SANS | GIAC CERTIFICATIONS

2025

Leitfaden für Karrieren in Cybersicherheit

Finden Sie Ihren Weg. Entwickeln Sie neue Kompetenzen. Weisen Sie Ihre Kenntnisse nach.

Über 80 praktische Kurse

Über 120 ausgezeichnete, von SANS zertifizierte Kursleiter

Über 55 GIAC Zertifizierungen

Neue Kurse im Spotlight

- **ICS310** ICS Cybersecurity Foundations™
- **ICS613** ICS/OT Penetration Testing & Assessments™
- **SEC547** Defending Product Supply Chains™
- **SEC673** Advanced Information Security Automation with Python™
- **LDR519** Cybersecurity Risk Management and Compliance™
- **FOR528** Ransomware and Cyber Extortion™
- **FOR577** Linux Incident Response and Threat Hunting™

Ihre Zukunft auf dem Gebiet der Cybersicherheit

Willkommen beim SANS 2025 Schulungskatalog. Seit mehr als 35 Jahren verfolgen wir das Ziel, Mitglieder der Cybersicherheits-Community in ihren Kompetenzen zu stärken.

Dieser Leitfaden – ein kuratiertes Portfolio von professionellen Rollen, Karrierepfaden und unverzichtbaren Kompetenzen – bietet einen umfassenden Rahmen zur Weiterentwicklung auf jedem Niveau. Hier finden Sie Schulungsempfehlungen für spezifische Rollen innerhalb von Fokusbereichen, die sich am NICE Framework orientieren, und die coolsten Karrieren der Branche.

Wir hoffen, dass Sie und Ihr Team diesen Leitfaden als Plan für Ihre gemeinsame Zukunft nutzen werden. Und wenn Sie so weit sind, vermittelt, validiert und zertifiziert SANS Ihnen die wesentlichen Fähigkeiten und Kenntnisse, die Ihre Kompetenzen in Cybersicherheit auf ein höheres Niveau anheben.

Echte Probleme, echte Experten

Cybersicherheit lernen von Kursleitern, die an vorderster Front aktiv sind

Sie erhalten fachkundige Anleitung von unseren renommierten Kursautoren und Kursleitern, die ausnahmslos alle praktisch an der Lösung profilierter, echter Sicherheitsprobleme arbeiten.

Heather Barnhart
Heather Barnhart hat Straftaten wie Kinderausbeutung und Morde und die Medien von Osama Bin Laden untersucht.

Robert M. Lee
Robert M. Lee hat vor dem US-Kongress mehrmals zum Thema der Cyberbedrohung kritischer Infrastruktur ausgesagt.

Vorgestellt:
Über 120
ausgezeichnete, von SANS zertifizierte Kursleiter

David Hoelzer
David Hoelzer ist Research Fellow beim Center for Cybermedia Research, beim Identity Theft and Financial Fraud Research Operations Center und beim Internet Forensics Lab.

Schulung, Zertifizierung, Erfolg

Kompetenzen verbessern mit topaktuellen Kursen, Laborübungen und Zertifizierungen

Ob Sie ganz am Anfang stehen oder Führungsstrategien ausarbeiten – bei SANS gibt es 80 praktische Kurse und Zugang zu über 55 GIAC-Zertifizierungen. Unser Ziel ist es, Ihnen unmittelbar anwendbare Kompetenzen zu vermitteln, ganz gleich, in welcher Phase Ihrer Karriere Sie sich befinden.

Flexible Lernoptionen

Präsenzkurs

- Immersives Lernen ohne Ablenkung
- Networking mit anderen Experten aus der Branche
- Bonus: praktische Workshops
- Exklusive Empfänge für Absolventen

Live online

- Interaktives Lernen im Büro oder bequem zu Hause
- Echtzeitzugriff auf Lehrkräfte, Kursleiter und Assistenten
- Bonus: themenbezogene Lernsitzungen

OnDemand

- Flexible SANS-Schulungen im individuellen Lerntempo
- Vier Monate lang Zugang zu Kursmaterialien und Laborübungen, jederzeit und überall
- Live-Support von GIAC-zertifizierten Fachexperten

Privat

- Maßgeschneiderte, branchenspezifische Diskussion
- Günstiger Veranstaltungsort, weniger Reisekosten
- Flexibler Zeitrahmen für Ihre Anforderungen

Finden Sie Ihren Kurs

Fokussierte Schulungen für Ihre Anforderungen und Branchenstandards

Sieben branchenweit führende Fokusbereiche für Cybersicherheits-Fachkräfte

Mit der Farbcodierung finden Sie in diesem Katalog leicht die ideale Schulung für Sie.

5 Kurse | 114 Laborübungen | 3 Zertifikate

New2Cyber

In diesen praktischen Einführungsschulungen zur Cybersicherheit lernen Sie und Ihr Personal, wie Angreifer vorgehen, wie Sie Verteidigungsmaßnahmen wirksam umsetzen und auf Vorfälle reagieren und wie Sie Risiken mindern und Systeme ordnungsgemäß sichern.

Kurse:

SEC275 AIS247
SEC301 ICS310
SEC401 SEC366
SEC402 SEC406
SEC403 SEC480

17 Kurse | 443 Laborübungen | 9 Zertifikate

Offensiv-operationen

Die SANS-Kurse zu Offensivoperationen beschäftigen sich mit Themen von der Einführung in Penetrationstests und Red Teams bis hin zur Verfassung von erweiterten Exploits und benutzerdefinierter C2-Entwicklung. Andere Kurse haben spezialisierte Themen wie z. B. Purple Teams, Sicherheit für kabellose oder mobile Geräte und mehr.

Kurse:

SEC504 SEC568 SEC617
SEC535 SEC575 SEC660
SEC542 SEC580 SEC670
SEC556 SEC588 SEC699
SEC560 SEC598 SEC760
SEC565 SEC599 SEC501

14 Kurse | 339 Laborübungen | 11 Zertifikate

Digitale Forensik und Incident Response

In unseren Kursen für Digitale Forensik und Incident Response lernen Sie, wie Sie kompromittierte Systeme erkennen, wie Sie identifizieren, wann und auf welche Weise ein Übergriff erfolgt ist, wie Sie verstehen, was die Angreifer gestohlen oder geändert haben, und wie Sie Vorfälle eindämmen und beheben.

Kurse:

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

15 Kurse | 193 Laborübungen | 7 Zertifikate

Führungskompeten-zen bei der Cybersi-cherheit

Die SANS-Kurse für Führungskompetenzen bei der Cybersicherheit vermitteln Führungskräften die praktischen Fertigkeiten, die sie benötigen, um Sicherheitsteams aufzubauen und zu führen, mit anderen Führungskräften im technischen und geschäftlichen Bereich zu kommunizieren und Fähigkeiten zu entwickeln, die den Erfolg Ihrer Organisation vorantreiben.

Kurse:

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

12 Kurse | 381 Laborübungen | 8 Zertifikate

Cyber-verteidigung

Unsere SANS-Kurse für Cyberverteidigung sind intensive und immersive Schulungen, in denen Sie und Ihr Personal die nötigen praktischen Schritte meistern, um Systeme und Anwendungen gegen die gefährlichsten Bedrohungen zu verteidigen.

Kurse:

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

7 Kurse | 105 Laborübungen | 3 Zertifikate

Industrielle Steuersysteme

Die SANS-Kurse für industrielle Steuersysteme (Industrial Control Systems, ICS) umfassen praktische Schulungen, die offensive wie defensive Strategien zur Sicherung von ICS-Umgebungen vermitteln.

Kurse:

ICS310 ICS515
ICS410 ICS612
ICS418 ICS613
ICS456

2 Kurse | 49 Laborübungen | 1 Zertifikat

Open-Source Intelligence

Kurse für Open-Source Intelligence unterstützen die findigen Fachkräfte in diesem Bereich, die herausfinden müssen, welche Anforderungen ihre Kunden haben, um dann mithilfe von offen zugänglichen Quellen und Ressourcen überwiegend im Internet relevante Daten für ihre Untersuchung zu sammeln.

Kurse:

SEC497
SEC587

8 Kurse | 172 Laborübungen | 6 Zertifikate

Cloud-Sicherheit

Die SANS-Kurse für Cloud-Sicherheit bereiten Sicherheitsfachkräfte darauf vor, sichere Infrastrukturen, Plattformen und Anwendungen für die Cloud zu entwerfen, zu erstellen, zu implementieren und zu verwalten, sowie die gefährlichsten Bedrohungen für die Cloud zu erkennen, zu verhindern und abzuwehren.

Kurse:

SEC480 SEC540 FOR509
SEC488 SEC541 LDR520
SEC510 SEC545 SEC588
SEC522 SEC549

Kurssuche anhand der beruflichen Rolle in NICE

Das NICE-Framework (National Initiative for Cybersecurity Education) ist eine grundlegende Referenz, mit der sich Informationen zur Arbeit im Bereich der Cybersicherheit beschreiben und austauschen lassen.

Das Framework soll Ihnen helfen, die richtigen Schulungen und Zertifizierungen für die Cybersicherheitsrolle zu identifizieren, in der Sie derzeit arbeiten oder die Sie anstreben.

NICE

Design und Entwicklung

In diesen Kursen geht es um Recherchen, Konzeptualisierung, Entwurf, Entwicklung und Tests sicherer Technologiesysteme, u. a. von Perimeter- und Cloud-Netzwerken.

Kurse:

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

Implementierung und Betrieb

Diese Kurse beschäftigen sich mit der Implementierung, Administration, Konfiguration, Operation und Wartung, die für eine effektive und effiziente Leistung von Technologiesystemen nötig sind.

Kurse:

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

Aufsicht und Governance

Diese Kurse beschäftigen sich mit Führung, Management, Leitung und Fürsprache, damit die Organisation Cybersicherheitsrisiken für das Unternehmen effektiv managen und Arbeit im Bereich der Cybersicherheit durchführen kann.

Kurse:

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

Schutz und Verteidigung

In diesen Kursen lernen Sie, Risiken für Technologiesysteme oder Netzwerke zu identifizieren und zu analysieren und vor ihnen zu schützen. Sie umfassen die Untersuchung von Ereignissen oder Straftaten im Bereich der Cybersicherheit in Bezug auf Technologiesysteme und Netzwerke.

Kurse:

FOR508 ICS515 SEC556
FOR509 LDR516 SEC560
FOR518 LDR553 SEC565
FOR528 SEC401 SEC568
FOR572 SEC450 SEC573
FOR577 SEC503 SEC588
FOR578 SEC504 SEC598
FOR585 SEC510 SEC599
FOR589 SEC511 SEC660
FOR608 SEC522 SEC670
FOR610 SEC540 SEC673
FOR710 SEC541 SEC699
ICS410 SEC542

Cyberspace-Informationen

In diesen Kursen geht es um die Sammlung, Verarbeitung, Analyse und Verbreitung von Informationen aus allen möglichen Informationsquellen zu Programmen, Absichten, Fähigkeiten, Forschung und Entwicklung und operativen Aktivitäten ausländischer Akteure im Cyberspace.

Kurse:

FOR578 SEC541 SEC599
FOR589 SEC542 SEC660
ICS515 SEC560 SEC699
LDR553 SEC565 SEC760
SEC504 SEC568

Cyberspace-Effekte

In diesen Kursen geht es um die Planung, Unterstützung und Umsetzung von Cyberspace-Kompetenzen, deren primärer Zweck in der externen Verteidigung oder in der Durchführung von Stärkeprognosen im oder durch den Cyberspace liegt.

Kurse:

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

Ermittlungen

In diesen Kursen geht es um die Untersuchung von Ereignissen oder Straftaten im Bereich der Cybersicherheit in Bezug auf IT-Systeme, Netzwerke und digitale Beweismittel.

Kurse:

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

Industrielle Steuersysteme

Diese Kurse bilden ein Sicherheitsrahmen, der Betriebstechnologie und industrielle Steuersysteme gegen unabsichtliche oder absichtliche Risiken schützt.

Kurse:

ICS410 ICS456 ICS612
ICS418 ICS515 ICS613

Kurssuche anhand der beruflichen Rolle mit ECSF

Die richtigen Schulungspfade für Sie und Ihre Organisation

ECSF (European Cybersecurity Skills Framework) ist ein praktisches Tool, das Ihnen bei der Identifizierung und Artikulierung von Aufgaben, Kompetenzen, Fertigkeiten und Kenntnissen hilft, die mit den Rollen europäischer Cybersicherheits-Fachkräfte verknüpft sind. Das ECSF bietet Profile für 12 typische berufliche Rollen im Bereich der Cybersicherheit. Der Hauptzweck des ECSF besteht darin, EU-weit ein gemeinsames Verständnis zwischen Individuen, Arbeitgebern und Schulungsanbietern zu schaffen. SANS hat seine Kurse zu den 12 Cybersicherheitsrollen im ECSF in Beziehung gesetzt, damit Sie leichter den richtigen Kurs für Ihre aktuelle oder zukünftige Rolle finden können.

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)

FOKUSBEREICH IM SANS-LEHRPLAN

NEW 2CYBER Grundlagen von Cybersicherheit und IT

Alle Fachkräfte, denen praktische Aufgaben der Cybersicherheit zufallen, sollten über einen gemeinsamen Satz an Kompetenzen verfügen: Sie müssen wissen, wie Angreifer vorgehen, wie Verteidigungsmaßnahmen wirksam umgesetzt werden und wie sie auf Vorfälle reagieren, um Risiken zu mindern und Systeme ordnungsgemäß zu sichern.

Im Interesse der Sicherheit sollte die Messlatte für die Grundkompetenzen in Ihrer Organisation hoch angesetzt sein. Die New2Cyber-Kurse von SANS vermitteln folgende Kompetenzen:

- Techniken übernehmen, die den Fokus auf Sicherheitsprobleme mit hoher Priorität in Ihrer Organisation lenken
- Eine solide Grundlage von Kernrichtlinien und -praktiken aufbauen, mit denen Sie und Ihre Sicherheitsteams angemessen auf Vorfälle reagieren können
- Strategien und Techniken umsetzen, die Ihnen helfen, ein Unternehmen aus allen Richtungen zu verteidigen
- Die neuesten Angriffsvektoren identifizieren und Kontrollmaßnahmen umsetzen, die sie verhindern und aufdecken
- Angriffe mithilfe von Strategien und Tools erkennen
- Effektive Sicherheitskennzahlen für ein fokussiertes Playbook entwickeln, das IT-Fachkräfte implementieren, Auditoren validieren und Führungskräften verstehen können
- Ein umfassendes Sicherheitsprogramm umsetzen, dessen Fokus darauf liegt, Angriffe zu verhindern, aufzudecken und zu bekämpfen
- Eine interne Roadmap für die Sicherheit aufbauen, die heute und in Zukunft skalierfähig bleibt

„Bei dieser Schulung habe ich einen prima Überblick über alles erhalten, was mit Sicherheit zu tun hat. Sie hat gezeigt, dass es eine breite Fülle an Informationen gibt, mit denen man Sicherheitsprobleme findet, die man vorher vielleicht nicht in Betracht gezogen hätten.“

– Frank Perrelli, **IESO**

Stellenprofil für New2Cyber:

- Sicherheitsanalyst
- Analyst für digitale Forensik
- Sicherheitsingenieur
- Technischer Manager
- Auditor

SEC275: Foundations: Computers, Technology & Security™

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

4	38	80
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Die wichtigsten Hardwarekomponenten und zugehörige Arbeitsspeicherkonzepte verstehen
- Die Anwendungen von Virtualisierung und Containern samt ihrer Vor- und Nachteile verstehen
- Mit der Anatomie und Methodik häufiger Exploits und den von Angreifern verwendeten Tools vertraut werden
- Mit Tools für forensische Untersuchungen und ihrer Funktion vertraut werden
- Grundkenntnisse der am häufigsten verwendeten Befehle und Berechtigungen und der Zugriffskontrolle bei Linux erlangen
- Die Kernkonzepte von Netzwerken, Protokolle, verschiedene Servertypen und ihre Anwendungen verstehen
- In der Lage sein, das Ergebnis einfacher logischer Operationen zu ermitteln
- Mit Programmierungssyntax, Konstrukten und Fehlern in verbreiteten Sprachen vertraut werden
- Verschiedene Dateisysteme, Webtechnologie und Cloud-Computing-Modelle erkennen
- Mit den Konzepten und der Terminologie der Kryptografie vertraut werden
- Mit ethischen und rechtlichen Bedenken in Bezug auf Hacking vertraut werden
- Die Phasen eines Angriffs und wichtige Verteidigungsstrategien und -konzepte kennen
- Mit wichtigen Befehlen und Berechtigungen und der Zugriffskontrolle bei Windows CLI vertraut werden

Zielgruppe

- Quereinsteiger
- Selbstmotivierte Online-Lernende auf der Suche nach neuen Kompetenzen
- Studierende an Hochschulen und Fachhochschulen
- Geschäftsleute ohne speziellen Hintergrund in der Cybersicherheit
- Neueinstellungen in IT/Cybersicherheit
- Teilnehmer an Umschulungsprogrammen

James Lyne
Kursautor

* DoD 8140 APPROVED
sans.org/8140

SANS Foundations ist der umfassendste zertifizierte Einführungskurs für Cybersicherheit auf dem Markt. SEC275™ wurde von führenden Fachexperten entwickelt und baut eine Wissens- und Kompetenzgrundlage für Cybersicherheit auf, die Teilnehmern ohne technische Vorkenntnisse oder einschlägiger Erfahrung in der Branche ein Kompetenzniveau vermittelt, auf dem sie dieselbe Sprache sprechen können wie Fachkräfte. Erlernen Sie Grundkonzepte von Computer und Sicherheit und entwickeln Sie Programmierfähigkeiten in einer interaktiven Lernumgebung, unterstützt von weltweit anerkannten Kursleitern, Videovorträgen, praktischen Laborsegmenten und Übungen. SANS Foundations verwandelt Lernen in praktische Kompetenzen der wirklichen Welt und geht weit über das hinaus, was andere Grundkurse in Cybersicherheit bieten.

Meistern Sie die Grundlagen der Cybersicherheit.

Geschäftsorientierte Lernergebnisse

- Das Risiko grundlegender Kenntnislücken in Bezug auf Cybersicherheit in Ihrer Organisation reduzieren
- Kosten für externe Anstellungen reduzieren, indem latente Talente in Ihrem derzeitigen IT-Team entdeckt werden
- Den Erfolg von Neulingen bei weiterführenden Kursen verbessern, indem zunächst die Grundlagen abgedeckt werden
- Geschäftliches Wachstum ermöglichen, indem alle technischen Beschäftigten auf den höchsten Standard geschult werden
- Ihre Schulungsinvestitionen validieren, da Ihre Beschäftigten die GFACT-Zertifizierung erhalten
- Effektive Onboarding-Rahmen für Ihre Beschäftigten entwerfen, im Wissen, dass die Grundlagen der Cybersicherheit abgedeckt sind

„Meiner Meinung nach ist der Kurs SANS Foundation der beste Anfangspunkt, egal, ob Sie einen IT-Hintergrund haben oder nicht. Es gibt reichlich Beispiele für Einsteiger und Fortgeschrittene."
– Sri Ayu Ningsih, **Aleph-Labs**

„Obwohl ich eine höhere Rolle in der Sicherheit habe, war SANS Foundations fantastisch dafür, wichtige Konzepte zu wiederholen, die mir helfen, meine Aufgaben besser zu erfüllen."
– Noah Pack

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC275**

KURSFORMATE 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	30	14
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Selbstsicher über Themen, Begriffe und Konzepte der Informationssicherheit sprechen
- Die Prinzipien der geringsten Rechte verstehen und anwenden
- Den Dreiklang aus Vertraulichkeit, Integrität und Verfügbarkeit von Informationen verstehen und anwenden
- Bessere Passwörter erstellen, die sicherer, aber auch leichter zu merken und einzugeben sind
- Grundlegende Prinzipien, Prozesse, Verfahren und Anwendungen der Kryptografie verstehen
- Verstehen, wie ein Computer funktioniert

Zielgruppe

- Menschen, die neu im Bereich der Informationssicherheit sind und eine Einführung in die Grundlagen der Sicherheit brauchen
- Alle, die sich mit komplexen Fachbegriffen der Sicherheit konfrontiert sehen, die sie nicht verstehen, aber verstehen möchten
- Fachkräfte, die mit den grundlegenden Konzepten, Prinzipien und Begriffen der Sicherheit vertraut sein müssen, aber keine detaillierten Kenntnisse benötigen
- Alle, die sich zu einem Karrierewechsel entschlossen haben und eine formelle Schulung und Zertifizierung brauchen, damit sie sich auf Stellenangebote in der Cybersicherheit bewerben können
- Manager, die Sorge haben, dass ihr Unternehmen wegen eines großen Datenlecks Schlagzeilen in den Abendnachrichten machen könnte

Berufliche Rollen im NICE Framework

- 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)

Rich Greene
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Dieser Zertifizierungskurs zur Einführung ist der schnellste Weg, sich in die Informationssicherheit einzuarbeiten. Dieser Einführungskurs auf Einsteigerniveau, von kampferprobten Veteranen der Cybersicherheit verfasst und gelehrt, deckt ein breites Spektrum von Sicherheitsthemen ab und ist mit zahlreichen Beispielen aus dem richtigen Leben gespickt. Der Kursvortrag erläutert Begriffe und Konzepte im Detail. Praktische Laborübungen vertiefen diese Konzepte. Die ausgewogene Mischung aus technischen Themen, die leicht verständlich erklärt werden, macht diesen Kurs attraktiv für Teilnehmer, die wichtige Facetten der Cybersicherheit verstehen müssen. Wenn Sie sich die Grundlagen der Cybersicherheit schnell aneignen müssen, sind die Erklärungen bei SEC301 und die 14 praktischen Laborübungen genau das Richtige!

Geschäftsorientierte Lernergebnisse

- Die Assets Ihrer Organisation durch Anwendung der Prinzipien der geringsten Rechte sichern
- Die Grundlagen von Authentifizierung, Autorisierung, Kryptografie und defensiven Technologien wie Firewalls verstehen
- Über eine breite Fülle von Angriffen informieren, u. a. Social Engineering, Drive-by-Downloads, Watering-Hole-Angriffe, Lateralbewegung, Bot-Nets, Puffer-Überlauf und mehr
- Vermeiden, zur nächsten Schlagzeile in den Abendnachrichten zu werden

Zusammenfassung der Kursinhalte

TEIL 1: Grundlagen der Cybersicherheit

TEIL 2: Einführung in die Kryptografie

TEIL 3: Authentifizierung, Autorisierung und Netzwerke

TEIL 4: Wireless-Sicherheit, Netzwerkattacken und Malware

TEIL 5: Cybersicherheitstechnologien und Web-Sicherheit

„Der Inhalt von SEC301 war ausgezeichnet. Eine Fülle von Informationen wurde bereitgestellt, die bei der Arbeit und im Leben allgemein Anwendung finden werden. Die Laborübungen hatten hervorragende Anweisungen und waren prima zur Vertiefung des Materials."

– Jimmy T., **US-amerikanisches Militär**

„Ein sehr guter Kurs für die einfachen Grundlagen. Sehr hilfreich, weil auf einige Grundkonzepte näher eingegangen wird."

– Shruti Iyer, **DCS Corporation**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC301**

KURSFORMATE SEC301

Präsenzkurs | **Live online** | **OnDemand**

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

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

6	46	20
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Die Kernbereiche der Cybersicherheit meistern und wissen, wie ein Sicherheitsprogramm auf der Basis von Detektion, Reaktion und Prävention geschaffen wird
- Praktische Tipps und Tricks anwenden, die sich auf Sicherheitsprobleme mit hoher Priorität in Ihrer Organisation konzentrieren, und die richtigen Schritte ergreifen, die zu funktionierenden Sicherheitslösungen führen
- Verstehen, wie Kontrahenten ihre Taktiken und Techniken anpassen und wie Sie Ihrerseits Ihre Verteidigung entsprechend anpassen
- Identifizieren, was Ransomware ist und wie man sich besser dagegen verteidigt
- Eine verteidigungsfähige Netzwerkarchitektur (VLANs, NAC und 802.1x) auf Basis fortschrittlicher, beständiger Bedrohungsindikatoren einer Kompromittierung nutzen
- Die IAM-Methode (Identity and Access Management) verstehen und anwenden, einschließlich Aspekten der starken Authentifizierung (Mehrfaktor-Authentifizierung)

Zielgruppe

- Sicherheitsfachkräfte
- Manager
- Betriebspersonal
- IT-Ingenieure und Supervisoren
- Administratoren
- Forensikexperten, Penetrationstester und Auditoren
- Alle, die neu im Bereich der Informationssicherheit sind und einen Hintergrund in Informationssystemen und Netzwerken haben

Berufliche Rollen im NICE Framework

- 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
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Organisationen sind ständigen Bedrohungen ausgesetzt und müssen darauf vorbereitet sein, dass es früher oder später zu einer Kompromittierung kommen wird. Angriffe zeitnah zu erkennen und sofort darauf zu reagieren, ist wichtiger denn je. Je länger ein Widersacher in Ihrer Umgebung präsent ist, desto verheerender ist der Schaden, den er anrichtet. Vielleicht die wichtigste Frage in der modernen Informationssicherheit ist: „Wie schnell können wir einen Gegner entdecken, auf ihn reagieren und den Schaden beheben?“

Bei Informationssicherheit geht es darum, sich auf die Verteidigungsmaßnahmen in den wichtigsten Bereichen zu konzentrieren, insbesondere in Bezug auf die individuellen Anforderungen Ihrer Organisation. Bei SEC401™ lernen Sie die grundlegende Terminologie und die innere Funktionsweise von Computer- und Informationssicherheit kennen und erfahren, wie sie sich effektiv auf Ihre spezifischen Herausforderungen anwenden lassen. Sie erlangen wesentliche Kenntnisse, die Sie brauchen, um Systeme und Organisationen zuversichtlich zu sichern.

SEC401™ vermittelt Ihnen die effektivsten Schritte zur Verhinderung von Angriffen und zur Erkennung von Gegnern und gibt Ihnen umsetzbare Techniken an die Hand, die Sie an Ihrem Arbeitsplatz unmittelbar anwenden können. Durch praktische Tipps und Einblicke sind Sie besser vorbereitet, im fortlaufenden Kampf gegen eine breite Fülle von Cybergegnern, die Ihre Umgebung zu infiltrieren versuchen, die Oberhand zu behalten.

Geschäftsorientierte Lernergebnisse

- Sicherheitsbedenken mit hoher Priorität angehen
- Stärken und Unterschiede in der Sicherheit bei den größten Cloud-Anbietern nutzen
- Einen Netzwerktransparenzplan erstellen, der bei der Validierung von Angriffsflächen hilft
- Durch Härtung und Konfigurationsmanagement die Angriffsfläche einer Organisation reduzieren

Zusammenfassung der Kursinhalte

TEIL 1: Netzwerksicherheit und Cloud-Grundlagen
TEIL 2: Wirksame Verteidigung
TEIL 3: Schwachstellenmanagement und Reaktion
TEIL 4: Technologien der Datensicherheit
TEIL 5: Sicherheit bei Windows und Azure
TEIL 6: Sicherheit bei Containern, Linux und Mac

„SEC401 bietet einen ausgezeichneten Überblick über die Grundlagen der Sicherheit, der von erfahrenen Fachkräften vermittelt wird.“
– Jason W., **US-Bundesbehörde**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC401**

KURSFORMATE SEC401

Präsenzkurs | **Live online** | **OnDemand**

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

2 Kurstage | 12 CPEs

Vermittelte Kompetenzen

- Die fünf „goldenen Elemente“ von effektiven Berichten, Briefings, E-Mails und anderen Texten zur Cybersicherheit entdecken
- Sich diese Elemente als Teil Ihres Arsenals aneignen, durch praktische Übungen, die auf häufige Sicherheitsszenarien zurückgehen
- Erfahren, welche wichtigen Themen in Sicherheitsberichten und anderen schriftlichen Mitteilungen angegangen werden sollten
- Verstehen, wie Sie Formulierungen, Struktur, Optik und Ton optimal wählen
- Schwachstellen in Textbeispielen erkennen und verbessern, um die eigenen Fähigkeiten zu üben
- Mithilfe praktischer Checklisten von Anfang an klar und effektiv schreiben

Zielgruppe

- Manager oder Teammitglieder
- Berater oder Beschäftigte mit internem Fokus
- Experten oder Anfänger
- Verteidiger oder Angreifer
- Erdlinge oder Außerirdische

Berufliche Rollen im NICE Framework

- 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
Kursautor

Möchten Sie besser schreiben? Dann lernen Sie, sich in die Köpfe Ihrer Leserschaft zu versetzen! Entdecken Sie, wie Sie Aufmerksamkeit wecken, Widerstand abbauen und das Interesse fesseln, damit Ihre Botschaft ankommt – selbst wenn Ihre Zielgruppe beschäftigt oder gleichgültig ist. Dieser besondere Kurs ist ganz auf Fachkräfte für Cybersicherheit abgestimmt. Stärken Sie Ihre Schreibkompetenz und bringen Sie Ihre Sicherheitskarriere einen großen Schritt voran!

Geschäftsorientierte Lernergebnisse

- Die Assets Ihrer Organisation durch Anwendung der Prinzipien der geringsten Rechte sichern
- Die Grundlagen von Risikomanagement, Sicherheitsrichtlinien und Authentifizierung/Autorisierung/Verantwortlichkeit verstehen
- In der Lage sein, über eine breite Fülle von Angriffen zu informieren, u. a. Social Engineering, Drive-by-Downloads, Watering-Hole-Angriffe, Lateralbewegung und mehr
- Vermeiden, zur nächsten Schlagzeile in den Abendnachrichten zu werden

Zusammenfassung der Kursinhalte

TEIL 1: Cybersecurity Writing: Hack the Reader – Tag 1

TEIL 2: Cybersecurity Writing: Hack the Reader – Tag 2

„Schreibkompetenz im Bereich Cybersicherheit ist unerlässlich für die berufliche Weiterentwicklung.“

– R. Wajda, **Secure Cloud LLC**

„Ich habe kurz vor diesem Kurs bei meinem Unternehmen eine Schulung zur Verbesserung der schriftlichen Kommunikation gemacht. Dieser Kurs ist ähnlich, aber der Fokus auf Cybersicherheit ist von unschätzbarem Wert!“

– Andrew Walker, **Novant Health**

„Ausgezeichneter Kurs. Er bietet einen Beurteilungsrahmen und einen Leitfaden zum Verfassen zukünftiger Texte.“

– Jordan Whitley, **New York Life**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC402**

KURSFORMATE SEC402

OnDemand

FOKUSBEREICH IM SANS-LEHRPLAN

Offensivoperationen

Organisationen verlassen sich auf offensive Taktiken, wenn es darum geht, ihre Systemschwachstellen aufzudecken und zu verstehen, damit sie bekannte Probleme beheben können, bevor der Feind angreift.

Je weiter sich Widersacher und Angriffe entwickeln, desto besser müssen Penetrationstester und Team Rot aktuelle Angriffe aus der wirklichen Welt emulieren, Probleme entdecken und ihre Ergebnisse angemessen melden, wenn sie dem Sicherheitsteam nützliche Erkenntnisse bereitstellen wollen.

SANS-Kurse für Offensivoperationen vermitteln Ihnen folgende Kompetenzen:

- Die stärksten und gängigsten Angriffe von heute emulieren
- Schwachstellen in Zielsystemen entdecken
- Schwachstellen unter kontrollierten Umständen ausnutzen
- Technisch kompetent das Risiko und potenzielle geschäftliche Auswirkungen ermitteln und dokumentieren
- Professionelle und sichere Tests durchführen, deren Umfang und Einsatzregeln sorgfältig entworfen wurden
- Einer Organisation helfen, Ressourcen die richtige Priorität zu verleihen

„Innerhalb einer Woche hat mein Kursleiter eine Brücke geschlagen von der Suche nach typischen Schwachstellen zur wahren Kunst der Penetrationstests. Meinen Dank an SANS, weil ich und mein Unternehmen nun viel bessere Fähigkeiten auf dem Gebiet der Informationssicherheit haben.“

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

Stellenprofil für Offensivoperationen:

- System-/Netzwerk-Penetrationstester
- Penetrationstester für Anwendungen
- Incident Handler
- Schwachstellenforscher
- Exploit-Entwickler
- Mitglied im Red Team
- Mobile Security Manager

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

GCIH Incident Handler
giac.org/gcih
CyberLive
DoD 8140*

6	38	Über 30
Tage Programm	CPEs	Laborübungen

Zielgruppe

- Incident Handler
- Leiter von Incident-Response-Teams
- Systemadministratoren, die an vorderster Front ihre Systeme verteidigen und auf Angriffe reagieren
- Anderes Sicherheitspersonal, das als Erstes reagiert, wenn Systeme angegriffen werden
- Allgemeine Sicherheitsfachkräfte und Sicherheitsarchitekten, die ihre Systeme so entwerfen, erstellen und betreiben möchten, dass Angriffe verhindert, erkannt und abgewehrt werden

Berufliche Rollen im NICE Framework

- 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
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Mit SEC504™ transformieren Sie Ihre Kompetenzen bei der Incident Response und versetzen sich in die Angreifer hinein. Durch mehr als 30 praktische Laborübungen lernen Sie, wie Sie Cybersicherheitsvorfälle untersuchen, Threat Intelligence entwickeln und Verteidigungsstrategien gegen reale Bedrohungen anwenden. Von Passwortangriffen bis zu MFA-Bypass-Techniken auf Cloud-Diensten bietet dieser Kurs eine eingehende Einführung in die neuesten Hackertaktiken. Sie beschäftigen sich mit hochmodernen Tools und simulieren Live-Angriffe, um Ihre Verteidigungskompetenzen zu schärfen. Gleichzeitig bereiten Sie sich auf die GIAC-Zertifizierung GCIH vor. Nach dem Kurs sind Sie bereit, sowohl Cloud- als auch On-Premise-Umgebungen gegen neu aufkommende Cyberbedrohungen zu verteidigen.

Geschäftsorientierte Lernergebnisse

- Einen dynamischen Ansatz auf die Incident Response anwenden
- Bedrohungen mit Host-, Netzwerk- und Protokollanalyse identifizieren
- Best Practices für effektive Incident Response in der Cloud erlernen
- PowerShell zur Datenerfassung und Cyberbedrohungsanalyse nutzen
- Prozesse für Cyberermittlungen mit Live-Analysen, Netzwerkeinblicken und Arbeitsspeicherforensik erlernen
- Spotlight-Verteidigungsstrategien zum Schutz kritischer Assets erlernen
- Lernen, wie Angreifer Cloud-Systeme gegen Organisationen nutzen
- Angreifertechniken zur Umgehung von Endpunkt-Detektionstools verstehen
- Lernen, wie Angreifer komplexe Cloud-Schwachstellen ausnutzen
- Verstehen, mit welchen Schritten Angreifer sich nach der anfänglichen Kompromittierung intern umsehen und weiterbewegen
- Lernen, wie Angreifer öffentlich zugängliche Systeme einschl. Microsoft 365 ausnutzen

Zusammenfassung der Kursinhalte

TEIL 1: Incident Response und Cyberermittlungen
TEIL 2: Scanning- und Enumerationsangriffe
TEIL 3: Passwortangriffe und Exploit-Frameworks
TEIL 4: Angriffe auf Web-Anwendungen
TEIL 5: Evasion- und Post-Exploitation-Angriffe
TEIL 6: „Capture-the-Flag"-Übung

„Incident Response ist in kleinen Unternehmen der Aspekt, der am schlechtesten genutzt wird. SEC504 befähigt uns, dem Management ihren Wert zu vermitteln."

– David Freedman, **Nationwide Payment Solutions**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC504**

KURSFORMATE SEC504

Präsenzkurs **Live online** **OnDemand**

SEC542: Web App Penetration Testing and Ethical Hacking™

GWAPT
Web Application Penetration Tester
giac.org/gwapt
CyberLive

6	36	Über 30
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Die Methodik der Open Source Foundation for Application Security auf Penetrationstests für Web-Anwendungen übertragen, um sicherzustellen, dass sie einheitlich, reproduzierbar und gründlich sind und unter Qualitätskontrolle stehen
- Die Ergebnisse aus automatisierten Web-Testtools analysieren, um Ergebnisse zu validieren, ihre geschäftlichen Auswirkungen herauszufinden und falsch positive Ergebnisse zu eliminieren
- Wichtige Mängel in Web-Anwendungen manuell aufdecken
- Während eines Penetrationstests mit Python Test- und Exploitskripts erstellen
- Mängel in Bezug auf SQL Injections entdecken und ausnutzen, um das wahre Risiko für die betroffene Organisation festzustellen
- Schwachstellen durch unsichere Deserialisierung verstehen und mit Ysoserial und ähnlichen Tools ausnutzen
- Konfigurationen erstellen und Payloads innerhalb anderer Web-Angriffe testen
- Mit ZAP, Intruder von Burp Suite und ffuf mögliche Eingaben für Fuzz-Injection-Angriffe erstellen
- Den Einfluss von Mängel-Exploits bei Web-Anwendungen erläutern

Zielgruppe

- Allgemeine Sicherheitsfachkräfte
- Penetrationstester
- Ethische Hacker
- Entwickler von Web-Anwendungen
- Designer, Architekten und Entwickler von Websites

Berufliche Rollen im NICE Framework

- 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
Kursautor

Timothy McKenzie
Kursautor

Bojan Zdrnja
Kursautor

SEC542™ befähigt die Teilnehmer, Sicherheitsschwachstellen in Web-Anwendungen schnell zu beurteilen und offenzulegen und dabei zu zeigen, welche Folgen es für das Unternehmen haben könnte, wenn sie ausgenutzt würden. Sie sammeln praktische Erfahrung bei der Ausnutzung von Web-Anwendungen innerhalb Ihres Unternehmens und meistern die Tools und Methoden von Angreifern. Durch praktische Übungen erlernen sie einen bewährten Prozess für Penetrationstests bei Web-Anwendungen, schleusen eine SQL Injection in Back-End-Datenbanken ein, um zu lernen, wie Angreifer sensible Daten herausfiltern, und dominieren eine Zielinfrastruktur mithilfe von Cross-Site-Scripting-Angriffen.

Geschäftsorientierte Lernergebnisse

- Eine wiederholbare Methodik für hochwertige Penetrationtests anwenden
- Wichtige Mängel in Web-Anwendungen entdecken und ausnutzen
- Die potenziellen Auswirkungen von Schwachstellen in Web-Anwendungen erklären
- Die Bedeutung der Sicherheit von Web-Anwendungen für den Sicherheitsstatus insgesamt vermitteln
- Wichtige Tools zum Angriff auf Web-Anwendungen effizienter einsetzen
- Berichte über Penetrationstest bei Web-Anwendungen verfassen

Zusammenfassung der Kursinhalte

TEIL 1: Einführung und Informationserfassung

TEIL 2: Fuzzing-, Scanning-, Authentifizierungs- und Sitzungstests

TEIL 3: Injection

TEIL 4: XSS, SSRF und XXE

TEIL 5: CSRF, Logikfehler und erweiterte Tools

TEIL 6: „Capture-the-Flag"-Übung

„In diesem Kurs habe ich gelernt, mich bei der Durchführung eines Penetrationstests wirklich auf die Methodik zu konzentrieren. Während der „Capture-the-Flag"-Übung wurde mir klar, wie viel Zeit man verschwenden kann, wenn man die Methodik nicht berücksichtigt."

– Sean Rosado, **RavenEye**

„SEC542 macht schnell mit verschiedenen Tools und Techniken zur Erkundung einer Ziel-Website vertraut."

