentiel NICE

- Process Control Engineer/Instrument & Control Engineer
- ICS/OT Systems Engineer

Tim Conway
Auteur de la formation

Jason Dely
Auteur de la formation

Christopher Robinson
Auteur de la formation

Jeffrey Shearer
Auteur de la formation

La sécurisation des environnements OT et IT exige des perspectives et approches différentes. Chaque système OT étant conçu spécifiquement pour les besoins opérationnels propres à une organisation, comment aborder la sécurisation de ces systèmes ? Dans un environnement d'exploitation immersif, ICS612 vous fait passer de la théorie à l'apprentissage pratique en cinq jours. Vous apprenez la méthodologie nécessaire pour identifier les vulnérabilités opérationnelles et bâtir des défenses en tant que membre du groupe ingénierie, opérations, red team ou blue team. Vous explorez les opérations fondamentales des PLC et IHM jusqu'aux composants d'architecture et de surveillance les plus complexes de la sécurité IT et OT, en étudiant comment les attaques utilisent les systèmes ICS et le personnel pour toucher l'exploitation. Vous renforcez ces compétences par des exercices pratiques en labo. La formation se conclut par un scénario de réponse à incident dans lequel vous investiguez et récupérez des opérations dans l'environnement de test. Vous repartez avec une connaissance approfondie de la manière d'analyser un système inconnu et de maintenir la résilience opérationnelle.

Les notions et les objectifs pédagogiques du cours sont principalement abordés par le biais d'exercices pratiques. Le labo en salle de cours est prévu pour simuler un environnement réel où un contrôleur supervise et contrôle les appareils déployés sur le terrain. Une interface homme-machine (IHM) tactile installée dans l'atelier est accessible au personnel en local pour lui permettre d'effectuer les changements de procédure nécessaires. Via les postes de travail des opérateurs d'un centre de contrôle distant, les opérateurs système supervisent et contrôlent les équipements industriels avec un système SCADA. Représentatif d'un véritable environnement ICS, la configuration comprend une connexion à l'entreprise pour le transfert de données (à savoir un logiciel d'historisation dit « historian »), l'accès à distance et d'autres fonctions classiques d'entreprise.

Programme

SECTION 1 : Le processus local
SECTION 2 : Système de systèmes
SECTION 3 : Infrastructure réseau ICS
SECTION 4 : Gestion des systèmes ICS
SECTION 5 : Covfefe ne répond plus !

« J'ai adoré que la formation mette l'accent sur les labos. Je suis désormais totalement à l'aise avec les équipements OT. Et ce n'est pas rien, car mon profil et mon expérience sont strictement IT. »

—Jim J., **Pilot Flying J**

Consultez le descriptif détaillé de la formation sur **SANS.ORG/ICS612**

MODES DE FORMATION DE ICS612

In-Person

ZOOM NOUVELLE FORMATION

ICS613: **ICS/OT Penetration Testing & Assessments™**

5 jours	30 crédits CPE	25 labos

Vous apprendrez à...

- Planifier et exécuter des évaluations de sécurité et des tests d'intrusion sûrs, efficaces et utiles à l'aide de techniques passives et actives afin de mesurer la résilience opérationnelle dans des environnements ICS
- Créer des tests d'intrusion et des évaluations de sécurité ICS sur mesure au service des objectifs de sécurité opérationnels et organisationnels du client
- Collaborer avec des clients pour déterminer les scénarios d'attaque d'ICS réalistes ciblant les joyaux de la couronne
- Communiquer avec les parties prenantes et se coordonner avec elles pour définir les attentes, les objectifs et les résultats escomptés des évaluations de sécurité des ICS
- Comprendre les atouts d'une approche descendante/ascendante de test actif et comment l'alignement des méthodologies de test d'intrusion avec la Cyber Kill Chain des ICS situe les activités d'engagement, les résultats et les recommandations dans le contexte approprié
- Évaluer le niveau d'efficacité et de sécurité des outils et techniques avant de s'en servir pour les équipements et réseaux ICS
- Identifier les cibles pertinentes et sélectionner les TTP d'attaque applicables pour développer des scénarios efficaces pour les tests d'intrusion et les évaluations de la sécurité des systèmes de contrôle industriel, quel que soit le secteur d'activité
- Rédiger et fournir des points d'état actualisés en temps voulu et des rapports fiables et exploitables qui étayent les objectifs des clients