– Gareth Grindle, **QA Ltd.**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC542**

KURSFORMATE SEC542

Präsenzkurs | **Live online** | **OnDemand**

SEC556: **IoT Penetration Testing™**

3	18	15
Kurstage	CPEs	Laborübungen

Vermittelte Kompetenzen

- IoT-Steuerelemente auf Netzwerkseite, Web-Anwendungen und API-Endpunkte mit IoT-Fokus beurteilen
- Hardware untersuchen, um die Funktionalität festzustellen und Interaktionspunkte zu finden und damit Daten aus der Hardware zu gewinnen
- Firmware aus Hardware und mit anderen Mitteln freigeben und auf Geheimnisse und Implementierungsfehler untersuchen
- Die Wireless-Technologien WiFi, LoRA und Zigbee mit Sniffern untersuchen, damit interagieren und sie manipulieren, und Sicherheitsfehler bei der Implementierung verstehen
- Zur Gerätemanipulation mit Bluetooth Low Energy interagieren
- Die Wiederherstellung unbekannter Funkprotokolle automatisieren, um Angriffe nachzuspielen und eine zusätzliche Analyse durchzuführen

Zielgruppe

- Penetrationstester
- Entwickler von eingebetteten Systemen
- Sicherheitsanalysten
- Sicherheitsarchitekten
- Produktsicherheitsingenieure
- IoT-Produktentwickler
- Alle, die ein IoT-Gerät auf den Markt bringen

Berufliche Rollen im NICE Framework

- 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
Kursautor

James Leyte-Vidal
Kursautor

Ein wachsender Trend in den letzten Jahren bestand darin, dass kleinformatige Computergeräte auf Netzwerke zugreifen. Dadurch soll Konnektivität für Geräte geschaffen werden, die bisher normalerweise nicht vernetzt waren. Die Meinungen gehen auseinander, ob Haushaltsgeräte wirklich Zugang zum Internet benötigen, aber unbestritten ist, dass das Internet der Dinge (Internet of Things, IoT) nicht mehr wegzudenken ist. Es ermöglicht vielen wirklich nützlichen Geräten größere Konnektivität und bringt zu Hause wie in der Arbeitswelt erhebliche Vorteile.

Leider beachten bei dieser Ausbreitung der vernetzten Technologie viele dieser Geräte die Sicherheit im Designprozess nur ungenügend oder gar nicht. Dieses Verhalten kennen wir von anderen Testarten. Bei IoT ist die Lage jedoch anders, weil es eine Mischung vieler verschiedener Technologiestacks nutzt, z. B. angepasste Versionen von Betriebssystemen, Web- und API-Schnittstellen, verschiedene Netzwerkprotokolle (z. B. Zigbee, LoRA, Bluetooth/BLE, WiFi) und herstellerspezifische Funkverbindungen. Dieses breite Spektrum diverser, schlecht gesicherter Technologien stellt eine willkommene Chance dar, in Netzwerke einzugreifen, und bietet Gelegenheiten zur Modifizierung von Benutzerdaten, zur Manipulation von Netzwerkverkehr und mehr.

Bei SEC556™ werden Sie mit den häufigsten Schnittstellen von IoT-Geräten vertraut und lernen einen Prozess sowie ein IoTA-Test-Framework (Internet of Things Attack) kennen, mit dem Sie diese Geräte in vielen Layern des OSI-Modells (Open Systems Interconnection) auswerten können. Von der Analyse der Firmware und Netzwerkprotokolle über Probleme bei der Hardware-Implementierung bis hin zu Anwendungsmängeln geben wir Ihnen Tools und praktische Techniken für die Beurteilung des stetig wachsenden Sortiments an IoT-Geräten an die Hand. Der Kursansatz lehrt, wie das IoT-Ökosystem vieler verschiedener Branchen untersucht werden kann, von Kfz-Technik über Gesundheitswesen und Produktion bis zu industriellen Steuersystemen. Alle Fälle verwenden die gleiche Methodik, aber unterschiedliche Risikomodelle.

Zusammenfassung der Kursinhalte

TEIL 1: Einführung in IoT-Netzwerkverkehr und Web-Services

TEIL 2: Exploits von IoT-Hardwareschnittstellen und Firmware-Analyse

TEIL 3: Ausnutzung von Wireless-IoT: WiFi, BLE, Zigbee, LoRA und SDR

„Es gelingt den Laborübungen gut, Konzepte zu vertiefen und zu verdeutlichen. Die Arbeit, die nötig war, um sie skalierbar, virtualisierbar und wiederholbar zu machen, ist wirklich erstaunlich."

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

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC556**

KURSFORMATE SEC556

Präsenzkurs | **Live online** | **OnDemand**

SEC560: **Enterprise Penetration Testing™**

GPEN
Penetration Tester
giac.org/gpen

ANAB ACCREDITED
CyberLive
DoD 8140*

6	36	Über 30
Tage Programm	CPEs	Laborübungen

Zielgruppe

- Sicherheitspersonal, dessen Aufgabe es ist, Netzwerke und Systeme zu bewerten, um Schwachstellen zu finden und zu beheben
- Penetrationstester
- Ethische Hacker
- Verteidiger, die Offensivmethodik, -tools und -techniken besser verstehen möchten
- Auditoren, die ihre technische Kompetenzen vertiefen müssen
- Mitglieder eines Red Teams
- Mitglieder eines Blue Teams
- Forensikfachkräfte, die Offensivtaktiken besser verstehen möchten
- Incident Responder, die verstehen möchten, wie Angreifer denken

Berufliche Rollen im NICE Framework

- 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
Kursautor

Jeff McJunkin
Kursautor

* DoD 8140 APPROVED
sans.org/8140

SEC560: Enterprise Penetration Testing™, der beste SANS-Kurs für Penetrationstests, vermittelt Ihnen, wie Sie geschäftliche Risiken für komplexe moderne Unternehmen bewerten und mindern. In praktischen Laborübungen lernen Sie, wie Sie Penetrationstests mit den neuesten Tools und Techniken planen, ausführen und anwenden. SEC560™ ist ideal für Penetrationstester, Systemadministratoren und Verteidiger. Sie lernen verstehen, wie Angreifer denken, damit Sie die Sicherheit Ihrer Organisation sofort verbessern können. Bei SEC560™ lernen Sie, wie Sie einen umfassenden, hochwertigen Penetrationstest durchführen, und erproben es am Ende des Kurses. Nachdem Sie Ihre Kompetenzen in umfassenden und anspruchsvollen Laborübungen aufgebaut haben, gipfelt der Kurs in einem letzten, wirklichkeitsgetreuen Penetrationstest-Szenario. Sie führen einen End-to-End-Penetrationstest durch, bei dem Sie die im gesamten Kurs erworbenen Kenntnisse, Tools und Prinzipien anwenden, während Sie Schwachstellen in einer realistischen Zielorganisation entdecken und ausnutzen.

Vermittelte Kompetenzen

- Einen Penetrationstest in einem Unternehmen ordnungsgemäß planen und vorbereiten
- Durch detaillierte Aufklärung Social Engineering und Phishing unterstützen, die richtigen Daten anvisieren und angemessene Zielsetzungen demonstrieren
- Passwörter auf sichere und effektive Weise erraten, um sich Zugang zur Zielumgebung zu verschaffen oder tiefer in das Netzwerk einzudringen
- Zielsysteme auf verschiedene Weisen ausnutzen, um sich Zugang zu verschaffen und das echte Risiko für das Geschäft zu messen
- Ausgenutzte Systeme gründlich ausplündern, um Informationen zu sammeln, und tiefer in das Netzwerk eindringen, um Ihren Zielen näherzukommen
- Mit Techniken zur Berechtigungseskalation den Zugriff auf Windows- oder Linux-Systeme oder sogar Active Directory selbst verbessern
- Durch flexible Fortbewegung im System den Zugriff auf die Organisation weiter ausbauen und Risiken identifizieren, die bei oberflächlichen Scans nicht gefunden wurden
- Mit mehreren C2-Frameworks (Command & Control) kompromittierte Hosts aus der Ferne managen und ausplündern
- Angriffe auf die Domänen und Strukturen von Active Directory ausführen, die von den meisten Organisationen genutzt werden
- Mehrere Kerberos-Angriffe ausführen, u. a. Kerberoasting, Golden Ticket und Silver Ticket
- Azure aus der Ferne auskundschaften, sowohl mit als auch ohne Anmeldeinformationen
- Entra ID-Passwort-Sprühangriffe ausführen

Zusammenfassung der Kursinhalte

TEIL 1: Planung, Umfang, Erkundung und Scanning für umfassende Penetrationstests
TEIL 2: Anfänglicher Zugriff, Payloads und Situationsbewusstsein
TEIL 3: Berechtigungseskalation, Persistenz und Passwortangriffe
TEIL 4: Lateralbewegung und Berichte
TEIL 5: Domänendominierung und Azure Annihilation
TEIL 6: Penetrationstest und „Capture-the-Flag"-Übung

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC560**

KURSFORMATE SEC560

Präsenzkurs | **Live online** | **OnDemand**

SEC565: Red Team Operations and Adversary Emulation™

GRTP
Red Team Professional
giac.org/grtp

6	36	Über 25
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Threat Intelligence konsumieren und einen Red-Team-Einsatz planen
- Die erforderliche Infrastruktur für eine erfolgreiche Operation einrichten und dabei die Betriebssicherheit berücksichtigen
- Waffen entwickeln, mit denen Sie eine Organisation infiltrieren können
- Wertvolle Daten auflisten und extrahieren, um Ihre Ziele mit automatisierten Tools, bei Bedarf aber auch manuell zu erreichen
- Sich in einem Unternehmensnetzwerk lateral bewegen und einnisten
- Berechtigungen mit einer Vielzahl von Angriffsvektoren und Fehlkonfigurationen erweitern, die Sie nun identifizieren können
- Sinnvolle Ergebnisberichte formulieren, die für Ihren Kunden optimal wertvoll sind

Zielgruppe

- Sicherheitsfachkräfte
- Penetrationstester
- Mitglieder eines Red Teams
- Mitglieder eines Blue Teams
- Auditoren
- Informationssicherheitsmanager

Berufliche Rollen im NICE Framework

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

Jean-François Maes
Kursautor

David Mayer
Kursautor

Penetrationstests sind effektiv in der Lage, Schwachstellen aufzulisten, aber weniger effektiv, was die Kommunikation mit Personal und Prozessen auf der defensiven Seite angeht. So wird Blue Teams oder Verteidigern möglicherweise nicht ausreichend klar, welche Verbesserungen sie vornehmen müssen. Und damit wiederum stecken Organisationen in einem Kreislauf fest, in dem sie sich lediglich auf die Schwachstellen in ihren Systemen konzentrieren, anstatt Verteidigern zu vermitteln, wie sie Angriffe effektiv erkennen und auf sie reagieren.

Bei SEC565™ lernen die Teilnehmer, wie sie Red-Team-Einsätze mit Gegneremulation vom Anfang bis zum Ende planen und ausführen. Sie lernen, wie sie ein Red Team organisieren, Threat Intelligence konsumieren, um Maßnahmen gegen Gegner-TTPs (Taktiken, Techniken und Prozeduren) zu erstellen, diese TTPs emulieren, die Ergebnisse des Red-Team-Einsatzes melden und analysieren und letztlich den Sicherheitsstatus der Organisation insgesamt verbessern. Im Rahmen des Kurses führen die Teilnehmer eine Gegneremulation gegen eine Zielorganisation durch, die anhand einer Unternehmensumgebung modelliert wurde, mit Active Directory, indizienreichen E-Mails, Dateiservern und Endpunkten, die in Windows ausgeführt werden.

Lerninhalte

- Gegner mithilfe von Threat Intelligence studieren, damit sie emuliert werden können
- Einen Gegneremulationsplan erstellen
- Maßnahmen dem Framework MITRE® ATT&CK™ zuordnen, um die Kommunikation mit dem Blue Team zu erleichtern
- Eine widerstandsfähige, fortschrittliche C2-Infrastruktur aufbauen
- Während des Einsatzes die Betriebssicherheit aufrechterhalten
- Den anfänglichen Zugang nutzen, ausbauen und sich durch ein Netzwerk verbreiten
- Active Directory auflisten und angreifen
- Sensible Daten auf sichere Weise erfassen und exfiltrieren
- Einen Einsatz abschließen, Ergebnisse liefern und einen erneuten Test planen

Zusammenfassung der Kursinhalte

TEIL 1: Gegneremulation und Threat Intelligence planen
TEIL 2: Infrastruktur und Betriebssicherheit angreifen
TEIL 3: Eindringen und verharren
TEIL 4: Angriffe auf Active Directory und Lateralbewegung
TEIL 5: Ziel erreichen und melden
TEIL 6: Immersive „Capture-the-Flag"-Übung für ein Red Team

„Der Kursinhalt ist absolut toll. Selbst wenn Sie bereits einiges über das Thema wissen, gibt es immer noch eine Menge von Informationen, die Ihr Verständnis weiter verbessern und Ihre Verfahren stärken werden!"

– Kemmner Lankfurd, **NetPlas Neckarsulm**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC565**

KURSFORMATE SEC565

Präsenzkurs | **Live online** | **OnDemand**

SEC568: Product Security Penetration Testing – Safeguarding Supply Chains and Managing Third-Party Risk™

5	30	Über 20
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Den gesamten Produktsicherheits-Testprozess auf kommerzielle Anwendungen anwenden
- Die Auswirkungen von Drittanbieter-Anwendungen und das Risiko von Lieferkettenangriffen mindern
- Durch Analyse statischer Firmware feststellen, was auf einem Gerät ausgeführt wird
- Proprietäre Protokolle analysieren
- Daten mit Python, Pandas DataFrame und Jupyter Notebooks sammeln, vorbereiten und analysieren
- Angriffsstrukturen konstruieren und mithilfe der Risk-Scoring-Methodik das Risiko der einzelnen erkannten Bedrohungen feststellen

Zielgruppe

- Netzwerk- und System-Penetrationstester, die fundierte Fähigkeiten zur Durchführung erweiterter Tests benötigen (z. B. Analyse unbekannter Netzwerkprotokolle)
- Anwendungsentwickler, die lernen müssen, welche Auswirkungen schlechte Programmierung hat und wie Sie aus der Perspektive eines Angreifers Produktmängel aufspüren können
- Sicherheitsauditoren, die Kernkompetenzen zur eingehenden Prüfung von Produkten benötigen und gleichzeitig wissen müssen, wie sie den Audit auf eine spezifische Organisation abstimmen können
- SOC-Analysten, Incident Responder und Sicherheitsingenieure, die ergänzende Kompetenzen benötigen, um Bedrohungen aufzuspüren, die neue Produkte in Netzwerke und Endpunkte einführen können

Berufliche Rollen im NICE Framework

- Cyber Defense Infrastructure Support Specialist (OPM 521)
- System Testing and Evaluation Specialist (OPM 671)

Douglas McKee
Kursautor

Ismael Valenzuela
Kursautor

Angreifer nutzen zur Kompromittierung von Software-Lieferketten neue Methoden, die herkömmliche Sicherheitskontrollmaßnahmen auf mehreren Angriffsflächen umgehen. SEC568™ ist eine umfassende Schulung, die Ihnen das technische Know-how an die Hand gibt, um präzise Einschätzungen der Produktsicherheit und Risikoanalysen durchzuführen. Sie erwerben die Kenntnisse und Kompetenzen, die Sie brauchen, um Ihre digitalen Assets in einer von stetigem und raschem Wandel geprägten Bedrohungslandschaft zu schützen.

SEC568: Product Security Penetration Testing™ vermittelt Ihnen Grundkenntnisse und praktische Methodiken für Produktsicherheitstests und Risikoanalyse. Die Teilnehmer nutzen offensive Taktiken mit einer defensiven Denkweise und lernen dadurch, wie sie die Risiken bei der Einführung von Desktop-, Mobil- und proprietären Protokollen sowie Hardwaregeräten in die Umgebung analysieren können. Sie nutzen eine breite Fülle von technischen Kompetenzen, um ein tieferes Verständnis für die Arbeitsweise eines Ziels zu entwickeln.

Jeder Kursabschnitt wird von Flussdiagrammen begleitet, die den Teilnehmern eine Roadmap zur Navigation komplexer Themen mit dokumentierten Prozessen und klar definierten Zielsetzungen bereitstellen. Durch mehr als 20 praktische Übungen und eine vollständig angeleitete Abschlussübung sammeln sie praktische Erfahrungen, die im Laufe des Kurses technisch immer mehr in die Tiefe gehen.

Zusammenfassung der Kursinhalte

TEIL 1: Penetrationstests für die Produktsicherheit

TEIL 2: Einfache Enumeration, Bedrohungsmodellierung und Einführung in Deep Enumeration

TEIL 3: Analyse von Binärcode und Deep-Network-Analyse

TEIL 4: Deep-Network-Analyse und Risikoanalyse

TEIL 5: Abschlussübung

„Das Material und die Kursleiter sind ausgezeichnet. Doug und Ismael gaben Informationen zu diesem Thema weiter, die ich nirgendwo sonst gefunden habe."

– Brian Wiggins, **National Hockey League**

„Das ist genau das, worüber wir bei der Arbeit in Bezug auf Bedrohungsmodellierung und neue Software im Netzwerk gesprochen haben."

– Steven Ostrander, **Booz Allen Hamilton**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC568**

KURSFORMATE SEC568

Präsenzkurs **Live online**

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

GMOB
Mobile Device Security Analyst
giac.org/gmob

6	36	Über 20
Tage Programm	CPEs	Laborübungen

Zielgruppe

- Penetrationstester
- Ethische Hacker
- Auditoren, die ihre technische Kompetenzen vertiefen müssen
- Sicherheitspersonal, dessen Aufgaben die Bewertung, Bereitstellung oder Sicherung von Smartphones und Tablets umfassen
- Netzwerk- und Systemadministratoren, die Smartphones und Tablets unterstützen

Stellen Sie sich eine Angriffsfläche vor, die in Ihrer gesamten Organisation verbreitet ist und sich in den Händen eines jeden Benutzers befindet. Sie wechselt regelmäßig den Ort, dient zur Speicherung hoch sensibler und geschäftskritischer Daten und nutzt zahlreiche verschiedene Wireless-Technologien, die allesamt anfällig für einen Angriff sind. Leider ist diese Angriffsfläche bereits Realität: durch Mobilgeräte. Diese Geräte stellen in den meisten Organisationen die größte Angriffsfläche dar, und gleichzeitig sind diese Organisationen oft nicht in der Lage, sie richtig einzuschätzen.

SEC575: iOS and Android Application Security Analysis and Penetration Testing™ versetzt Sie in die Lage, die Stärken und Schwächen von Apple iOS- und Android-Geräten (einschl. Android 14 und iOS 17) in Bezug auf die Sicherheit zu verstehen. Mobilgeräte sind nicht länger einfach nur bequem: Für Benutzer weltweit haben sie sich zu einem unverzichtbaren Hilfsmittel entwickelt, das tagtäglich dabei ist und oft sogar konventionelle Computer ersetzt, was die alltäglichen Datenanforderungen im Unternehmen betrifft. Dieser Trend ist in Unternehmen, Krankenhäusern, Banken, Schulen und Ladengeschäften auf der ganzen Welt zu beobachten. Heute verlassen sich Benutzer mehr denn je auf Mobilgeräte. Wir wissen das, und Kriminelle wissen es auch. SEC575™ untersucht das gesamte Spektrum dieser Geräte.

Zusammenfassung der Kursinhalte

TEIL 1: iOS

TEIL 2: Android

TEIL 3: Analyse statischer Applikationen

TEIL 4: Analyse und Manipulation dynamischer Mobile-Apps

TEIL 5: Penetrationstests

TEIL 6: Praktische „Capture-the-Flag“-Übung

„Du denkst, du kennst dich bei der Cybersicherheit aus, und dann sitzt du in SANS SEC575 und dir wird plötzlich klar, dass es noch sehr viel mehr zu lernen gibt!“

– Steve M.

„SEC575 ist eine Schulung, die unmittelbar praktisch angewandt werden kann – sowohl von Penetrationstestern als auch von Entwicklern.“

– Roy Cabaniss, **LGS**

„Sehr gut organisiert, absolut interessant und auch noch unterhaltsam. Sehr effektiv, um Interesse für die App-Analyse zu entwickeln und sie zu erlernen.“

– Myriam Leggieri, **Google**

Jeroen Beckers
Kursautor

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC575**

KURSFORMATE SEC575

Präsenzkurs | **Live online** | **OnDemand**

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

2	12	Über 20
Kurstage	CPEs	Laborübungen

Zielgruppe

- IT-Sicherheitsingenieure
- Penetrationstester
- Sicherheitsberater
- Personal, das Schwachstellen beurteilt
- Personal, das Schwachstellen managt
- Netzwerksicherheitsanalysten
- Auditoren
- Allgemeine Sicherheitsingenieure
- Sicherheitsforscher

Erklärung des Autors

Metasploit ist derzeit das beliebteste Gratis-Exploit-Tool. Es wird von Penetrationstestern und Schwachstellenbeurteilern, Auditoren und böswilligen Akteuren in der wirklichen Welt weithin genutzt. Die meisten Benutzer verstehen und nutzen jedoch nur etwa 10 Prozent der Funktionalität und sind sich nicht im Klaren, welche anderen immens nützlichen Funktionen Metasploit noch zu bieten hat. Nach diesem Kurs sind die Teilnehmer in der Lage, die bisher genutzten 10 Prozent wirklich zu meistern, d. h. umfassender und sicherer anzuwenden. Außerdem werden sich ihnen die restlichen 90 Prozent der Funktionen erschließen, mit denen sie ihre Tests effektiver gestalten können. In diesem Kurs lernen die Teilnehmer, wie sie mit einem kostenlosen Tool genau so viel erreichen können wie mit vielen erheblich teureren kommerziellen Tools.

– Jeff McJunkin

Jeff McJunkin
Kursautor

Viele Unternehmen müssen heute regulatorische Auflagen oder Compliance-Anforderungen erfüllen, die regelmäßige Penetrationstests und Schwachstellenbeurteilungen vorschreiben. Kommerzielle Tools und Services zur Durchführung solcher Tests können teuer sein. Zwar gibt es wirklich zuverlässige Gratistools wie z. B. Metasploit, aber viele Tester verstehen die umfassende Funktionalität dieser Tools nicht und können sie nicht in einer professionellen Testmethodik anwenden. Metasploit soll Testern helfen, Schwachstellen in einem benutzerfreundlichen Open-Source-Framework zu bestätigen. In diesem Kurs lernen die Teilnehmer, wie sie dieses Gratistool optimal nutzen.

SEC580™ zeigt den Teilnehmern, wie sie die erstaunlichen Fähigkeiten des Metasploit-Frameworks in einem umfassenden Regime für Penetrationstests und Schwachstellenbeurteilung gemäß einer gründlichen Methodik zur Durchführung effektiver Tests anwenden. Nach Abschluss des Kurses verfügen sie über ein fundiertes Verständnis, wie Metasploit sich in ihre Penetrationstests und tagtäglichen Beurteilungsaktivitäten einfügen kann. Dabei wird den Teilnehmern nicht nur gezeigt, wie sie ein Remote-System ausnutzen, sondern sie erhalten ein detailliertes Verständnis des Metasploit-Frameworks. Der Kurs deckt Exploits, anschließende Erkundung, Anti-Virus-Umgehung, Spear-Phishing-Angriffe und die reichhaltigen Funktionen von Meterpreter ab, einer angepassten Shell-Umgebung, die speziell erstellt wurde, um Sicherheitsmängel auszubeuten und zu analysieren.

Der Kurs behandelt außerdem viele der Fallstricke, auf die Tester bei der Nutzung des Metasploit-Frameworks stoßen können, und wie sie sich für effizientere und sicherere Tests vermeiden und umgehen lassen.

Zusammenfassung der Kursinhalte

TEIL 1: Metasploit for Enterprise Penetration Testing – Teil 1

TEIL 2: Metasploit for Enterprise Penetration Testing – Teil 2

„SEC580 ist der weltweit beste Kurs für detaillierte Kenntnisse über Metasploit.“

– Tom Reeves, **Northrup Grumman**

„SEC580 umfasst wohldurchdachtes Kursmaterial, das Sie Schritt für Schritt durch die Grundlagen von Metasploit führt.“

– Scott Tirapelle, **Franchise Tax Board**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC580**

KURSFORMATE SEC580

Präsenzkurs **Live online**

SEC588: **Cloud Penetration Testing™**

GCPN
Cloud Penetration Tester
giac.org/gcpn

6	36	27
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Cloud-basierte Penetrationstests durchführen
- Cloud-Umgebungen beurteilen und dem Unternehmen durch Identifizierung von Schwachstellen einen Mehrwert bereitstellen
- Aus erster Hand verstehen, wie Cloud-Umgebungen konstruiert sind und wie die Indizienerfassung skaliert werden kann
- Sicherheitsrisiken in Amazon- and Microsoft Azure-Umgebungen beurteilen, den zwei größten Cloud-Plattformen, die heute verfügbar sind
- Das Gelernte bei der Arbeit sofort anwenden

Zielgruppe

- Sicherheitsfachkräfte sowohl auf der Angriffs- als auch auf der Verteidigungsseite werden von diesem Kurs erheblich profitieren, da sie ein gründliches Verständnis für Schwachstellen, unsichere Konfigurationen und die damit einhergehenden geschäftlichen Risiken für ihre Organisationen gewinnen
- Penetrationstester
- Schwachstellenanalysten
- Risikobewertungsbeauftragte
- DevOps-Ingenieure
- Ingenieure für Standortzuverlässigkeit

Berufliche Rollen im NICE Framework

- 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)

„SEC588 ist sorgfältig konzipiert und findet ein gutes Gleichgewicht zwischen eingehender Theorie und praktischen Übungen zu den drängenden Sicherheitsproblemen moderner Cloud-Umgebungen. Dieser Kurs ist unverzichtbar für Sicherheitsfachkräfte, die Kenntnisse auf dem neuesten Stand suchen.“

– Armin Iraqi, **Fortum**

Aaron Cure
Kursautor

Moses Frost
Kursautor

SEC588™ bietet eine Einführung in die neuesten Cloud-fokussierten Techniken für Penetrationstests und zeigt Ihnen, wie Sie Cloud-Umgebungen beurteilen. Der Kurs beschäftigt sich mit Themen wie Cloud-basierten Microservices, Datenbeständen im Arbeitsspeicher, serverlosen Funktionen, Kubernetes-Netzen und Containern. Außerdem geht er darauf ein, wie Sie Cloud-First- und Cloud-native Anwendungen identifizieren und testen. Sie erlernen darüber hinaus spezifische Taktiken für Penetrationstest in Azure und Amazon Web Services – besonders wichtig, da AWS und Microsoft mehr als die Hälfte des Marktes abdecken. Ein Rechenzentrum zu beurteilen und zu sichern, ist eine Sache, aber es erfordert Spezialkenntnisse, die Risiken, denen eine Organisation durch ungesicherte Cloud-Services ausgesetzt ist, wirklich einschätzen und in einem Bericht darstellen zu können.

Geschäftsorientierte Lernergebnisse

- In realistischen, Cloud-basierten Laborübungen lernen, wie Cloud-Umgebungen bewertet und getestet werden
- Verstehen, welche Unterschiede zwischen Cloud-nativen, Multi-Cloud- und Cloud-Hybrid-Infrastrukturen bestehen
- Penetrationstests an realistischen Microservices durchführen
- Lernen, wie Container und CI/CD-Pipelines missbraucht werden
- Kubernetes, serverlose Funktionen und Windows-Container angreifen
- Verstehen, wie Identitätssysteme in der Cloud funktionieren und wie man sie angreift

Zusammenfassung der Kursinhalte

TEIL 1: Architektur, Erkennung und Erkundung im großen Maßstab

TEIL 2: Identitätssysteme angreifen

TEIL 3: Cloud-Services angreifen und missbrauchen

TEIL 4: Schwachstellen Cloud-nativer Anwendungen

TEIL 5: Infrastrukturangriffe und Arbeit in Red Teams

TEIL 6: Abschlussübung

„Bei SEC588 habe ich mehr gelernt, als ich erwartet hatte. Angesichts der schnellen Entwicklung neuer Technologien, die von Cloud-Anbietern bereitgestellt werden, hat mir SEC588 ein wichtiges Framework für Cloud-Penetrationstests an die Hand gegeben.“

– Jonus Gerrits, **Phillips66**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC588**

KURSFORMATE SEC588

Präsenzkurs | **Live online** | **OnDemand**

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

6	36	Über 15
Tage Programm	CPEs	Laborübungen

Erlernte Fähigkeiten

- Die Sicherheitsprobleme verstehen, denen die meisten Organisationen heute ausgesetzt sind
- Sicherheitsprobleme in kleinere Probleme aufschlüsseln, automatisierte Lösungen für diese spezifischen Probleme definieren und dann Funktionen, mit denen mehrere Probleme angegangen werden können, in einem automatischen Workflow arrangieren
- Mit Tools wie Terraform, Ansible, CHEF Puppet und vielen anderen sichere Konfigurationen lokal automatisieren, eine Konfiguration für den Wunschzustand festlegen, Infrastruktur als Code in verschiedenen Umgebungen implementieren und Sicherheitsvorfälle automatisch erkennen und darauf reagieren
- Szenarien aus der wirklichen Welt in einer Kombination aus On-Premise- und Cloud-Umgebungen mithilfe eines Referenzrahmens bewerten, der in Ihrer Organisation sofort angewandt werden kann

Zielgruppe

- Sicherheitsarchitekten
- Automatisierungsingenieure
- Sicherheitsingenieure
- Detektionsingenieure
- Incident Responder
- Unternehmens-Risikoanalysten
- Ethische Hacker
- Penetrationstester
- Betreiber eines Red Teams
- Mitglieder eines Blue Teams
- Mitglieder eines Purple Teams
- Analysten im Security Operations Center
- Cloud-Ingenieure

Berufliche Rollen im NICE Framework

- 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
Kursautor

Jeroen Vandeleur
Kursautor

Es sind nicht die Maschinen, die die Macht ergreifen. Es sind Sie!

Ein Sicherheitsteam, das Automatisierungsworkflows gemeistert hat, ist um ein Vielfaches stärker. Die Arbeit in modernen Unternehmen wird immer umfangreicher und komplizierter. Sicherheitsteams finden es schwierig, Bedrohungen, die gegen ihre Organisation gerichtet sind, zu verhindern, zu entdecken, zu emulieren und darauf zu reagieren.

Besonders gute Sicherheitsteams lösen dieses Problem durch Automatisierung. Hoch kompetente Sicherheits- und Automatisierungstechniker können Lösungen implementieren, die es ihren Teams ermöglichen, ihre tägliche Aufmerksamkeit weg von umfangreichen Aufgaben mit niedriger Priorität zu lenken und sich stattdessen auf geschäftskritische Initiativen mit hoher Priorität zu konzentrieren.

Im Laufe dieses Kurses interagieren Sie mit einer realistischen, aber fiktiven Organisation, GLOBEX. In über 15 Laborübungen und einer Abschlussübung geht es um Anwendungsfälle für Sicherheitsautomatisierung, die Sie anschließend in Ihrer eigenen Organisation umsetzen können.

Vermittelte Kompetenzen

- Wiederholbare Aktivitäten in automatisierte Aufgaben umwandeln
- Präventions-, Detektions- und Reaktionsfähigkeiten für spezifische Angriffstechniken automatisieren, die von echten Angreifern und Red Teams genutzt werden
- Die Effektivität Ihres SOC verbessern, indem Gelegenheiten zur Effizienzsteigerung bei Zuständigkeiten in Stufe 1 und Stufe 2 aufgedeckt werden
- Lernen, wie Gelegenheiten für erweiterte Fähigkeiten und IaC-Module geschaffen werden und wie eine dynamische Infrastruktur für das Red Team und Penetrationstests eingerichtet wird
- Zur Cloud-Gegner-Emulation befähigen und mit Cloud-nativen Tools Detektionsfähigkeiten und automatisierte Reaktionsumsetzung messen
- Infrastruktur-als-Code-Tools nutzen, um automatisierte Workflows für Threat Hunting, Eindämmung, Akquisition, Quarantäne und Incident Response einzurichten
- Mit Infrastruktur als Code automatisierte Cyber-Ranges-Fähigkeiten für On-Premise-, Cloud-native und hybride Systeme implementieren und dadurch Sicherheitsprogramme und das Verständnis von Angriffstools und Kontrollmaßnahmen zur Verteidigung verbessern

Zusammenfassung der Kursinhalte

TEIL 1: Konzepte der Sicherheitsautomatisierung
TEIL 2: Technik der Sicherheitsautomatisierung
TEIL 3: Sicherheitsautomatisierung in der Cloud
TEIL 4: Offensive Sicherheitsautomatisierung
TEIL 5: Defensive Sicherheitsautomatisierung
TEIL 6: Abschlussübung zur Sicherheitsautomatisierung

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC598**

KURSFORMATE SEC598

Präsenzkurs **Live online**

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

GDAT
Defending Advanced Threats
giac.org/gdat

6	36	Über 20
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Verstehen, wie berüchtigte Angriffe in jüngster Zeit ausgeführt wurden und wie sie hätten verhindert werden können
- Sicherheitskontrollmaßnahmen in verschiedenen Phasen der Cyber Kill Chain und des MITRE ATT&CK Framework implementieren, um Angriffe zu verhindern, zu erkennen und darauf zu reagieren

Zielgruppe

- Sicherheitsarchitekten und Sicherheitsingenieure
- Mitglieder von Red Teams und Penetrationstester
- Technische Sicherheitsmanager
- Analysten, Ingenieure und Manager im Security Operations Center
- Alle, die besser verstehen möchten, wie hartnäckige Cybergegner operieren und wie die IT-Umgebung gestärkt werden kann, um Vorfälle besser zu verhindern, zu erkennen und darauf zu reagieren

Berufliche Rollen im NICE Framework

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

„SEC599 umfasst fantastische Laborübungen und Demonstrationen moderner Offensivtechniken und Defensivoptionen. Mir gefiel, dass es Themen gab, die in einer breiten Fülle von Umgebungen helfen können, von den Grundlagen bis zu erweiterten Lösungen für verschiedene Reifegrade der Sicherheit."

– Michael Ebrahimi, **Accenture**

Erik Van Buggenhout
Kursautor

Stephen Sims
Kursautor

Cyberbedrohungen sind im Vormarsch: Ransomware-Taktiken beeinträchtigen kleine, mittelgroße und große Unternehmen gleichermaßen, und staatlich gesponserte Widersacher versuchen, sich Zugriff zu Ihren wertvollsten Assets zu verschaffen. SEC599™ gibt Ihnen die Kenntnisse und das Know-how an die Hand, die Sie brauchen, um die Bedrohungen von heute zu überwinden. In der Erkenntnis, dass sich die Strategie nicht auf die Prävention beschränken darf, führen wir Sicherheitskontrollmaßnahmen ein, mit denen Widersacher erkannt, bekämpft und gestoppt werden sollen.

Die Kursautoren Stephen Sims und Erik Van Buggenhout (beide GIAC-zertifizierte Sicherheitsexperten) sind erfahrene Praktiker, die sich durch Penetrationstests und Incident Response ein fundiertes Verständnis für die Funktionsweise von Cyberangriffen angeeignet haben. Während sie Kurse in Penetrationstests unterrichteten, wurden sie oft gefragt: „Wie verhindere oder erkenne ich diese Art des Angriffs?" Das ist die entscheidende Frage. SEC599™ zeigt den Teilnehmern an Beispielen aus der Praxis, wie sich Angriffe verhindern lassen. Der Kurs umfasst mehr als 20 Laborübungen sowie eine ganztägige „Defend-the-Flag"-Übung, bei der die Teilnehmer eine virtuelle Organisation vor verschiedenen Angriffswellen auf ihre Umgebung zu verteidigen versuchen.

Geschäftsorientierte Lernergebnisse

- Verstehen, wie berüchtigte Angriffe in jüngster Zeit ausgeführt wurden und wie sie hätten verhindert werden können
- Sicherheitskontrollmaßnahmen in verschiedenen Phasen der Cyber Kill Chain und des MITRE ATT&CK Framework implementieren, um Angriffe zu verhindern, zu erkennen und darauf zu reagieren

Zusammenfassung der Kursinhalte

TEIL 1: Einführung und Erkundung

TEIL 2: Payload-Lieferung und Ausführung

TEIL 3: Exploitation, Persistenz und Command & Control

TEIL 4: Lateralbewegung

TEIL 5: Maßnahmen für Zielsetzungen, Threat Hunting und Incident Response

TEIL 6: Abschlussübung zur APT-Verteidigung

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC599**

KURSFORMATE SEC599

Präsenzkurs | **Live online** | **OnDemand**

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

GAWN
Assessing and Auditing Wireless Networks
giac.org/gawn

6	36	Über 20
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Schädliche, betrügerische Zugangspunkte mit kostenlosen oder günstigen Tools identifizieren und finden
- Einen Penetrationstest gegen energiearme Funkgeräte durchführen, um Schwachstellen im Kontroll- und Funksystem zu identifizieren
- In Bluetooth-Netzwerken Schwachstellen identifizieren und Authentifizierungsmechanismen umgehen
- Einen WPA2-Unternehmens-Penetrationstest implementieren, um Anmeldedaten aus nicht ausreichend geschützten Wireless-Client-Systemen zu erfassen
- Mithilfe von Scapy angepasste Pakete zwingen, Funknetzwerke auf neue Weisen zu manipulieren, und dabei schnell angepasste Angriffstools für spezifische Anforderungen des Penetrationstests erstellen
- WLAN-Angriffe mit Netzwerkpaket-Erfassungsverfolgung und kostenlos verfügbaren Analysetools identifizieren
- Mängel in der Sicherheit von berührungslosen Schlüsselkarten identifizieren und ausnutzen
- Proprietäre Funksignale mit Software-Defined Radio decodieren
- Einen Penetrationstest gegen zahlreiche standardbasierte oder proprietäre Funktechnologien durchführen

Zielgruppe

- Ethische Hacker und Penetrationstester
- Netzwerksicherheitspersonal
- Netzwerk- und Systemadministratoren
- Incident Response Teams
- Entscheidungsträger für Richtlinien zur Informationssicherheit
- Technische Auditoren
- Informationssicherheitsberater
- Funksystemingenieure
- Entwickler von eingebetteten Funksystemen

Larry Pesce
Kursautor

James Leyte-Vidal
Kursautor

Dieser Kurs richtet sich an Fachkräfte, die eine umfassende technische Kompetenz erlangen möchten, um verschiedene Wireless- oder Funktechnologien zu verstehen, zu analysieren und zu verteidigen. Diese Technologien sind in unseren Umgebungen allgegenwärtig geworden und stellen zunehmend wichtige Einfallstore für Angreifer dar.

Die Autoren von SEC617™ sind selbst Penetrationstester. Sie wissen, dass viele Organisationen Funksicherheit als Angriffsfläche übersehen und deshalb nicht die nötigen Maßnahmen für Verteidigung und Überwachung ergreifen – und das, obwohl Funktechnologien heute gang und gäbe sind, von der Vorstandsetage und Finanzabteilungen über Behörden, Fertigungsanlagen, Einzelhandelsnetze und Medizintechnik bis hin zur Flugsicherung. Angesichts der bekannten Risiken, die unsichere Funktechnologien mit sich bringen, und der Angriffe gegen sie möchte SEC617™ den Teilnehmern die grundlegenden Kompetenzen vermitteln, die sie brauchen, um diese Bedrohungen zu identifizieren, auszuwerten, zu beurteilen und sich gegen sie zu verteidigen. Diese Kompetenzen sind für jede leistungsstarke Sicherheitsorganisation unverzichtbar.

Zusammenfassung der Kursinhalte

TEIL 1: Sammlung und Analyse von WLAN-Daten

TEIL 2: WLAN-Angriffs- und Exploitation-Techniken

TEIL 3: WLAN- und Zigbee-Angriffe in Unternehmen

TEIL 4: Angriffe bei Bluetooth und Software-Defined Radio

TEIL 5: Hacking bei RFID, Smart Cards und NFC

TEIL 6: „Capture-the-Flag"-Übung

„Durch die detaillierten Erklärungen zur Kryptografie bei SEC617 ist es leichter zu verstehen, wie verschiedene Verschlüsselungsalgorithmen funktionieren – das war mir bisher nicht gelungen!"