Public visé :

- Professionnels de la cybersécurité devant évaluer des environnements industriels
- Professionnels de la cybersécurité devant mener des évaluations cyber et des tests d'intrusion à des fins de conformité réglementaire
- Chargés de tests d'intrusion, de réponse aux incidents, de recherche de compromissions et équipes de sécurité défensive ou offensive de systèmes ICS qui cherchent à améliorer leurs capacités individuelles et collectives
- Équipes d'évaluation des systèmes d'armement ou des installations industrielles nationales ou des armées
- Professionnels de la cybersécurité souhaitant acquérir l'expérience nécessaire pour travailler en sûreté avec les machines industrielles et les systèmes numériques de contrôle-commande
- Chargés de tests d'intrusion et professionnels cyber chevronnés cherchant à améliorer leurs compétences et savoir-faire appliqués au domaine ICS

Jason Dely
Auteur de la formation

Don Weber
Auteur de la formation

Tyler Webb
Auteur de la formation

Les équipes d'ingénierie, des opérations et de la sécurité en environnement industriel ou dans les secteurs des infrastructures essentielles du monde entier sont de plus en plus soumises à l'obligation de mener des tests d'intrusion et des évaluations de la sécurité des principaux systèmes et équipements. Cette formation arme les stagiaires des connaissances et compétences pour mener ces tâches à bien en toute sécurité, tout en assurant la fiabilité et la résilience opérationnelles et en produisant des résultats en cybersécurité.

ICS613™ traite des leviers et des contraintes spécifiques aux environnements ICS et dispense une formation pratique pour développer les capacités de tests d'intrusion et d'évaluation propres aux systèmes de contrôle industriel – machines, applications, architectures, communications et environnements de fabrication. À l'issue de cette semaine, les stagiaires seront armés pour mener des tests d'intrusion sur le terrain et des évaluations de la sécurité d'environnements totalement opérationnels.

Programme

SECTION 1 : Types et concepts d'évaluation

SECTION 2 : Engagements d'évaluation

SECTION 3 : Méthodologie active descendante

SECTION 4 : Méthodologie passive ascendante

SECTION 5 : Évaluation active et exercice CTF

Consultez le descriptif détaillé de la formation sur **SANS.ORG/ICS613**

MODES DE FORMATION D'ICS613

In-Person

STAY SHARP

Formation en cybersécurité à fort impact

Renforcez vos compétences en seulement 1 à 3 jours.

Les formations SANS Stay Sharp sont :

- Dispensées par les meilleurs professionnels mondiaux de la cybersécurité
- Courtes et ciblées pour vous aider à acquérir des compétences et connaissances techniques spécifiques
- Un enseignement de qualité qui vous détourne moins longtemps de vos responsabilités professionnelles et personnelles
- Pratiques et applicables dans la même semaine
- Délivrées en direct en ligne via Live Online

L'offre SANS Stay Sharp :

ICS418: ICS Security Essentials for Leaders™

ICS418™ dote les leaders des compétences pour bâtir et maintenir un programme de sécurité des ICS mature par la gestion efficace des équipes, processus et technologies, tout en alignant le cyber-risque industriel sur les objectifs de l'entreprise afin d'assurer la sûreté, la fiabilité et la sécurité.

LDR419: Performing A Cybersecurity Risk Assessment™

LDR419™ montre aux stagiaires les risques à chercher dans leur cadre organisationnel précis, comment mettre au jour efficacement ces risques, et comment présenter les résultats à la direction pour mener à une implémentation concrète.

LDR433: Managing Human Risk™

LDR433™ permet aux organisations de gérer et mesurer efficacement leur risque humain en façonnant les comportements et une forte culture de la sécurité.

« Cette formation renforce les compétences dont j'ai besoin dans mon poste. Au lieu d'apprendre en trois mois sur le tas, je suis une formation SANS et je suis prêt à m'atteler à la tâche. »

— Bryan G., **Réserve fédérale des États-Unis**

SEC467: Social Engineering for Security Professionals™

SEC467™ vous prépare à intégrer des compétences d'ingénierie sociale à votre stratégie de cybersécurité.

SEC535: Offensive AI – Attack Tools & Techniques™ NOUVEAUTÉ

SEC535™ vous apprend à vous servir de l'IA pour la reconnaissance, la création d'outils personnalisés, le développement de logiciels malveillants, et des simulations avancées d'attaques pour vous défendre contre les menaces modernes dopées à l'IA.

SEC547: Defending Product Supply Chains™ NOUVEAUTÉ

SEC547™ vise à réduire au maximum le risque d'attaque sur la supply chain par le biais de stratégies et tactiques approfondies de gestion des risques liés aux fournisseurs.

SEC556: IoT Penetration Testing™

SEC556™ facilite l'examen de tout l'écosystème des objets connectés (IoT), et vous aide ainsi à acquérir les compétences vitales pour identifier, évaluer et exploiter des mécanismes de sécurité élémentaires et complexes des appareils IoT.

SEC580: Metasploit for Enterprise Penetration Testing™

SEC580™ vous apprend à appliquer les incroyables capacités de Metasploit Framework dans un protocole complet de tests d'intrusion et d'évaluation des vulnérabilités.

Live Online

sans.org/mlp/stay-sharp

SANS

CYBER RANGES

Renforcez vos compétences pratiques en cybersécurité à travers des simulations terrain. Acquérez une expérience concrète dans des environnements sûrs mais réalistes, et soyez à la hauteur de votre mission quand la menace réelle se matérialisera.

SANS CYBER RANGES : UN LARGE SPECTRE DE DISCIPLINES ET DES NIVEAUX DE NOVICE À EXPERT

Choisissez une expérience pratique organisée lors d'un événement de formation SANS ou contactez-nous pour une solution intra-entreprise personnalisée.

CYBER RANGE
BOOTUP CTF

BootUp CTF

Testez vos compétences en cybersécurité lors d'un BootUp CTF, un exercice de capture du drapeau aux plus de 125 défis multidisciplinaires. Connectez-vous à des scénarios de terrain : exploitez outils et compétences pratiques pour vous attaquer à des cibles authentiques et capturer la mémoire.

CYBER RANGE
NETWARS

NetWars Tournament

La suite SANS NetWars de six entraînements avancés convient à tous les niveaux de compétence, sur une trame haletante qui favorise l'acquisition interactive de connaissances. Les défis multiformes issus du terrain mettent l'accent sur l'application et l'évaluation en profondeur de compétences de cybersécurité essentielles pour un domaine d'intérêt.

CYBER RANGE
CYBER CITY

Cybercity

Plongez dans Cybercity, ville miniature à l'échelle 1:87 contrôlée par de vrais équipements de production. Acquérez l'expérience pratique de systèmes SCADA – électricité, eau, transports… – et préparez-vous aux défis de la cybersécurité dans les environnements d'infrastructure critique.

CYBER RANGE
SANS SKILLS QUEST
BY NETWARS

Skills Quest by NetWars

Tracez votre parcours cyber quand et où vous le voulez avec des défis à votre rythme et, si nécessaire, des indices pensés pour développer toujours plus vos compétences. Cet entraînement cyber range est disponible vingt-quatre heures sur vingt-quatre et sept jours sur sept pendant six mois pleins pour une flexibilité totale.

SOLUTION DE FORMATION PRATIQUE À LA CYBER

La source la plus respectée de formation en cybersécurité

Mettez au jour les talents cyber
Repérez et recrutez les personnes à fort potentiel cyber.