– Jonathan Wilhoit, **Fluor**

„SEC617 vermittelt nicht nur ein grundlegendes Verständnis der Bedrohungen und Schwachstellen bei Funksystemen, sondern kann weiter in die Tiefe gehen, wenn Sie die entsprechenden Fragen stellen."

– Daniel Mayernik, **Integrity Applications Incorporated**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC617**

KURSFORMATE SEC617

Präsenzkurs | **Live online** | **OnDemand**

SEC660: Advanced Penetration Testing, Exploit Writing & Ethical Hacking

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

6	46	Über 30
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Fuzz-Tests durchführen, um den Lebenszyklusprozess zur Sicherheitsentwicklung Ihres Unternehmens zu verbessern
- Netzwerkgeräte ausnutzen und Netzwerk-Anwendungsprotokolle beurteilen
- Aus beschränkten Umgebungen auf Linux und Windows entkommen
- Kryptografische Implementierungen testen
- Die Techniken modellieren, mit denen Angreifer Zero-Day-Schwachstellenerkennung und Exploit-Entwicklung durchführen
- Mithilfe von Validierung korrektere quantitative und qualitative Risikobeurteilungen entwickeln
- Demonstrieren, warum moderne Exploit-Gegenmaßnahmen benötigt werden und welche Auswirkungen sie haben

Zielgruppe

- Netzwerk- und System-Penetrationstester
- Incident Handler
- Anwendungsentwickler
- IDS-Ingenieure

Berufliche Rollen im NICE Framework

- 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)

„Die Qualität der Laborübungen und der Kursarbeit bei SEC660 zeigt, welchen Mehrwert SANS-Schulungen gegenüber anderen Anbietern gewähren. Es war ein ausgezeichneter, anspruchsvoller und lohnender Kurs."

– Michael R., **US-amerikanisches Militär**

James Shewmaker
Kursautor

Stephen Sims
Kursautor

SEC660™ ist der logische Folgekurs für Teilnehmer, die SANS SEC560: Enterprise Penetration Testing™ abgeschlossen oder bereits Erfahrung in Penetrationstests gesammelt haben. Lernende mit den nötigen Vorkenntnissen für diesen Kurs werden durch Dutzende von Angriffen aus der wirklichen Welt geführt, die von den versiertesten Penetrationstestern herangezogen werden. Erst wird die Methodik eines bestimmten Angriffs diskutiert. Darauf folgen praktische Laborübungen, in denen erweiterte Konzepte gefestigt werden. Dadurch können die Techniken zurück am Arbeitsplatz sofort angewandt werden. Jeder Kurstag umfasst ein zweistündiges Bootcamp am Abend, in dem die diskutierten Techniken weiter gemeistert werden können. Unter anderem werden folgende Themen abgedeckt: NAC-Angriffe (Network Access Control) und VLAN-Manipulation (Virtual Local Area Network), Exploits für Netzwerkgeräte, Ausbruch aus beschränkten Linux- und Windows-Umgebungen, IPv6, Linux-Berechtigungseskalation und Exploit-Verfassung, Tests kryptografischer Implementierungen, Fuzzing, Überlistung moderner OS-Kontrollmaßnahmen wie ASLR (Adress Space Layout Randomization) und DEP (Data Execution Prevention), ROP (Return-Oriented Programming), Verfassung von Exploits für Windows und vieles mehr.

Geschäftsorientierte Lernergebnisse

- Netzwerk-Penetrationstests an Netzwerkgeräten wie Routern, Switches und NAC-Implementierungen sicher ausführen
- Kryptografische Implementierungen testen
- Identity Sprawl und Tech Debt durch Zentralisierung vemeiden helfen
- Eine errungene Stellung ohne Berechtigungen für Post-Exploitation und Eskalation nutzen
- Fuzzing im Netzwerk und bei eigenständigen Anwendungen durchführen
- Exploits gegen Anwendungen verfassen, die auf Linux- und Windows-Systemen ausgeführt werden
- Exploit-Gegenmaßnahmen wie z. B. ASLR, DEP und Stack-Canaries umgehen

Zusammenfassung der Kursinhalte

TEIL 1: Netzwerkangriffe für Penetrationstester

TEIL 2: Krypto- und Post-Exploitation

TEIL 3: Produktsicherheitstests, Fuzzing und Code-Abdeckung

TEIL 4: Linux-Exploits für Penetrationstester

TEIL 5: Windows-Exploits für Penetrationstester

TEIL 6: „Capture-the-Flag"-Übung

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC660**

KURSFORMATE SEC660

Präsenzkurs | **Live online** | **OnDemand**

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

6	46	Über 22
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

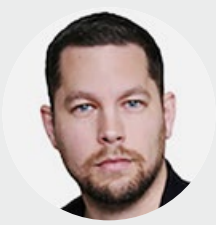
- Benutzerdefiniert kompilierte Windows-Implants erstellen
- Zielinformationen sammeln
- Prozesse vor Benutzermodustools verbergen
- Funktionen für AV-Umgehungen mit Hooks verstehen und die Hooks entfernen
- Angepassten Shellcode generieren und ausführen
- Berechtigungen von mittleren zu hohen Integritätsstufen eskalieren (NT AUTHORITY\SYSTEM)
- Über Neustarts hinweg persistieren
- An konfigurierte C2-Infrastruktur ausstrahlen

Zielgruppe

- Betreiber eines Red Teams
- Exploit-Entwickler
- Penetrationstester
- Linux-CNO-Entwickler
- Windows-Entwickler
- AV/EDR-Entwickler

Berufliche Rollen im NICE Framework

- Adversary Emulation Specialist/Red Teamer (OPM 541)



Jonathan Reiter
Kursautor

Die Entwicklung benutzerdefinierter kompilierter Tools für Windows ist eine Kompetenz, die an Universitäten und in anderen akademischen Organisationen nicht gelehrt wird. Deshalb gibt es in der Cybersicherheitsbranche ein erhebliches Kompetenzdefizit, das die Fähigkeiten von Red Teams allgemein einschränkt. Verteidigungsunternehmen und Branchen, die Windows-Tool-Entwickler einstellen möchten, sehen sich mit einem erheblichen Talentmangel konfrontiert und sind nicht in der Lage, ihre Verteidigung weiter zu verbessern.

SEC670™ ist der erste Kurs seiner Art, bei dem die Teilnehmer in praktischen Laborübungen Erfahrung damit sammeln können, wie benutzerdefiniert kompilierte Programme speziell für Windows mit den Programmiersprachen C/C++ erstellt werden. Die Teilnehmer lernen die internen Funktionsweisen bestehender Offensivtools kennen, die Fähigkeiten wie Berechtigungseskalation, Persistenz und Sammlung bieten, indem sie ihre eigenen Tools mit Windows-APIs erstellen. Windows-Verteidigungsmaßnahmen sind robuster geworden, und durch Cloud-vernetzte AV-Lösungen ist es schwieriger, unentdeckt zu bleiben. Als Reaktion führt dieser Kurs die Teilnehmer in Techniken ein, die echte Malware-Autoren in staatlichem Auftrag derzeit in ihren Implants implementieren.

Lerninhalte

- Neue Aufrufkonventionen und Datentypen spezifisch für Windows erstellen
- Verstehen, wie Prozesse, Threads und Dienste in Windows intern funktionieren
- Windows-APIs missbrauchen, um Shellcode unentdeckt in andere Prozesse einzuschleusen
- Einen verborgenen, persistenten Dienst erstellen
- Sich vor Benutzermodustools wie dem Task Manager verstecken
- Shellcode erstellen und ohne Detektion ausführen
- Land Hooks von Benutzern umgehen und Ihre eigenen implementieren
- Ihre Implantate von Ihrer C2 aus steuern

Zusammenfassung der Kursinhalte

TEIL 1: Windows-Tool-Entwicklung

TEIL 2: Ihr Ziel kennenlernen

TEIL 3: Operationelle Maßnahmen

TEIL 4: Persistenz: Stirb an einem anderen Tag

TEIL 5: Implants verbessern: Shellcode, Evasion und C2

TEIL 6: „Capture-the-Flag"-Übung

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC670**

KURSFORMATE SEC670

Präsenzkurs | **Live online** | **OnDemand**

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

5	36	29
Tage Programm	CPEs	Laborübungen

Geschäftsorientierte Lernergebnisse

- Realistische Gegner-Emulationspläne erstellen, um Ihre Organisation besser zu schützen
- Erweiterte Angriffe durchführen, u. a. Umgehung von Anwendungen auf einer Positivliste, Cross-Forest-Angriffe (Missbrauch der Delegation) und Stealth-Persistence-Strategien
- Aufbau von SIGMA-Regeln zur Erkennung versierter Angreifertechniken

Zielgruppe

- Penetrationstester
- Ethische Hacker
- Verteidiger, die Offensivmethodik, -tools und -techniken besser verstehen möchten
- Mitglieder eines Red Teams
- Mitglieder eines Blue Teams
- Mitglieder eines Purple Teams
- Forensikfachkräfte, die Offensivtaktiken besser verstehen möchten

Berufliche Rollen im NICE Framework

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

Jean-François Maes
Kursautor

Erik Van Buggenhout
Kursautor

In dieser hochmodernen Purple-Team-Schulung tauchen Teilnehmer in die Welt der Gegneremulation ein, um die Verteidigung gegen Datenschutzverstöße zu stärken. Die Teilnehmer versetzen sich in Angreifer aus dem wirklichen Leben hinein und sammeln praktische Erfahrungen in einer dynamischen Unternehmensumgebung. Dabei meistern Sie die Kunst der Detektion und emulieren die Techniken von Widersachern. Sechzig Prozent der Kurszeit entfallen auf Laborübungen. Zu den Kursaktivitäten gehören:

- Ein Kursabschnitt zu typischen Automatisierungsstrategien wie Ansible, Docker und Terraform, mit denen umfassende Multi-Domain-Unternehmensumgebungen zur Gegneremulation auf Knopfdruck implementiert werden können
- Aufbau von ordentlichen Prozessen sowie Tools und Plänen für das Purple Team
- Aufbau von Gegneremulationsplänen, die Akteure aus dem wirklichen Leben wie APT-28, APT-34 und Turla nachahmen, und Ausführung dieser Pläne mit Tools wie Covenant und Caldera
- Detaillierte Techniken wie Kerberos-Delegationsangriffe, Reduktion der Angriffsfläche und Applocker-Umgehung, EDR-Umgehung, AMSI, Prozesseinschleusung und COM-Object-Hijacking
- Detection Engineering und Delemetry Review zur Erkennung der obigen Techniken
- Eine dynamische Abschlussübung, bei der Ihre Kompetenzen zur Gegneremulation praktisch erprobt werden

SEC699™ ist ein natürlicher Folgekurs für SEC599™. Die Kursautoren Erik Van Buggenhout (Leitautor von SEC599™) und Jean-Francois Maes (Leitautor von SEC565™) sind beide zertifizierte GIAC-Sicherheitsexperten und erfahrene Praktiker, die durch Aktivitäten in Red Teams und Blue Teams ein eingehendes Verständnis für die Funktionsweise von Cyberangriffen entwickelt haben. Bei SEC699™ kombinieren sie diese Kompetenzen, um den Lernenden Gegner-Emulationsmethoden zur Prävention und Detektion von Datenschutzverletzungen zu vermitteln.

Zusammenfassung der Kursinhalte

TEIL 1: Einführung und wichtige Tools

TEIL 2: Emulation und Detektion von Strategien zum ersten Eindringen

TEIL 3: Berechtigungseskalation, Emulation der Lateralbewegung und Detektion

TEIL 4: Persistenzemulation und -detektion

TEIL 5: Emulationspläne (erweiterter Zugriff auf CTF-Range)

„Insgesamt war SEC699 der beste Kurs, den ich als Incident Responder und SOC-Analyst absolviert habe. Er simuliert die realen Angriffe und die Verteidigungsmöglichkeiten anhand zahlreicher Techniken. Er vermittelte mir eine Struktur und einen Fokus, mit denen wir unsere aktuellen SOC-Fähigkeiten zu größerer Reife führen können.“

– Maurice von Wintersdorff, **Philips**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC699**

KURSFORMATE SEC699

Präsenzkurs | **Live online** | **OnDemand**

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

6	46	Über 30
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Zero-Day-Schwachstellen in Programmen entdecken, die auf vollständig gepatchten modernen Betriebssystemen ausgeführt werden
- Die erweiterten Funktionen von IDA Pro nutzen und eigene IDAPython-Skripts schreiben
- Remote-Debugging von Linux- und Windows-Anwendungen durchführen
- Linux-Heap-Overflows verstehen und ausnutzen
- Fuzzing an Closed-Source-Anwendungen
- Windows-Update-Pakete entpacken und untersuchen
- Patch-Abgleiche anhand von Programmen, Bibliotheken und Treibern ausführen, um gepatchte Schwachstellen zu finden
- Windows-Kernel-Debugging B durchführen
- Reverse Engineering und Exploitation von Windows-Kernel-Treibern

Zielgruppe

- Leitende Netzwerk- und System-Penetrationstester mit Erfahrung bei der Exploit-Entwicklung
- Entwickler sicherer Anwendungen (C und C++)
- Reverse-Engineering-Fachkräfte
- Leitende Incident Handler mit Erfahrung in der Exploit-Entwicklung
- Leitende Threat Analysts mit Erfahrung in der Exploit-Entwicklung
- Schwachstellenforscher
- Sicherheitsforscher

Berufliche Rollen im NICE Framework

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

Jaime Geiger
Kursautor

Stephen Sims
Kursautor

Schwachstellen in modernen Betriebssystemen wie Microsoft Windows 10 und 11 und den neuesten Linux-Distributionen sind oft sehr komplex und subtil. Aber wenn sie von äußerst geschickten Angreifern ausgenutzt werden, können diese Schwachstellen die Verteidigungsmaßnahmen einer Organisation untergraben und sie dem Risiko erheblicher Schäden aussetzen. Nur wenige Sicherheitsfachkräfte haben die nötigen Kompetenzen, um zu erkennen, warum eine komplexe Schwachstelle vorhanden ist, und ein Exploit zu schreiben, das sie kompromittiert. Angreifer hingegen müssen diese Kompetenzen auf dem aktuellen Stand halten, auch wenn die Komplexität steigt. SANS SEC760: Advanced Exploit Development for Penetration Testers™ vermittelt Kompetenzen, die benötigt werden, um durch Reverse Engineering von Anwendungen ihre Schwachstellen aufzuspüren, Benutzeranwendungen und Kernel-Debugging remot durchzuführen, Patches für One-Day-Exploits zu analysieren, erweitertes Fuzzing durchzuführen und komplexe Exploits gegen Ziele wie den Windows-Kernel und den modernen Linux-Heap zu verfassen, und all das, während Sie moderne Exploit-Gegenmaßnahmen umgehen oder gegen sie arbeiten.

Vermittelte Kompetenzen

- Wie Sie moderne Exploits gegen die Betriebssysteme Windows 10 und 11 schreiben
- Wie Sie Exploit-Entwicklungstechniken durchführen, z. B. erweitertes Fuzzing, Kernel- und Treiber-Exploits, One-Day-Exploits durch Patch-Analyse, Linux-Heap-Overflows und andere anspruchsvolle Themen
- Wie Sie mit verschiedenen Debuggern und Plug-ins Schwachstellenforschung und Geschwindigkeit effektiv verbessern
- Wie Sie mit modernen Exploit-Gegenmaßnahmen umgehen, die den Erfolg vereiteln sollen

Zusammenfassung der Kursinhalte

TEIL 1: Exploit-Gegenmaßnahmen und Reverse Engineering mit IDA

TEIL 2: Erweiterte Linux-Exploitation

TEIL 3: Erweitertes Fuzzing

TEIL 4: Patch-Diffing, One-Day-Exploits und Windows-Kernel

TEIL 5: Debugging und Exploitation des Windows-Kernel

TEIL 6: „Capture-the-Flag"-Übung

„Ich habe schon viele andere Kurse in erweiterter Exploit-Entwicklung absolviert, aber nirgends wurde sie so aufgeschlüsselt und schrittweise demonstriert wie hier."

– Adam Logue, **SecureWorks**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC760**

KURSFORMATE SEC760

Präsenzkurs | **Live online** | **OnDemand**

FOKUSBEREICH IM SANS-LEHRPLAN

Cloud-Sicherheit

Cloud-Computing ist in unserer Ära die Technologie mit dem größten Umwälzungspotenzial, und die Cloud-Sicherheit wird bei ihrem Siegeszug eine entscheidende Rolle spielen. Bei der Cloud-Sicherheit muss der Fokus darauf liegen, wohin sich die Cloud entwickelt – nicht darauf, wo sie heute ist. Die Zukunft verlangt detaillierte technische Cloud-Fähigkeiten in Kombination mit Kenntnissen der Sicherheits- und Servicefunktionen für alle großen Cloud-Serviceanbieter (CSP). Ihre Entwicklung zum Experten in Cloud-Sicherheit beginnt hier.

Unser Lehrplan wurde durch einen Konsensprozess in der Branche entwickelt und nimmt sich der Sicherheit in der öffentlichen Cloud mit einem holistischen, praktischen Ansatz an, mit Multicloud- und Hybrid-Cloud-Szenarien für große Unternehmen sowie für Organisationen, die sich noch in der Entwicklungsphase befinden. Hier lernen Sie, wie verschiedene CSP miteinander interagieren und welche Nuancen sie unterscheiden, anstatt sich nur intensiv mit einer der Plattformen zu beschäftigen.

Bei diesen praktischen Cloud-Sicherheitsschulungen lernen Sie folgende Kompetenzen:

- Public-Cloud-Services von AWS, Azure und Google Cloud Platform (GCP) härten und konfigurieren
- Best Practices für Sicherheit und Compliance automatisieren
- Systeme und Anwendungen mit Cloud-Services auf sichere Weise aufbauen und implementieren
- Sicherheit nahtlos in Ihre DevOps-Toolchain integrieren
- Container und Kubernetes sicher erstellen, implementieren und managen
- Schwachstellen und Mängel in Ihren Cloud-Umgebungen aufdecken
- Angreiferaktivitäten in Ihren Cloud-Protokollen finden

„Die Welt verlagert sich in die Cloud, und wir als Sicherheitsfachleute müssen da mitziehen.“

– Daniel Harrison, **Capital One**

Stellenprofil in der Cloud-Sicherheit:

- Cloud-Sicherheitsanalyst
- Cloud-Sicherheitsingenieur
- Cloud-Sicherheitsarchitekt
- Cloud-Sicherheitsmanager
- DevOps-Fachkraft

SEC480: **AWS Secure Builder™**

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

2	12	8
Kurstage	CPEs	Laborübungen

Vermittelte Kompetenzen

- Bewährte Sicherheitspraktiken nach Branchenstandard in AWS-Workloads implementieren
- AWS-IAM (Identity and Access Management) samt Rollen, Richtlinien und Berechtigungen für sichere Zugriffskontrolle meistern
- AWS-Services basierend auf Sicherheitsdokumentation, Kontrollmaßnahmen und Audit-Risiken evaluieren und bewerten
- Sicherheitsvorfälle mit AWS-Sicherheitstools für Detektion, Reaktion und Mitigation überwachen und auf sie reagieren
- Sicherheitsprozesse mit AWS-Services wie AWS Lambda und AWS GuardDuty automatisieren
- Sicherheitsmängel in CICD-Pipelines (Continuous Integration Continuous Delivery) identifizieren und Lücken in aktuellen Cloud-Sicherheitspraktiken erkennen
- Daten während der Übertragung und im Ruhezustand mit Verschlüsselung und anderen Schutzmaßnahmen sichern
- Umfassende Sicherheitsaudits und -bewertungen durchführen, um für Compliance und Risikoidentifizierung zu sorgen
- Sicherstellen, dass AWS-Implementierungen Branchenstandards und regulatorische Anforderungen erfüllen
- Auf AWS-Umgebungen abgestimmte Incident-Response-Pläne entwickeln und implementieren
- Den Sicherheitsstatus kontinuierlich mit regelmäßigen Prüfungen und Updates optimieren

Zielgruppe

AWS-Ersteller und Erstellungsteams:

- Entwickler von Cloud-Anwendungen
- Führende Cloud-Ingenieure
- Cloud-Ingenieure
- Cloud-Architekten
- Cloud-Administratoren
- Alle technischen Beschäftigten, die in AWS-Cloud-Umgebungen operieren, sie konfigurieren und/oder verwalten

Serge Borso
Kursautor

Sicherheit von Anfang an integriert

Datenschutzverletzungen in der Cloud-Infrastruktur lassen sich oft auf versehentliche Fehlkonfigurationen durch Nicht-Sicherheitspersonal zurückführen. Cloud-Entwickler, Cloud-Ingenieure, Cloud-Architekten und andere Rollen, die nicht direkt unter den Sicherheitsbereich fallen, benötigen plattformspezifische Schulungen, damit Sicherheit effektiv Priorität erhalten und die Wahrscheinlichkeit von schädlichen Verletzungen reduziert werden kann. SEC480: AWS Secure Builder™ erfüllt diese Anforderung, da technische Fachkräfte in diesem Kurs die benötigten Kompetenzen erlernen um Sicherheitsgrundlagen von Anfang an in AWS-Workloads (Amazon Web Services) einzubetten. Dieser Kurs enthält acht umfassende Module, die jeweils von praktischen Laborübungen begleitet werden, damit die Teilnehmer praktische Erfahrung beim Aufbau sicherer AWS-Umgebungen sammeln.

Geschäftsorientierte Lernergebnisse

- Skalierbare Sicherheitslösungen in der gesamten Organisation ermöglichen
- Vertrauen und Zufriedenheit der Kunden erhöhen
- Sicherheitsstatus der Organisation stärken
- Selbstvertrauen und Kompetenzen der Beschäftigten in Bezug auf die sichere AWS-Entwicklung fördern
- Compliance mit Cloud-Sicherheitsstandards verbessern
- Unternehmensagilität durch sichere Cloud-Praktiken verbessern
- Arbeitsbelastung und Stress für Ihr Sicherheitsteam reduzieren

Zusammenfassung der Kursinhalte

MODUL 1: Verantwortung an, für und von Sicherheit

MODUL 2: Identifizierung und Autorisierung

MODUL 3: Continuous Integration Continuous Delivery (CICD)

MODUL 4: Workload- und Service-Härtung

MODUL 5: Sicherheitsüberwachung

MODUL 6: Exposition und Angriffvektoren

MODUL 7: Incident Response

MODUL 8: Vertrauen, Kontrolle und die Lieferkette

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC480**

KURSFORMATE SEC480

OnDemand

SEC488: Cloud Security Essentials™

GRUNDLEGEND ÜBERARBEITET

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

6	36	40
Tage Programm	CPEs	Laborübungen (für beide Lernmethoden)

Vermittelte Kompetenzen

- **Schwachstellen in der Cloud-Sicherheit aufdecken:** Sammeln Sie Erfahrung bei der Identifizierung von Lücken im Cloud-Sicherheitsstatus Ihrer Organisation.
- **Cloud-Sicherheitskommunikation meistern:** Diskutieren Sie Cloud-Sicherheitskonzepte selbstbewusst mit technischen Leitern und der Unternehmensführung.
- **Bei Cloud-Herausforderungen den Weg weisen:** Führen Sie Ihre Organisation gekonnt durch die wechselnde Landschaft der Probleme und Chancen, die Cloud-Sicherheit mit sich bringt.
- **Cloud-Service-Risiken identifizieren:** Erkennen und bewerten Sie die Risiken, die mit den Angeboten verschiedener Cloud-Service-Provider (CSP) verknüpft sind.
- **Effektive Sicherheitskontrollmaßnahmen wählen:** Wählen Sie die richtigen Sicherheitsmaßnahmen für verschiedene Sicherheitsarchitekturen im Cloud-Netzwerk aus.
- **CSP kritisch bewerten:** Beurteilen Sie CSP anhand ihrer Sicherheitsdokumentation, Kontrollmaßnahmen und Auditberichte.
- **Führende CSP-Services nutzen:** Nutzen Sie Services von Top-CSP wie AWS, Azure und GCP mit Zuversicht.

Zielgruppe

- Cloud-Sicherheitsingenieure
- Cloud-Sicherheitsanalysten
- Systemadministratoren
- Risikomanager
- Sicherheitsmanager
- Cloud-Sicherheitsauditoren
- Cloud-Sicherheitsfachkräfte
- Cloud-Architekten
- IT-Fachkräfte
- Entwickler, die in Cloud-Umgebungen arbeiten
- Compliance-Beauftragte, die für Cloud-Sicherheit zuständig sind
- Netzwerkingenieure, die auf Cloud-Sicherheitsrollen umstellen

Berufliche Rollen im NICE Framework

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

Ryan Nicholson
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Grundwissen für eine sichere Cloud-Umgebung

Selbst wenn Ihre Organisation On-Premise-Umgebungen ausgezeichnet sichert, wirft der Umzug in die Cloud besondere Probleme auf, die Sie völlig unvorbereitet treffen können. Weltweit stellen Organisationen rapide auf Cloud-Technologien um, ohne wichtige Sicherheitsprobleme wirklich zu verstehen, z. B. wie sie Umgebungen so konfigurieren, dass sensible Daten geschützt sind, wie sie Vorschriften einhalten und unbefugten Zugriff erkennen. Viele Kurse zur Cloud-Sicherheit greifen zu kurz, weil sie sich zu sehr auf die Theorie konzentrieren. SEC488: Cloud Security Essentials™ nimmt sich dieser Herausforderungen mit mehr als 20 praktischen Laborübungen, einer „Capture-the-Flag"-Abschlussübung und hervorragenden Inhalten an, die Ihnen helfen, ein sicheres Cloud-Fundament aufzubauen.

Geschäftsorientierte Lernergebnisse

- **Cloud-Risiko minimieren:** Sichern Sie Ihre Cloud-Umgebungen proaktiv, um Schwachstellen erheblich zu reduzieren.
- **Rechnerressourcen behüten:** Schützen Sie Ihre Rechenleistung und damit Ihr Budget.
- **Compliance verbessern:** Stärken Sie Ihre Cloud-Sicherheits-Compliance, um regulatorische Standards zu erfüllen und sogar zu übertreffen.
- **Effizienz steigern:** Nutzen Sie Automatisierung, um den Betrieb zu optimieren und die Produktivität insgesamt zu verbessern.
- **Personalbindung stärken:** Verbessern Sie die Sicherheit in der Organisation und sorgen Sie dadurch für zufriedenere und loyalere Beschäftigte.
- **Markenreputation schützen:** Bewahren und stärken Sie die Marke Ihrer Organisation, indem Sie Ihren Cloud-Betrieb sichern.
- **Kundenvertrauen aufbauen:** Erhöhen Sie das Vertrauen Ihrer Kunden durch robuste und zuverlässige Cloud-Sicherheitsmaßnahmen.

Zusammenfassung der Kursinhalte

TEIL 1: Identitäts- und Zugriffmanagement
TEIL 2: Computing- und Konfigurationsmanagement
TEIL 3: Datenschutz
TEIL 4: Netzwerke und Detektion
TEIL 5: Compliance, Incident Response und Penetrationstests
TEIL 6: CloudWars

„Ich habe eine Menge gelernt, bin technisch tiefer vorgedrungen, als ich erwartet hätte, und habe absolut das Gefühl, dass ich meine Zeit gut genutzt habe. Die Kursleiter und Assistenten waren hervorragend und haben diesen Kurs zu einer sehr positiven Erfahrung gemacht."

– Marni Reemer, **AWS**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC488**

KURSFORMATE SEC488

Präsenzkurs | **Live online** | **OnDemand**

SEC510: Cloud Security Controls and Mitigations™ GRUNDLEGEND ÜBERARBEITET

GPCS
Public Cloud Security
giac.org/gpcs

5	38	Über 20
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Fundierte Entscheidungen bei den großen drei CSP fällen, die auf einem guten Verständnis der inneren Funktionsweise ihrer PaaS- (Platform as a Service) und Iaas-Angebote (Infrastructure as a Service) beruhen
- Sicheres Identitäts- und Zugriffmanagement mit mehreren Ebenen wirksamer Verteidigung implementieren
- Multi-Cloud-Netzwerke mit Segmentierung und Zugriffskontrolle aufbauen und sichern
- Daten im Ruhezustand und während der Übertragung in der gesamten jeweiligen Cloud verschlüsseln
- Die Vertraulichkeit, Integrität und Verfügbarkeit von Daten im jeweiligen Cloud-Speicherservice steuern
- Auch unübliche Computing-Plattformen unterstützen, z. B. Anwendungsservices und serverlose FaaS (Functions as a Service)
- Einen der Cloud-Anbieter ohne langlebige Anmeldeinformationen in einen anderen integrieren
- Sicherheits- und Compliance-Prüfungen mit Cloud-nativen Plattformen automatisieren
- Technische Teams mit Terraform und IaC (Infrastructure-as-Code) bei der Durchsetzung von Kontrollmaßnahmen anleiten

Zielgruppe

- Sicherheitsanalysten
- Sicherheitsingenieure
- Sicherheitsforscher
- Cloud-Ingenieure, DevOps-Ingenieure
- Sicherheitsauditoren
- Systemadministratoren
- Betriebspersonal

Berufliche Rollen im NICE Framework

- 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
Kursautor

Eric Johnson
Kursautor

Wirkliche Angriffe mit wirksamen Kontrollmaßnahmen verhindern

Moderne Organisationen sind von komplexen Multicloud-Umgebungen abhängig, die Hunderte verschiedener Services in mehreren Clouds unterstützen müssen. Diese Services sind oft standardmäßig nicht sicher. Ähnliche Services bei verschiedenen Cloud Service Providern (CSP) müssen mit sehr unterschiedlichen Methoden geschützt werden. Sicherheitsteams benötigen ein eingehendes Verständnis von AWS-, Azure- und Google-Cloud-Services, um sie ausreichend sichern zu können. Einfach nur eine Liste von Compliance-Anforderungen abzuarbeiten, reicht nicht aus, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten Ihrer Organisation zu schützen, noch hält es Angreifer davon ab, Ihre kritischen Systeme zu sabotieren. Mit den richtigen Kontrollmaßnahmen können Organisationen ihre Angriffsfläche verringern und verhindern, dass sich Sicherheitsvorfälle zu Datenschutzverstößen auswachsen. Fehler wird es immer geben. Aber ihre Auswirkungen lassen sich beschränken.

Geschäftsorientierte Lernergebnisse

- Die Angriffsfläche der Cloud-Umgebungen Ihrer Organisation verkleinern
- Durch wirksame Verteidigung verhindern, dass sich Vorfälle zu Datenschutzverstößen auswachsen
- Die Vertraulichkeit, Integrität und Verfügbarkeit von Daten bei den drei größten CSP steuern
- Die Nutzung sicherer Automatisierung erhöhen, um mit der Schnelligkeit der modernen Geschäftsumgebung Schritt zu halten
- Unbeabsichtigten Zugriff auf sensible Cloud-Assets verhindern
- Das Risiko senken, dass Ransomware die Cloud-Daten Ihrer Organisation beeinträchtigt

Zusammenfassung der Kursinhalte

TEIL 1: Identitäts- und Zugriffmanagement in der Cloud

TEIL 2: Virtuelle Netzwerke in der Cloud

TEIL 3: Datensicherheit in der Cloud

TEIL 4: Anwendungsservices und Benutzersicherheit in der Cloud

TEIL 5: Verwaltung des Multicloud- und Cloud-Sicherheitsstatus

„Ein hervorragender Kurs. Alle Materialien sind gut umsetzbar."

– Jordan N., **US-Bundesbehörde**

„Erstaunlich, wie die Laborübung auf drei Live-Cloud-Anbieter gleichzeitig eingehen konnte. Das war beeindruckend."

– Christopher Hearn, **Harris County, Texas**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC510**

KURSFORMATE SEC510

Präsenzkurs | **Live online** | **OnDemand**

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

GWEB
Web Application Defender
giac.org/gweb

6	36	Über 20
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Gegen Angriffe in den OWASP Top 10 verteidigen
- Infrastruktursicherheit und Konfigurationsmanagement
- Cloud-Komponenten sicher in eine Web-Anwendung integrieren
- Mechanismen für Authentifizierung und Autorisierung, u. a. Single-Sign-On-Muster
- Sicherheit bei domänenübergreifenden Web-Anfragen
- Schützende HTTP-Header
- SOAP-, REST- und GraphQL-APIs verteidigen
- Microservice-Architektur sicher implementieren
- Gegen Mängel im Zusammenhang mit der Eingabe verteidigen, z. B. SQL-Injection, XSS und CSRF

Zielgruppe

- Anwendungsentwickler
- Anwendungssicherheits-Analysten oder -Manager
- Anwendungsarchitekten
- Penetrationstester, die mehr über defensive Strategien lernen möchten
- Sicherheitsfachkräfte, die mehr über Web-Anwendungssicherheit lernen möchten
- Auditoren, die Verteidigungsmechanismen in Web-Anwendungen verstehen müssen
- Beschäftigte bei Organisationen, die zur PCI-Compliance verpflichtet sind und in der Einhaltung dieser Anforderungen geschult werden müssen

Berufliche Rollen im NICE Framework

- 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
Kursautor

Dr. Johannes Ullrich
Kursautor

Die Frage ist nicht „Ob“, sondern „Wann“. Auf einen Angriff aus dem Web müssen Sie vorbereitet sein. Wir zeigen Ihnen, wie.

Anwendungen, die für Buchhaltung, Sicherheitsüberwachung und industrielle Steuersysteme verwendet werden, haben Eines gemeinsam: sie basieren auf Web-Anwendungen und APIs. Ein Verständnis von Web-Schwachstellen ist unabdingbar, wenn Sie Ihre Organisation schützen möchten, sei es On-Premise oder in der Cloud. Die Schulung SEC522 gibt Sicherheitsfachkräften die Kompetenzen an die Hand, die sie benötigen, um häufige Schwachstellen in Web-Anwendungen, Cloud-nativen Services und APIs zu identifizieren und zu mindern und gleichzeitig bewährte Branchenpraktiken in die Entwicklungsprozesse zu integrieren. Dieser Kurs umfasst 20 praktische Laborübungen und eine „Defend-the-Flag“-Übung in Teil 6.

Geschäftsorientierte Lernergebnisse

- PCI DSS und andere Compliance-Anforderungen einhalten
- Das Anwendungsrisiko insgesamt reduzieren und die Reputation des Unternehmens schützen
- Sicherheitsprobleme frühzeitig und schnell angehen, um kostenträchtige Nachbesserungen zu vermeiden
- In der Lage sein, moderne Apps mit API und Microservices auf sichere Weise einzuführen
- Dieser Kurs bereitet die Teilnehmer auf die GWEB-Zertifizierung vor

Zusammenfassung der Kursinhalte

TEIL 1: Web-Grundlagen und sichere Konfigurationen

TEIL 2: Eingabebezogene Verteidigungsmaßnahmen

TEIL 3: Authentifizierung und Autorisierung

TEIL 4: Web-Services und Front-End-Sicherheit

TEIL 5: APIs und Microservices-Sicherheit

TEIL 6: DevSecOps und „Defend-the-Flag“-Übung

„[Die Laborübungen sind] wohl durchdacht und leicht zu verstehen und vermittelten gute praktische Kenntnisse.“

– Barbara Boone, **CDC**

„SEC522 vermittelt nicht nur Verteidigungsmaßnahmen zur Sicherung von Web-Apps, sondern zeigt auch, wie häufig und leicht die Angriffe sind – warum also diese Apps gesichert werden müssen.“

– Brandon Hardin, **ITC**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC522**

KURSFORMATE SEC522

Präsenzkurs | **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	38	Über 35
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Verstehen, wie DevOps funktioniert, und Schlüssel zum Erfolg identifizieren
- Sicherheitsscans in automatisierte CI/CD-Pipelines und -Workflows einbauen
- Die Ergebnisse von Sicherheitsscans analysieren und die Daten in CI/CD-Dashboards anzeigen
- Geheimnisse für CI/CD-Server und Cloud-native Anwendungen verwalten
- Konfigurationsmanagement mit IaC (Infrastructure as Code) automatisieren
- Golden Images virtueller Maschinen mit CI/CD-Workflows erstellen, härten und veröffentlichen
- Container-Technologien mit Docker und Kubernetes betreiben und sichern
- Kubernetes-Cluster mit Workload-Identität und Zugangskontrolle härten

Zielgruppe

- Alle, die in einer öffentlichen Cloud/DevOps-Umgebung arbeiten oder darauf umstellen
- Alle, die verstehen möchten, wo Sicherheitsprüfungen, Tests und andere Kontrollmaßnahmen in der Cloud und in DevOps-Pipelines zur kontinuierlichen Bereitstellung hinzugefügt werden sollten
- Alle, die lernen möchten, wie DevOps-Workloads in die Cloud verlagert werden können, speziell zu Amazon Web Services (AWS) und Microsoft Azure
- Alle, die von AWS oder Azure bereitgestellte Services für die Cloud-Anwendungssicherheit nutzen möchten
- Entwickler
- Software-Architekten
- Betriebsingenieure
- Systemadministratoren
- Sicherheitsanalysten
- Sicherheitsingenieure
- Auditoren
- Risikomanager
- Sicherheitsberater

Berufliche Rollen im NICE Framework

- 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
Kursautor

Eric Johnson
Kursautor

Ben Allen
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Sichern Sie Ihre Systeme mit Cloud-nativer Schnelligkeit.

Organisationen ziehen in die Cloud, um den digitalen Wandel zu ermöglichen und die Vorteile des Cloud-Computings nutzen zu können. Aber Sicherheitsteams finden es schwer zu verstehen, wie die DevOps-Toolchain funktioniert und wie sie Sicherheitskontrollmaßnahmen in ihre automatisierten Pipelines integrieren können, die Änderungen in Cloud-basierte Systeme einführen. Ohne effektive Pipeline-Sicherheitskontrollmaßnahmen, sind die Änderungen, die in Produktionsumgebungen eingeführt werden, für die Sicherheitsteams nicht transparent. SEC540™ gibt Sicherheitsfachkräften die Kenntnisse an die Hand, die sie benötigen, um Leitlinien und Sicherheitsrichtlinien in den DevOps-Pipelines, der Cloud-Infrastruktur, den Container-Orchestratoren und den Microservice-Umgebungen ihrer Organisation zu automatisieren. Bei SEC540™ werden die Teilnehmer mit der DevOps-Kultur vertraut. Nach dem Kurs sind sie kampferprobt und bereit, das Cloud-native und das DevSecOps-Sicherheitsprogramm ihrer Organisation auszubauen.

Geschäftsorientierte Lernergebnisse

- Ein Sicherheitsteam aufbauen, das moderne Cloud-native Sicherheit und DevSecOps-Workflows versteht
- In Partnerschaft mit DevOps-Team und Technikteam Sicherheit in automatisierte Pipelines und noch früher im Entwicklungsprozess einschleusen
- Cloud-native Services zur Implementierung, Härtung und Überwachung von Software-Produkten nutzen
- Dafür sorgen, dass die Organisation bereit ist, Produkte während der Cloud-Migration zu überarbeiten, zu revidieren und neu zu erstellen
- Mithilfe von Cloud-Überwachung und durch Ereignisse ausgelöste Automatisierung die Sicherheitsfähigkeiten verbessern und effektiv auf Risiken reagieren

Zusammenfassung der Kursinhalte

TEIL 1: DevOps-Sicherheitsautomatisierung
TEIL 2: Sicherheit in der Cloud-Infrastruktur
TEIL 3: Cloud-nativer Sicherheitsbetrieb
TEIL 4: Microservice- und serverlose Sicherheit
TEIL 5: Kontinuierliche Compliance und Absicherung

„Der BESTE Kurs, den ich bei SANS je belegt habe. Das ist einer der Kurse, bei dem ich mich anschließend bei der Arbeit einloggen und das Gelernte sofort bei meinen täglichen Aufgaben und Zuständigkeiten anwenden kann. Ich war bereits im Slack-Kanal meines Teams und habe allen geraten, sich für diesen Kurs anzumelden."