Contenus experts
Toutes dernières tactiques et connaissances en cybersécurité pour rester en lice.

Consolidez votre protection
Renforcez la posture de sécurité de votre organisation par la pratique.

Crédits CPE
Obtenez des crédits de formation continue à mesure que vous vous formez.

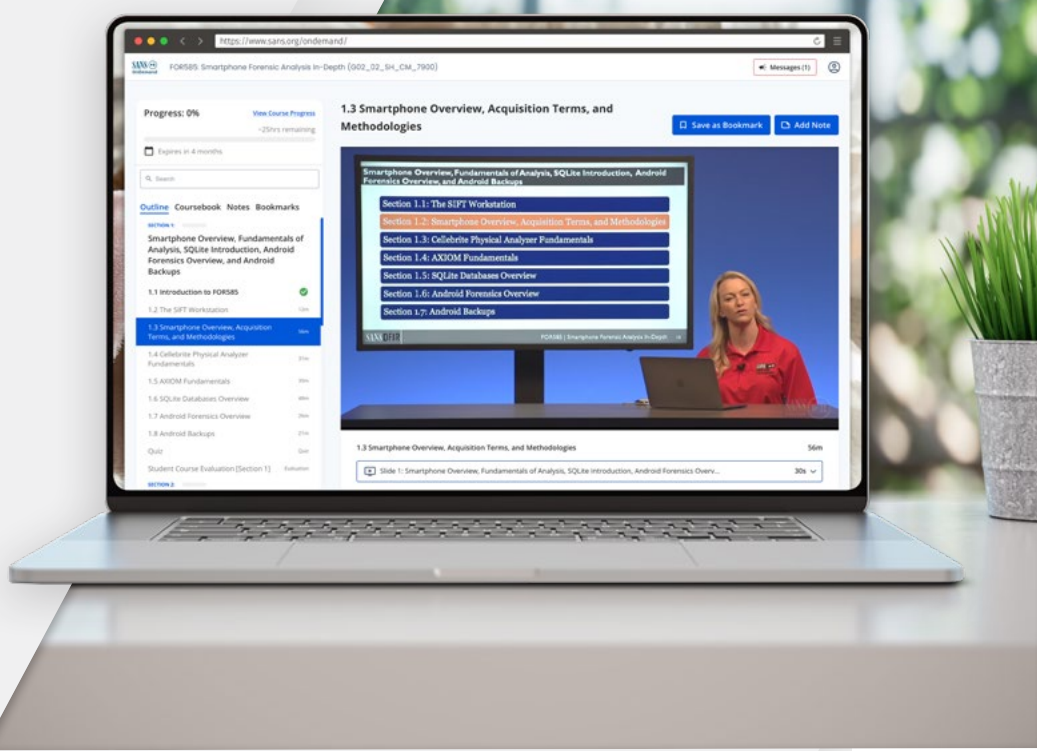
Un plan clair
Suivez un parcours de formation structuré vers la maîtrise des compétences clés en cybersécurité.

Classement
Suivez vos progrès et rivalisez avec vos pairs pour vous pousser à vous améliorer continuellement.

En savoir plus sur les Cyber Ranges
sans.org/cyber-ranges

SANS OnDemand

Formez-vous à votre rythme, partout et à tout moment avec SANS OnDemand.



SANS OnDemand délivre nos formations d'excellence en cybersécurité en ligne et à votre rythme, avec quatre mois d'accès plein et entier aux cours et aux labos. Profitez de la flexibilité extrême de l'apprentissage OnDemand : revenez en arrière et replongez-vous dans le contenu pour renforcer l'apprentissage et ancrer durablement vos connaissances.

Le rythme d'apprentissage à la carte de SANS OnDemand convient à tous les styles.

- **E-learning SANS flexible à votre rythme**
- **Quatre mois d'accès aux supports de formation et aux labos, en tout lieu et à tout moment**
- **Accompagnement en direct des experts techniques certifiés GIAC**

> « Je ne crois pas que cette formation me serait aussi profitable si je recevais les supports autrement que par la plateforme OnDemand. C'est un excellent moyen de réviser le contenu et les sujets critiques. »
>
> — Kenneth Huss, **Cisco**

Nouvelle application de formation SANS OnDemand

Formez-vous à la cybersécurité **où vous voulez, quand vous voulez.**

Formation intra-entreprise en cybersécurité

Maîtrisez des compétences pratiques pour anticiper les menaces

Pratique et délivrée par des experts, la formation intra-entreprise SANS à la cybersécurité colle aux besoins de votre organisation. Que ce soit pour répondre à des objectifs internes, réduire les frais de déplacement ou garantir la confidentialité, nos solutions de formation flexibles produisent un impact maximum.

Pourquoi choisir la formation intra-entreprise de SANS ?

À huis clos et sur mesure

Formez votre équipe en intra, dans un environnement privé et sûr, avec un focus sur les sujets qui vous sont pertinents.

Calendrier flexible

Choisissez les horaires de formation qui conviennent aux besoins de votre organisation.

Des éclairages par secteur

Des échanges sur mesure et un apprentissage pratique adapté à votre secteur.

Pratique et économique

Réduisez les frais de déplacement et formez-vous dans un environnement contrôlé.

Plusieurs modes de formation

Différents formats disponibles : In-Person, Live Online ou hybride.

Formation augmentée

Ajoutez des Cyber Ranges, du contenu OnDemand en E-learning et des certifications GIAC pour une expérience encore plus poussée.

Témoignages

« SANS propose la meilleure formation en cybersécurité que vous puissiez trouver : pratique, concrète et immédiatement applicable. »
— Jeff Stebelton, NetJets Inc.

« La formation intra-entreprise s'est avérée extrêmement précieuse – les stagiaires apprennent aux côtés des collègues avec qui ils partagent les responsabilités, rendant l'expérience encore plus pertinente. »
— Tonya Henderson, département de la Santé et des Services sociaux (États-Unis)

EN SAVOIR PLUS

68 % des violations de données impliquent un élément humain*. Gérez efficacement ce risque critique avec

SANS SECURITY AWARENESS

Gérez le risque humain par la sensibilisation

Pensée pour un impact fort, la formation à la sensibilisation SANS Security Awareness s'intègre aisément aux cadres existants. Elle renforce l'acquisition des connaissances et s'adapte aux demandes organisationnelles pour former des effectifs cyber-résilients.

End-User Training

Découvrez une formation de sensibilisation à la sécurité sur mesure, façonnée par des spécialistes et axée sur des impacts mesurables.
+50 modules | 6 thématiques | 34 langues

Phishing Simulation

Recevez nos modèles conçus par les meilleurs spécialistes pour repérer les zones à risques, encouragez les pratiques de messagerie sûre, et offrez une formation adaptée à votre contexte.
5 niveaux de difficulté | 34 langues | Détection humaine avancée

EN SAVOIR PLUS
sans.org/security-awareness-training

* DBIR de Verizon

Gérez le risque humain : sensibilisez par métier

Les modules par profil métier de SANS sont conçus pour encourager l'investissement durable des collaborateurs dans la formation. Cette approche modulaire délivre des contenus pertinents sur les cybermenaces actuelles.

AI Security Essentials for Business Leaders – Enterprise Edition

Couvre des domaines critiques du codage sécurisé, dont le Top 10 des vulnérabilités OWASP et la sécurité des applications mobiles. **8 modules** | **75 minutes**

Formation pour développeurs

La formation au codage sécurisé couvre des domaines critiques comme le Top 10 des vulnérabilités OWASP et la sécurité des applications mobiles. **70 modules** | **270 minutes**

Security Essentials Training – Business Leaders and Managers

Équipe les leaders responsables pour établir et maintenir un environnement sécurisé essentiel au succès stratégique et opérationnel de l'entreprise. **10 modules** | **60 minutes**