– Brian Esperanza, **Teradata**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC540**

KURSFORMATE SEC540

Präsenzkurs | **Live online** | **OnDemand**

SEC541: Cloud Security Threat Detection™ GRUNDLEGEND ÜBERARBEITET

GCTD
Cloud Threat Detection
giac.org/gctd

5	30	21
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Verstehen, wie Identitäten in Cloud-Umgebungen missbraucht werden können
- Böswillige Akteure mit Cloud-nativen Protokollierungstools überwachen
- Computing-Ressourcen wie z. B. virtuelle Maschinen (VM) und Container definieren und verstehen
- Bewegungen des Angreifers in Ihrer Cloud-Infrastruktur erkennen und angehen
- Mit Tools von Cloud-Anbietern effektive Detektionsstrategien umsetzen
- Instanzen in Ihren Computing-Ressourcen auf verdächtige Aktivitäten untersuchen und analysieren
- Detaillierte Analyse und Bedrohungsdetektion in Microsoft 365- und Azure-Umgebungen durchführen
- Flexibel zwischen verschiedenen Protokollquellen wechseln, um den vollständigen Ablauf eines Angriffs aufzudecken
- Automatisierungsworkflows erstellen, die repetitive Sicherheitsaufgaben reduzieren
- Daten aus verschiedenen Quellen zentralisieren und normalisieren, um Analyse und Bedrohungsdetektion zu verbessern

Zielgruppe

- Cloud-Sicherheitsanalysten
- Ingenieure für Bedrohungsdetektion
- SOC-Betreiber (Security Operations Center)
- Ersthelfer bei Sicherheitsvorfällen
- Cloud-Sicherheitsarchitekten
- Penetrationstester
- SOC-Manager
- Mitglieder eines Blue Teams
- Forensikanalysten
- Fachkräfte für Offensivsicherheit, die defensive Techniken verstehen möchten
- IT-Fachkräfte, die auf Cloud-Sicherheitsrollen umstellen
- Alle, die in beliebigen Branchen für die Sicherung von Cloud-Umgebungen zuständig sind

Berufliche Rollen im NICE Framework

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

Shaun McCullough
Kursautor

Ryan Nicholson
Kursautor

Versteckt euch ruhig – wir kriegen euch doch. Unser Radar sieht alle Bedrohungen.

Der Umzug in eine Cloud-Infrastruktur bietet zahlreiche Vorteile, setzt Organisationen aber auch neuen Bedrohungen aus, die sich kontinuierlich weiterentwickeln. Viele Organisationen sind sich nicht bewusst, dass zwischen On-Premise- und Cloud-Umgebungen entscheidende Unterschiede bestehen, und verstehen daher nur schwer, was protokolliert werden muss und wie Bedrohungen effektiv erkannt werden können. Im Gegensatz zu anderen Kursen, die sich primär mit der Theorie beschäftigen, bietet SEC541™ praxisbezogene Erfahrung durch 21 praktische Laborübungen, die AWS, Azure und Microsoft 365 abdecken. Dieser Kurs befähigt Ihr Team, Cloud-native Protokollierung, Bedrohungsdetektion und Überwachung zu meistern, und räumt dadurch versteckte Probleme aus dem Weg, die sich durch eine leichte Lösung schnell auszahlen. Mit SEC541™ geben Sie Ihrem Team die Kompetenzen an die Hand, die es braucht, um den Cloud-Sicherheitsstatus Ihrer Organisation zu stärken und potenziellen Schwachstellen vorzubeugen.

Geschäftsorientierte Lernergebnisse

- **Detektions- und Reaktionszeit reduzieren:** Identifizieren und mitigieren Sie kritische Cloud-Bedrohungen schnell.
- **Transparenz verbessern:** Gewinnen Sie umfassende Einblicke in Ihre Cloud-Umgebung.
- **Sicherheitsstatus verbessern:** Implementieren Sie effektive, Cloud-spezifische Strategien zur Bedrohungsdetektion.
- **Proaktives Bedrohungsmanagement:** Gehen Sie Bedrohungen frühzeitig an, damit Vorfälle schnell beigelegt werden.
- **Effizienz und Automatisierung:** Erhöhen Sie die Effizienz durch automatisierte Detektions- und Reaktions-Workflows.
- **Kosteneinsparungen:** Vermeiden Sie finanzielle Folgen, indem Sie Ihre Cloud-Umgebung proaktiv sichern.
- **Personalkompetenzen verbessern:** Geben Sie Ihrem Team die neuesten Kenntnisse und Techniken zur Cloud-Sicherheit an die Hand, damit sie Ihre Organisation gegen ausgereifte Cloud-Bedrohungen verteidigen können.

Zusammenfassung der Kursinhalte

TEIL 1: Angriffe auf Managementebene und im Netzwerk
TEIL 2: Computing- und Anwendungsangriffe
TEIL 3: Sicherheitsservices und Datenentdeckung
TEIL 4: Das Microsoft-Ökosystem
TEIL 5: Datenversand, Automatisierung und CloudWars

„Der Kurs ist sehr gut konzipiert. Shaun und Ryan haben ihn prima zusammengestellt. Der Inhalt ist ausgezeichnet und es gibt eine Menge zu lernen."

– Scott Perry

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC541**

KURSFORMATE SEC541

Präsenzkurs **Live online** **OnDemand**

KURS NEU IM FOKUS

SEC545: GenAI and LLM Application Security™

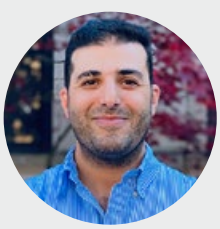
3	18	11
Kurstage	CPEs	Laborübungen

Vermittelte Kompetenzen

- **Wichtige Konzepte und Begriffe verstehen:** Gewinnen Sie ein eingehendes Verständnis von GenAI, LLM-Architekturen und ihrer Anwendung in Szenarien aus der wirklichen Welt.
- **Verschiedene Modelle und Tools erkunden:** Untersuchen Sie die Arten von Modellen und Tools, die zur Erstellung und Bereitstellung von GenAI-Anwendungen verfügbar sind.
- **Anpassung erkunden:** Lernen Sie, wie Sie Modelle für spezifische Nutzungsfälle abstimmen.
- **Risiken und Minderungsstrategien bewerten:** Identifizieren Sie die besonderen Sicherheitsrisiken von GenAI-Anwendungen und erkunden Sie effektive Minderungstechniken.
- **RAG, Einbettungen und Vektordatenbanken sichern:** Lernen Sie RAG (Retrieval-Augmented Generation), Einbettungen und VektorDB kennen und verstehen Sie, wie verschiedene Komponenten sicher konfiguriert werden.
- **Betriebs- und Sicherheitskontrollmaßnahmen erkunden:** Erkunden Sie die betrieblichen Aspekte der Erstellung und Bereitstellung von GenAI-Anwendungen und lernen Sie die relevanten Sicherheitskontrollmaßnahmen kennen.
- **Hosting-Optionen vergleichen:** Lernen Sie die verschiedenen GenAI-Hosting-Optionen und ihre Unterschiede aus der Perspektive der Sicherheit verstehen.
- **Cloud-Sicherheitskontrollmaßnahmen nutzen:** Lernen Sie mehr über die Sicherheitskontrollmaßnahmen, die von Cloud-Anbietern für LLM-Hostingservices angeboten werden.
- **Andere Technologien im Umfeld von GenAI erkunden:** Untersuchen Sie Technologien wie LangChain, Agenten und MCP und verstehen Sie, welche Sicherheitsrisiken sie mit sich bringen.
- **GenAI in den Sicherheitsrahmen integrieren:** Lernen Sie, wie Sie GenAI-Sicherheitspraktiken aufstellen oder in den bestehenden Sicherheitsrahmen Ihrer Organisation integrieren.

Zielgruppe

- Anwendungs-Sicherheitsingenieure
- Cloud-Sicherheitsingenieure
- SOC-Analysten, Incident Handler und Threat-Intelligence-Fachkräfte
- Sicherheitsfachkräfte
- Sicherheitsauditoren, Compliance- und Risikomanager



Ahmed Abugharbia
Kursautor

Das Feld der Generativen KI (GenAI) entwickelt sich schnell weiter – oft zu schnell, als dass etablierte Sicherheitspraktiken Schritt halten könnten. Dieser Kurs möchte einen Beitrag zur Schaffung effektiver Ansätze für die GenAI-Sicherheit leisten, indem er die Sicherheitsgemeinschaft durch kontinuierliche Forschung und praktische Einblicke unterstützt.

SEC545 bietet ein umfassendes Fundament in GenAI-Technologien und den Sicherheitsstrategien, die zu ihrem Schutz nötig sind. Der Kurs stellt Kernkonzepte wie Large Language Models (LLMs), Einbettung und Retrieval-Augmented Generation (RAG) vor und untersucht anschließend wichtige Risiken wie Prompt-Injection, schädliche Modelle und Schwachstellen in der Lieferkette. Die Teilnehmer erkunden, wie sie mit Tools wie LangChain, AI-Agenten, Vektordatenbanken und MCP (Model Context Protocol) sichere GenAI-Anwendungen erstellen können. Den Abschluss des Kurses bildet ein Überblick über Hosting-Strategien, von lokalen Bereitstellungen bis zu Cloud-Plattformen wie AWS Bedrock. Während des Kurses lernen die Teilnehmer, wie sie Bedrohungen identifizieren, bewährte Sicherheitspraktiken anwenden und GenAI-Systeme in einem Umfeld des raschen Wandels verteidigen.

Geschäftsorientierte Lernergebnisse

- GenAI-Anwendungen verstehen
- Potenzielle Risiken bei GenAI-Anwendungen identifizieren
- Lernen, wie sich GenAI-Risiken effektiv mindern lassen

Zusammenfassung der Kursinhalte

TEIL 1: : GenAI, Large Language Models (LLMs) und Sicherheitsrisiken

TEIL 2: GenAI-Anwendungen sichern

TEIL 3: MLSecOps und GenAI-Anwendungslebenszyklus sichern

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC545**

KURSFORMATE SEC545

Präsenzkurs | Live online

SEC549: Cloud Security Architecture™

GRUNDLEGEND ÜBERARBEITET

GCAD
Cloud Security Architecture and Design
giac.org/gcad

5	30	Über 20
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Das Unternehmen durch ein sicheres Architekturdesign für die Enterprise-Cloud befähigen
- Die Verbindung zwischen Cloud-Architekturdesigns und echten Lösungen herstellen
- Ein sicheres, skalierbares Identitätsfundament in der Cloud aufbauen
- Die Personalidentität Ihrer Organisation zentralisieren, um Identity Sprawl zu vermeiden
- Mikrosegmentierte Netzwerke mit Hub-and-Spoke-Mustern aufbauen
- Zentralisierte Netzwerk-Firewalls zur Untersuchung des Nord-Süd- und Ost-West-Verkehrs konfigurieren
- Lernen, wie Sie sowohl netzwerkbasierte als auch identitätsbasierte Kontrollmaßnahmen einbauen
- Datenperimeter für in der Cloud gehostete Daten-Repositorys erstellen
- KMS-Ressourcen (Key Management Service) zentralisieren und organisationsweit freigeben
- Security Operations und Incident Response in der Cloud ermöglichen
- Verstehen, welche Telemetrie und Protokollierung in den Servicemodellen verfügbar sind (IaaS, PaaS und SaaS)
- Push- und Pull-Protokollierungsarchitekturen zur zentralisierten Protokollaggregierung entwerfen
- Pläne für Cloud-Wiederherstellungsprozesse mit mehreren Ebenen von Notfallkonten erstellen

Zielgruppe

- Lösungsarchitekten
- Sicherheitsauditoren
- Cloud-Architekten
- Sicherheitsingenieure
- Sicherheitsarchitekten
- Cloud-Ingenieure
- DevOps-Ingenieure
- Systemadministratoren
- Operations
- Alle, die dafür zuständig sind:
  - Das Unternehmen durch sichere Architekturmuster für die Cloud zu befähigen
  - Neue Cloud-Angebote zu beurteilen und einzuführen
  - Cloud-Migrationen zu planen
  - Identitäts- und Zugriffmanagement in der Cloud umzusetzen oder zu verwalten
  - Ein virtuelles Netzwerk in der Cloud zu verwalten

Eric Johnson
Kursautor

David Hazar
Kursautor

Gregory Leonard
Kursautor

Viele Organisationen sind dabei, Infrastruktur und Anwendungen rasch in die Cloud zu verlegen. Während dieser Migrationen fällt Sicherheitsarchitekten die Aufgabe zu, hybride und Cloud-native Lösungen zu entwerfen, die die Sicherheitsanforderungen ihrer Organisation erfüllen. Der Umzug in die Cloud erfordert ein eingehendes Verständnis der Bedrohungen, die durch eine Cloud-Migration eingeführt werden, und wie die einzelnen Anbieter diese Bedrohungen mit ihrem gut konzipierten Framework mindern. SEC549™ vermittelt Sicherheitsfachkräften, wie sie eine Enterprise-fähige, skalierbare Cloud-Organisation entwerfen können. In fast 20 praktischen Laborübungen lernen die Teilnehmer, Cloud-Lösungen für ihre Organisation zu entwerfen, die für jede Phase der Cloud-Migration geeignet sind – ob sie die erste Workload planen, komplexe Legacy-Umgebungen verwalten oder in einem erweiterten Cloud-nativen Ökosystem operieren müssen.

Geschäftsorientierte Lernergebnisse

- Die Risiken durch aufkommende Cloud-Technologien und ihre rasche Verbreitung mindern
- Das Risiko bei Cloud-Migrationen durch Planung für einen phasenweisen Ansatz senken
- Identity Sprawl und technische Schulden durch Zentralisierung verhindern
- Geschäftliches Wachstum durch Schaffung übergreifender Leitlinien fördern
- Verhindern, dass sich kostspielige Anti-Patterns durch die gesamte Cloud-Organisation verbreiten
- Gelernte Zugriffsmuster anwenden, um Ihre Organisation in Richtung Zero-Trust zu bewegen
- Effektive konditionelle Zugriffsrichtlinien entwerfen und lernen, wie Sie geschäftsorientierte Richtlinienausnahmen mit Leitlinien umgeben

Zusammenfassung der Kursinhalte

TEIL 1: Cloud-Kontomanagement und Identitätsgrundlagen

TEIL 2: Implementierung eines Identitätsperimeters in der Cloud

TEIL 3: Cloud-nativer Sicherheitsbetrieb

TEIL 4: Datenzugriff-Perimeter in der Cloud

TEIL 5: Befähigung eines Cloud-fokussierten SOC

„Die Laborübungen haben den Arbeitstag eines Sicherheitsarchitekten realistischer simuliert, als ich es je gesehen habe. Alle, die Architekten werden wollen, erhalten hier einen guten Eindruck, wie ihr Arbeitsalltag aussehen wird."
– Maciej Bak, **Standard Chartered**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC549**

KURSFORMATE SEC549

Präsenzkurs | **Live online** | **OnDemand**

SANS-Schulungen nun über AWS Marketplace erhältlich

Stärken Sie die Cloud-Sicherheit und maximieren Sie gleichzeitig Ihre Vorteile aus AWS EDP.

Statten Sie Ihre Teams mit dem nötigen Know-how zum Schutz Ihrer Cloud-Infrastruktur aus. Greifen Sie nahtlos durch AWS Marketplace auf SANS-Kurse für Cloud-Sicherheit zu und erstellen Sie skalierbare, flexible und effektive Schulungspakete, die ganz auf die individuellen Bedürfnisse Ihrer Organisation abgestimmt sind.

Lernen nach Wunsch:

Maßgeschneiderte Schulungen

Wählen Sie unseren neuesten Kurs, **SEC480: AWS Secure Builder**, sowie eine umfassende Auswahl von Kursen zu Themen wie IAM-Konfiguration, Berechtigungsmanagement und Best Practices der Cloud-Sicherheit.

Jederzeit und überall lernen

Greifen Sie auf On-Demand-Schulungen zu, mit denen Sie von überall aus in Ihrem eigenen Tempo lernen können. Die Arbeit wird möglichst wenig unterbrochen und mehr Beschäftigte können teilnehmen.

Von Experten geleitet und an GIAC orientiert

Bleiben Sie mit unseren hochaktuellen Schulungen aufkommenden Bedrohungen stets einen Schritt voraus. Sie werden von führenden Köpfen in der Cybersicherheit präsentiert und von GIAC mit branchenweit anerkannten Zertifizierungen honoriert.

Vereinfachtes Procurement

Optimieren Sie Ihren Kaufprozess und Ihre Ausgaben in AWS EDP (Enterprise Discount Program).

Sehen Sie sich die SANS-Schulungen auf AWS Marketplace an.

Hier scannen und einen angepassten Schulungsplan erstellen.

→

FOKUSBEREICH IM SANS-LEHRPLAN

Cyberverteidigung

In der Cybersicherheit liegt der Fokus eines Verteidigers darauf, die Organisation gegen Cyberangriffe zu verteidigen. Durch die Entwicklung und Implementierung von Sicherheitskontrollmaßnahmen, die Verifizierung der Effektivität dieser Kontrollmaßnahmen und kontinuierliche Überwachung und Verbesserung stärken Cyberverteidiger die Fähigkeiten einer Organisation, potenzielle Angriffe abzuwehren.

In Kursen zur Cyberverteidigung lernen Sie Folgendes:

- Die nötigen Tools und Techniken einsetzen, um Ihre Netzwerke verständnisvoll und bewusst zu verteidigen
- Ein modernes Sicherheitsdesign implementieren, mit dem Sie Ihre Assets schützen und gegen Bedrohungen verteidigen können
- Einen holistischen und mehrschichtigen Ansatz zur Sicherheit begründen und pflegen
- Angriffe erkennen und Netzwerkverkehr analysieren
- Einen proaktiven Ansatz bei NSM (Network Security Monitoring)/CDM (Continuous Diagnostics and Mitigation)/CSM (Continuous Security Monitoring) verfolgen
- Vorhandene Protokollierungslösungen mithilfe von Methoden und Prozessen verbessern
- Technische Sicherheitsprinzipien und Kontrollmaßnahmen für die Cloud anwenden

„Mit den Techniken aus diesem Kurs kann ich unsere Protokollierungs- und Detektionsfähigkeiten sofort verbessern."

– Kendon Emmons, **Dart Container**

Berufliche Rollen in der Cyberverteidigung:

- SOC-Analyst/-Manager
- Ingenieur für Bedrohungsdetektion, Threat Hunter
- Sicherheits- und Netzwerkingenieur/-architekt
- Ermittler/OSINT-Analyst
- Endpunkt-/Serversystem-Administrator
- Automatisierung und DevSecOps
- Incident Responder
- Cyber Threat Intelligence-Analyst

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

5	30	40
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Die Linux-Befehlszeile souverän und effizient navigieren
  Linux-Systeme durch Härtungstechniken und Best Practices sichern
- Benutzerauthentifizierung, Zugriffskontrolle und Berechtigungen konfigurieren und verwalten
- Linux-Systeme auditieren und Sicherheitsprotokolle zur Bedrohungsdetektion analysieren
- Systemprozesse verwalten, Leistung überwachen und Ressourcennutzung optimieren
  Techniken der Vorfallsreaktion für Linux-basierte Sicherheitsereignisse implementieren
- Fernverwaltung mit SSH, SCP und OpenSSL sichern
  Firewalls konfigurieren und die Linux-Netzwerkkommunikation sichern
- Linux-Software mithilfe von Paketmanagement sicher installieren, aktualisieren und verwalten

Zielgruppe

- Alle, die Linux-Server verwalten und für die Sicherheit dieser Systeme verantwortlich sind
- Alle, die Anwendungen auf Linux-basierten Cloud-Lösungen implementieren und verwalten
- Sicherheitsfachkräfte, die mehr über Best Practices der Linux-Sicherheit erfahren und wissen möchten, wie sie sich in ihrer Organisation implementieren lassen
- Technologiefachkräfte, die ein tieferes Verständnis von Konzepten der Linux-Sicherheit entwickeln und ihre Kompetenzen bei der Sicherung von Linux-Systemen verbessern möchten
- Alle, die mehr über Linux-Sicherheit lernen und erfahren möchten, wie sie die Systeme und Daten ihrer Organisation vor Cyberbedrohungen schützen können

Mark Baggett
Kursautor

Charles Goldner
Kursautor

Sicherung, Befehle, Schutz: Praktische Linux-Sicherheitsschulung

Die meisten neuen InfoSec-Fachkräfte sind mit Windows besser vertraut als mit Linux. Aber viele der Tools, die heute in Offensive, Defensive, ICS und Forensik unverzichtbar sind, erfordern ein solides Verständnis von Linux. Für alle, denen die benötigte Erfahrung fehlt, stellt das eine große Herausforderung dar, denn diese Systeme werden häufig in stark exponierten Umgebungen wie DMZ und der Cloud eingesetzt. Die Ironie dabei ist, dass es nun gerade unsere Plattformen für Informationssicherheit sind, die neue Sicherheitsrisiken verursachen. Dieser Linux-Sicherheitskurs löst das Problem: In zahlreichen praktischen Übungen entwickeln die Teilnehmer rasch Linus-Kompetenzen, die sie zu einem wertvollen Zuwachs für jedes Informationssicherheits-Team machen.

Diese Linux-Sicherheitsschulung konzentriert sich auf grundlegende Aspekte der Linux-Administration. Die Teilnehmer lernen, wie sie ein sicheres Linux-System konfigurieren, mit der Befehlszeile arbeiten und Benutzer und Berechtigungen verwalten. Außerdem geht die Schulung auf die Sicherheitsaspekte dieser Kompetenzen ein und vermittelt den Teilnehmern, wie sie ihre Linux-Systeme sichern und gegen potenzielle Angriffe verteidigen können. Sie lernen, wie eine Fehlkonfiguration eine Schwachstelle verursachen kann, wie diese Schwachstelle angegriffen werden kann und wie sich diese Risiken mindern lassen. Nach Abschluss des Kurses haben die Teilnehmer die erforderlichen Kenntnisse und Fähigkeiten, um Linux-Systeme zu sichern, potenzielle Sicherheitsbedrohungen zu identifizieren und sie durch angemessene Maßnahmen zu verhindern. Mit unserem Kurs können Sie sich zu einem erfahrenen, kompetenten und selbstbewussten Linux-Benutzer entwickeln und in Ihrer Organisation einen positiven Beitrag leisten.

Zusammenfassung der Kursinhalte

TEIL 1: Linux-Befehlszeile

TEIL 2: Shell-Syntax und Kontomanagement

TEIL 3: Datei- und Benutzer-Zugriffskontrolle

TEIL 4: Prozess- und Protokollmanagement

TEIL 5: Paket-, SSH- und Netzwerkmanagement

„Obwohl ich Linux bereits eine Weile nutze, habe ich eine Menge Dinge gelernt, die ich nicht wusste oder nicht verstanden hatte, und die nun Sinn ergeben.“

– John R., **US-amerikanisches Militär**

„Mir gefiel gut, wie der Kurs präsentiert wurde. Der Ablauf war flüssig und man konnte gut folgen.”

– Christopher Hannon, **SEC406-Teilnehmer**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC406**

KURSFORMATE SEC406

Live online **OnDemand**

SEC450: **Blue Team Fundamentals: Security Operations and Analysis™**

GSOC
Security Operations
giac.org/gsoc

6	36	16
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Sicherheitstelemetrie optimal nutzen, u. a. Endpunkt-, Netzwerk- und Cloud-basierte Sensoren
- Die besten Gelegenheiten für die SOAR-Plattform und andere skriptbasierte Automatisierung identifizieren
- Den Sicherheitsbetrieb auf Tempo halten, indem Sie eingehend diskutieren, was ein SOC- oder SecOps-Team bei jedem Schritt tun sollte, von Datengenerierung bis zu Detektion, Triage, Analyse und Incident Response
- Typische, häufige Angriffsalarme schnell identifizieren und von größeren Angriffen mit hohem Risiko und schweren Auswirkungen unterscheiden und Sicherheitsvorfälle sorgfältig, gründlich und unvoreingenommen analysieren
- Detaillierte Erklärungen von Prozessen und Techniken geben, um falsch positive Meldungen auf ein Minimum zu reduzieren
- Sicherheitsvorfälle durch kluge Datenkorrelierung und Anreicherungstechniken, die falsch positive Meldungen sofort erkennen und von den wirklich positiven Meldungen unterscheiden, schnell und korrekt triagieren
- Automatisierungsworkflows für häufige SOC-Aktivitäten einrichten, um Analysten von langweiligen Aufgaben zu entlasten, damit ihnen mehr Zeit für Threat Hunting und Detektionstechniken bleibt

Zielgruppe

- Sicherheitsanalysten
- Vorfallsermittler
- Sicherheitsingenieure und -architekten
- Technische Sicherheitsmanager
- SOC-Manager, die zusätzliche technische Perspektiven dazu gewinnen möchten, wie sie die Analysequalität verbessern, die Personalfluktuation verringern und ein effizientes SOC leiten können
- Alle, die eine Karriere im Blue Team anstreben

Berufliche Rollen im NICE Framework

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

John Hubbard
Kursautor

Die Blaupause für ausgezeichnete SOC-Analysen

SEC450™ ist von Grund darauf ausgelegt, eine allumfassende Schulung für SOC-Analysten bereitzustellen. Wenn Sie in der Cyberverteidigung tätig sind, ein SOC aufbauen oder ein bestehendes SOC mit besseren Daten-, Workflow- und Analysetechniken ausstatten möchten, ist SEC450™ der Kurs für Sie! Mit detaillierten Erklärungen des Ziels und der Denkweise der modernen Cyberverteidigung wendet sich dieser Kurs an alle, die zur nächsten Generation der Blue Teams gehören möchten. Mit sechs Schulungstagen, sechs Kursbüchern, zwanzig praktischen Laborübungen und einer ganztägigen „Defend-the-Flag"-Abschlussübung ist SEC450™ schlicht und einfach der umfassendste Kurs für SOC- und Sicherheitsanalysten, der derzeit auf dem Markt angeboten wird.

Geschäftsorientierte Lernergebnisse

- Eine Paketlösung zur Schulung von SOC-Analysten, in der sie die Tools, Daten und Verteidigungsprioritäten verstehen lernen, die zur Verteidigung Ihres Netzwerks vor folgenreichen Cyberangriffen erforderlich sind
- Wie klare strategische Prioritäten für Ihr SecOps-Team ermittelt werden
- Wie Sicherheitstelemetrie optimal genutzt wird, u. a. Endpunkt-, Netzwerk- und Cloud-basierte Sensoren
- Eine kampferprobte Methode zur Reduzierung von falsch positiven Meldungen auf das absolute Minimum
- Techniken zur schnellen und korrekten Triage von Sicherheitsvorfällen
- Methoden zur Verbesserung der Effektivität, Effizienz und Wirksamkeit Ihres SOC

Zusammenfassung der Kursinhalte

TEIL 1: Übersicht über Teams, Tools und Ziel des Sicherheitsbetriebs

TEIL 2: Analyse des Netzwerkverkehrs

TEIL 3: Übersicht über Endpunktverteidigung, Sicherheitsprotokollierung und Identifizierung

TEIL 4: Effiziente Alarmtriage und E-Mail-Analyse

TEIL 5: Kontinuierliche Verbesserung, Analyse und Automatisierung

TEIL 6: Abschlussübung: „Defend the Flag"

„Bislang erfüllt SEC450 nicht nur meine Erwartungen, sondern übertrifft sie. Vor einem Jahr wurde ich zum Leiter des SOC-Teams ernannt. Dieser Kurs hat meine Kenntnisse erweitert und mir ermöglicht, mein SOC mit einem stärker strukturierten Ansatz zu leiten."

– Radek Ochrymowicz, **Frontex**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC450**

KURSFORMATE SEC450

Präsenzkurs | **Live online** | **OnDemand**

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

1 Kurstag | 5 CPEs

Vermittelte Kompetenzen

- Eine End-to-End-RAG-Back-End-Lösung erstellen
- Eine RAG erweitern, um kontextuelle RAG-Lösungen zu implementieren
- KI-Agenten verstehen und in einem LLM-Kontext zur RAG-Überwachung implementieren
- Sicherheitskontrollmaßnahmen implementieren, um die Offenlegung von Informationen aus einem LLM einzuschränken
- Prompt-Injection-Angriffe verhindern und dagegen verteidigen

Zielgruppe

- Alle, die eine Lösung mit generativer KI zum Informationsabruf implementieren möchten
- Alle, die SEC595 erfolgreich abgeschlossen haben und mehr über LLMs wissen möchten
- Fachkräfte, die verstehen möchten, wie sie LLMs für den internen und kundenseitigen Informationsabruf nutzen können

Geschäftsorientierte Lernergebnisse

- Verstehen, wie man mit Vektordatenbanken arbeitet und sie nutzt
- In der Lage sein, Chatbot-Lösungen u. ä. intern zu implementieren
- KI/LLM-Lösungen erstellen können, ohne sensible interne Informationen gegenüber einem Dritten offenzulegen oder eine öffentliche oder kommerzielle API zu verwenden
- Verstehen, wie man hochmoderne kontextuelle RAG-Lösungen erstellt
- Verstehen, wie agentenbasierte KI-Lösungen in Bezug auf LLMs implementiert werden

David Hoelzer
Kursautor

In vielen Organisationen sind Führungsteams an Gelegenheiten interessiert, KI im Geschäftsprozess zu nutzen. Es ist jedoch nicht klar, welchen Zweck KI im Unternehmen eigentlich hat.

SEC595™ vermittelt den Teilnehmern alles, was sie wissen müssen, um hochmoderne Maschinenlern- und KI-Lösungen für echte Cybersicherheitsprobleme zu erstellen. SEC495™ hingegen verfolgt ein ganz anderes Ziel. Die Erfahrung lehrt, dass die meisten Managementteams, die an KI interessiert sind, auf die Large Language Models (LLMs) reagieren, die in den letzten Jahren die Schlagzeilen dominiert haben. Bei SEC495™ erstellen Sie zusammen mit dem Kursleiter ein komplett eigenständig gehostetes RAG-System (Retrieval Augmented Generation), das ein LLM nutzt. Darüber hinaus lernen Sie, wie Sie Sicherheitskontrollmaßnahmen implementieren, die das LLM vor Prompt-Injection schützen, und wie Sie Kontrollmaßnahmen für Informationssensibilität umsetzen, die anhand der Rechte des Benutzers einschränken, welche Antworten das LLM geben kann.

Wenn Sie eine LLM-basierte Lösung zur Beantwortung von Fragen, zum Abruf von Knowledgebases, zur Richtlinienerstellung oder für eine ähnliche Aufgabe erstellen müssen, eignen Sie sich in diesem Kurs schnell die Grundlagen an.

Erklärung des Autors

Das Management erwartet zunehmend, dass wir KI sinnvoll im Unternehmen nutzen. Wie können wir das tun? Wie sieht das aus? Es gibt zahlreiche Antworten auf diese Fragen, und SEC595 bietet klare Antworten im Hinblick auf Threat Hunting und Überwachung. SEC495™ hingegen vermittelt Ihnen alles, was Sie wissen müssen, um mit der Erstellung von LLM-Lösungen zu beginnen. Die Lösungen bei SEC595™ sind extrem nützlich und auf dem neuesten Stand der Technik. Bei SEC495 geht es hingegen um die Erstellung von RAG-Lösungen mit LLMs, die für Managementteams sehr viel leichter verständlich sind, da sie sofort sehen und verstehen können, warum diese Lösungen praktisch sind.

Wir konzentrieren uns auf die Nutzung (und Sicherung) von RAGs zum Informationsabruf. Es gibt jedoch auch einige natürliche Erweiterungen, z. B. die Identifizierung der Standard-Compliance basierend auf Richtlinien, automatisierte Berichterstellung und vieles mehr. Vielleicht der größte Vorteil von SEC495™ ist, dass alles in On-Premise-Containern stattfindet. Natürlich können Sie diese in der Cloud hosten, hochskalieren oder sogar gegen kommerzielle APIs auswechseln, aber Sie lernen, wie Sie alle diese Komponenten implementieren, ohne sensible Informationen an Dritte senden zu müssen. Das ist ein großer Vorteil!

– Dave Hoelzer

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC495**

KURSFORMATE SEC495

OnDemand

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

GOSI
Open Source Intelligence
giac.org/gosi

6	36	Über 29
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

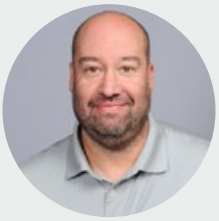
- Verschiedene OSINT-Ermittlungen durchführen und gleichzeitig gute OPSEC praktizieren
- Sock-Puppet-Konten erstellen
- Informationen im Internet finden, einschl. einiger schwer zu findender und gelöschter Daten
- Personen online finden und ihre Onlinepräsenz untersuchen
- Das Dark Web verstehen und effektiv durchsuchen
- Einen korrekten Bericht über die Online-Infrastruktur erstellen, der für Cyberverteidigung, zur Analyse bei Fusionen und Übernahmen, für Penetrationstests und für andere entscheidend wichtige Bereiche einer Organisation genutzt werden kann
- Methoden nutzen, die oft enthüllen können, wem eine Website gehört und welche anderen Websites diese Person besitzt oder betreibt
- Verstehen, welche verschiedenen Arten von abgegriffenen Daten verfügbar sind und wie sie für offensive und defensive Zwecke genutzt werden können
- Daten aus sozialen Medien effektiv erfassen und nutzen

Zielgruppe

- OSINT-Ermittler
- Informationsanalysten für Cyberbedrohungen
- Geheimdienstpersonal
- Strafverfolgungsbehörden
- Penetrationstester/Mitglieder eines Red Teams
- Cyberverteidiger
- Personalvermittler
- Journalisten
- Ermittler
- Fachkräfte für digitale Forensik
- Beschäftigte in Personalabteilungen

Berufliche Rollen im NICE Framework

- 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
Kursautor

Der Durchbruch zur Beherrschung von OSINT

SEC497™ ist ein umfassender Schulungskurs zu OSINT (Open-Source Intelligence), der von einem Branchenexperten mit mehr als zwei Jahrzehnten Erfahrung verfasst wurde. Der Kurs vermittelt Ihnen die wichtigsten Fertigkeiten, Tools und Methoden, die Sie benötigen, um Ihre Ermittlungskompetenzen auf den richtigen Weg zu bringen oder weiter auszubauen. SEC497™ bietet umsetzbare Informationen für alle, die in der Welt von OSINT zu Hause sind: Intelligence-Analysten, Strafverfolger, Fachkräfte auf dem Gebiet der Cyber Threat Intelligence, Cyber-Verteidiger, Penetrationstester, Ermittler und alle anderen, die ihre OSINT-Kompetenzen verbessern möchten. Von Neulingen bis hin zu erfahrenen Praktikern ist für jeden etwas dabei.

SEC497™ konzentriert sich auf praktische Techniken, die sich tagein, tagaus als nützlich erweisen werden. Der Kurs ist so aufgebaut, dass er für Neulinge auf dem Gebiet der OSINT zugänglich ist und gleichzeitig das Arsenal erfahrener Praktiker um bewährte Tools zur Lösung echter Probleme erweitert. Der Fokus des Kurses liegt auf dem Verständnis, wie Systeme funktionieren, damit fundierte Entscheidungen möglich werden. Er umfasst praktische Übungen, die auf tatsächlichen Szenarien aus dem Regierungssektor und der privaten Wirtschaft basieren. Wir diskutieren aktuelle Forschung und Techniken für Sonderfälle und reden nicht nur darüber, was möglich ist, sondern setzen es in die Tat um! Im Kurslehrplan unten finden Sie eine detaillierte Aufschlüsselung der abgedeckten Themen.

Geschäftsorientierte Lernergebnisse

Dieser Kurs hilft Ihrer Organisation:

- Competitive Intelligence durch OSINT-Techniken zu verbessern
- Das Risikomanagement zu verbessern, indem Schwachstellen identifiziert werden
- Die Incident Response durch schnelle Informationssammlung zu stärken
- Potenzielle Bedrohungen aus öffentlich verfügbaren Daten zu identifizieren und zu mindern
- Die Prozesse für Datensammlung und -analyse auf betriebliche Effizienz hin zu optimieren

Zusammenfassung der Kursinhalte

TEIL 1: Grundlagen von OSINT und OPSEC
TEIL 2: Grundlegende OSINT-Kompetenzen
TEIL 3: Personen untersuchen
TEIL 4: Websites und Infrastruktur untersuchen
TEIL 5: Automatisierung, Dark Web und große Data Sets
TEIL 6: Abschlussübung: „Capture-the-Flag"-Übung

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC497**

KURSFORMATE SEC497

Präsenzkurs | **Live online** | **OnDemand**

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

GCED
Enterprise Defender
giac.org/gced

6	38	25
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Durch Analyse der Konfigurationen von Netzwerkgeräten und Angriffssimulationen Bedrohungen der Netzwerkinfrastruktur identifizieren und verteidigungsfähige Netzwerke aufbauen, bei denen Angriffe minimale Auswirkungen haben
- Pakete mit verschiedenen Tools decodieren und analysieren, um Anomalien zu identifizieren und die Netzwerkverteidigung zu verbessern
- Verstehen, wie Gegner Systeme kompromittieren und wie mit einem Sechs-Schritte-Verfahren auf Angriffe reagiert werden kann
- Penetrationstest gegen ein Unternehmen durchführen, um Schwächen und gefährdete Stellen zu finden
- Aktive Verteidigungstechniken verstehen und nutzen
- Forensikartefakte mit Details zur früheren Systemaktivität sammeln, gelöschte Daten aus Speichergeräten wiederherstellen, Super-Timelines analysieren und eine Forensikanalyse am Netzwerk durchführen
- Mit verschiedenen Tools Malware im gesamten Unternehmen identifizieren und analysieren

Zielgruppe

- Erfahrene Technologen, die sich für den Bereich der Cybersicherheit umschulen und weiterbilden möchten
- CERT-/CSIRT-Mitglieder, die breite Erfahrung in mehreren Unterdisziplinen der Cybersicherheit benötigen
- InfoSec-Fachkräfte
- IT-Fachkräfte
- Softwareingenieure
- Ingenieure und Analysten im Security Operations Center
- Allrounder und Sicherheitsfachkräfte, die zahlreiche Aufgaben übernehmen müssen

Berufliche Rollen im NICE Framework

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

Ross Bergman
Kursautor

Umschulung und Weiterbildung im Cyberbereich sind für große wie kleine Unternehmen ein wichtiges Anliegen. Technologen müssen über breit gefächertes Wissen und gewisse Grundkompetenzen in mehreren Bereichen verfügen. Alle Mitglieder von Sicherheitsteams, und in zunehmendem Maße auch IT und DevOps, müssen dafür sorgen können, dass jedes System, jede Software und jede Infrastruktur, die codiert, erstellt und implementiert wird, Angriffen widerstehen kann. Teammitglieder müssen die nötigen Kenntnisse haben, um die Gegner in ihrer Mitte identifizieren zu können. Dazu müssen sie die Taktiken, Techniken und Verfahren der Widersacher kennen und wissen, welche Tools deren Aktivitäten im Unternehmen enthüllen können. Gegnern muss Einhalt geboten werden, sobald sie erkannt werden. Wenn ihre Lateralbewegung unterbunden und das Ausmaß der Infiltrierung begrenzt wird, minimiert sich das Risiko, dass kritische Unternehmensdaten offengelegt, geändert oder zerstört werden. Dabei ist es entscheidend, dass alle dazu beitragen können, den Kontrahenten zu eliminieren, kompromittierte Systeme zu sanieren und verlorene Assets wiederherzustellen. Vorbeugen. Erkennen. Reagieren.