Security Essentials Training – IT Administrators

Une immersion dans des scénarios réalistes où les professionnels IT affûtent leurs compétences dans un parcours à la difficulté progressive. **12 modules** | **90 minutes**

Industrial Control Systems Training

Les techniques essentielles pour protéger les systèmes de contrôle industriel et les infrastructures critiques. **22 modules** | **144 minutes**

Role-Based PCI DSS Training

Formation adaptée au profil sur la sécurisation des moyens de paiement et la mise en conformité avec les normes PCI DSS. **6 parcours pédagogiques** | **28 minutes**

La puissance de la certification

Les études prouvent immuablement que les employés certifiés apportent invariablement une plus grande valeur ajoutée à leur organisation.

Avantages pour les entreprises

Source : « 2024 Value of certification report » de Pearson VUE

81 % produisent un travail de meilleure qualité

77 % innovent davantage et améliorent les résultats obtenus

72 % sont plus efficaces et productifs

82 % ont renforcé leurs compétences de mentorat et d'accompagnement de leurs collègues

74 % ont gagné en autonomie et en indépendance

74 % réalisent une tâche ou tiennent un rôle qu'ils n'auraient pas pu réaliser ou tenir avant

Avantages pour les employés

Source : « 2024 Value of certification report » de Pearson VUE

92 % ont plus confiance en leurs capacités

84 % sont plus déterminés à réussir leur vie professionnelle

78 % sont plus satisfaits de leur travail

74 % ont gagné en autonomie et en indépendance

80 % atteignent leur objectif – augmentation de salaire, promotion professionnelle, performances ou satisfaction personnelle

GIAC®, la référence des certifications en cybersécurité

- Chaque domaine de la cybersécurité est couvert par une des plus de 50 certifications
- Des tests concrets et issus du terrain pour valider les compétences
- Des correspondances avec plus de 100 fonctions et exigences
- Actualisation annuelle pour rester à l'avant-garde de l'évolution des menaces
- Reconnue dans le monde entier par les entreprises du classement Fortune 100 et les administrations publiques
- Approuvée par le ministère américain de la Défense et conforme à la Directive 8140
- Conformité juridiquement démontrable avec la norme ISO 17024

Des certifications pour un ROI maximum

L'investissement dans la certification IT se répercute directement dans les résultats financiers.

Le **ROI** par employé certifié atteindrait jusqu'à

30 000 $

64 % des décisionnaires IT estiment que chaque employé IT certifié contribue une ***valeur ajoutée*** de

10 000 $

ou plus par rapport à ses collègues non certifiés.

« J'apprécie la crédibilité et le respect immédiats que GIAC confère. Les autres savent que vous avez travaillé dur pour obtenir la certification et ils connaissent les compétences et connaissances critiques qui y sont attachées. »

Ben Boyle, GWAPT®, GXPN™, GPEN®

« Les attaquants mutent sans cesse. Une certification GIAC vous prépare à évoluer en conséquence. Elle vous permet de mettre en œuvre dans votre entreprise les bonnes pratiques et les méthodes appropriées en sachant que c'est un combat permanent. »

Jason Sevilla, GCIH®, CMON®, GSEC®

Préparez votre équipe de direction

Exercices en immersion pour entraîner l'équipe de direction

Les Executive Cyber Exercises (ECE) de SANS sont conçus pour accompagner les dirigeants dans une simulation de crise. Nos spécialistes, professionnels du secteur, déroulent un incident de sécurité en coachant vos parties prenantes sur les bonnes pratiques de gestion de crise.

Les organisations qui s'exercent avec nous à répondre aux crises seront capables de :

- Évaluer l'état de préparation organisationnelle aux crises au niveau de la direction
- Utiliser des stratégies d'atténuation
- Appliquer les bonnes pratiques sectorielles à la cybersécurité, à la structure de l'organisation et aux communications de crise
- Respecter les obligations réglementaires ou de gouvernance

SANS | EXECUTIVE CYBER EXERCISES

PREPARE | PRACTICE | PREVAIL

SANS Summits

CONTENU EXCLUSIF

RECHERCHE JAMAIS DIVULGUÉE

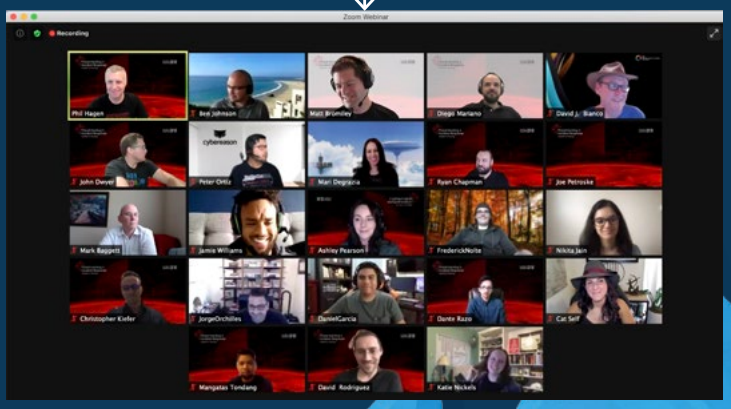
DES SOLUTIONS EXPLOITABLES

VOTRE communauté – ENSEMBLE pour résoudre AUJOURD'HUI les défis cyber

In-Person avec des avantages exclusifs

OU

En ligne, pour la communauté mondiale



5 bonnes raisons de venir aux SANS Summits

№ 1 Des communications techniques approfondies sur des compétences et techniques en avant-première ou ZERO-DAY.

№ 2 Échanges avec des groupes d'experts.

№ 3 Rencontres avec les plus grands experts et avec vos pairs confrontés aux mêmes casse-têtes.

№ 4 Accès aux enregistrements et aux présentations du Summit.

№ 5 Vous repartirez de l'expérience Summit avec de nouvelles perspectives, un lien plus fort à la communauté et de nouveaux outils exploitables immédiatement dans votre quotidien.

« Chaque séance m'a appris quelque chose, et j'ai découvert des outils et des méthodologies complémentaires qui vont m'être utiles. »

— Dallas M., **PepsiCo**

Prochains sommets en cybersécurité

- Cyber Threat Intelligence
- Neurodiversity in Cybersecurity
- Cybersecurity Leadership
- ICS Security
- AI Cybersecurity
- Blue team
- Digital Forensics & Incident Response (DFIR)
- SANS Security Awareness: Managing Human Risk
- Ransomware
- Open-Source Intelligence (OSINT)
- CloudSecNext
- New2Cyber

En savoir plus

Ressources gratuites en cybersécurité

sans.org/free

Formations et événements gratuits

Testez les formations SANS
Repérez la formation qui convient : prévisualisez-en gratuitement une heure, explorez les thèmes abordés et vérifiez que le niveau des supports correspond à vos compétences.
sans.org/course-preview

Summit Presentations
Explorez les enseignements issus des présentations des Summits SANS.
sans.org/presentations

SANS Workshops
Ces ateliers pratiques virtuels sont l'occasion de revoir en profondeur les supports de formation.
sans.org/workshops

NetWars Tournaments
Rejoignez gratuitement un entraînement cyber NetWars pour toute inscription à un événement de formation en direct de 4 à 6 jours.
sans.org/cyber-ranges/upcoming-netwars-tournament

Réseaux sociaux

Retrouvez-nous sur **@SANSInstitute** et suivez-nous pour vous tenir informé de nos ressources les plus récentes.

New2Cyber
Cyber Defense
Offensive Ops
DFIR
Leadership
Cloud
ICS
Security Awareness
Cyber Ranges

https://x.com/sansinstitute

Webcasts

sans.org/webcasts

Blogs

sans.org/blog

Podcasts

Blueprint
Développez vos compétences en cyberdéfense.