Geschäftsorientierte Lernergebnisse

- Technologen umschulen und weiterbilden, damit sie einen wesentlichen Beitrag zur Cybersicherheit im Unternehmen leisten
- Effektivität, Effizienz und Erfolg von Cybersicherheitsinitiativen verbessern
- Verteidigungsfähige Netzwerke aufbauen, in denen Angriffe nur minimale Folgen haben
- Expositionspunkte identifizieren, damit die Schwachstellen priorisiert und behoben werden können, was die Sicherheit in der Organisation insgesamt erhöht
- Den Gegner durch Überwachung und Analyse der Netzwerkaktivität und systemübergreifende Korrelierung von Aktivitäten in On-Premise-Systemen und in der Cloud erkennen
- Methoden für Angriffe auf Systeme, Netzwerkgeräte und Web-Anwendungen verstehen

Zusammenfassung der Kursinhalte

TEIL 1: Verteidigungsfähige Netzwerkarchitektur
TEIL 2: Penetrationstests
TEIL 3: Grundlagen des Sicherheitsbetriebs
TEIL 4: Digitale Forensik und Incident Response
TEIL 5: Malware-Analyse
TEIL 6: Abschlussübung zur Unternehmensverteidigung

„Die beste technische Schulung, die ich je absolviert habe. SEC501 hat mich mit zahlreichen wertvollen Konzepten und Tools bekannt gemacht, aber auch eine solide Einführung in diese Tools vermittelt, sodass ich selbstständig weiterlernen und meine Kompetenz verbessern kann."

– Curt Smith, **Hildago Medical Services**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC501**

KURSFORMATE SEC501

Präsenzkurs | **Live online** | **OnDemand**

SEC503: Network Monitoring and Threat Detection In-Depth™

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

6	46	Über 37
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Snort und Suricata konfigurieren und ausführen
- Effektive und effiziente Regeln für Snort, Suricata und FirePOWER erstellen und schreiben
- Open Source Zeek konfigurieren und ausführen, um ein hybrides Framework zur Analyse des Datenverkehrs bereitzustellen
- Automatisierte Korrelierungsskripts zum Threat Hunting in Zeek erstellen
- TCP/IP-Komponentenlayer verstehen, um normalen und abnormalen Datenverkehr zur Bedrohungsidentifizierung unterscheiden zu können
- Mithilfe von Analysetools für den Datenverkehr Anzeichen einer Kompromittierung oder einer aktiven Bedrohung identifizieren
- Netzwerkforensik durchführen, um den Datenverkehr zu untersuchen, TTPs zu identifizieren und aktive Bedrohungen zu finden
- Dateien und andere Arten von Inhalten aus dem Netzwerkverkehr extrahieren, um Ereignisse zu rekonstruieren
- BPF-Filter erstellen, um ein bestimmtes Merkmal des Datenverkehrs selektiv zu untersuchen
- Pakete mit Scapy gestalten
- Mithilfe von NetFlow/IPFIX-Tools Anomalien und potenzielle Bedrohungen im Netzwerkverhalten finden
- Anhand Ihrer Kenntnisse der Netzwerkarchitektur und -hardware die Platzierung von Netzwerk-Überwachungssensoren anpassen und den Datenverkehr „off the wire“ mit Sniffern untersuchen

Zielgruppe

- Netzwerküberwachungs-, System-, SOC- und Sicherheitsanalysten
- Netzwerkingenieure/-administratoren
- Sicherheitsmanager in praktischen Rollen

Berufliche Rollen im NICE Framework

- Cyber Defense Analyst (OPM 511)

David Hoelzer
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Erkennen, analysieren, schützen: Proaktive Netzwerk-Bedrohungsdetektion meistern

SEC503 ist eine der wichtigsten Schulungen, die Sie in Ihrer Karriere auf dem Gebiet der Informationssicherheit absolvieren werden. Dem Feedback vergangener Teilnehmer nach zu urteilen, ist der Kurs besonders schwierig, aber auch besonders lohnend. Wenn Sie in der Lage sein möchten, effektives Threat Hunting durchzuführen, um Zero-Day-Aktivitäten in Ihrem Netzwerk zu finden, bevor sie öffentlich bekannt werden, ist dieser Kurs genau richtig für Sie. SEC503 beschäftigt sich nicht mit den Alarmmeldungen, die von Standard-Überwachungstools generiert werden. Vielmehr wendet sich die Schulung an alle, die wirklich verstehen möchten, was heute in ihrem Netzwerk vor sich geht, und die den Verdacht haben, dass wichtige Dinge passieren, die durch ihre Tools nicht aufgedeckt werden.

SEC503 zeichnet sich dadurch aus, dass Netzwerküberwachung und Netzwerkforensik ausgehend von den Grundlagen gelehrt werden, was auf natürliche Weise zu effektivem Threat Hunting führt. Anstatt mit einem Tool zu beginnen und zu erläutern, wie dieses Tool in verschiedenen Situationen genutzt wird, erklärt Ihnen dieser Kurs das Wie und Warum hinter der Funktionsweise von TCP/IP-Protokollen. Nachdem in den ersten zwei Teilen „Pakete als Zweitsprache“ untersucht wurden, beschäftigen wir uns mit verbreiteten Anwendungsprotokollen und einem allgemeinen Ansatz für Recherche und Verständnis neuer Protokolle. Während der gesamten Diskussion werden die vermittelten Kenntnisse direkt angewendet, um sowohl Zero-Day-Bedrohungen als auch bekannte Gefahren zu identifizieren.

Geschäftsorientierte Lernergebnisse

- Vermeiden, dass Ihre Organisation in die Schlagzeilen gerät
- Die Detektion in herkömmlichen, hybriden und Cloud-Netzwerkumgebungen augmentieren
- Die Bedrohung bei Netzwerkaktivitäten effizienter modellieren
- Die Verweilzeit der Angreifer verkürzen

Zusammenfassung der Kursinhalte

TEIL 1: Netzwerküberwachung und -analyse: Teil I
TEIL 2: Netzwerküberwachung und -analyse: Teil II
TEIL 3: Signaturbasierte Bedrohungsdetektion und Reaktion
TEIL 4: Systeme zur Zero-Day-Bedrohungsdetektion aufbauen
TEIL 5: Bedrohungsdetektion, Forensik und Analyse in großem Stil
TEIL 6: Erweiterte Netzwerküberwachung und Abschlussübung zur Bedrohungsdetektion

„Ich brachte einen fundierten Hintergrund in Host-Forensik und begrenzte Kenntnisse in Netzwerkanalyse und -forensik mit. SEC503 hat eine Menge von Kenntnislücken geschlossen, die sich durch meine ganze Karriere zogen.“

– Jared H., **US-amerikanisches Militär**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC503**

KURSFORMATE SEC503

Präsenzkurs | **Live online** | **OnDemand**

SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring™ GRUNDLEGEND ÜBERARBEITET

GMON Continuous Monitoring giac.org/gmon — DoD 8140*

6	46	23
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Umfassende Bewertungen des aktuellen Status durchführen, um moderne Verteidigungsmaßnahmen zu konstruieren und zu priorisieren
- Verteidigungsrahmen anwenden, die sich an den Bedrohungen orientieren, z. B. MITRE ATT&CK und Zero-Trust
- Threat Hunting mithilfe von erweiterten Techniken und Tools durchführen
- Für Transparenz in der gesamten modernen, hybriden, dezentralen Infrastruktur sorgen
- Eine moderne Umgebung mit Domänennamensystem und Transport-Layer-Sicherheitsverschlüsselung navigieren, um Schutz, Detektion und Datenschutz gegeneinander abzuwägen
- Den Stack und die Tools für Cloud-Sicherheit verstehen, u. a. Cloud-native Anwendungsschutzplattform, Cloud-Sicherheitsstatusmanagement, Cloud-Infrastruktur-Berechtigungsmanagement und Cloud-Workload-Schutzplattform für robusten Cloud-Schutz
- Anwendungskontrolle und EPP für die Endpunktsicherheit implementieren
- KI-/LLM-Anwendungen verteidigen und die KI-/Software-Lieferkette sichern

Zielgruppe

- Sicherheitsarchitekten
- Leitende Sicherheitsingenieure
- Technische Sicherheitsmanager
- Analysten, Ingenieure und Manager im Security Operations Center
- Analysten für Computernetzwerk-Verteidigung
- Alle, die an der Implementierung folgender Aspekte arbeiten: kontinuierliche Diagnose und Schadensminderung, kontinuierliche Sicherheitsüberwachung oder Netzwerk-Sicherheitsüberwachung

Berufliche Rollen im NICE Framework

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

Eric Conrad
Kursautor

Seth Misenar
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Überwachen, erkennen, schützen: Erweiterte Bedrohungsdetektion für Cloud, Netzwerk und Endpunkte

Im schnellen Wandel der Bedrohungslandschaft von heute reichen herkömmliche Maßnahmen für Cybersicherheit nicht mehr aus. Diese fortgeschrittene Schulung nimmt sich der Herausforderung an, indem sie die Teilnehmer mit topaktuellen Kompetenzen in Cybersicherheits-Engineering und erweiterter Bedrohungsdetektion für Cloud-, Netzwerk- und Endpunkt-Umgebungen ausstattet. Mit 18 praktischen Laborübungen, einem Abschlussprojekt und gamifizierten Bootcamp-Aufgaben tauchen Sie ein in Szenarien aus der wirklichen Welt. Meistern Sie NDR, EDR und MITRE ATT&CK und bauen Sie ein robustes SOC mit Verteidigungsmaßnahmen auf, die sich an den Bedrohungen orientieren. Sammeln Sie in diesem umfassenden Kurs mehr Know-how und bleiben Sie Ihren Gegnern einen Schritt voraus.

Geschäftsorientierte Lernergebnisse

Dieser Kurs hilft Ihrer Organisation:

- Effektive Schutz- und Detektionsstrategien für Cloud, Netzwerk und Endpunkte zu ermöglichen
- Sicherheitsarchitektur und -betrieb für moderne hybride Unternehmen verteidigungsfähig zu konzipieren
- Die Fähigkeiten Ihrer Organisation für den Sicherheitsbetrieb wesentlich zu verbessern
- Schutz- und Detektionslücken in der gesamten hybriden Infrastruktur zu identifizieren
- Die Fähigkeiten der aktuellen Infrastruktur und Assets zu maximieren
- Daten zu verstehen, um eine schnelle Detektion potenzieller Intrusionen oder unbefugter Aktionen zu ermöglichen

Zusammenfassung der Kursinhalte

TEIL 1: Verteidigung, die sich an den Bedrohungen orientiert: Frameworks, Threat Hunting und Bewertung des aktuellen Status

TEIL 2: Cloud, Edge und Netzwerk: Transparenz und Schutz

TEIL 3: Threat Hunting mit NDR (Network Detection and Response)

TEIL 4: Sicherheit in hybriden Unternehmen: Schutz und Detektion für Benutzer und Endpunkte

TEIL 5: Verteidigung von GenAI-Anwendungen, Automatisierung, Schutz der Lieferkette und SOC

TEIL 6: Abschlussübung: Design, Detektion, Defensive

„Die Laborübungen bei SEC511 vermittelten entscheidende praktische Erfahrung und halfen, die theoretischen Konzepte zu festigen."

– Olivia M., **BAH**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC511**

KURSFORMATE SEC511

Präsenzkurs | **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	36	19
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Eine Sicherheitsarchitektur auf Mängel analysieren
- Daten, Anwendungen, Assets und Dienste entdecken und den Compliance-Status beurteilen
- Technologien für bessere Präventions-, Detektions- und Reaktionsfähigkeiten implementieren
- Defizite in Sicherheitslösungen erfassen und verstehen, wie sie getunt und betrieben werden
- Verstehen, was es mit sich bringt, alles zu verschlüsseln
- Anhand der im Kurs erlernten Prinzipien eine verteidigungsfähige Sicherheitsarchitektur entwerfen
- Den angemessenen Bedarf an Sicherheitsüberwachung für Unternehmen aller Größen ermitteln
- Bestehende Investitionen in Sicherheitsarchitektur optimal nutzen, indem bestehende Technologien neu konfiguriert werden
- Feststellen, welche Fähigkeiten benötigt werden, um eine kontinuierliche Überwachung kritischer Sicherheitskontrollmaßnahmen zu unterstützen
- Ordnungsgemäße Protokollierung und Überwachung konfigurieren, um ein SOC und ein kontinuierliches Überwachungsprogramm zu unterstützen

Zielgruppe

- Sicherheitsarchitekten
- Netzwerkingenieure
- Netzwerkarchitekten
- Sicherheitsanalysten
- Leitende Sicherheitsingenieure
- Systemadministratoren
- Technische Sicherheitsmanager
- CND-Analysten
- Fachkräfte für Sicherheitsüberwachung
- Cyberrisiko-Ermittler

Berufliche Rollen im NICE Framework

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

Ismael Valenzuela
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Sicher per Design: Zero Trust für moderne hybride Netzwerke

Dieser Kurs soll Ihnen helfen, eine wirklich verteidigungsfähige Sicherheitsarchitektur aufzubauen und aufrechtzuerhalten, indem Sie die Prinzipien, Stützpfeiler und Fähigkeiten von Zero Trust implementieren, mit einem starken Fokus auf der Nutzung aktueller Infrastrukturen und Investitionen. Sie lernen, wie Sie bestehende Technologien beurteilen, neu konfigurieren und validieren, um die Präventions-, Detektions- und Reaktionsfähigkeiten ihrer Organisation erheblich zu verbessern, die Transparenz zu erhöhen, die Angriffsfläche zu verringern und sogar auf innovative Weise Angriffe vorauszuahnen. Der Kurs geht auch auf einige der neuesten Technologien und ihre Fähigkeiten, Stärken und Schwächen ein. Sie nehmen Empfehlungen und Vorschläge mit nach Hause, die Ihnen helfen, eine robuste Sicherheitsinfrastruktur Layer für Layer über hybride Umgebungen hinweg aufzubauen, während Sie sich in Richtung Zero Trust bewegen.

Geschäftsorientierte Lernergebnisse

- Mängel in Sicherheitslösungen identifizieren und begreifen
- Zero-Trust-Strategien entwerfen und implementieren, die aktuelle Technologien und Investitionen ausnutzen
- Bestehende Investitionen in die Sicherheitsarchitektur optimal nutzen, indem bestehende Technologien neu konfiguriert werden
- Verteidigungsmaßnahmen in Layern anordnen, um sowohl die Schutzzeit als auch die Wahrscheinlichkeit der Detektion zu erhöhen
- Präventions-, Detektions- und Reaktionsfähigkeiten verbessern
- Die Angriffsfläche reduzieren

Zusammenfassung der Kursinhalte

TEIL 1: Verteidigungsfähige Sicherheitsarchitektur und -technik: Hin zu Zero Trust

TEIL 2: Netzwerk-Sicherheitsarchitektur und -technik

TEIL 3: Netzwerkzentrische Architektur für Anwendungssicherheit

TEIL 4: Datenzentrische Architektur für Anwendungssicherheit

TEIL 5: Zero-Trust-Architektur: Gegner stellen, die bereits in unseren Netzwerken sind

TEIL 6: Praktische „Secure-the-Flag"-Übung

„Diese Schulung zeigte, wie der Sicherheitsstatus einer Organisation insgesamt verbessert werden kann. Sie hilft, Verbindungen zwischen verschiedenen Bereichen innerhalb der Sicherheitsinfrastruktur knüpfen."

– Farruk Ali, **UPS**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC530**

KURSFORMATE SEC530

Präsenzkurs | **Live online** | **OnDemand**

KURS NEU IM FOKUS

SEC547: **Defending Product Supply Chains™**

3	18	13
Kurstage	CPEs	Laborübungen

Vermittelte Kompetenzen

- SBOMs aus Quellcode erstellen
- Attestation-Pipelines erstellen
- Verstehen, wie Schwachstellen veröffentlicht werden
- Lernen, wie anfällige Komponenten validiert werden
- Gefälschte Komponenten identifizieren
- Ein Sicherheitsprogramm für die Lieferkette schaffen
- Verstehen, wie ausländische Gegner Lieferketten manipulieren
- Open-Source-Tools für die Lieferkettensicherheit nutzen lernen
- In Zusammenarbeit mit Entwicklern Sicherheit in Ihren Produktentwicklungsprozess integrieren
- Effektiver auf Bedrohungen der Lieferkette reagieren
- Effektive Techniken zur Reaktion auf die nächste große Schwachstelle in der Lieferkette erlernen

Zielgruppe

- Fachkräfte für das Risikomanagement in der Lieferkette
- Teams für Produktsicherheit und PSIRT
- Anlageneigentümer und -betreiber, die für die Sicherheit zuständig sind
- Sicherheitsanalysten und Incident Responder
- Leitende Sicherheitsbeschäftigte, die für die Produktsicherheit zuständig sind

Berufliche Rollen im NICE Framework

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

Tony Turner
Kursautor

Vom Procurement zum Produkt: Sicherung der gesamten Lieferkette

Die Bedrohungslandschaft hat sich geändert. Heutzutage reicht es nicht mehr, einen starken Perimeter zu errichten, um Gegner fernzuhalten. Angriffe in der Lieferkette sind einer der vielen effektiven Wege, herkömmliche, perimeterbasierte Kontrollmaßnahmen zu umgehen. Bei diesen schwierig zu erkennenden Attacken gewähren Unternehmen dem Gegner unbeabsichtigterweise Zugang, indem sie angeblich „vertrauenswürdige" Technologien verwenden, die jedoch nicht validiert sind. SEC547: Defending Product Supply Chains™ vermittelt den Teilnehmern, wie sie das Risiko von Lieferkettenangriffen durch eingehende Strategien und Taktiken zum Risikomanagement in der Lieferkette auf ein Minimum beschränken. Der Kurs deckt die gesamte Bedrohungslandschaft ab. Er lehrt in 13 maßgeschneiderten Laborübungen entscheidende Kompetenzen für Verteidiger und erläutert anhand von realen Beispielen, wie diese Angriffe funktionieren und wie Sie verhindern können, dass Ihr Unternehmen ihnen zum Opfer fällt. Sie verlassen diesen Kurs mit bewährten Branchenpraktiken zur Sicherung der Technologieakquisitionen Ihrer Organisation.

Geschäftsorientierte Lernergebnisse

- Die Resilienz Ihrer Organisation angesichts von Bedrohungen erhöhen
- Die Kosten Ihres Sicherheitsprogramms durch Risikosenkung verringern
- Bewertungen von Anbieter- und Produktlieferketten durchführen
- Die Auswirkungen von Lieferkettenangriffen auf Ihre Organisation reduzieren
- Risiken innerhalb Ihres Lieferkettenprogramms priorisieren
- Zugriff auf sensibles geistiges Eigentum identifizieren
- Risiken einer fremden Präsenz in Ihrer Lieferkette identifizieren
- Das Thema Sicherheit in der Lieferkette mit Stakeholdern zur Sprache bringen

Zusammenfassung der Kursinhalte

TEIL 1: Anbieter und Produkte

TEIL 2: HBOM und SBOM

TEIL 3: Softwaretransparenz und -reaktion

„Dieser [Kurs] hat mir geholfen, wichtige Faktoren und Verfahren sowie relevante Tools und Leitlinien zu identifizieren, mit denen ich eine strategisch ausgerichtete, effiziente und doch systematische Methode zur Lösung der Probleme im Lieferkettenprozess entwickeln kann."

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

„Der Kurs hat mir gut gefallen. [Er ist] voll von nützlichen Informationen, die ich in meine internen Projekte aufnehmen werde!"

– Rossano Ferraris, **Accenture**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC547**

KURSFORMATE SEC547

Live online **OnDemand**

SEC555: Detection Engineering and SIEM Analytics™

GCDA
Detection Analyst
giac.org/gcda

5	30	18
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Ein Detektionslabor aufbauen
- Regeln für die Gegnerdetektion erstellen
- Die SIEM-Architektur optimieren
- Tools zur Gegneremulation nutzen, damit Sie zugehörige Aktivitätsprotokolle prüfen können
- Anhand von Protokolldaten effektive Sicherheitskontrollmaßnahmen einrichten
- Die Handhabung und Filterung großer Datenmengen, die von verschiedenen Geräten generiert werden, vereinfachen
- Einblicke in On-Premise- und Cloud-SIEM-Tools und Protokollquellen gewinnen
- Kenntnisse von MITRE ATT&CK erlangen und lernen, wie die aufgedeckten Fakten spezifischen Taktiken und Techniken zugeordnet werden können
- Detektionsfähigkeiten über zahlreiche Datenquellen hinweg aufzeichnen und überwachen
- Verstehen, wie SOAR-Optimierung Detection Engineering erheblich verbessern und die Reaktionszeit verkürzen kann
- Eine Ausgangsbasis aufstellen, Trends identifizieren und Ausreißer entdecken, die auf Gegneraktivität hinweisen

Zielgruppe

- Detektionsingenieure
- Detektionsanalysten
- Sicherheitsanalysten
- Sicherheitsingenieure
- Threat Hunter
- Incident Handler/Responder
- Sicherheitsarchitekten
- Fachkräfte für Sicherheitsüberwachung
- Cyberrisiko-Ermittler
- Penetrationstester

Berufliche Rollen im NICE Framework

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

Nick Mitropoulos
Kursautor

Meistern Sie die Kunst der Cyberverteidigung mit Detection Engineering und SIEM-Analyse

In einer Welt, in der Cyberbedrohungen immer raffinierter werden, brauchen Organisationen kompetente Verteidiger, die stets einen Schritt voraus sind. Dieser Kurs ist Ihr Einstieg in das Detection Engineering – die Kunst, proaktive Verteidigungsmaßnahmen zu schaffen – und SIEM, den Kern der modernen Bedrohungsdetektion und -reaktion. Ob Sie ein Sicherheitsanalyst sind, der seine Kenntnisse verbessern möchte, oder eine neue Stelle als Detektionsanalyst antreten: Hier gewinnen Sie praktisches Know-how, wie Sie Angriffe erkennen und untersuchen. SEC555™ vermittelt den Teilnehmern Kenntnisse, Methoden und Prozesse zur Verbesserung bestehender Protokollierungslösungen und fördert die Erstellung von sinnvollen Detektionsregeln, die eine proaktive Überwachung ermöglichen.

Geschäftsorientierte Lernergebnisse

- Geschäftliche Risiken reduzieren, indem Bedrohungen fast in Echtzeit identifiziert und gemindert werden
- Einen Prozess zur ordentlichen Bewertung von Anbietern aufstellen, damit geeignete Sicherheitspartner gewählt werden
- Bedrohungen basierend auf den potenziellen Auswirkungen auf das Unternehmen und die Kritikalität der Assets priorisieren
- Eine effektive Asset-Datenbank kompilieren, die bei der Überwachung kritischer Assets hilft
- Verstehen, wie Detection Engineering mit den breiteren Zielen der Organisation zusammenhängt. z. B. regulatorische Compliance und betriebliche Effizienz
- Einblicke in die Bedeutung einer präzisen Detektion gewinnen, um Alarmermüdung und betriebliche Ineffizienzen zu vermeiden
- Erkunden, wie Detection Engineering die abteilungsübergreifende Zusammenarbeit mit Teams wie IT, Sicherheit und Compliance unterstützt
- Risiken bewerten und effektiv managen, indem Detektionsdaten für fundierte Entscheidungen zu geschäftskritischen Fragen genutzt werden
- Eine Strategie ergreifen, die Systemskalierbarkeit fördert

Zusammenfassung der Kursinhalte

TEIL 1: Detection Engineering und SIEM-Architektur

TEIL 2: Netzwerk- und Endpunktanalyse

TEIL 3: Asset-Erkennung, Ausgangsbasen und UEBA

TEIL 4: Cloud-Protokollierung und -Überwachung

TEIL 5: Alarm- und Detektions-Technikpipelines

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC555**

KURSFORMATE SEC555

Präsenzkurs **Live online**

SEC573: Automating Information Security with Python™

GPYC Python Coder
giac.org/gpyc

6	36	Über 128
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Routineaufgaben mithilfe von Python schnell und effizient durchführen
- Protokoll- und Paketanalyse mit Dateioperationen, regulären Ausdrücken und Analysemodulen zur Aufspürung schädlichen Codes automatisieren
- Forensik-Tools entwickeln, die Binärdaten bergen und neue Artefakte extrahieren
- Daten aus Datenbanken und der Windows-Registry lesen
- Mit Websites interagieren, um Informationen zu sammeln
- UDP- und TCP-Client- und -Serveranwendungen entwickeln
- Systemprozesse automatisieren und ihre Ausgaben verarbeiten

Zielgruppe

- Sicherheitsfachkräfte, die von der Automatisierung von Routineaufgaben profitieren, da sie sich auf das Wesentliche konzentrieren können
- Forensikanalysten, die nicht mehr darauf warten müssen, dass jemand anderes ein kommerzielles Tool zur Artefaktanalyse entwickelt
- Netzwerkverteidiger, die sich durch Berge von Protokollen und Paketen arbeiten müssen, um die Gegner in ihren Netzwerken zu finden
- Penetrationstester, die bereit sind, sich vom Skriptneuling zur professionellen offensiven Computerbetriebsfachkraft zu entwickeln
- Sicherheitsfachkräfte, die sich vom Benutzer von Sicherheitstools zum Lösungsanbieter entwickeln möchten

Berufliche Rollen im NICE Framework

- 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
Kursautor

Vielseitig, wiederholbar, effizient: Mit Python automatisierte Sicherheitsaufgaben

Die Herausforderungen, denen sich Sicherheitsfachkräfte stellen müssen, entwickeln sich ständig weiter. Personal, das Technologieprobleme verstehen und schnell eine Lösung entwickeln kann, ist deshalb immer gefragt. Wenn Sie darauf warten müssen, dass ein Anbieter ein Tool zur Bergung von Forensikartefakten oder einen Patch oder ein Exploit für eine neue Schwachstelle entwickelt, sind Sie stets im Rückstand. Für Arbeitgeber, die Informationssicherheit ernst nehmen, ist die Fähigkeit, rasch ihre eigenen Tools zu entwickeln, unabdingbar. Dieser Kurs vermittelt Ihnen die nötigen Kompetenzen zur Lösungsentwicklung, damit Ihre Organisation ebenso schnell operieren kann wie ihre Gegner. SEC573™ ist ein immersiver, praktischer Kurs für Ihr individuelles Lerntempo mit zahlreichen Laborübungen. Nachdem die Grundlagen für Teilnehmer, die noch nie programmiert haben, abgedeckt wurden, präsentiert der Kurs Forensik-, Defensiv- und Offensivaufgaben aus der wirklichen Welt. Sie entwickeln einen Malware-Dropper für eine Offensivoperation, lernen, wie Sie Ihre Protokolle nach den neuesten Angriffen durchsuchen, entwickeln Code, um Forensikartefakte aus Arbeitsspeicher, Festplatten und Paketen zu bergen, automatisieren die Interaktion mit der API einer Online-Website und schreiben einen angepassten Paket-Sniffer. In ansprechenden und interessanten Laborübungen entwickeln Sie nützliche Tools und erlernen grundlegende Kompetenzen, mit denen Sie zu einem der wertvollsten Mitglieder Ihres Informationssicherheitsteams werden.

Geschäftsorientierte Lernergebnisse

Dieser Kurs hilft Ihrer Organisation:

- Systemprozesse zu automatisieren und ihre Eingaben schnell und effizient zu verarbeiten
- Programme zu erstellen, die Effizienz und Produktivität erhöhen
- Tools zu entwickeln, die unverzichtbare Verteidigungsmaßnahmen für die Anforderungen unserer Organisationen bereitstellen

Zusammenfassung der Kursinhalte

TEIL 1: Grundlagen-Workshop mit pyWars
TEIL 2: Grundlagen-Workshop mit WEITEREN pyWars
TEIL 3: Python für die Defensive
TEIL 4: Python für Forensik
TEIL 5: Python für die Offensive
TEIL 6: „Capture-the-Flag"-Übung

„Python ist ein Muss in der Welt von InfoSec, und SEC573 hat mir mehr Python-Kompetenzen vermittelt."

– Ben Weber, **Raymond James**

„Sehr gut konzipiert. Seit Jahren fürchte ich mich davor, Programmieren lernen zu müssen. Nach den ersten paar Tagen war die Furcht verflogen."

– Blake Thompson, **Merrick Bank**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC573**

KURSFORMATE SEC573

Präsenzkurs | **Live online** | **OnDemand**

SEC587: Advanced Open-Source Intelligence (OSINT) Gathering and Analysis™ GRUNDLEGEND ÜBERARBEITET

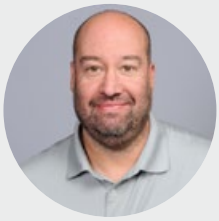
6	36	20
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Öffentliche Daten erfassen und analysieren, um mit erweiterten OSINT-Tools und -Techniken umsetzbare Informationen zu generieren
- Den OSINT-Prozess mithilfe von automatisierten Systemen optimieren und dadurch Effizienz und Korrektheit bei der Informationssammlung erhöhen
- Sicherheitsbedrohungen identifizieren und mindern, indem OSINT korrekt angewendet wird, um potenzielle Schwachstellen vorherzusagen und zu verhindern
- Rechtliche und ethische Erwägungen bei der Informationssammlung berücksichtigen, um die Einhaltung anwendbarer Gesetze und Standards sicherzustellen
- OSINT als Wettbewerbsvorteil nutzen, indem Markt- und Branchentrends überwacht und analysiert werden und in die Unternehmensstrategie einfließen
- Prozesse zur Entscheidungsfällung mit datengesteuerten Einblicken in Echtzeit aus einer Fülle offener und öffentlich zugänglicher Quellen verbessern
- Technologische Lösungen implementieren, um große Datenmengen aus verschiedenen Quellen effektiv zu verwalten und zu analysieren, was besser fundierte Geschäftsentscheidungen fördert

Zielgruppe

- OSINT-Analysten und Analysten für alle Quellen
- Ermittler bei Strafverfolgungsbehörden
- Ermittler beim Militär
- Private Ermittler
- Ermittler bei Versicherungen
- Informationsanalysten
- Geopolitische Analysten
- Journalisten
- Forscher
- Social Engineers
- Rechercheure für politische Kampagnen und Informationskampagnen
- Incident Responder
- DFIR-Analysten (Digitalforensik)
- Fachkräfte für Informationen zu Cyberbedrohungen



Matt Edmondson
Kursautor

Jenseits der Grundlagen: Erweiterte OSINT-Techniken

Da OSINT (Open-Source Intelligence) der Motor hinter den meisten großen Ermittlungen in diesem digitalen Zeitalter ist, besteht ein unmittelbarer Bedarf nach einem fortgeschrittenen Kurs. Bei fast allen OSINT-Untersuchungen wird es zunehmend komplexer, die Daten zu sammeln, auszunutzen und zu analysieren. OSINT-Fachkräfte weltweit müssen umfangreiche OSINT durchführen und benötigen Mittel und Methoden, um die Zuverlässigkeit ihrer Analyse zu prüfen und fundierte und unvoreingenommene Berichte zu erstellen. Bei SEC587™ erfahren Sie, wie Sie eine erweiterte OSINT-Erfassung und -Analyse durchführen, und lernen verbreitete Programmiersprachen wie JSON und Python verstehen und verwenden. SEC587™ geht außerdem auf Themen im Bereich Dark Web und Finanzen (Kryptowährung) ein, sowie auf Desinformation und erweiterte Bild- und Video-OSINT-Analyse. Dieser fortgeschrittene Kurs vermittelt erfahrenen OSINT-Ermittlern in schnellem Tempo neue Techniken und Methodiken. Für OSINT-Analysten auf Einsteigerniveau vertieft er, wie sie Datenquellen aus der ganzen Welt finden, erfassen und analysieren.

Geschäftsorientierte Lernergebnisse

- Entscheidungsfällung durch umsetzbare Einblicke aus öffentlichen Daten verbessern
- Risiken proaktiv mithilfe erweiterter OSINT-Techniken identifizieren
- Effizienz durch automatisierte Informationssammlung erhöhen
- Durch Überwachung von Branchen- und Markttrends einen Wettbewerbsvorteil gewinnen
- Durch legale und ethische Informationssammlung für Compliance sorgen

Zusammenfassung der Kursinhalte

TEIL 1: Desinformation, Informationsanalyse, OSINT für Russland und China

TEIL 2: Python für OSINT

TEIL 3: Video-, Bild- und Audio-Analyse, KI für OSINT, erweiterte Enumeration und Gaming

TEIL 4: Sock Puppets, OPSEC, Dark Web, Kryptowährung und Wireless

TEIL 5: Automatisierte Überwachung, Fahrzeugverfolgung und Umgang mit passwortgeschützten Dateien

TEIL 6: Abschlussübung

„Ein breiter Überblick über mehrere Bereiche von OSINT ist wirklich hilfreich, um die Grundlagen zu festigen und zu verstehen, auf welch verschiedene Weisen die Kompetenzen eines Open-Source-Ermittlers Anwendung finden können.“

– Dan Black

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC587**

KURSFORMATE SEC587

Präsenzkurs **Live online** **OnDemand**

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

GMLE
Machine Learning Engineer
giac.org/gmle

6	36	30
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Statistische Modelle sinnvoll auf Probleme der wirklichen Welt anwenden
- Visualisierungen Ihrer Daten erzeugen
- Bedrohungen in Ihrem Netzwerk auf mathematischer Basis aufspüren
- Vorliegende Daten in Repräsentierungen umwandeln, auf die ML-/KI-Techniken angewendet werden können
- Unbeaufsichtigte Lern-/Cluster-Methoden verstehen und anwenden
- Neuronale „Deep Learning"-Netzwerke aufbauen
- Konvolutionale neuronale Netzwerke aufbauen und verstehen
- Verstehen, wie repräsentative synthetische Daten aufgebaut werden
- Genetische Suchalgorithmen verstehen und aufbauen
- Die Grundlagen containerisierter Bereitstellung verstehen

Zielgruppe

- InfoSec-Fachkräfte, die Maschinenlernen verstehen möchten
- Fachkräfte, die Prinzipien der Data Science auf Probleme der wirklichen Welt anwenden möchten
- Alle, die die Grundlagen erlernt haben, aber ihr Problem nicht so darstellen können, dass es sich durch Maschinenlernen lösen lässt
- Blue-Team- und SOC-Mitglieder, die Anomalien identifizieren und Bedrohungen flexibel aufspüren möchten

Berufliche Rollen im NICE Framework

- Data Analyst (OPM 422)

David Hoelzer
Kursautor

Data Science und KI für Cybersicherheit: erweiterte Lösungen zum Threat Hunting

SEC595™ ist ein Crashkurs, der die Teilnehmer in praktische Data Science, Statistik, Wahrscheinlichkeitsrechnung, Maschinenlernen und KI einführt. Die Kursstruktur besteht aus einer Reihe kurzer Diskussionen mit ausgiebigen praxisnahen Laborübungen, bei denen die Teilnehmer ein praktisches und intuitives Verständnis dafür entwickeln, wie diese Konzepte zusammenhängen und zur Lösung realer Probleme herangezogen werden können. Die beste Analogie wäre eine Lehre, die Sie in KI und verwandten Feldern vom Neuling zur Gesellenprüfung bringt. Wenn Sie noch nie etwas mit Data Science oder Maschinenlernen zu tun hatten, aber diese KI-Techniken einsetzen möchten, ist dies der richtige Kurs für Sie!

Geschäftsorientierte Lernergebnisse

- Nützliche Visualisierungs-Dashboards generieren
- Probleme mit neuronalen Netzwerken lösen
- Effektivität, Effizienz und Erfolg von Cybersicherheitsinitiativen verbessern
- Angepasste Maschinenlernlösungen für die spezifischen Bedürfnisse Ihrer Organisation erstellen
- Sich auf die GMLE-Zertifizierung vorbereiten

Zusammenfassung der Kursinhalte

TEIL 1: Datenakquisition, -säuberung und -manipulation

TEIL 2: Datenexploration und -statistiken

TEIL 3: Grundlagen des Maschinenlernens: Trees, Forests und K-Means

TEIL 4: Grundlagen des Maschinenlernens: Deep Learning

TEIL 5: Grundlagen des Maschinenlernens: Autoencoder

TEIL 6: Grundlagen des Maschinenlernens: Funktionale Modelle und Bereitstellung

„Es mangelt noch am Verständnis von KI/ML für Cybersicherheit und sie werden oft falsch dargestellt. Dieser Kurs bietet einen Ausgleich zwischen dem, was das Management wissen muss, um das Verständnis der Technologien zu fördern, und praktischer Erfahrung."

– Thomas L., **US-amerikanisches Militär**

„Besonders gefällt mir, dass der Kurs auf Erfahrungen basiert, nicht auf einem Lehrbuch. Die Anekdoten über den Hintergrund der verschiedenen Themen haben mir sehr geholfen, alles zueinander in Beziehung zu setzen."

– Brian Morris, **Stadt Austin**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC595**

KURSFORMATE SEC595

Präsenzkurs | **Live online** | **OnDemand**

KURS NEU IM FOKUS

SEC673: Advanced Information Security Automation with Python™

6	36	27
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Pakete durch PIP (Paket-Installationsprogramm für Python) installierbar machen, damit sie leichter verteilt und aktualisiert werden können
- Eine angepasste Datenstruktur für Ihre Anwendung erstellen, damit sie schneller entwickelt werden kann
- Den Code mit erweiterten Funktionen wie Decorators, Generatoren und Kontextmanagern vereinfachen
- Programme mit Multi-Threading und Multi-Processing beschleunigen
- Fehlerkaskaden durch Einführung von Einheitstests ausmerzen, damit sich kleine Änderungen nicht zu großen Fehlern auswachsen
- Angemessene Protokolle in Python erstellen und sie korrekt handhaben, um Fehler zu identifizieren, die sich aus persönlichen Eigenarten bei der Arbeitsweise ergeben
- Anwendungsautomatisierung und -interaktion implementieren, damit Sie Zeit für wichtigere Aufgaben haben

Zielgruppe

- Sicherheitsfachkräfte, die in Python programmieren können und bereit sind, ihre Codekompetenzen einen Schritt weiter zu entwickeln
- Toolentwickler, die in der Lage sein möchten, installierbare und bedienungsfreundliche Python-Pakete zu veröffentlichen
- Netzwerkverteidiger, die in der Lage sein möchten, die Fähigkeiten verbreiteter Python-Pakete zu erweitern, um neue Detektionsfähigkeiten zu erstellen
- Sicherheitsfachkräfte, deren Tools mithilfe von Multi-Processing und Multi-Threading schneller ausgeführt werden müssen

Mark Baggett
Kursautor

Skalierbar, zuverlässig, optimiert: Erweiterte Sicherheitsautomatisierung mit Python

Wenn das Sicherheitsteam ein Problem hat, das es nicht lösen kann, kommt es zu Ihnen. Sie können programmieren und Sie können Tools entwickeln, die Lücken in der bestehenden Technologie schließen. Aber ein annehmbares Skript zu schreiben ist eine Sache, den Code angemessen zu pflegen schon schwieriger. Jede neue Funktion scheint wie eine komplette Neuüberarbeitung. Ihr Code muss schneller ausgeführt und die Workload über mehrere Threads oder sogar mehrere Prozessoren verteilt werden können. Wenn ein Benutzer einen Fehler erhält, müssen Sie raten, was schief gegangen ist, weil Ihre Anwendung keine ausreichende Protokollierung zur Verfügung stellt. Sie wünschen, dass Ihre Anwendungen so funktionsstark, wartungs- und bedienungsfreundlich wären wie die beliebtesten Open-Source-Projekte für die Cybersicherheit. Sie machen sich Sorgen, dass Sie ein Programm mit Sicherheitsschwachstellen entwickeln. Oder sollten sich vielleicht Sorgen darüber machen. Eines ist klar: Sie sind bereit, Ihre Programmierkompetenzen auf ein höheres Niveau anzuheben. SEC673™ ist der Kurs für Sie!