Cloud Ace
Le futur de la sécurité du cloud.

GIAC: Trust Me, I'm Certified
Grands acteurs de la cybersécurité.

Internet Storm Center
Alertes quotidiennes d'InfoSécurité sur les menaces.

sans.org/podcasts

SANS Cyber Academies

VetSuccess Academy

Women's Immersion Academy

Cyber Workforce Academy

Cyber Diversity Academy

HBCU Academy

sans.org/scholarship-academies

Newsletters

NewsBites
Synthèse bihebdomadaire des articles d'information cyber les plus importants publiés récemment.

@Risk
Récapitulatif hebdomadaire sur les vecteurs d'attaque mis au jour, les vulnérabilités exposées à de nouveaux exploits actifs, le fonctionnement des attaques récentes et d'autres informations utiles.

OUCH!
Lettre d'information mensuelle et gratuite qui s'adresse aux utilisateurs non spécialistes dans plus de 20 langues.

sans.org/newsletters

Ressources gratuites en cybersécurité

Internet Storm Center
Service gratuit d'alerte et d'analyse.
isc.sans.edu

Outils gratuits
+150 outils open source créés par les SANS Instructors.
sans.org/tools

Livres blancs
Accédez aux livres blancs SANS rédigés par des experts.
sans.org/white-papers

Affiches et aide-mémoire
sans.org/posters

Modèles de politiques de sécurité
Ces modèles de politiques de sécurité à votre disposition ont été conçus par des leaders et des experts techniques en sécurité des informations.
sans.org/information-security-policy

CIS Controls v8
Les contrôles CIS forment un ensemble de mesures recommandées de cyberdéfense qui indiquent des moyens précis et exploitables d'arrêter les attaques dangereuses et répandues actuellement.
sans.org/blog/cis-controls-v8

Rapport annuel sur la sensibilisation à la sécurité
Laissez les données guider vos actions de gestion du risque humain et faire avancer votre programme vers le futur de l'acculturation à la sécurité.
go.sans.org/lp-wp-2022-sans-security-awareness-report

NICE Framework
Dynamisez votre carrière : faites le lien entre le référentiel NICE et les certifications GIAC reconnues en cybersécurité.
giac.org/workforce-development/government/niceframework

Rejoignez gratuitement la communauté SANS.org

Intégrer la communauté SANS.org vous donne accès en exclusivité aux ressources pointues que nos experts formateurs produisent chaque jour, notamment des informations, des formations et des outils gratuits.

Rendez-vous sur sans.org/account/create pour créer gratuitement votre compte dès aujourd'hui et vous ouvrir l'accès à toutes ces ressources cyber et plus encore !

Au cœur de tout ce que nous faisons se trouve la mission de SANS : donner aux professionnels de la cybersécurité les compétences pratiques et les connaissances nécessaires pour rendre le monde plus sûr.

Nous croyons qu'on ne peut diriger que ce que l'on vit pleinement. C'est pourquoi nous collaborons avec les meilleurs praticiens du secteur pour concevoir et dispenser des formations de pointe, des certifications et des programmes académiques. Nos stagiaires apprennent de ceux qui sont sur le terrain aujourd'hui, les experts en première ligne qui testent, innovent et conçoivent de nouvelles façons de sécuriser le domaine cyber.

Quand vous choisissez SANS, vous ne suivez pas simplement un cours : vous intégrez notre communauté. Que vous soyez novice en cyber ou à un poste de direction, nous nous engageons à vous accompagner tout au long de votre parcours. Pour ce faire, nous proposons de nombreux parcours adaptés aux profils, des ressources gratuites, des sommets, et différents modes d'enseignement pour vous former. Investir dans SANS, c'est investir dans votre carrière, dans votre organisation et dans votre avenir.

La promesse SANS : toute personne formée par SANS peut appliquer les compétences et les connaissances acquises dès son retour au travail.

Retrouvez le calendrier des formations à jour à la page www.sans.org/events

SANS | GIAC CERTIFICATIONS