SEC673™ ist der logische Folgekurs für Teilnehmer, die SEC573: Automating Information Security with Python,™ abgeschlossen haben oder die bereits mit den grundlegenden Konzepten der Python-Programmierung vertraut sind. Der Kurs behandelt von Anfang an fortgeschrittene Konzepte. Er geht auf Codierungstechniken ein, die von beliebten Open-Source-Paketen für Informationssicherheit genutzt werden, und erläutert, wie sie auf Ihre eigenen Python-Cybersicherheitsprojekte angewendet werden können. Wir lernen aus den besten von ihnen und verbringen die Woche damit, die Informationssicherheit für unser Projekt namens SPF100 so entwicklungs- und wartungsfreundlich zu machen wie die beliebtesten Cybersicherheitsprojekte. Sie lernen, wie Sie Ihren Code organisieren und ihn mithilfe von erweiterten Programmierungskonzepten schneller, effizienter und wartungsfreundlicher gestalten.

Zusammenfassung der Kursinhalte

TEIL 1: Grundlagen von Python-Paketen

TEIL 2: Python-Objekte

TEIL 3: Python-Objekte (Fortsetzung)

TEIL 4: Erweiterte Konzepte

TEIL 5: Erweiterte Konzepte (Fortsetzung)

TEIL 6: „Capture-the-Flag“-Übung

„Der Inhalt [von SEC673] ist wirklich gut! Mir gefällt, dass beim Erlernen von Python Optimierung und Effizienz betont werden. Das hebt den Kurs auf ein höheres Niveau.“

– Samuel Cosentino, CISCO

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC673**

KURSFORMATE SEC673

Präsenzkurs | **Live online** | **OnDemand**

FOKUSBEREICH IM SANS-LEHRPLAN

Führungskompetenzen in Cybersicherheit

Die Bedrohungslandschaft entwickelt sich immer weiter, und damit wird auch Cybersicherheit für Organisationen immer wertvoller. Moderne Führungskräfte verstehen, wie wichtig es ist, hochwertige Informations-Assets zu sichern, und welche erheblichen Risiken mit einer Datenschutzverletzung oder einem Angriff verknüpft sind.

Organisationen brauchen Leiter und Manager auf dem Gebiet der Cybersicherheit, die technische Kenntnisse mit unverzichtbaren Führungskompetenzen kombinieren, damit sie Projekte, Teams und Initiativen effektiv leiten und gleichzeitig die Unternehmensziele fördern können.

Der Fokusbereich für Führungskompetenzen in Cybersecurity bietet anwendbare und praktische Ansätze für den Umgang mit Cyberrisiken. Diese Serie praktischer, interaktiver Kurse hilft derzeitigen und künftigen Führungskräften auf dem Gebiet der Cybersicherheit, ihre Führungsqualitäten auf das Niveau ihrer technischen Kenntnisse anzuheben.

In SANS-Kursen zu Führungskompetenzen in Cybersicherheit lernen Sie:

- Ihre Managementqualitäten und Führungskompetenzen zu entwickeln
- Risiken zu verstehen und zu analysieren
- Effektive Cybersicherheitsrichtlinien zu erstellen
- Ein Programm zum Schwachstellenmanagement aufzubauen
- Strategische Sicherheitspläne zu entwickeln, die geschäftliche und organisationsbezogene Ziele berücksichtigen
- Effektiv mit wichtigen Stakeholdern im Unternehmen zu interagieren und zu kommunizieren
- Den Einfluss Ihres Sicherheitsprogramms zu messen
- Eine Sicherheitskultur zu begründen und reifen zu lassen
- Unternehmens- und Cloud-Umgebungen zu schützen und zu leiten

„Dieser Kurs brachte für mich wirklich eine Menge zusammen und war von großem Wert. Ich bin sicher, dass Teile davon meinen Ansatz bei der Arbeit beeinflussen werden, sobald ich wieder im Büro bin.“

– Merewyn Boak, **Apple**

Führungsrollen auf dem Gebiet der Cybersicherheit:

- SOC-Analyst/-Manager
- Ingenieur für Bedrohungsdetektion, Threat Hunter
- Sicherheits- und Netzwerkingenieur/-architekt
- Ermittler/OSINT-Analyst
- Endpunkt-/Serversystem-Administrator
- Automatisierung und DevSecOps
- Incident Responder
- Cyber Threat Intelligence-Analyst

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

1/2 Kurstag	2 CPEs

Vermittelte Kompetenzen

- Lernen, wie GenAI funktioniert und wie sie bei der Produktivitätssteigerung helfen kann
- Prompt-Engineering verstehen, um die Interaktionen und Ausgaben aus GenAI-Systemen auf Klarheit und Relevanz hin zu optimieren
- Risiken durch KI angehen und mindern, u. a. Voreingenommenheit, blindes Vertrauen und Datensicherheit
- Grundlagen über die Schnittstelle zwischen KI und Cybersicherheit würdigen und die damit verbundenen Risiken managen
- Einblicke in die ethischen Erwägungen und bewährte Praktiken für die KI-Nutzung gewinnen
- Grundkompetenzen zur Bewertung von KI-Initiativen und zur Förderung erfolgreicher KI-Strategien erlangen

Zielgruppe

- CISOs, CIOs, CTOs, CMOs
- Leitende Führungskräfte in Unternehmen und Geschäftsbereichen, Manager
- Leitende Fachkräfte in Rechts-, Personal-, Marketing-, Vertriebs- und Finanzabteilung
- Beauftragte für Informationssicherheit
- Führungskräfte, Manager und Teamleiter in IT
- Sicherheitsleiter, -manager und -ingenieure
- Chief Product Officers, Produktmanager
- Ingenieure, Softwareentwickler und Analysten, die an der Einführung von KI beteiligt sind

Dan deBeaubien
Kursautor

AIS247: AI Security Essentials for Business Leaders™ ist eine Grundlagenschulung für Fachkräfte, die sich einer Geschäftswelt, die vom raschen Wandel und künstlicher Intelligenz geprägt ist, zurecht finden möchten. In dieser Schulung wird generative KI (GenAI) eingehend untersucht, beginnend mit einem fundamentalen Verständnis, warum sich GenAI in verschiedenen Branchen zu einem wichtigen Baustein der Strategie entwickelt hat. Sie beschäftigt sich mit den Mechanismen von GenAI, u. a. Themen wie Prompt-Engineering und den Komplexitäten von LLMs (Large Language Models). Die Teilnehmer gewinnen wertvolle Einblicke in die Risiken, die mit der Nutzung von GenAI häufig einhergehen, und lernen Strategien und Taktiken zur Risikominderung kennen.

Ein wichtiger Aspekt der Schulung AIS247 ist ihr Fokus auf dem Risikomanagement in Bezug auf die Cybersicherheit bei KI und auf der Entwicklung von KI-Richtlinien. Den Teilnehmern wird das nötige Wissen vermittelt, um KI-Innovationen verantwortlich und sicher zu managen. Die Schulung richtet sich an ein breites Spektrum von Fachkräften mit Aufgaben bei der KI-Implementierung, von Entscheidungsträgern bei KI-relevanten Themen bis zu Technologen und Endbenutzern, und zielt auf ein umfassendes Verständnis der Rolle von GenAI im Privat- und Berufsleben ab.

Die Schulung betont die praktische Anwendung von KI am Arbeitsplatz und stellt heraus, wie GenAI die Produktivität steigern, Kosten senken und die Qualität der Arbeit verbessern kann. Beispielanwendungen und Anwendungsfälle sind ein integraler Teil der Schulung und decken eine Reihe von Wegen ab, in denen sich GenAI bemerkbar macht, u. a. Inhaltserstellung, Datenanalyse, Software-Engineering, Kundenunterstützung und Cybersicherheit. Durch diese praktischen Beispiele verstehen die Teilnehmer, warum Unternehmen so stark motiviert sind, KI in ihrer eigenen Arbeitsumgebung einzusetzen, und wie sich die Produktivitätsgewinne gegen das Risikomanagement abwägen lassen.

AIS247™ nimmt sich der Herausforderungen der KI-Implementierung an und diskutiert die ethische und sichere Verwendung von KI-Technologien sowie die Bedeutung von Transparenz und Verantwortlichkeit. Außerdem wird erörtert, inwiefern KI-Richtlinien nötig sind und wie sie so entwickelt werden können, dass sie mit den Zielen der Organisation in Einklang stehen. Nach Abschluss der Schulung verstehen die Teilnehmer die technologischen Aspekte von KI, warum sie die Kraft hat, Unternehmen zu wandeln, und wie diese Tools am Arbeitsplatz sicher, ethisch und effektiv angewendet werden können.

Geschäftsorientierte Lernergebnisse

- Ein klares Verständnis dafür entwickeln, warum der Siegeszug von GenAI kaum aufzuhalten ist und warum es von entscheidender Bedeutung ist, die damit verbundenen Risiken zu managen
- Einblicke gewinnen, welche Rolle KI in Unternehmen spielt und wie sie für Produktivitätsgewinne genutzt wird
- Besser in der Lage sein, die primären Risiken, die sich aus der Implementierung und Integration von KI und ihrer Nutzung im Alltag ergeben, direkt anzugehen
- Entdecken, welche Inhalte, Teams und Prozesse nötig sind, um effektive KI-Richtlinien in Ihrer Organisation zu implementieren
- Verstehen, warum es am modernen Arbeitsplatz wichtig ist, KI auf ethische und transparente Weise zu nutzen, u. a. wegen Druck, Cyberrisiken und dem Risikofaktor Mensch, Minderungs- und Richtlinienstrategien.

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/AIS247**

KURSFORMATE AIS247

OnDemand

LDR414: SANS Training Program for the CISSP® Certification™

GISP
Information Security Professional
giac.org/gisp

6 Tage Programm | 52 CPEs

Vermittelte Kompetenzen

- Die acht Wissensbereiche verstehen, die im CISSP®-Examen abgedeckt werden
- Fragen im Examen analysieren und in der Lage sein, die richtige Antwort auszuwählen
- Die im Kurs gelernten Kenntnisse und Testkompetenzen anwenden, um das CISSP®-Examen zu bestehen
- Alle Konzepte verstehen und erklären, die in den acht Wissensbereichen abgedeckt werden
- Die gelernten Kompetenzen in den acht Wissensbereichen anwenden, damit Sie Sicherheitsprobleme lösen können, wenn Sie wieder bei der Arbeit sind

Zielgruppe

- Sicherheitsfachkräfte, die die Konzepte im CISSP®-Examen (wie vom ISC2 festgelegt) verstehen möchten
- Manager, die entscheidende wichtige Bereiche der Informationssicherheit verstehen möchten
- System-, Sicherheits- und Netzwerkadministratoren, die die pragmatischen Anwendungen der CISSP®-Wissensbereiche verstehen möchten
- Sicherheitsfachkräfte und -manager, die nach praktischen Wegen suchen, die acht Wissensbereiche auf ihre aktuellen Aktivitäten anzuwenden

„Dieser Kurs konzentriert sich sehr gezielt auf die wichtigsten Konzepte, die man für das CISSP®-Examen verstehen muss. Geben Sie sich nicht mit tausendseitigen Lehrbüchern ab. Lassen Sie sich von diesem Kurs leiten!“

– Carl Williams, **Harris Corporation**

Eric Conrad
Kursautor

Seth Misenar
Kursautor

Bereiten Sie sich auf das CISSP®-Examen vor?

SANS LDR414: SANS Training Program for CISSP® Certification™ ist ein beschleunigter Revisionskurs zur Vorbereitung auf das CISSP®-Examen.

Der Kurs konzentriert sich ausschließlich auf die von ISC2 festgelegten acht Wissensbereiche, die einen entscheidenden Teil des CISSP®-Examens bilden. Jeder Wissensbereich wird in seine wesentlichen Komponenten aufgespalten. Diese Komponenten werden dann im Hinblick auf ihre Beziehung zueinander und zu anderen Bereichen der Informationssicherheit diskutiert.

Erklärung der Kursautoren

„Die CISSP®-Zertifizierung gibt es seit fast 25 Jahren. Das Examen soll Ihr Verständnis des „Common Body of Knowledge“ prüfen, eines allgemeinen Wissensfundus, den man sich als Universalsprache der Fachkräfte auf dem Gebiet der Informationssicherheit vorstellen kann. Es geht um eine sehr umfangreiche Menge an Kenntnissen, die jedoch nicht in die Tiefe gehen. Das CISSP®-Examen deckt eine Menge theoretischer Informationen ab, die eine Sicherheitsfachkraft unbedingt verstanden haben muss. Dieses Material kann jedoch recht trocken sein, und da die meisten Lernenden nicht sehen, wie es bei ihren Aufgaben direkt anwendbar ist, finden sie es langweilig. Dieser Kurs möchte die acht Wissensbereiche von CISSP® in Bezug zur Realität setzen. Die praktischen Anwendungen dieser Informationen werden demonstriert, indem wichtige Themen mit Anekdoten, Beispielen und Fallstudien erläutert werden. Entdecken Sie in diesem SANS-Schulungskurs zu CISSP® die spannenden Aspekte der acht Wissensbereiche!“
– Eric Conrad und Seth Misenar

Zusammenfassung der Kursinhalte

TEIL 1: Einführung, Sicherheits- und Risikomanagement

TEIL 2: Asset-Sicherheit und Sicherheitstechnik (Teil 1)

TEIL 3: Sicherheitstechnik (Teil 2): Kommunikations- und Netzwerksicherheit

TEIL 4: Identitäts- und Zugriffmanagement (IAM)

TEIL 5: Sicherheitsbewertung und -tests; Sicherheitsbetrieb

TEIL 6: Sicherheit bei der Softwareentwicklung

„Dieser Kurs schlüsselt die dicken CISSP®-Lehrbücher in überschaubare Teile auf und hat mir geholfen, meine Schwächen gezielt zu identifizieren. Die Kursleiter waren mit der Materie vertraut und konnten sie gut vermitteln.“

– Jeff Jones, **Constellation Energy Group**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/LDR414**

KURSFORMATE LDR414

Präsenzkurs | **Live online** | **OnDemand**

LDR419: **Performing a Cybersecurity Risk Assessment**

2	12	7
Kurstage	CPEs	Laborübungen

Vermittelte Kompetenzen

- Den geschäftlichen Kontext für ein Risikomanagementprogramm verstehen
- Eine Charta für ein Cybersicherheitsprogramm erstellen
- Die Grundelemente von Risiken verstehen
- Angemessene Schutzmaßnahmen für Cybersicherheit wählen
- Risikobewertungen für Drittparteien durchführen
- Eine Risikobewertung für Cybersicherheit durchführen
- Cybersicherheitsdokumentation auswerten
- Die Implementierung von Schutzmaßnahmen für Cybersicherheit untersuchen
- Risiken gründlich an geschäftliche Stakeholder melden
- Risiken effektiv an technische Stakeholder melden
- Produktiv auf Risiken reagieren, die während einer Bewertung identifiziert wurden

Zielgruppe

- Fachkräfte für Risikomanagement
- Governance-, Risiko- und Compliance-Fachkräfte
- IT-Auditoren
- Leitung Sicherheits-Compliance
- Management Informationssicherung
- Systemadministratoren/-ingenieure

Berufliche Rollen im NICE Framework

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

„Der Kurs vermittelt ein gutes Verständnis dafür, wie wir bei den Risikobewertungen und Audits in unsere derzeitige Lage geraten sind und welche politischen Aspekte oft involviert sind.“

– Kevin Shivers, **University of Maryland**

James Tarala
Kursautor

Neue Gesetze verlangen, dass Organisationen für Compliance und Audits eine Risikobewertung in Bezug auf die Cybersicherheit durchführen. Viele Organisationen tun dies jedoch ohne eine spezifische Strategie, was zu willkürlichen Verteidigungsmaßnahmen, ineffektiven Programmen und finanziellen Verlusten führt. In dieser Einführung in Risikobewertungen für Cybersicherheit lernen Sie den geschäftlichen Kontext der Bewertung verstehen, sind besser in der Lage, geschäftliche Risiken korrekt zu erkennen, und können sich entsprechend besser schützen. Gehen Sie über die trockene Theorie hinaus und verstehen Sie wirklich, wie Sie sich ordentlich auf relevante Risikobewertungen vorbereiten und sie durchführen. Sie wissen, nach welchen Risiken Sie im spezifischen Kontext Ihrer Organisation suchen müssen, wie Sie diese Risiken effektiv aufdecken und wie Sie der Organisationsleitung Ergebnisse in einer Form präsentieren, die sich in Maßnahmen umsetzen lässt. LDR419™ vermittelt den Teilnehmern die Grundkenntnisse und praktischen Kompetenzen zur Durchführung solcher Risikobewertungen.

Praktische Schulung zu Risikobewertungen für Cybersicherheit

Jede der Fallstudien in diesem Kurs basiert auf einem fiktiven Technologieunternehmen namens Initech Systems, das auf der Suche nach einem ausgereifteren Cybersicherheitsprogramm ist. Die Teilnehmer haben Gelegenheit, Initechs spezifische Strategien und taktische Pläne zur Cybersicherheit zu erkunden, die auf Beispielen aus der wirklichen Welt beruhen. Für diese Fallstudien nutzen die Teilnehmer das Tabletop-Simulationsspiel Cyber42, das sie in Szenarien aus der wirklichen Welt versetzt. Dabei werden sie zu Diskussionen und kritischem Nachdenken über Situationen angeregt, mit denen sie bei der Arbeit konfrontiert werden.

- Das Governance-Modell einer Organisation beurteilen
- Die Ziele eines Cybersicherheitsprogramms beurteilen, um eine Bestandsaufnahme der Schutzmaßnahmen zu erstellen
- Einen umfassenden Risikobewertungsplan für interne und externe Parteien erstellen
- Eine Cybersicherheitsrichtlinie beurteilen
- Technische Schutzmaßnahmen für Cybersicherheit beurteilen
- Ein Risikobriefing für die Organisationsleitung erstellen
- Einen persönlichen Maßnahmenplan verfassen

Geschäftsorientierte Lernergebnisse

- Den Business Case für eine Risikobewertung der Cybersicherheit erstellen
- Auf eine Risikobewertung vorbereiten, die für das Unternehmen relevant ist
- Regulatorische Anforderungen erfüllen und übertreffen
- Die Ergebnisse der Risikobewertung effektiv exportieren und an wichtige Stakeholder melden
- Eine Strategie zur Reaktion auf identifizierte Cybersicherheitsrisiken erstellen

Zusammenfassung der Kursinhalte

TEIL 1: Eine Risikobewertung für Cybersicherheit vorbereiten

TEIL 2: Eine Risikobewertung für Cybersicherheit durchführen

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/LDR419**

KURSFORMATE LDR419

Präsenzkurs | **Live online** | **OnDemand**

LDR433: **Managing Human Risk™**

SSAP
SANS Security Awareness Professional
sans.org/ssap

3 Kurstage | 18 CPEs

Vermittelte Kompetenzen

- Lernen, wie der Reifegrad Ihres Programms ermittelt und mit anderen Programmen verglichen werden kann
- Das Reifemodell für Sicherheitsbewusstsein verstehen und wissen, wie Sie es als Roadmap für Ihr Programm nutzen
- Für die Einhaltung wichtiger Standards und Auflagen sorgen
- Modelle für Lerntheorie, Verhaltensänderung und Kulturanalyse implementieren
- Den Risikofaktor Mensch definieren und erläutern, aus welchen drei Variablen er besteht
- Verfahren zur Risikobeurteilung erklären
- Die neuesten Aspekte von KI erklären und nutzen, um Ihre Wirkungskraft exponentiell zu erhöhen
- Das Neueste in Cyber Threat Intelligence nutzen und die häufigsten Taktiken, Techniken und Verfahren beschreiben, die heute bei Angriffen durch Cyberkontrahenten zur Anwendung kommen
- Den Risikofaktor Mensch in Ihrer Organisation identifizieren, messen und priorisieren, und Verhaltensweisen zum Umgang mit diesen Risiken definieren
- Rollen mit hohem Risiko und die für diese Rolle erforderlichen spezialisierten Schulungen identifizieren

Zielgruppe

- Beauftragte für Sicherheitsbewusstsein, Schulung, Beteiligung oder Unternehmenskultur
- Alle, die für das Sicherheitsmanagement zuständig sind
- Sicherheitsauditoren und Beauftragte für Governance, Recht, Datenschutz oder Compliance
- Beschäftigte in Schulungs-, Personal- und Kommunikationsabteilung
- Vertreter von Organisationen in regulierten Branchen, z. B. durch HIPAA, DSGVO, FISMA, FERPA, PCI-DSS, ISO/IEC 27001 SOX, NERC oder andere Compliance-Standards
- Alle, die an der Planung, Bereitstellung oder Aufrechterhaltung von Sicherheitsschulungen, Einfluss- oder Kommunikationsprogrammen beteiligt sind

Berufliche Rollen im NICE Framework

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

Lance Spitzner
Kursautor

Cybersicherheit ist nicht mehr bloß eine technische Herausforderung, sondern auch eine menschliche, denn Menschen sind an 80 % aller Datenschutzverletzungen beteiligt. Für die meisten Organisationen besteht die größte Herausforderung im Umgang mit dem Risikofaktor Mensch. Dieser Kurs befähigt Sicherheitsfachkräfte, diesen Risikofaktor zu managen und zu messen, indem sie das Verhalten der Beschäftigten wandeln und sicherer machen. Die Teilnehmer erhalten eine strukturierte Roadmap mit einer schrittweisen Strategie, wie sie das Personal einbinden und sicherer machen können. Der Kurs umfasst sieben hoch interaktive Teamlaborübungen und ein digitales Kurspaket zum Download. Außerdem ist dies der einzige SANS-Kurzkurs mit einem branchenweit anerkannten Abschluss (SSAP).

Geschäftsorientierte Lernergebnisse

- Ihre Programme zum Sicherheitsbewusstsein an den strategischen Sicherheitsprioritäten Ihrer Organisation ausrichten
- Die wichtigsten menschlichen Risiken in Ihrer Organisation identifizieren, priorisieren und managen
- Maßnahmen zum Sicherheitsbewusstsein besser in das Risikomanagement Ihres Sicherheitsteams insgesamt einfügen
- Ihre Investition durch ein langfristiges Programm zum Sicherheitsbewusstsein, das nicht nur das Verhalten, sondern die Organisationskultur ändert, optimal nutzen
- Der Unternehmensführung den Wert der Veränderung für das Geschäft vermitteln und demonstrieren

Zusammenfassung der Kursinhalte

TEIL 1: Grundlagen und Identifizierung/Priorisierung menschlicher Risiken

TEIL 2: Verhalten identifizieren und ändern

TEIL 3: Sicherheitskultur und Veränderungen messen

„Der Inhalt war relevant und aktuell und wurde mit einer klaren praktischen Anwendung präsentiert."
– Rhys Arnold Arnold, **Bridewill**

„Ausgezeichnetes Wissen, das jede Organisation haben sollte."
– Mtinawa Banda, **Britische Zivilluftfahrtbehörde**

„Alle Unternehmen brauchen diese Art von Schulung."
– Nelson Estrada, **GoodFarms**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/LDR433**

KURSFORMATE LDR433

Präsenzkurs | **Live online** | **OnDemand**

LDR512: Security Leadership Essentials for Managers™

GSLC
Führung im Bereich Sicherheit
giac.org/gslc

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

5	30	23
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Verschiedene Frameworks der Cybersicherheit verstehen
- Risiken verstehen und analysieren
- Die Vor- und Nachteile verschiedener hierarchischer Strukturen verstehen
- Technische Teams und Projekte managen und leiten
- Ein Programm zum Schwachstellenmanagement aufbauen
- Sicherheit in moderne DevOps-Workflows integrieren
- Ein SIEM-Tool (Security Information and Event Management) strategisch nutzen
- Ein Security Operations Center leiten
- Verhalten ändern und eine sicherheitsbewusste Organisationskultur aufbauen
- Sicherheitsprojekte effektiv managen
- Moderne Sicherheitsarchitekturen und die Cloud ermöglichen
- Mit Automatisierung und Infrastruktur als Code Kompetenzen für die Sicherheitstechnik aufbauen

Zielgruppe

- CISOs
- Beauftragte für Informationssicherheit
- Sicherheitsleiter
- Sicherheitsmanager
- Personen, die die Position der Leitung Informationssicherheit anstreben
- Sicherheitspersonal mit Teamführungs- oder Managementverantwortung
- Alle, die über technische Kompetenzen hinaus weiterbilden möchten
- Technische Fachkräfte, die geschäftsbezogene Kommunikation mit höheren Führungskräften lernen möchten

Berufliche Rollen im NICE Framework

- 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
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Sicherheitsinitiativen zum Umgang mit Informationsrisiken leiten

Sicherheitsführungskräfte benötigen sowohl technische Kenntnisse als auch Führungskompetenzen, um sich den Respekt der Mitglieder von technischen Teams zu verdienen, zu verstehen, was das technische Personal eigentlich macht, und Sicherheitsprojekte und -initiativen angemessen zu planen und zu managen. Diese Schulung für Sicherheitsmanager vermittelt Führungskräften die wichtigsten Elemente eines jeden modernen Sicherheitsprogramms. Entscheidende Probleme der Cybersicherheit und die zugehörige Terminologie werden Ihnen schnell nähergebracht. Der Fokus liegt dabei auf Sicherheits-Frameworks, Sicherheitsarchitektur, Sicherheitstechnik, Computer-/Netzwerksicherheit, Schwachstellenmanagement, Kryptografie, Datenschutz, Sicherheitsbewusstsein, Anwendungssicherheit, DevSecOps, Cloud-Sicherheit und Sicherheitsbetrieb. Das ist mehr als eine Sicherheitsschulung. In 23 Cyber42-Aktivitäten, die über die gesamte Schulung verteilt sind (60–80 Minuten täglich), lernen Sie, wie Sie Sicherheitsteams führen und Programme managen.

Geschäftsorientierte Lernergebnisse

- Führungskräfte heranziehen, die wissen, wie man ein modernes Sicherheitsprogramm aufbaut
- Im Voraus wissen, welche Sicherheitsfähigkeiten aufgebaut werden müssen, damit das Unternehmen befähigt und Bedrohungen verringert werden
- Sicherheitsteams mit besserer Performance aufbauen

Zusammenfassung der Kursinhalte

TEIL 1: Ein Sicherheitsprogramm aufbauen

TEIL 2: Verteidigungsfähige Sicherheitsarchitektur

TEIL 3: Sicherheitstechnik

TEIL 4: Sicherheitsmanagement und Führungskompetenz

TEIL 5: Angriffe erkennen und darauf reagieren

„Der Wechsel zwischen dem Vortrag der Inhalte und dem Cyber42-Game hat mir gut gefallen."

– Jamil A., **US-Regierung**

„Der Kurs war toll. Wertvolle Informationen in einem großartigen Crashkurs zur Führung im Bereich Sicherheit."

– Ian D., **US-Regierung**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/LDR512**

KURSFORMATE LDR512

Präsenzkurs | **Live online** | **OnDemand**

LDR514: Security Strategic Planning, Policy, and Leadership™

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

5	30	15
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Strategische Sicherheitspläne entwickeln
- Eine effektive Informationssicherheitsrichtlinie erstellen
- Die verschiedenen Phasen des strategischen Planungsprozesses verstehen
- Umfassendere Kenntnisse wichtiger Planungstools anwenden
- Grundlegende Kompetenzen zur Erstellung strategischer Pläne zum Schutz Ihres Unternehmens erweitern
- Wichtige Innovationen ermöglichen
- Effektive Zusammenarbeit mit Geschäftspartnern fördern
- Strategische Sicherheitspläne fördern, die treibende geschäftliche und organisatorische Faktoren berücksichtigen

Zielgruppe

- CISOs
- Beauftragte für Informationssicherheit
- Sicherheitsleiter
- Sicherheitsmanager
- Personen, die die Position der Leitung Informationssicherheit anstreben
- Sicherheitspersonal mit Teamführungs- oder Managementverantwortung
- Alle, die über technische Kompetenzen hinaus weiterbilden möchten
- Technische Fachkräfte, die geschäftsbezogene Kommunikation mit höheren Führungskräften lernen möchten

Berufliche Rollen im NICE Framework

- 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
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Sicherheitsinitiativen an der Strategie ausrichten

Die nächste Führungsgeneration im Bereich Sicherheit muss die Kluft zwischen Sicherheitspersonal und der Unternehmensführung überbrücken, indem sie strategisch plant, wie effektive Sicherheitsprogramme aufgebaut und ausgeführt werden können. Für IT- und Sicherheitsfachkräfte ist es jedoch schwierig, eine Sicherheitsstrategie zu erstellen und einen Plan auszuführen, der solide Richtlinien und ausgezeichnete Führungskompetenzen umfasst, da wir so viel Zeit damit verbringen, auf Vorfälle zu reagieren. Bevor wir in eine Führungsposition befördert werden, beschäftigen wir uns fast nie mit strategischer Planung. Deshalb fehlt uns dann die Kompetenz, um uns auf dieser Ebene zurechtzufinden. Dieser Informationssicherheitskurs gibt Ihnen die Tools an die Hand, die Sie benötigen, um einen strategischen Plan für Cybersicherheit und eine umfassende IT-Sicherheitsrichtlinie zu erstellen und Ihre Teams bei der Ausführung von Plan und Richtlinie anzuleiten. Im Laufe dieses Kurses bereiten Sie eine Präsentation für die Unternehmensführung vor, lesen drei Business-Case-Studien, reagieren auf Probleme, die sich vier fiktiven Unternehmen stellen, analysieren neun Fallszenarien und reagieren auf 20 Cyber42-Ereignisse.

Geschäftsorientierte Lernergebnisse

- Einen Sicherheitsplan erstellen, der bei Kunden Anklang findet
- Führungskräfte weiterentwickeln, die wissen, wie sie Cybersicherheit mit geschäftlichen Zielen vereinbaren
- Sicherheitsteams mit besserer Performance aufbauen

Zusammenfassung der Kursinhalte

TEIL 1: Grundlagen strategischer Planung

TEIL 2: Entwicklung einer strategischen Roadmap

TEIL 3: Entwicklung und Bewertung einer Sicherheitsrichtlinie

TEIL 4: Führungs- und Managementkompetenzen

TEIL 5: Workshop zur strategischen Planung

„Cyber 42 hat mir gut gefallen. Insbesondere, dass wir die Antworten durchgehen und diskutieren konnten, welche Auswirkungen sie jeweils auf die Ergebnisse hatten."

– Alexander Walker, **TechVets**

„Ich wünschte, ich hätte diesen Kurs vor 10 Jahren absolviert, als ich meine Rolle als CISO angetreten habe. Die Gruppendiskussionen, die Tools und die Theorie sind praktisch und auf meine alltägliche Arbeit anwendbar."

– Mark Potter, **NewWave**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/LDR514**

KURSFORMATE LDR514

Präsenzkurs | **Live online** | **OnDemand**

LDR516: Building and Leading Vulnerability Management Programs™

5	30	16
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Ein Programm zum Schwachstellenmanagement erstellen, implementieren und zur Reife bringen und Stakeholder auf Ihre Seite holen
- Techniken zum Aufbau und zur Pflege eines korrekten und nützlichen Inventars von IT-Assets im Unternehmen und in der Cloud umsetzen
- Verfahren und Technologien identifizieren, die für Infrastruktur und Anwendungen effektiv sind, und wissen, wie sie angemessen konfiguriert werden
- Wissen, welche Meldungen in Ihrem Identifizierungsarsenal häufig falsch positiv oder falsch negativ sind
- Nicht blockierten Schwachstellen bei der Behebung mit einer Reihe verschiedener Techniken Priorität einräumen
- Schwachstellendaten innerhalb Ihrer Organisation effektiv melden und mitteilen
- Das Risiko identifizieren, das mit Schwachstellen verbunden ist, die blockiert sind und derzeit nicht mit Priorität ausgeräumt werden können

Zielgruppe

- Manager von Schwachstellenprogrammen und Analysten, die Schwachstellen im Unternehmen oder in der Cloud managen
- Manager, Architekten, Analysten, Beauftragte und Leiter für Informationssicherheit
- Personen, die eine Führungsposition im Bereich Informationssicherheit anstreben
- Fachkräfte für Risikomanagement, Business Continuity und Notfallwiederherstellung
- IT-Betriebsmanager und -administratoren
- CISOs
- Manager, Administratoren, Integratoren, Entwickler und Broker für Cloud-Services
- Sicherheits- und Risikomanager für Cloud-Services
- IT-Fachkräfte in Behörden, die Schwachstellen im Unternehmen oder in der Cloud managen (FedRAMP, NIST CSF)

Berufliche Rollen im NICE Framework

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

Jonathan Risto
Kursautor

David Hazar
Kursautor

Sind Sie es leid, Symptome zu kurieren? Packen wir das Problem an der Wurzel.

Schwachstellen-, Patch- und Konfigurationsmanagement sind keine neuen Themen bei der Sicherheit. Vielmehr handelt es sich um einige der ältesten Sicherheitsfunktionen. Dennoch kämpfen wir damit, diese Fähigkeiten effektiv zu managen. Die meisten großen Organisationen haben eine überwältigende Menge ausstehender Schwachstellen, und alle Organisationen finden es schwer, mit der nimmer endenden Flut neuer Schwachstellen in Infrastruktur und Anwendungen Schritt zu halten. Dazu kommen noch die Cloud und die Tatsache, dass Organisationen Systeme, Anwendungen und Funktionen für interne und externe Kunden immer schneller bereitstellen müssen. Sicherheit scheint da mitunter ein unerreichbares Ziel. Dieser Kurs zeigt Ihnen die effektivsten Wege, Ihrem Schwachstellenmanagement-Programm zu mehr Reife zu verhelfen und von der Identifizierung von Schwachstellen zu ihrer erfolgreichen Behebung überzugehen.

Geschäftsorientierte Lernergebnisse

Dieser Kurs hilft Ihrer Organisation:

- Zu verstehen, was bei modernen Schwachstellenprogrammen funktioniert und was nicht
- Die Auswirkungen von Cloud-Betriebsumgebungen vorherzusehen und dafür zu planen
- Zu verstehen, warum Kontext wichtig ist und wie Kontextdaten effektiv erfasst, gespeichert, gepflegt und genutzt werden
- Schwachstellendaten und die damit verbundenen Risiken wichtigen Stakeholdern effektiv und effizient zu vermitteln
- Herauszufinden, wie sich Schwachstellen sinnvoll gruppieren lassen, um aktuelle Hindernisse oder Mängel zu identifizieren
- Zu wissen, welche Kennzahlen Annahme und Veränderung innerhalb der Organisation schneller voranbringen
- Zu verstehen, welche Sanierungsfähigkeiten verfügbar sind, um Technologieteams bei der Behebung von Schwachstellen zu helfen

Zusammenfassung der Kursinhalte

TEIL 1: Schwachstellenmanagement konzipieren und planen
TEIL 2: Schwachstellen identifizieren
TEIL 3: Schwachstellen analysieren, messen und vermitteln
TEIL 4: Abhilfemaßnahmen und Automatisierung vorantreiben
TEIL 5: Zusammenarbeit und kontinuierliche Verbesserung

„Dieser Kurs sollte für alle Mitglieder von Schwachstellenmanagementteams obligatorisch sein. Die Einblicke, die hier bereitgestellt werden, sind für jede Organisation unmittelbar hilfreich."

– Brandi Loveday-Chesley

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/LDR516**

KURSFORMATE LDR516

Präsenzkurs | **Live online** | **OnDemand**

KURS NEU IM FOKUS

LDR519: Cybersecurity Risk Management and Compliance™

5 Tage Programm | 30 CPEs

Vermittelte Kompetenzen

- Durch strukturierte Bedrohungsmodellierung und Bewertungsmethodiken praktische Kompetenzen bei der Identifizierung und beim Management von Cybersicherheitsrisiken erlangen
- Verstehen, wie kritisch verschiedene Bedrohungen und Schwachstellen in Bezug auf Cybersicherheit sind, und dadurch lernen, wie Ressourcen effektiv priorisiert und zugewiesen werden können
- Kompetenz bei der Nutzung von Branchenstandard-Frameworks entwickeln, z. B. NIST Risk Management Framework (RMF) und FAIR, um den Cybersicherheitsstatus Ihrer Organisation zu verbessern
- Praktische Übungen und Fallstudien aus der wirklichen Welt anwenden, um theoretische Kenntnisse zu vertiefen und Cybersicherheitsstrategien zu validieren
- Den Prozess meistern, mit dem umfassende Risikobewertungen und Audits für Cybersicherheit durchgeführt werden, um für Compliance mit aufsichtsrechtlichen Standards zu sorgen
- Die Fähigkeiten zur Entscheidungsfällung durch datengestützte Einblicke und Simulationen verbessern und die Teilnehmer auf die Herausforderungen von Cybersicherheit in der wirklichen Welt vorbereiten

Zielgruppe

- Fachkräfte für Risikomanagement
- Governance-, Risiko- und Compliance-Fachkräfte
- IT-Auditoren
- Leitung Sicherheits-Compliance
- Management Informationssicherung
- Systemadministratoren/-ingenieure

Berufliche Rollen im NICE Framework

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

James Tarala
Kursautor

LDR519™ nimmt sich eines erheblichen Problems im Bereich der Cybersicherheit an: wie man Cybersicherheitsrisiken effektiv managt und mindert und gleichzeitig die regulatorische Compliance wahrt. Dieses Problem ist zunehmend relevant, da Cyberbedrohungen komplex sind und sich ständig weiterentwickeln, was erhebliche Auswirkungen auf den Betrieb, die Datensicherheit und die Business Continuity einer Organisation insgesamt haben kann. Dieser umfassende Kurs beschäftigt sich mit Bedrohungsmodellierung, Schutz-Frameworks und Risikoanalyse und stattet Sie mit den Kompetenzen aus, die Sie brauchen, um Cybersicherheitsrisiken effektiv zu managen. Sie lernen, Bedrohungen zu priorisieren, angemessene Schutzmaßnahmen auszuwählen und für regulatorische Compliance zu sorgen. Sie gewinnen praktische Einblicke durch mehrere Fallstudien aus der wirklichen Welt und SANS-Cyber42-Simulationen, die Ihr Verständnis von Cybersicherheit-Governance und Programmmanagement vertiefen. Nehmen Sie teil, meistern Sie Risikomanagement und Compliance und sichern Sie die digitale Zukunft Ihrer Organisation.

Geschäftsorientierte Lernergebnisse

- Beschäftigten die erweiterten Kompetenzen an die Hand geben, die sie benötigen, um Cybersicherheitsrisiken zu identifizieren, zu bewerten und zu mindern und die Sicherheit der Organisation zu verbessern
- Cybersicherheitsmaßnahmen durch einen strukturierten Ansatz für Risikomanagement und Compliance mit den Geschäftszielen abstimmen
- Fähigkeiten zur Entscheidungsfällung verbessern, indem Bedrohungsmodellierung und Risikoanalysen in die strategische Planung integriert werden
- Die Resilienz der Organisation gegen aufkommende Cyberbedrohungen durch proaktive Strategien zum Risikomanagement stärken
- Compliance mit Branchenstandards und regulatorischen Vorschriften sicherstellen und dadurch das Risiko von rechtlichen und finanziellen Folgen reduzieren
- Robuste Schutzmaßnahmen für die Cybersicherheit implementieren, die auf das spezifische Risikoprofil Ihrer Organisation abgestimmt sind
- Bei Teammitgliedern eine Kultur von Sicherheitsbewusstsein und kritischem Denken fördern, um den Sicherheitsstatus allgemein zu verbessern

Zusammenfassung der Kursinhalte

TEIL 1: Strategien für das Risikomanagement bei Cybersicherheit

TEIL 2: Bedrohungsmodellierung für Cybersicherheit

TEIL 3: Schutzmaßnahmen-Frameworks für Cybersicherheit

TEIL 4: Schutzmaßnahmen validieren und Risikomanagement bei Dritten

TEIL 5: Risikoanalyse und -reaktion für Cybersicherheit

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/LDR519**

KURSFORMATE LDR519

Präsenzkurs **Live online**

LDR520: **Cloud Security for Leaders™**

5	30	Über 12
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Eine Cloud-Sicherheitsstrategie definieren, die mit den geschäftlichen Zielen des Unternehmens übereinstimmt
- Eine Roadmap erstellen, die eine schnelle, sichere Cloud-Adoption unterstützt
- Grundlagen der Cloud-Sicherheit verstehen und wichtige Entscheidungen rechtfertigen
- Mit Cloud-nativen Tools und Automatisierung für einen ausgereifteren Sicherheitsstatus sorgen
- Führungskräften und Teams die Vision der Cloud-Sicherheit vermitteln
- Den Sicherheitsstatus mit Benchmarks vergleichen und die Sicherheitsinvestitionen optimieren
- Skalierbare Leitlinien und Governance über mehrere Cloud-Umgebungen hinweg implementieren

Zielgruppe

- Primär Manager und Leiter, die wichtige Entscheidungen zur IT-Umstellung auf Cloud-Umgebungen anleiten oder fällen

Berufliche Rollen im NICE Framework

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

Jason Lam
Kursautor

Immer mehr Unternehmen in verschiedenen Branchen migrieren in die Cloud. Damit vervielfältigen sich auch die Risiken durch neue Bedrohungen und fehlkonfigurierte Cloud-Umgebungen. Dieser Kurs bietet einen praktischen Ansatz für Aufbau und Reifung der Cloud-Sicherheit mit einem strukturierten Modell für Sicherheitsreife. Die Teilnehmer erkunden wichtige Bereiche wie Workload-Schutz, Compliance, Incident Response und Transparenz über mehrere Cloud-Plattformen hinweg. In 12 interaktiven Cyber42-Führungssimulationen gewinnen die Teilnehmer realistische Erfahrung bei fundierten Entscheidungen im Zusammenhang mit Strategie, Investitionen und Teamfähigkeiten. So entwickeln sie Führungskompetenzen und technische Fertigkeiten, die unabdingbar sind, um sichere Cloud-Umgebungen erfolgreich zu planen, bereitzustellen und zu verwalten – vom ersten Tag bis zur hohen Reife.

Geschäftsorientierte Lernergebnisse

- Geschäftlichen Wandel durch wohl konzipierte Cloud-Sicherheitsstrategien beschleunigen
- Den Sicherheitsstatus mit Branchenbenchmarks vergleichen, um Wettbewerbsvorteile zu identifizieren
- Sicherheitsinvestitionen mit kennzahlgestützten ROI-Frameworks optimieren
- Automatisierte Leitlinien implementieren, um Assets zu schützen und gleichzeitig Innovation zu ermöglichen
- Sicherheitskontrollmaßnahmen gegen eine schnelle Cloud-Adoption abwägen, damit sie nicht zum Engpass werden
- Einheitliche Governance-Frameworks erstellen, die auf Multicloud-Umgebungen skaliert werden können

Zusammenfassung der Kursinhalte

TEIL 1: Grundlagen der Cloud-Sicherheit und Identitätsmanagement

TEIL 2: Schutz und Architektur der Cloud-Sicherheitsumgebung

TEIL 3: Datenschutz, Sicherheitsdetektion und Cloud-Sicherheits-Governance

TEIL 4: Sicherung der Workload und Gewährleistung von Sicherheit

TEIL 5: Mehrere Cloud-Systeme und Führung und Aufsicht über die Cloud

„Diese Art Schulung, also Cloud-Sicherheit aus Sicht des Managements, ist selten und die Qualität dieses Kurses ist wirklich hervorragend."

– Benoit Ramillon, **UEFA**

„Ein prima Kurs mit reichlich Material. Er zeigte wirklich das Modell, dem eine Organisation folgen sollte, um die Sicherheit in Cloud-Umgebungen zu erhöhen."

– Jesus Fernandez, **FEMSA**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/LDR520**

KURSFORMATE LDR520

Präsenzkurs | **Live online** | **OnDemand**

LDR521: **Security Culture for Leaders™**

5	30	Über 12
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Erklären, was eine Unternehmenskultur ist, welche Bedeutung sie für die Sicherheit hat und wie beide sich zur Gesamtkultur und Sicherheitskultur Ihrer Organisation verhalten
- Die Anzeichen einer starken Sicherheitskultur definieren, die Sicherheit an ihnen orientieren und sie in der bestehenden Organisationskultur verankern
- Ihrem Sicherheitsteam ein Framework und Leitlinien geben, wie es das Fundament für eine starke Sicherheitskultur legen kann
- Dem Vorstand und der Führungsebene den geschäftlichen Wert der Sicherheit effektiv vermitteln und sich ihre Unterstützung sichern
- Beschäftigte einbeziehen und motivieren, damit sie Cybersicherheit Priorität verleihen
- Sicherheit vereinfachen und Hindernisse aus dem Weg räumen, damit es für die Beschäftigten erheblich einfacher wird, Sicherheit in ihren Alltag einzubetten

Zielgruppe

- Chief Information Security Officers
- Chief Risk Officers/Leiter Risikomanagement
- Beauftragte für Sicherheitsbewusstsein, Beteiligung oder Unternehmenskultur
- Leitende Sicherheitsmanager, die große Sicherheitsinitiativen lenken
- Manager, Beauftragte und Leiter für Informationssicherheit
- Informationssicherheits-Architekten und -Berater
- Personen, die eine Führungsposition im Bereich Informationssicherheit anstreben
- Leiter für Business Continuity/ Notfallwiederherstellung
- Datenschutz- und Ethikbeauftragte

Berufliche Rollen im NICE Framework

- 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
Kursautor

Russell Eubanks
Kursautor

Anhand von Lehren, die weltweit aus der wirklichen Welt gezogen werden, vermittelt SANS LDR521™ Ihnen, wie Sie eine Unternehmenskultur aufbauen, in der sowohl die Unternehmensführung als auch die Beschäftigten von Cybersicherheit überzeugt sind und ihr Priorität einräumen. Durch praxisnahe Anweisungen und eine Reihe interaktiver Übungen wenden Sie die Konzepte des Organisationswandels auf eine Reihe verschiedener Sicherheitsinitiativen aus der wirklichen Welt an und lernen schnell, wie Sie Ihr Sicherheitsteam transformieren und Sicherheit von der Führungsebene herab in der Kultur Ihrer Organisation verankern. Sie wenden Erkenntnisse aus der Forschung an, für die Daniel Kahneman mit dem Nobelpreis ausgezeichnet wurde, aus der Nudge Theory von Thayler und Sunstein, dem ADKAR-Änderungsmodell und dem Goldenen Kreis von Simon Sinek. Sie lernen, was Spock, Homer Simpson, Elefant und Reiter und der Fluch des Wissens für eine starke Sicherheitskultur bei Ihrer Organisation bedeuten.

Geschäftsorientierte Lernergebnisse

- **Sicherheit im großen Stil:** Erleichtern Sie sich die Arbeit, indem Sie sich selbst und Ihr Sicherheitsteam hochskalieren. Schützen Sie Ihr Sicherheitsteam vor Burnout.
- **Eingebettete Sicherheit:** Verankern Sie Sicherheit von Anfang an in jedem Unternehmensprojekt und jeder Initiative in allen Geschäftsbereichen Ihrer Organisation.
- **Unterstützung durch die Führungsebene:** Sichern Sie sich die Unterstützung der Unternehmensführung für die wichtigsten Aspekte Ihrer Arbeit.
- **Sicheres Personal:** Die Beschäftigten zeigen die gewünschten Verhaltensweisen, ohne dass Sie ihnen sagen müssen, was sie tun und lassen sollen.
- **Erfolgreiche Initiativen:** Ihre Sicherheitsinitiativen haben mehr Erfolg, da sie die Unterstützung wichtiger Abteilungen haben, z. B. IT, Technik und Geschäft.
- **Befürworter:** Transformieren Sie Ihr Sicherheitsteam in Befürworter der Sicherheit, die das Personal einbeziehen und motivieren und es ihm ermöglichen, viel sicherer zu sein.

Zusammenfassung der Kursinhalte

TEIL 1: Grundlagen der Organisations- und Sicherheitskultur
TEIL 2: Für eine Sicherheitskultur motivieren
TEIL 3: Eine Sicherheitskultur ermöglichen und messen
TEIL 4: Die Führung einbeziehen
TEIL 5: Abschlussworkshop

„Ich bin so froh, dass sich dieses Material darauf konzentriert, Sicherheitswerte in unsere weltweite Unternehmenskultur einzubetten. Das ist genau das, was mein Unternehmen JETZT braucht."
– Laura M., **KPMG LLP**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/LDR521**

KURSFORMATE LDR521

Präsenzkurs | **Live online** | **OnDemand**

LDR551: Building and Leading Security Operations Centers™

GSOM
Security Operations Manager
giac.org/gsom

5	30	Über 17
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Ein starkes SOC-Fundament mit einer klaren Mission, Charta und organisatorischen Zielsetzung aufbauen
- Die wichtigsten Protokolle und Netzwerkdaten erfassen
- Ein vielfältiges Team aufbauen, schulen und befähigen
- Playbooks erstellen und Anwendungsfälle für die Detektion managen
- Mithilfe von Threat Intelligence Detektionsbemühungen auf die wahren Prioritäten richten
- Den Threat-Hunting-Prozess und aktive Verteidigungsstrategien anwenden
- Einen effizienten Workflow für Alarmtriage und Ermittlungen umsetzen
- Die Incident Response effektiv planen und ausführen
- Kennzahlen und eine langfristige Strategie zur Verbesserung des SOC wählen
- Teammitglieder schulen und binden und Burnouts verhindern
- Eine Beurteilung des SOC durch Kapazitätsplanung, Purple-Team-Tests und Gegneremulation durchführen

Zielgruppe

Alle, die ihr erstes SOC aufbauen oder ein SOC verbessern möchten, das die Organisation bereits führt.

Ideale berufliche Rollen für diesen Kurs:

- Manager oder Leiter von Security Operations Centers
- Sicherheitsleiter
- Neue SOC-Teammitglieder
- Leitende oder höhere SOC-Analysten
- Technische CISOs und Sicherheitsleiter

Berufliche Rollen im NICE Framework

- 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
Kursautor

Mark Orlando
Kursautor

Prävention – Detektion – Reaktion | Menschen – Verfahren – Technologie

Wenn Sie ein SOC (Security Operations Center) managen oder leiten und die Power einer proaktiven, informationsgestützten Cyberverteidigung entfesseln möchten, dann ist LDR551™ der perfekte Kurs für Sie! In einer Welt, in der IT-Umgebungen und böswillige Akteure sich so schnell entwickeln, dass viele Teams nicht Schritt halten können, müssen Sie Ihr SOC so positionieren, dass es hoch motivierte Gegner abwehren kann. Hoch dynamische moderne Umgebungen benötigen eine Fähigkeit zur Cyberverteidigung, die nach vorn schaut, schnell reagiert und sich auf Informationen stützt. Dieser Schulungskurs für SOC-Manager führt Sie von Anfang bis Ende durch diese kritischen Aktivitäten und zeigt Ihnen, wie Sie Verteidigungsmaßnahmen für das individuelle Risikoprofil Ihrer Organisation entwerfen. Nach Abschluss des Kurses sind Sie in der Lage, Ihre SOC-Aktivitäten mit den Zielen der Organisation in Einklang zu bringen.

Geschäftsorientierte Lernergebnisse

- Strategien implementieren, um die Cyberverteidigung an den Organisationszielen auszurichten
- Das Risikoprofil durch verbesserte Tools und Techniken zur Sicherheitsvalidierung verbessern
- Methodiken zur Rekrutierung, Einstellung, Schulung und Bindung talentierter Cyberverteidiger anwenden
- Effektive teamübergreifende Koordination und Zusammenarbeit fördern
- Mit vorhandenen Assets sofortige Verbesserungen der Sicherheit durchführen
- Die Ausgaben senken, da die Cybersicherheit reibungsloser operiert

Zusammenfassung der Kursinhalte

TEIL 1: SOC-Design und Betriebsplanung

TEIL 2: SOC-Telemetrie und -Analyse

TEIL 3: Angriffsdetektion, Hunting und Triage

TEIL 4: Incident Response

TEIL 5: Kennzahlen, Automatisierung und kontinuierliche Verbesserung

„Dieser Kurs erweitert Ihren Toolkit zur Problemlösung im NOSC-Betriebsmanagement sofort."

– Ron L., **US-Regierung**

„Großartige Inhalte. Der Kurs deckt eine Menge ab, stellt neue Konzepte und Ideen vor und setzt den Inhalt in Bezug zu aktuellen, echten Beispielen."

– Prasanth Chatti, **Campbells Soup Company**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/LDR551**

KURSFORMATE LDR551

Präsenzkurs | **Live online** | **OnDemand**

LDR553: Cyber Incident Management™

GCIL
Cyber Incident Leader
giac.org/gcil

5	30	Über 26
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Vorfälle korrekt kategorisieren und abschätzen und Ziele für das Vorfallsmanagementteam erstellen
- Beim Management eines schweren Vorfalls alle Mitteilungen entwerfen, korrigieren, veröffentlichen und steuern
- Ein Team unter extremem Druck managen und seine natürlichen menschlichen Reaktionen und ihre Bedeutung erkennen
- Das Team führen, das Vertrauen der Organisationsführung gewinnen und die Erwartungen aller Beteiligten übertreffen
- Aktivitäten zur Konterung von System- und Datenkompromittierungen berechnen, koordinieren und ausführen
- Strategien für Ransomware-Vorfälle entwickeln und auf Ransomware reagieren, einschl. der Entwicklung von Übungen und Schulungen zu diesen verheerenden Angriffen
- Briefings für das Team, die Unternehmensführung und Vorstandsmitglieder strukturieren, managen und abhalten
- Den Übergang vom aktiven Vorfall zum normalen Geschäftsbetrieb organisieren und den Plan ausführen
- Übungen zum Cybervorfallsmanagement vorbereiten, einrichten und ausführen

Zielgruppe

- Sicherheitsmanager
- Sicherheitsfachkräfte
- Manager
- Beschäftigte in der Rechts-/Personal-/PR-Abteilung

Berufliche Rollen im NICE Framework

- 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
Kursautor

Was tun, wenn der Ernstfall eintritt?

Wenn Sie Angst davor haben, einen großen Cybervorfall leiten oder unterstützen zu müssen, ist dies der richtige Kurs für Sie. LDR553: Cyber Incident Management™ legt den Fokus auf Herausforderungen nicht technischer Natur, denen sich Führungskräfte unter extremem Druck stellen müssen. Sie haben vielleicht ein umfassendes Team technischer Beschäftigter, die bereitstehen, die Angreifer zu finden, zu verstehen und zu entfernen, aber sie brauchen Informationen, müssen Aufgaben zugeteilt bekommen, gemanagt und unterstützt werden und ein offenes Ohr finden, damit Sie sie mit optimaler Effektivität einsetzen können. Wir konzentrieren uns darauf, ein Team aufzubauen, das bei einem Vorfall Abhilfe schafft, dieses Team zu managen, die kritischen Daten für Briefings herauszufiltern und ein solches Briefing zu leiten. Wir sehen uns die Kommunikation auf allen Ebenen an, vom aktiven Team bis zu Führungskräften und Unternehmensleitung, Enthüllungsjournalisten und sogar Angreifern. Dieser Kurs umfasst neun Fallstudien zum praktischen Lernen.

Geschäftsorientierte Lernergebnisse

- Personal heranziehen, das in der Lage ist, Managementteams für Cybervorfälle zu führen oder sich an ihnen zu beteiligen
- Vorfallsmanagementprozesse optimieren, damit sie schneller zur Lösung führen
- Lücken in Sicherheitsvorfallsplänen und Reaktionsstrategien identifizieren und schließen
- Die Performance von Sicherheitsvorfallteams erhöhen, um den sich ständig wandelnden Herausforderungen gewachsen zu sein
- Mit einem widerstandsfähigen Framework strategisch für hoch profilierte Angriffe wie E-Mail-Kompromittierung und Ransomware planen und sie bewältigen
- Für einen stärker integrierten Ansatz während der Incident Response eine nahtlose Zusammenarbeit zwischen technischen und nicht technischen Teams fördern
- Eine Kultur der kontinuierlichen Verbesserung schaffen, in der Lehren, die aus Vorfällen gezogen werden, zukünftige Reaktionsstrategien verbessern
- Threat Intelligence proaktiv integrieren, um potenzielle Bedrohungen vorherzusehen und zu mindern, bevor sie eskalieren

Zusammenfassung der Kursinhalte

TEIL 1: Den Vorfall verstehen und darüber informieren

TEIL 2: Den Schaden abschätzen, Abhilfemaßnahmen planen und den Plan ausführen

TEIL 3: Schulungen, Threat Intelligence für Cybersicherheit und Bug Bounties

TEIL 4: Cloud-Vorfälle, kompromittierte Geschäfts-E-Mail, Diebstahl von Anmeldeinformationen und Vorfallskennzahlen

TEIL 5: KI für Vorfälle, Angreifererpressung, Ransomware und Abschlussübung

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/LDR553**

KURSFORMATE LDR553

Präsenzkurs | **Live online** | **OnDemand**

SEC405: **Business Finance Essentials™** GRUNDLEGEND ÜBERARBEITET

1 Kurstag | 6 CPEs

Vermittelte Kompetenzen

- Kenntnisse in Geschäftsfinanzen erweitern
- Das Verständnis und Bewusstsein dafür verbessern, was gesunde Geschäftsfinanzen ausmacht
- Auf die Partnerschaft mit dem Finanzteam Ihrer Organisation vorbereiten
- Kompetenzen und Kenntnisse weiterentwickeln, die Sie brauchen, um Ihrer Organisation als vertrauenswürdiger Finanzberater zu dienen

Zielgruppe

- Informationssicherheits-Direktoren
- Informationssicherheits-Manager
- Informationssicherheits-Leiter
- Alle, die eine Führungsposition im Bereich Informationssicherheit anstreben

Geschäftsorientierte Lernergebnisse

- Effektiv mit Ihrem CFO und dem Finanzteam kommunizieren, da Sie dieselbe Sprache sprechen
- Ihre Ideen und Initiativen mit soliden Finanzdaten präsentieren, um Investitionen selbstbewusst zu rechtfertigen und die Zustimmung der Organisationsführung zu erhalten
- Ein wiederholbares Finanz-Framework mit acht Schritten anwenden, um die Kommunikation zu Finanzthemen effektiver zu gestalten
- Die finanziellen Ziele einer Organisation erkennen und erfolgreich interpretieren
- Das Cybersicherheitsprogramm an den strategischen Prioritäten der Organisation ausrichten
- Ein besseres Verständnis für geschäftliche Entscheidungen und Kompromisse im Unternehmen entwickeln
- Partnerschaften mit wichtigen Führungskräften verbessern, indem Sie finanzielle Expertise und strategisches Denken demonstrieren

Russell Eubanks
Kursautor

Wäre es nicht besser, sich wirklich mit den Geschäftsfinanzen auszukennen, bevor Sie weitere Arbeitszeit für Cybersicherheitsprojekte aufwenden oder jeden Euro Ihres Sicherheitsbudget einzeln aushandeln müssen? Bei finanzieller Verantwortung geht es nicht nur um Budgets, sondern darum, fundierte, strategische Entscheidungen zu fällen, die sowohl die Sicherheit als auch den geschäftlichen Erfolg fördern.

Im Kurs Business Finance Essentials lernen Sie nicht nur Konzepte – Sie wenden sie auch an. Durch praktische Übungen bauen Sie einen überzeugenden Business Case für Investitionen in die Cybersicherheit auf und entwerfen ein mehrjähriges Budget. Diese praktischen Frameworks dienen als Vorlagen für Entscheidungen in der wirklichen Welt. Sie sorgen dafür, dass Sie auf allen Ebenen Ihrer Organisation selbstbewusst für Cybersicherheit argumentieren können.

Dieser Kurs vermittelt Ihnen Kompetenzen in Geschäftsfinanzen und Entscheidungsfällung, die Sie benötigen, um den Wert der Cybersicherheit effektiv zu vermitteln, kritische Investitionen zu rechtfertigen und Cybersicherheitsinitiativen mit geschäftlichen Prioritäten in Einklang zu bringen. Die Kenntnisse und Tools, die Sie bei SEC405™ erwerben, verbessern nicht nur Ihre Führungskompetenz, sondern befähigen auch Ihr Team und stärken die finanzielle Situation und den Sicherheitsstatus Ihrer Organisation.

Was macht Kompetenz in Geschäftsfinanzen aus?

Kompetenz in Geschäftsfinanzen ist die Fähigkeit, finanzielle Prinzipien zu verstehen und anzuwenden, um fundierte Geschäftsentscheidungen zu fällen. Für Fachkräfte im Bereich der Cybersicherheit ist es entscheidend wichtig, diese Kompetenz zu entwickeln, damit sie Sicherheitsinitiativen mit Geschäftszielen in Einklang bringen, weitere Geldmittel sichern und effektiv mit der Organisationsführung kommunizieren können. Fachkräfte im Bereich der Cybersicherheit können von diesen Kenntnissen profitieren und sich durch ihre Anwendung bei der Organisationsführung profilieren.

Praktischer Business Case und Schulung zur Budgetplanung

In den praktischen Übungen in diesem Kurs entwickeln Sie Ihre Fähigkeit weiter, Investitionen in Cybersicherheit zu rechtfertigen, Ressourcen effizient zuzuweisen und Sicherheitsinitiativen mit geschäftlichen Zielen in Einklang zu bringen. Sie erstellen einen klaren Business Case, in dem Sie Investitionen in die Cybersicherheit auf eine Weise strukturieren und rationalisieren, die die Prioritäten und finanziellen Ziele der Organisation unterstützt. Diese praktische Übung vermittelt Ihnen das nötige Wissen, um den Prozess effektiv in Ihrer beruflichen Rolle nachzuahmen.

Außerdem entwerfen Sie ein mehrjähriges Budget, durch das Sie wertvolle Einblicke in die strategische Planung gewinnen und lernen, welche Schritte nötig sind, um die Geldmittel für kritische Cybersicherheitsprojekte langfristig zu sichern. Diese Übungen vertiefen nicht nur die Kernkonzepte, sondern stellen wiederverwendbare Vorlagen und umsetzbare Kompetenzen dar, die Ihnen helfen:

- Effektiv mit dem Finanzteam zusammenzuarbeiten
- Starke finanzielle Verantwortung zu zeigen
- Sich als vertrauenswürdiger Finanzberater für Ihre Organisation zu positionieren

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC405**

KURSFORMATE SEC405

OnDemand

SEC566: Implementing and Auditing CIS Controls™

GCCC Critical Controls
giac.org/gccc

5	30	Über 17
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Sicherheitskontrollmaßnahmen anwenden, die auf tatsächlichen Bedrohungen basieren und messbar und skalierfähig sind, bekannte Angriffe zuverlässig stoppen und wichtige Informationen und Systeme von Organisationen schützen
- Die Bedeutung der einzelnen Kontrollmaßnahmen verstehen und wissen, welche Folgen es hat, wenn sie ignoriert werden
- Die defensiven Ziele erklären, die schnelle Gewinne zeitigen und die Transparenz von Netzwerken und Systemen verbessern
- Tools identifizieren und nutzen, die Kontrollmaßnahmen durch Automatisierung identifizieren
- Ein Scoring-Tool erstellen und damit die Effektivität der einzelnen Kontrollmaßnahmen messen
- Anhand spezifischer Kennzahlen eine Ausgangsbasis etablieren und die Effektivität der Sicherheitskontrollmaßnahmen messen
- CIS-Kontrollmaßnahmen kompetent zu Compliance und Standards wie PCI-DSS, das NIST Cybersecurity Framework (CSF), ISO 27000 und mehr zuordnen
- Einen Audit der einzelnen CIS-Kontrollmaßnahmen durchführen, wobei spezifische, bewährte Vorlagen, Checklisten und Skripts zur Unterstützung des Audit-Prozesses zur Verfügung gestellt werden

Zielgruppe

- Informationssicherungs-Auditoren
- Systemadministratoren oder Implementierungsbeauftragte
- Compliance-Analysten
- IT-Administratoren
- Personal oder Auftragnehmer des Verteidigungsministeriums
- Bundesbehörden oder -kunden
- Organisationen im Privatsektor, die ihre Sicherheitsverfahren verbessern und ihre Systeme schützen möchten
- Sicherheitsanbieter und Beratungsgruppen, die bei Frameworks für Informationssicherung auf dem Laufenden bleiben möchten

Berufliche Rollen im NICE Framework

- Security Control Assessor (SP-RSK-002)

Brian Ventura
Kursautor

Spektakuläre Cybersicherheitsattacken lassen erkennen, dass Offensivangriffe besser sind als die Defensivmaßnahmen. Ingenieure und Auditoren im Bereich der Cybersicherheit und Mitglieder von Datenschutz- und Compliance-Teams fragen sich, wie sie ihre Systeme und Daten praktisch schützen und verteidigen können und wie sie eine Prioritätenliste von Schutzmaßnahmen für Cybersicherheit umsetzen können. Bei SANS SEC566™ lernen die Teilnehmer, wie eine Organisation ihre Informationen durch einen geprüften Standard für Cybersicherheits-Kontrollmaßnahmen verteidigen kann. Die Teilnehmer lernen insbesondere, wie sie die Sicherheitskontrollmaßnahmen implementieren, managen und beurteilen können, die in den CIS-Kontrollmaßnahmen des Center for Internet Security definiert sind. Die Teilnehmer erwerben direkte Kenntnisse der CIS-Kontrollmaßnahmen und des Ökosystems der Tools, mit denen die CIS-Kontrollmaßnahmen in den komplexen Netzwerken, einschließlich Cloud-Assets, eines Unternehmens implementiert werden.

Geschäftsorientierte Lernergebnisse

- Die wichtigsten Cyberrisiken effizient reduzieren
- Compliance-Anforderungen mit Sicherheits- und Geschäftszielen und -lösungen in Einklang bringen
- Der Organisationsführung den Status der defensiven Bemühungen zur Cybersicherheit klar und im geschäftlichen Kontext vermitteln
- Beruhigt sein, dass Ihre Organisation eine umfassende Strategie für Verteidigung und Compliance hat

Zusammenfassung der Kursinhalte

TEIL 1: Einführung und Übersicht über die CIS Critical Controls

TEIL 2: Datenschutz, Identität und Authentifizierung, Zugriffskontrollmanagement, Audit-Protokollmanagement

TEIL 3: Schutzmaßnahmen für Server, Workstation, Netzwerkgeräte (Teil 1)

TEIL 4: Schutzmaßnahmen für Server, Workstation, Netzwerkgeräte (Teil 2)

TEIL 5: Governance und betriebliche Sicherheit

„SEC566 war für mich sehr nützlich. Ich dachte, ich kenne mich mit Sicherheitskontrollmaßnahmen aus, aber dieser Kurs hat mir gezeigt, dass ich lediglich die Grundlagen kannte. Nun habe ich fundierte Kenntnisse auf dem Gebiet."
– Keri Powell, **Textron**

„Nach diesem Kurs freute ich mich, zur Arbeit zurückzukehren, meinen Schwachstellenscanner zu verbessern und meine Scans durchzuführen."
– Jason Hinojosa, **Rush Enterprises**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/SEC566**

KURSFORMATE SEC566

Präsenzkurs | **Live online** | **OnDemand**

FOKUSBEREICH IM SANS-LEHRPLAN

Digitale Forensik & Incident Response (DFIR) und Threat Hunting

Organisationen aller Größen brauchen Personal, das Incident-Response-Techniken meistern kann, damit kompromittierte Systeme korrekt identifiziert, Lücken effektiv eingedämmt und Vorfälle rasch behoben werden.

Auch Regierungs- und Strafverfolgungsbehörden benötigen kompetentes Personal, das Medien-Exploitation durchführen und wichtige Indizien von Systemen und Geräten ihrer Kontrahenten sichern kann. SANS-Kurse zu Incident Response, Threat Hunting und digitaler Forensik vermitteln die folgenden Kompetenzen:

- Den Gegner vor und während eines Vorfalls unternehmensweit aufspüren
- Detaillierte Kenntnisse in digitaler Forensik für die Betriebssysteme Microsoft Windows, Linux und Apple OSX erlangen
- Smartphones und Mobilgeräte auf Malware und Digitalforensik-Artefakte untersuchen
- Netzwerkforensik in die Ermittlungen integrieren, um bessere Erkenntnisse zu erlangen und Aufgaben schneller zu erledigen
- Arbeitsspeicher-Forensik in die Ermittlungen integrieren, um alle Möglichkeiten auszuschöpfen
- Neue Indizienquellen, die nur in der Cloud existieren, sichten, konservieren, konfigurieren und untersuchen und diese neuen Quellen in die Ermittlungen integrieren
- Die Fähigkeiten von Malware verstehen, um daraus Threat Intelligence abzuleiten, auf Informationssicherheits-Vorfälle zu reagieren und die Verteidigung zu stärken
- Cyber Threat Intelligence aus APT-Intrusionen (Advanced Persistent Threat) identifizieren, extrahieren, priorisieren und nutzen
- Erkennen, dass ein ordentlich ausgebildeter Incident Responder möglicherweise das einzige Bollwerk ist, das eine Organisation während einer Kompromittierung schützt
- Daten aus einer Fülle verschiedener Speichergeräte und Repositorys identifizieren, sammeln, konservieren und darauf reagieren, und dabei sicherstellen, dass die Integrität der Indizien über jeden Vorwurf erhaben bleibt
- Mit den Besonderheiten von Ransomware umzugehen wissen, um sich auf Ransomware-Angriffe vorzubereiten, sie zu erkennen, zu verfolgen, darauf zu reagieren und mit den Folgen umzugehen
- Threat Intelligence im cyberkriminellen Untergrund aufspüren: mit HUMINT-Techniken in Form von Informanten und mit Blockchain-Analysetools zur Nachverfolgung krimineller Kryptowährungs-Transaktionen

„Diese Schulungen sind für Praktiker von unschätzbarem Wert! Die Tools und die Kenntnisse, die Sie hier erlangen, sind einfach ausgezeichnet!“

– James Tayler, **Context Information Security**

Berufliche Rollen bei DFIR und Threat Hunting:

- Threat Hunter
- Analyst für digitale Forensik
- Malware-Analyst
- Cloud-Sicherheitsanalyst
- Incident Responder
- Analyst für Medienexploitation
- Analyst für Bedrohungsinformationen
- Strafverfolger

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

GBFA
Battlefield Forensics and Acquisition
giac.org/gbfa

6	36	34
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

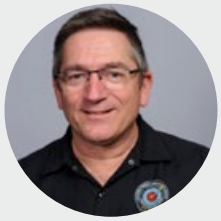
- Tools, Techniken und Verfahren erlernen und meistern, die benötigt werden, um Daten überall, wo sie gespeichert sind, effektiv zu finden, zu identifizieren und zu erfassen
- Spurensicherung am Tatort durchführen, damit Indizien unversehrt erhalten bleiben
- Daten aus Datenspeichern im Ruhezustand erfassen, sowohl von rotierenden Medien als auch von Solid-State-Speichern
- Zahlreiche Orte identifizieren, an denen sich Daten für die Ermittlungen befinden könnten
- Zur Forensik im Ernstfall innerhalb von 90 Minuten von der Indizienbeschlagnahme zu verwertbaren Informationen gelangen
- Bei der Vorbereitung der nötigen Dokumentation helfen, die zur Kommunikation mit Online-Unternehmen wie Google, Facebook, Microsoft usw. benötigt wird
- Die Konzepte und Nutzung von großvolumigen Speichertechnologien verstehen, u. a. JBOD, RAID-Speicher, NAS-Geräte und andere große, netzwerkadressierbare Speicher
- Benutzerdaten in großen Unternehmensumgebungen, in denen mit SMB darauf zugegriffen wird, identifizieren und erfassen
- Flüchtige Daten wie z. B. den RAM eines Computersystems erfassen
- Digitale Beweise auf Smartphones oder anderen tragbaren Geräten erfassen und korrekt konservieren

Zielgruppe

- Beschäftigte bei Strafverfolgungsbehörden
- Notfalldienste
- Analysten für digitale Forensik
- Fachkräfte für Informationssicherheit
- Mitglieder von Incident Response Teams
- Analysten für Medienexploitation
- Fachkräfte beim Verteidigungsministerium und den Nachrichtendiensten
- Alle, die verstehen möchten, wie man Systeme richtig konserviert, und die einen Hintergrund in Informationssystemen, Informationssicherheit und Computern haben

Berufliche Rollen im NICE Framework

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



Kevin Ripa
Kursautor

Eric Zimmerman
Kursautor

Die Uhr tickt. Sie müssen den wertvollsten Indizien bei der Verarbeitung Priorität einräumen. Wir zeigen Ihnen, wie!

FOR498™, ein Schulungskurs in digitaler Forensikakquisition, vermittelt die nötigen Kompetenzen zur Identifizierung der zahlreichen und vielfältigen Datenspeichermedien, die heute verwendet werden, und zeigt, wie diese Daten unabhängig von Speichermethode und -ort für die Forensik erfasst und konserviert werden können. Er deckt die digitale Akquisition von Computern, tragbaren Geräten und Netzwerken und aus der Cloud ab. Anschließend lernen die Teilnehmer, eine schnelle Triage durchzuführen, bei der umsetzbare Informationen identifiziert und in 90 Minuten oder noch schneller von einer Festplatte extrahiert werden.

FOR498 hilft Ihnen:

- Daten von folgenden Geräten effektiv zu erfassen:
  - PCs, Microsoft Surface und Tablets
  - Apple-Geräte, Mac und Macbooks
  - RAM (Arbeitsspeicher)
  - Smartphones und tragbare Mobilgeräte
  - Cloud-Speicher und -Services
  - Netzwerkspeicher-Repositorys
  - Umgebungen mit virtuellen Maschinen
- Innerhalb von 90 Minuten oder noch schneller umsetzbare Informationen vorzulegen

Zusammenfassung der Kursinhalte

TEIL 1: Tatortvorbereitung, Management und Speicherschnittstellen

TEIL 2: Tragbare Geräte und Akquisitionsverfahren

TEIL 3: Triage und Datenakquisition

TEIL 4: Akquisition von nicht herkömmlichen Geräten und aus der Cloud

TEIL 5: Akquisition von Apple und aus dem Internet der Dinge

TEIL 6: Über Forensiktools hinaus: Eingehendere Betrachtung

„FOR498 bietet eine solide Grundlage für neue Forensikspezialisten, die Indizien erfassen und triagieren müssen. Die Laborübungen bieten verschiedene Möglichkeiten, grundlegende und komplexe Szenarien zur Datenakquisition zu üben."

– Chris G., **US-Bundesbehörde**

„Bei DFIR geht selten alles nach Plan. In diesem Kurs lernen Sie, wie Sie die Kontrolle behalten können, wenn die Dinge nicht wie erwartet laufen."

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

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR498**

KURSFORMATE FOR498

Präsenzkurs | **Live online** | **OnDemand**

FOR500: Windows Forensic Analysis™

GRUNDLEGEND ÜBERARBEITET

GCFE Forensic Examiner
giac.org/gcfe
CyberLive
DoD 8140*

6	36	22
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Eingehende Forensikanalyse des Betriebssystems Windows und Medienexploitation durchführen
- Speicherorte von Artefakten und Indizien identifizieren, um entscheidende Fragen zu beantworten
- Vom individuellen Tool unabhängig werden und sich stattdessen auf Analysefähigkeiten konzentrieren
- Entscheidende Ergebnisse extrahieren und Forensikfähigkeiten innerhalb der Organisation aufbauen
- Strukturierte Analysetechniken schaffen, die in jeder Sicherheitsrolle zum Erfolg verhelfen

Zielgruppe

- Fachkräfte für Informationssicherheit, die sich eingehend in die Konzepte digitaler Forensikuntersuchungen in Windows einarbeiten möchten
- Mitglieder des Incident Response Teams, die mithilfe von eingehender Digitalforensik Fälle von Datenschutzverletzungen und Intrusionen in Windows lösen, den Schaden beurteilen und Anzeichen für eine Kompromittierung entwickeln müssen
- Strafverfolgungs-, Geheimdienst- und Kriminalbeamte, die Fachexperten für digitale Forensik in Windows-basierten Betriebssystemen werden möchten
- Analysten für Medienexploitation, die taktische Exploitation und DOMEX (Document and Media Exploitation) meistern müssen
- Alle, die ein fundiertes Verständnis der Windows-Forensik entwickeln möchten und die einen Hintergrund in Informationssystemen, Informationssicherheit und Computern haben

Berufliche Rollen im NICE Framework

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

Heather Barnhart
Kursautorin

Rob Lee
Kursautor

Mattia Epifani
Kursautor

Ovie Carroll
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Meistern Sie die Windows-Forensik – denn Unbekanntes können Sie nicht schützen.

FOR500: Windows Forensic Analysis™ konzentriert sich darauf, fundierte Kenntnisse für die Digitalforensik in Microsoft Windows-Betriebssystemen aufzubauen. Sie können nicht schützen, was Sie nicht kennen. Deshalb ist das Verständnis der Forensikkompetenzen und der verfügbaren Artefakte eine Kernkomponente der Informationssicherheit. Sie lernen, wie Sie forensische Daten auf Windows-Systemen wiederherstellen, analysieren und authentifizieren, die Aktivität einzelner Benutzer in Ihrem Netzwerk verfolgen und die Erkenntnisse zur Nutzung bei Incident Response, internen Ermittlungen, Untersuchungen zum Diebstahl geistigen Eigentums und zivil- oder strafrechtlichen Gerichtsverfahren aufbereiten. Damit können Sie Sicherheitstools validieren, Schwachstellenbeurteilungen verbessern, Bedrohungen durch Insider identifizieren, Hacker verfolgen und Sicherheitsrichtlinien verbessern. Ob Sie es wissen oder nicht: Windows zeichnet in aller Stille eine unglaubliche Menge an Daten über Sie und Ihre Benutzer auf. Bei FOR500™ lernen Sie, wie Sie diesen Datenberg für Ihre Zwecke nutzen können.

Geschäftsorientierte Lernergebnisse

- Innerhalb der Organisation die Fähigkeit für digitale Forensik aufbauen, damit wichtige geschäftliche Fragen schnell beantwortet und Straftaten untersucht werden können
- Mithilfe eingehender digitaler Forensik Fälle von Datenschutzverstößen in Windows lösen
- Verstehen, welche Fülle von Telemetrie in Windows Enterprise verfügbar ist
- Speicherorte von Forensikartefakten und Indizien identifizieren, um entscheidende Fragen zu beantworten
- Ein vorgefertigtes Forensiklabor aus kostenlosen Open-Source-Tools und kommerziellen Tools erhalten
- Durch einen Fokus auf Analysetechniken Ermittlungsfähigkeiten aufbauen, die vom individuellen Tool unabhängig sind

Zusammenfassung der Kursinhalte

TEIL 1: Digitale Forensik und erweiterte Datentriage
TEIL 2: Registry-Analyse, Anwendungsausführung und Cloud-Speicherforensik
TEIL 3: Shell-Komponenten und Profilierung von Wechseldatenträgern
TEIL 4: E-Mail-Analyse, Windows-Suche, SRUM und Ereignisprotokolle
TEIL 5: Web-Browser-Forensik
TEIL 6: Windows-Forensikübung

„Dies ist ein sehr intensiver Kurs mit extrem aktuellem Kursmaterial, der meiner Erfahrung nach nirgendwo sonst angeboten wird."
– Alexander Applegate, **Universität Auburn**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR500**

KURSFORMATE FOR500

Präsenzkurs | **Live online** | **OnDemand**

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics™ GRUNDLEGEND ÜBERARBEITET

GCFA Forensic Analyst giac.org/gcfa — ANAB ACCREDITED ISO/IEC 17024 PERSONNEL CERTIFICATION BODY — CyberLive DoD 8140*

6	36	Über 35
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Tools und Techniken zur Erkennung, Eindämmung und Sanierung von Angriffen meistern
- Aktive, inaktive und angepasste Malware in Windows-Systemen unternehmensweit feststellen
- Bedrohungen aufspüren und im großen Stil auf Vorfälle reagieren
- Malware-Beaconing, Lateralbewegung und C2-Aktivitäten durch Arbeitsspeicheranalyse und Windows-Hostforensik identifizieren
- Datenschutzverstöße analysieren, um die Grundursache, Angriffsvektoren und Persistenzmechanismen festzustellen
- Antiforensiktechniken kontern, gelöschte Daten wiederherstellen und Angreiferaktivität verfolgen
- Mithilfe von Forensiktools Bedrohungen beheben und das Unternehmen sichern

Zielgruppe

- Mitglieder von Incident Response Teams
- Threat Hunter
- Analysten im Security Operations Center
- Erfahrene Analysten für digitale Forensik
- Fachkräfte für Informationssicherheit
- Beschäftigte bei Strafverfolgungsbehörden
- Mitglieder eines Red Teams, Penetrationstester und Exploit-Entwickler
- Absolventen von SANS FOR500 und SEC504, die ihre Kompetenzen ausbauen möchten

Berufliche Rollen im NICE Framework

- 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
Kursautor

Mike Pilkington
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Taktiken und Verfahren für Threat Hunting und Incident Response entwickeln sich rapide weiter. Ihr Team kann es sich nicht mehr leisten, antiquierte Techniken für Incident Response und Threat Hunting einzusetzen, die kompromittierte Systeme nicht korrekt identifizieren, Übergriffe nur ineffektiv eindämmen und letztlich den Vorfall nicht schnell beheben oder Ransomware nicht an der Verbreitung hindern können. Teams für Incident Response und Threat Hunting sind von entscheidender Bedeutung, wenn es darum geht, Anzeichen für Malware und Aktivitätsmuster zu identifizieren und zu beobachten, um präzise Threat Intelligence zu generieren, mit der sich aktuelle und zukünftige Intrusionen erkennen lassen. Dieser intensive Kurs in Incident Response und Threat Hunting vermittelt Einsatzkräften und Threat-Hunting-Teams die fortgeschrittenen Kompetenzen, die sie benötigen, um eine Fülle von Bedrohungen in Unternehmensnetzwerken (u. a. APT von staatlichen Gegnern, Syndikaten des organisierten Verbrechens, Ransomware-Angreifern und Hacktivisten) aufzuspüren, zu identifizieren, zu beheben und sich davon zu erholen.

Geschäftsorientierte Lernergebnisse

- Verstehen, wie Angreifer vorgehen, und proaktive Kompromittierungsbewertungen durchführen
- Detektionsfähigkeiten verbessern
- Threat Intelligence entwickeln, um erkannte Gegner zu verfolgen und sich auf zukünftige Übergriffe vorzubereiten
- Erweiterte Forensikkompetenzen aufbauen, um Antiforensik zu kontern

Zusammenfassung der Kursinhalte

TEIL 1: Erweiterte Incident Response und Threat Hunting

TEIL 2: Intrusionsanalyse

TEIL 3: Arbeitsspeicherforensik bei Incident Response und Threat Hunting

TEIL 4: Analyse des zeitlichen Verlaufs

TEIL 5: Incident Response und Hunting im gesamten Unternehmen | Erweiterte Detektion von Gegnern und Antiforensik

TEIL 6: Übung: APT Threat Group Incident Response

„So viele Inhalte! Endlich kann ich mich in die Materie vertiefen und Dinge lernen, die mir schon so lange ein Rätsel sind! Die Schulung FOR508 erklärt komplizierte Sachverhalte auf leicht verständliche Weise, und noch viel mehr. Der Kurs hat mir sehr gut gefallen."

– Zachary T., **US-Bundesregierung**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR508**

KURSFORMATE FOR508

Präsenzkurs | **Live online** | **OnDemand**

FOR509: Enterprise Cloud Forensics and Incident Response™

GRUNDLEGEND ÜBERARBEITET

GCFR Cloud Forensics Responder
giac.org/gcfr

CyberLive

6	36	22
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Forensische Daten verstehen, die nur in der Cloud verfügbar sind
- Best Practices bei der Cloud-Protokollierung für DFIR umsetzen
- Mit Ressourcen aus Microsoft Azure, AWS and Google Cloud Platform Indizien sammeln
- Verstehen, welche Protokolle Microsoft 365 und Google Workspace für Analysten zur Prüfung bereithalten
- Forensische Verfahren in die Cloud verlagern, um die Datenverarbeitung zu beschleunigen

Zielgruppe

- Mitglieder von Incident Response Teams
- Threat Hunter
- SOC-Analysten
- Erfahrene Analysten für digitale Forensik
- Fachkräfte für Informationssicherheit
- Fachkräfte bei Strafverfolgungsbehörden
- Absolventen von SANS FOR500, FOR508, SEC541 und SEC504, die ihre Toolbox für Cloud-basierte Forensik erweitern möchten

Berufliche Rollen im NICE Framework

- 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
Kursautor

Pierre Lidome
Kursautor

Josh Lemon
Kursautor

Megan Roddie-Fonseca
Kursautorin

Finden Sie sich im Wolkennebel der Cloud zurecht?

Die Welt ist im steten Wandel, und das gilt auch für die Daten, mit denen wir unsere Untersuchungen durchführen. Datenspeicherung und -zugriff funktionieren auf Cloud-Plattformen anders. Der Ermittler ist nicht in der Lage, direkt auf Systeme zuzugreifen und herkömmliche Methoden zur Datenextrahierung zu nutzen. Leider versuchen viele Ermittler, alte Methoden, die für Untersuchungen vor Ort entwickelt wurden, auf Plattformen in der Cloud zu übertragen. Aber anstatt sich gegen den Wandel zu sträuben, müssen Ermittler lernen, die neuen Chancen zu nutzen, die sich ihnen in Form neuer Indizienquellen bieten. FOR509: Enterprise Cloud Forensics and Incident Response™ bringt Ermittler in der von rapidem Wandel geprägten Welt der Enterprise-Cloud-Umgebungen auf den neuesten Stand, denn der Kurs deckt neue Indizienquellen auf, die es nur in der Cloud gibt.

Geschäftsorientierte Lernergebnisse

- Digitale Forensik und Incident Response in der Cloud verstehen
- Schädliche Aktivitäten in der Cloud identifizieren
- Cloud-native Tools und Services für DFIR kosteneffektiv nutzen
- Sicherstellen, dass das Unternehmen bereit ist, auf Vorfälle in der Cloud zu reagieren
- Dafür sorgen, dass Widersacher weniger Zeit in kompromittierten Cloud-Implementierungen verbringen

Zusammenfassung der Kursinhalte

TEIL 1: Microsoft 365 und Graph API

TEIL 2: Microsoft Azure

TEIL 3: Amazon Web Services (AWS)

TEIL 4: Google Workspace

TEIL 5: Google Cloud

TEIL 6: Übung: Intrusion in einer Multicloud-Umgebung

„Dieser Kurs ist meiner Meinung nach prima für eine wirklich komprimierte Einführung, welche verschiedenen Cloud-Serviceanbieter es gibt und was dort in Bezug auf die Forensik möglich ist."

– Marc Stroebel, **HvS-Consulting AG**

„FOR509 war einfach klasse! Das fundierte Wissen ist ohne gleichen. Das wird in Zukunft bestimmt ein beliebter Kurs."

– Terrie Myerchin, **AT&T**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR509**

KURSFORMATE FOR509

Präsenzkurs | **Live online** | **OnDemand**

FOR518: Mac and iOS Forensic Analysis and Incident Response™

GRUNDLEGEND ÜBERARBEITET

GIME
iOS and macOS Examiner
giac.org/gime

6	36	23
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Die feinen Unterschiede zwischen macOS- und iOS-Geräten verstehen
- Eingehend betrachten, wie die Apple-Magie zwischen verschiedenen Geräten funktioniert und wie das bei Ermittlungen helfen kann
- Die Bedeutung der einzelnen Dateisystemdomänen ermitteln und feststellen, wie Daten organisiert sind
- Eine zeitliche Analyse eines Systems durchführen, indem Datendateien und Protokollanalyse zueinander in Beziehung gesetzt werden
- Ein Profil dazu erstellen, wie Personen das System genutzt haben, u. a. wie oft sie es verwendet haben, welche Anwendungen sie häufig nutzen und welche persönlichen Systemeinstellungen sie haben
- Remote und lokale Datensicherungen, Disk-Images oder andere angeschlossene Geräte identifizieren
- Verschlüsselte Container und FileVault-Volumen finden, Keychain-Daten verstehen und Mac-Passwörter knacken
- macOS-Metadaten und ihre Bedeutung in der Spotlight-Datenbank, Time Machine und erweiterten Attributen analysieren und verstehen
- Safari Web Browser, Apple Mail und zahlreiche weitere Anwendungen durch Untersuchung ihrer internen Datenbanken eingehend kennenlernen

Zielgruppe

- Erfahrene Analysten für digitale Forensik
- Beamte, Beschäftigte und Ermittler bei Strafverfolgungsbehörden
- Analysten für Medienexploitation
- Mitglieder von Incident Response Teams
- Fachkräfte für Informationssicherheit
- Absolventen von SANS FOR500, FOR508, FOR526, FOR585 und FOR610, die ihre Forensikkompetenzen abrunden möchten

Berufliche Rollen im NICE Framework

- 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
Kursautorin

FOR518™ ist der erste Kurs in Incident Response und Forensik für Mac und iOS, der nicht von den Anbietern selbst ausgeht, sich auf die Rohdaten und eingehende, detaillierte Analyse konzentriert und den Teilnehmern vermittelt, wie sie ihre Mac- und iOS-Fälle optimal angehen. Die intensiven, praktischen Kompetenzen in Forensikanalyse und Incident Response, die in diesem Kurs vermittelt werden, befähigen Analysten, ihre Fertigkeiten zu erweitern und beliebige Mac- oder iOS-Geräte souverän und sachkundig zu analysieren.

Geschäftsorientierte Lernergebnisse

- Beschäftigte befähigen, verschiedene Straftaten zu untersuchen, z. B. Computermissbrauch, schädliche Geräteübergriffe, Wirtschaftsspionage, Bedrohungen durch Insider und Betrug
- Lernen, wie verschiedene Apple-Daten gespeichert werden und wie Analysen mit Methoden durchgeführt werden, die von individuellen Tools unabhängig sind, sodass keine teuren kommerziellen Forensiktools angeschafft werden müssen
- Verschiedene Forensikartefakte und feine Unterschiede zwischen den Apple-Plattformen (macOS und iOS) identifizieren
- Die Vielzahl der Informationen zu Benutzern verstehen, die zeigen können, wie ein Gerät verwendet oder missbraucht wurde
- Lernen, welche Unterschiede zwischen Forensik und Sicherheitsbewertungen bei Apple-Geräten im Gegensatz zu anderen Betriebssystemen bestehen, die in der Branche Standard sind

Zusammenfassung der Kursinhalte

TEIL 1: Grundlagen von Mac und iOS

TEIL 2: Protokollanalyse, Benutzerdaten und Systemkonfiguration

TEIL 3: Dateisysteme und zugehörige Artefakte

TEIL 4: Analyse von Anwendungsdaten

TEIL 5: Erweiterte Analysethemen

TEIL 6: Übung: Mac-Forensik und Incident Response

„Interessant war, dass bestimmte ‚Forensik'-Tools Daten als verschlüsselt melden konnten, obwohl man andere Daten dennoch erfassen konnte."

– Gary Titus, **Stroz Friedberg LLC**

„Der umfassendste Mac-Kurs, den ich je absolviert habe."

– Daniel M., **US-Bundesbehörde**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR518**

KURSFORMATE FOR518

Präsenzkurs | **Live online** | **OnDemand**

KURS NEU IM FOKUS

FOR528: Ransomware and Cyber Extortion™

4	24	13
Tage Programm	CPEs	Laborübungen

Vermittelte Konzepte

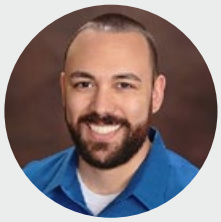
- Wie Ransomware sich zu einem großen Geschäft entwickelt hat
- Wie HumOR-Operatoren sich zu gut aufeinander eingespielten Angriffsteams entwickelt haben
- Wer und welche Organisationen das größte Risiko tragen, Ransomware zum Opfer zu fallen
- Wie Ransomware-Operatoren in die Umgebungen ihrer Opfer eindringen
- Wie Sie reagieren, wenn Ransomware aktiv in Ihrer Umgebung ausgeführt wird
- Welche Schritte Sie nach einem Ransomware-Angriff ergreifen
- Wie Sie Ihre Organisation am besten auf HumOR-Bedrohungen vorbereiten
- Wie Sie die Tools identifizieren, die HumOR-Operatoren oft nutzen, um während eines Ransomware-Angriffs in ein System einzudringen und Post-Exploitation-Aktivitäten durchzuführen
- Wie sich Ransomware- und Cybererpressungs-Kampagnen unterscheiden
- Wie Sie Ransomware-Operatoren innerhalb Ihres Netzwerks aufspüren
- Wie Sie Datenzugriff und -exfiltrierung identifizieren

Zielgruppe

- Fachkräfte für Informationssicherheit
- Mitglieder von Incident Response Teams
- Vorfalls-Triageanalysten
- Anbieter von gemanagten Services und Analysten bei Anbietern von gemanagten Sicherheitsservices
- Beamte, Beschäftigte und Ermittler bei Strafverfolgungsbehörden
- IT-Personal im Gesundheitssektor und Gastgewerbe
- Alle, die an einem tieferen Verständnis der Incident Response speziell bei Ransomware interessiert sind

Berufliche Rollen im NICE Framework

- 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
Kursautor

Schluss mit menschlich bedienter Ransomware – ein für alle Mal!

FOR528™ ist eine praktische Schulung für alle, die möglicherweise auf Ransomware-Vorfälle reagieren müssen. Der Begriff „Ransomware“ bezieht sich nicht mehr nur auf jemanden, der Ressourcen verschlüsselt und dadurch dem Zugriff entzieht. Der Siegeszug von HumOR (Human-Operated Ransomware) und RaaS (Ransomware-as-a-Service) hat ein ganzes Ökosystem von gut geplanten Angriffskampagnen geschaffen, bei denen ein Mensch an der Tastatur sitzt. Unser Kurs vermittelt Analysten mithilfe von ausgeklügelten Angriffen aus der wirklichen Welt und den von ihnen hinterlassenen Forensikartefakten alles, was sie für ihre Reaktion brauchen, wenn die Bedrohung Wirklichkeit wird.

Geschäftsorientierte Lernergebnisse

- Die Verteidigung durch die Implementierung von Präventivmaßnahmen stärken, die verhindern, dass Ransomware-Akteure Zugang zu Ihrer Organisation erhalten
- Schnell erkennen, wenn ein Ransomware-Akteur Zugang zu Ihrer Umgebung erlangt hat und Tools nutzt, die bei Ransomware häufig zum Einsatz kommen
- Identifizieren, wie Ransomware-Angriffe aussehen, um leichter einen Reaktionsplan auszuarbeiten, falls sie im Netzwerk erkannt werden
- Wissen, wo Sie in Ihrer individuellen Umgebung Ihre Bemühungen konzentrieren müssen, und daher schnell reagieren
- Identifizieren, welche Backups zur Wiederherstellung verwendet werden sollten, damit sie erfolgreich verläuft, ohne dass der Zugriff des Akteurs auf die Umgebung ebenfalls wiederhergestellt wird
- Feststellen, ob ein identifizierter Akteur in Ihrer Umgebung mit Ransomware in Verbindung steht
- Identifizieren, wie und wann auf welche Daten zugegriffen wurde
- Identifizieren, welche Daten von einem Ransomware-Akteur exfiltriert wurden
- Dieser Kurs bereitet Sie auf die GWEB-Zertifizierung vor, die die Anforderungen von DoD8140 IAT Level 2 erfüllt

Zusammenfassung der Kursinhalte

TEIL 1: Grundlagen der Incident Response bei Ransomware

TEIL 2: Der Modus Operandi von Ransomware

TEIL 3: Erweiterte Konzepte von Ransomware

TEIL 4: Übung: Incident Response bei Ransomware

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR528**

KURSFORMATE FOR528

Präsenzkurs | **Live online** | **OnDemand**

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response™ GRUNDLEGEND ÜBERARBEITET

GNFA Network Forensic Analyst | CyberLive
giac.org/gnfa

6	36	18
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Dateien aus Netzwerkpaket-Erfassungen und Proxy-Cache-Dateien extrahieren, damit die Malware anschließend analysiert oder definitiv festgestellt werden kann, welche Daten verloren gingen
- Anhand historischer NetFlow-Daten relevante Netzwerkvorgänge in der Vergangenheit identifizieren, damit der Umfang des Vorfalls korrekt eingeschätzt werden kann
- Angepasste Netzwerkprotokolle durch Reverse-Engineering nachbilden, um zu identifizieren, welche Command-and-Control-Fähigkeiten ein Angreifer erhält und welche Aktionen er hier durchführt
- Erfassten SSL/TLS-Datenverkehr entschlüsseln, um zu identifizieren, welche Aktionen die Angreifer ergriffen und welche Daten sie aus dem Opfer extrahiert haben
- Mithilfe von Daten aus typischen Netzwerkprotokollen die Glaubwürdigkeit der Ermittlungsergebnisse erhöhen
- Gelegenheiten identifizieren, um zusätzliche Indizien basierend auf vorhandenen Systemen und Plattformen innerhalb einer Netzwerkarchitektur zu sammeln
- Datenverkehr mit verbreiteten Netzwerkprotokollen untersuchen, um Aktivitätsmuster oder spezifische Aktionen zu identifizieren, die weiter untersucht werden sollten
- Protokolldaten in einen umfassenden Analyseprozess integrieren und damit Wissenslücken schließen, die vielleicht weit zurückliegen
- Lernen, wie Angreifer mithilfe von Meddler-in-the-Middle-Tools scheinbar sichere Kommunikation abfangen

Zielgruppe

- Mitglieder von Incident Response Teams
- Mitglieder eines Hunt Teams
- Beamte, Beschäftigte und Ermittler bei Strafverfolgungsbehörden
- SOC-Personal und praktische Fachkräfte für Informationssicherheit
- Netzwerkverteidiger
- Informationssicherheitsmanager
- Netzwerkingenieure
- Fachkräfte für Informationssicherheit

Berufliche Rollen im NICE Framework

- 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
Kursautor

Übertragen Sie Ihre Kenntnisse in systembasierter Forensik auf das Netzwerk. Integrieren Sie Netzwerkforensik in Ihre Ermittlungen, um bessere Erkenntnisse zu erlangen und Aufgaben schneller zu erledigen.

Ob es in Ihrem Fall um eine Intrusion, Datendiebstahl oder Missbrauch durch Beschäftigte geht oder ob Sie einen Gegner proaktiv aufspüren – das Netzwerk bietet oft eine ganz eigene Sicht der Ereignisse. SANS FOR572™ deckt die Tools, Technologien und Verfahren ab, die Sie benötigen, wenn Sie Indizienquellen in Netzwerken in Ihre Ermittlungen integrieren möchten, um bessere Ergebnisse schneller bereitzustellen.

Bei FOR572™ konzentrieren wir uns auf die Kenntnisse, die erforderlich sind, um Kommunikation zu untersuchen und zu charakterisieren, die in der Vergangenheit stattgefunden hat oder noch läuft. Selbst wenn der versierteste Remote-Angreifer ein System mit einem nicht nachweisbaren Exploit kompromittiert hat, muss das System immer noch über das Netzwerk kommunizieren. Ohne Kanäle für Command-and-Control und Datenextrahierung wäre ein kompromittiertes Computersystem für den Angreifer praktisch wertlos. Anders gesagt: Böswillige Akteure reden – und wir bringen Ihnen bei, zuzuhören.

Geschäftsorientierte Lernergebnisse

- Die Ermittlungen Ihres Teams mit Netzwerkperspektiven ergänzen, die in allen Umgebungen inhärent sind
- Eine Ausgangsbasis aufbauen, die herangezogen werden kann, um schädliche Aktivitäten bereits in der Frühphase einer Komprimittierung zu identifizieren, bevor großer Schaden angerichtet wird
- Bestehende Netzwerkdatenerfassungen noch wertvoller machen, damit sie bestehende Betriebsanforderungen unterstützen
- Sicherstellen, dass entscheidende Beobachtungen aus dem Netzwerk bei proaktiven Untersuchungen oder nachträglichen IR-Maßnahmen nicht übersehen werden

Zusammenfassung der Kursinhalte

TEIL 1: Runter vom Datenträger und rein in die Ermittlung
TEIL 2: Kernprotokolle und Protokollaggregation/-analyse
TEIL 3: NetFlow und Dateizugriffprotokolle
TEIL 4: Kommerzielle Tools, Wireless- und Full-Packet-Hunting
TEIL 5: Verschlüsselung, Protokollumkehrung, OPSEC und Informationen
TEIL 6: Abschlussübung zur Netzwerkforensik

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR572**

KURSFORMATE FOR572

Präsenzkurs | **Live online** | **OnDemand**

KURS NEU IM FOKUS

FOR577: Linux Incident Response and Threat Hunting™

GLIR
Linux Incident Responder
giac.org/glir

6	36	26
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Tools, Techniken und Verfahren nutzen, die benötigt werden, um verschiedene Kontrahenten effektiv aufzuspüren, zu entdecken und einzudämmen, sowie um Vorfälle zu beheben
- Mit der SIFT-Workstation Linux-Systeme durchforsten und auf Vorfälle auf ihnen reagieren
- Ausgehendes Malware-Beaconing identifizieren und durch Analysetechniken zum Command-and-Control-Kanal zurückverfolgen
- Durch Identifizierung von Beachhead- und Spearphishing-Angriffsmechanismen feststellen, wie ein Übergriff erfolgt ist
- Durch detaillierte Timeline- und Super-Timeline-Analyse Benutzer- und Angreiferaktivitäten Sekunde für Sekunde im analysierten System verfolgen
- Lateralbewegung in Ihrem Unternehmenssystem identifizieren und zeigen, wie Angreifer von System zu System fortschreiten, ohne erkannt zu werden
- Datenbewegungen verfolgen, während die Angreifer kritische Daten sammeln und diese Daten zu Sammelpunkten für die Exfiltration verschieben
- Archive und Archivdateien (.rar, .tar usw.) wiederherstellen und analysieren, mit denen APT-ähnliche Angreifer sensible Daten aus dem Unternehmensnetzwerk exfiltrieren
- Anhand der gesammelten Daten effektive Abhilfemaßnahmen im gesamten Unternehmen durchführen

Zielgruppe

- Mitglieder von Incident Response Teams
- Threat Hunter
- Erfahrene Analysten für digitale Forensik
- Erfahrene Analysten im Security Operations Center
- Fachkräfte für Informationssicherheit
- Fachkräfte bei Strafverfolgungsbehörden
- Mitglieder eines Red Teams
- Penetrationstester
- Exploit-Entwickler
- Absolventen von SANS SEC401, SEC450, SEC504 und SEC500, die ihre Kompetenzen ausbauen möchten
- Absolventen von SANS SEC508, die lernen möchten, wie sie ihre Kompetenzen auf ein andere Betriebssystem übertragen können

Tarot (Taz) Wake
Kursautor

FOR577™ vermittelt Einsatzkräften und Threat Hunting-Teams die fortgeschrittenen Kompetenzen, die sie benötigen, um eine Fülle von Bedrohungen in Unternehmensnetzwerken (u. a. APT (Advanced Persistent Threat) von staatlichen Gegnern, Syndikaten des organisierten Verbrechens und Hacktivisten) aufzuspüren, zu identifizieren, zu beheben und sich davon zu erholen. Der Kurs wird kontinuierlich aktualisiert und befasst sich mit aktuellen Vorfällen. Er vermittelt praktische Taktiken und Techniken für Incident Response und Threat Hunting, die Elite-Einsatzkräfte und Threat Hunter erfolgreich zur Bekämpfung echter Übergriffsfälle einsetzen.

FOR577™ vermittelt Ihnen die Kompetenzen, die Sie benötigen, um Angriffe auf Linux-Plattformen zu identifizieren, zu analysieren und darauf zu reagieren. Außerdem lernen Sie, wie Sie mit Hunting-Techniken heimliche Angreifer aufspüren, die bestehende Kontrollmaßnahmen umgehen können. Die vermittelten Konzepte bauen insofern auf gemeinsamen Grundlagen auf, als wir Indizien sammeln, sie analysieren und anhand dieser Analyse Entscheidungen fällen, wobei der Fokus immer auf den Besonderheiten der Linux-Plattform liegt. Da Tools genutzt werden, die in die SANS-SIFT-Workstation integriert sind, bietet der Kurs eine allumfassende Lösung, mit der Einsatzkräfte schnell und effektiv auf ausgereifte Übergriffe reagieren können.

Geschäftsorientierte Lernergebnisse

- Verstehen, wie Angreifer vorgehen, und proaktive Kompromittierungsbewertungen durchführen
- Durch ein besseres Verständnis neuartiger Angriffstechniken und verfügbarer Forensikartefakte und durch Konzentration auf kritische Angriffspfade die Detektionsfähigkeiten verbessern
- Threat Intelligence entwickeln, um erkannte Gegner zu verfolgen und sich auf zukünftige Übergriffe vorzubereiten
- Erweiterte Forensikkompetenzen aufbauen, um Antiforensik zu kontern und vor Technikern verborgene Daten aufzudecken, damit sie in internen und externen Ermittlungen genutzt werden können

Zusammenfassung der Kursinhalte

TEIL 1: Incident Response und Analyse bei Linux

TEIL 2: Datenträgeranalyse und Indiziensammlung

TEIL 3: Protokollierung und Protokollanalyse bei Linux

TEIL 4: Live-Reaktion und flüchtige Daten

TEIL 5: Erweiterte Techniken der Incident Response

TEIL 6: Übung: APT Incident Response

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR577**

KURSFORMATE FOR577

Präsenzkurs | **Live online** | **OnDemand**

FOR578: **Cyber Threat Intelligence™**

GCTI
Cyber Threat Intelligence | DoD 8140*
giac.org/gcti

6	36	24
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Analysefähigkeiten entwickeln, um komplexe Szenarien besser zu verstehen, zu synthetisieren und zu nutzen
- Informationsbedürfnisse durch Praktiken wie Bedrohungsmodellierung identifizieren und erstellen
- Taktische, betriebliche und strategische Threat Intelligence verstehen und Kompetenzen darin entwickeln
- Threat Intelligence generieren, um fokussierte und zielgerichtete Bedrohungen zu entdecken, darauf zu reagieren und sie zu besiegen
- Erfahren, aus welchen verschiedenen Quellen Daten über den Gegner gesammelt werden können und wie Sie diese Daten flexibel nutzen
- Extern erhaltene Informationen validieren, damit falsche Informationen möglichst wenig Kosten verursachen

Zielgruppe

- Praktische Sicherheitsfachkräfte
- Mitglieder von Incident Response Teams
- Threat Hunter
- SOC-Personal und praktische Fachkräfte für Informationssicherheit
- Analysten für digitale Forensik und Malware
- Beamte bei Strafverfolgungsbehörden
- Technische Manager

Berufliche Rollen im NICE Framework

- 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
Kursautor

Rebekah Brown
Kursautorin

* DoD 8140 APPROVED
sans.org/8140

Am Besten lernt man vom Feind!

Cyber Threat Intelligence stellt einen starken Multiplikator für Organisationen dar, die ihre Reaktions- und Detektionsprogramme aktualisieren möchten, um mit immer ausgeklügelteren Bedrohungen fertig werden zu können. Malware ist das Tool des Kontrahenten, aber die wirkliche Bedrohung ist der Mensch. Bei Cyber Threat Intelligence geht es darum, diesen flexiblen und beharrlichen menschlichen Bedrohungen befähigte und geschulte menschliche Verteidiger entgegenzustellen. Während eines gezielten Angriffs braucht Ihre Organisation ein exzellentes und topaktuelles Threat-Hunting- oder Incident-Response-Team, das mit der nötigen Threat Intelligence gewappnet ist, um zu verstehen, wie Gegner operieren, und die Bedrohung zu kontern. FOR578™ vermittelt Ihnen und Ihrem Team die taktischen, betrieblichen und strategischen Kompetenzen für Cyber Threat Intelligence, die nötig sind, um Sicherheitsteams zu stärken, Threat Hunting präziser und Incident Response effektiver zu gestalten und in Organisationen das Bewusstsein einer Bedrohungslandschaft im Wandel zu stärken.

Geschäftsorientierte Lernergebnisse

- Verstehen, dass sich das Umfeld der Cyberbedrohungen ständig wandelt und was das für Ihre Organisation bedeutet
- Analysetechniken üben, um wichtige Führungskräfte im Unternehmen zu informieren, wie sie sich und die Organisation am effektivsten gegen gezielte Bedrohungen verteidigen können
- Kosteneffektive Wege identifizieren, Open-Source- und Community-Tools für Threat Intelligence zu nutzen, und sich mit einigen der wirksamsten kommerziellen Tools vertraut machen
- Threat Intelligence auf taktischer, betrieblicher und strategischer Ebene effektiv vermitteln
- Ein Multiplikator für andere wichtige Geschäftsfunktionen werden, u. a. SecOps, Incident Response und Geschäftsbetrieb

Zusammenfassung der Kursinhalte

TEIL 1: Cyber Threat Intelligence und Anforderungen
TEIL 2: Grundkompetenz: Intrusionsanalyse
TEIL 3: Sammlungsquellen
TEIL 4: Informationsanalyse und -produktion
TEIL 5: Disseminierung und Zuordnung
TEIL 6: Abschlussübung

„Cyber Threat Intelligence ist eine ganze Disziplin, nicht nur ein Feed. Dieser Kurs bringt Sie dem Verständnis dieser schnell reifenden Fachrichtung einen großen Schritt weiter."
– Bertha Marasky, **Verizon**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR578**

KURSFORMATE FOR578

Präsenzkurs | **Live online** | **OnDemand**

FOR585: Smartphone Forensic Analysis In-Depth™ GRUNDLEGEND ÜBERARBEITET

GASF
Advanced Smartphone Forensics
giac.org/gasf

6	36	22
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Die effektivsten Forensiktools, -techniken und -verfahren zur effektiven Analyse von Smartphone-Daten auswählen
- Ereignisse im Zusammenhang mit einem Verbrechen rekonstruieren, einschl. Timeline-Entwicklung und Link-Analyse (z. B. wer wann, wo und mit wem kommuniziert hat)
- Verstehen, wie Smartphone-Dateisysteme Daten speichern, wie sie sich unterscheiden und wie die Indizien auf den einzelnen Geräten gespeichert werden
- Dateisysteme auf Smartphones interpretieren und Informationen finden, die für Benutzer im Allgemeinen nicht zugänglich sind
- Identifizieren, wie die Indizien auf das Mobilgerät gelangt sind – wir zeigen Ihnen, wie Sie wissen, ob der Benutzer die Daten erstellt hat oder ob sie von KI oder durch Datensynchronisierung erstellt wurden; damit können Sie den entscheidenden Fehler vermeiden, durch Tools erlangte Falschinformationen zu melden
- Manuelle Decodierungstechniken einbeziehen, um ungeparste Daten wiederherzustellen, die auf Smartphones gespeichert sind
- Nachweisen, dass ein Benutzer an einem Datum, zu einer Uhrzeit oder an einem Ort ein Smartphone genutzt hat
- Verborgene oder verschleierte Kommunikation von Anwendungen auf Smartphones erfassen

Zielgruppe

- Erfahrene Prüfer für digitale Forensik
- Analysten für Medienexploitation
- Fachkräfte für Informationssicherheit
- Incident Response Teams
- Beamte, Beschäftigte und Ermittler bei Strafverfolgungsbehörden
- Ermittler für Unfallrekonstruktion
- IT-Auditoren
- Absolventen von SANS SEC575, FOR308, FOR498, FOR563, FOR500, FOR508, FOR572, FOR526, FOR610 oder FOR518, die ihre Kompetenzen weiter ausbauen möchten

Berufliche Rollen im NICE Framework

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

Heather Barnhart
Kursautorin

Domenica Crognale
Kursautorin

Bei FOR585™ erlernen Prüfer und Ermittler die erweiterten Kompetenzen, mit denen sie Indizien von Mobilgeräten erkennen, decodieren, entschlüsseln und korrekt interpretieren können. Der Kurs wird kontinuierlich aktualisiert, um mit den neuesten Dateiformaten, Malwares, Smartphone-Betriebssystemen, Anwendungen von Drittanbietern, Akquisitionsmängeln, Extrahierungstechniken (zur Erfassung des gesamten Dateisystems oder zum physischen Zugriff) und Verschlüsselung Schritt zu halten. Er bietet eine einzigartige und topaktuelle Schulung und wappnet Sie mit Kenntnissen über Mobilgerätforensik, die Sie sofort nach dem Kurs unmittelbar auf Ihre Fälle anwenden können.

Geschäftsorientierte Lernergebnisse

- Android- und iOS-Artefakte verstehen, die bei Ermittlungen helfen können
- Anwendungsartefakte auf iOS- und Android-Geräten verstehen
- Anhand der Smartphone-Nutzung feststellen, wo sich ein Gerät befand, als „etwas passiert ist“
- Einblicke gewinnen, wie ein Gerät genutzt wird: Fahrzeugverbindungen, Datensynchronisierung, Freisprechbetrieb, Armbanduhren usw.
- Verstehen, wie Malware-Infektionen bei Mobilgeräten auftreten und wie Malware, die auf Mobilgeräten gelandet ist, untersucht werden kann, und dadurch ihr Potenzial verringern
- Besser verstehen, wie SQLite-Datenbanken funktionieren und warum Geräte eine Fülle von Smartphone-Daten enthalten
- Kommerzielle Tools, die Ihr Unternehmen bereits verwendet, besser verstehen, und gegebenenfalls Lücken bei diesen Tools mit den im Kurs bereitgestellten Gratisskripts schließen
- Erfahrung bei der Erstellung von SQLite-Abfragen und Python-Skripts zur Forensikuntersuchung sammeln
- Mit der SANS FOR585 Alumni Community Group bei Änderungen in der Mobilgerätetechnologie und Ermittlungstrends einen Schritt voraus bleiben

Zusammenfassung der Kursinhalte

TEIL 1: Übersicht über Smartphones, Grundlagen der Analyse und SQLite-Forensik

TEIL 2: Android-Forensik

TEIL 3: Forensik bei iOS-Geräten

TEIL 4: Datensicherung und Cloud-Daten, Malware- und Spyware-Forensik und Erkennung von Indizienzerstörung

TEIL 5: Analyse von Drittanbieteranwendungen

TEIL 6: Abschlussübung: Smartphone-Forensik

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR585**

KURSFORMATE FOR585

Präsenzkurs | **Live online** | **OnDemand**

FOR589: **Cybercrime Investigations™**

5	30	20
Tage Programm	CPEs	Laborübungen

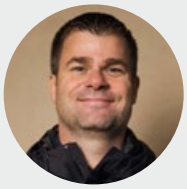
Vermittelte Kompetenzen

- Verstehen, wie sich herkömmliche Formen der Informationssammlung an das moderne, cyberzentrische Umfeld angepasst haben, und unterscheiden, was relevant ist und was nicht
- Risiken für die Assets und Elemente ihrer Organisation aufdecken und Akteuren und Bedrohungsvektoren als Informationsbedürfnisse mit hoher Priorität zuordnen
- Die risikoorientierten Informationsbedürfnisse Ihrer Organisation in bedrohungsgestützte Sammlungspläne und betriebliche Aufgaben übertragen
- Cyberkriminalitätsrisiken durch Entscheidungen angehen, die auf Bedrohungen beruhen, damit Sie Vorgehensweisen festlegen können, die sowohl defensiv als auch reaktiv sind, und entscheiden können, ob Sie Ihre Organisation schützen oder zum Gegenangriff übergehen sollten
- Den „Untergrund" entmystifizieren, damit Sie Communities, Marktplätze, Lösegeld-Websites, Datenschutzverletzungen, Malware-Protokolle und mehr navigieren und überwachen können

Berufliche Rollen im NICE Framework

- 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
Kursautor



Conan Beach
Kursautor

Will Thomas
Kursautor

Die Untersuchung von Cyberkriminalität ist unverzichtbar für Organisationen, die schädliche Aktivitäten erkennen, darauf reagieren und sie zuordnen wollen, wie auch für Strafverfolgungsbehörden und andere staatliche Stellen, deren Aufgabe es ist, Cyberkriminelle zu identifizieren, zu verhaften und strafrechtlich zu verfolgen. FOR589: Cybercrime Investigations™ bietet einen tiefen Einblick in den weltweiten Untergrund der Cyberkriminalität samt der Taktiken und Techniken, mit denen die Akteure Systeme ausnutzen und Angriffe monetarisieren. Dieser Kurs kombiniert das traditionelle Ermittlungshandwerk mit modernen Praktiken der Cybersicherheit zu einem überlegenen Ganzen. Ob Sie zu einem Sicherheitsteam im Unternehmen gehören, als Ermittler bei einer Behörde arbeiten oder einfach Ihre Kompetenzen bei der Verfolgung und beim Verständnis organisierter Cyberkriminalität erweitern möchten: Dieser Kurs wird Ihre Kompetenzen auf ein neues Niveau anheben.

Geschäftsorientierte Lernergebnisse

- Kenntnislücken in Cyber- und Kryptokriminalität in allen Ihren Ermittlungsteams schließen
- Kompetenzen für Betrugsermittlung, Incident Response und Cyber Threat Intelligence (CTI) durch einschlägiges Know-how stärken
- Aufkommende Bedrohungen durch Cyberkriminalität identifizieren und mindern, indem gegen Akteure ermittelt wird, bevor Angriffe eskalieren
- Proaktive Detektions- und Alarmmechanismen erstellen, die auf kriminellem Verhalten basieren
- Anfänglichen Zugriff, Malware-Einsatz und Partnerschaften im Untergrund untersuchen
- Anhaltspunkten bei der Untersuchung anhand von Trends im Untergrund und der Bewegung der Akteure Priorität verleihen
- Strukturierte Frameworks anwenden, um kriminelle Operationen von Anfang bis Ende zu verfolgen

Zielgruppe

- Informationsanalysten für Cyberbedrohungen
- Fachkräfte für Cyber Intelligence
- Ermittler für kriminelle Akteure
- Ermittler für Finanzkriminalität
- Threat Hunter
- Incident Responder
- Forensikanalysten
- InfoSec-Fachkräfte
- Fachkräfte bei Strafverfolgungsbehörden
- SANS-Absolventen, die ihre Kompetenzen ausbauen möchten

Zusammenfassung der Kursinhalte

TEIL 1: Informationen zu Cyberkriminalität
TEIL 2: Ermittlungen bei Kryptowährung
TEIL 3: Der cyberkriminelle Untergrund
TEIL 4: Verdeckte Ermittlungen
TEIL 5: Abschlussübung

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR589**

KURSFORMATE FOR589

Präsenzkurs **Live online**

FOR608: Enterprise-Class Incident Response & Threat Hunting™

GEIR
Enterprise Incident Responder
giac.org/geir

6	36	24
Tage Programm	CPEs	Laorübungen

Vermittelte Kompetenzen

- Verstehen, wann zur Incident Response eine detaillierte Host-Befragung oder Light-Weight Mass Collection erforderlich sind
- Plattformen für Zusammenarbeit und Analyse bereitstellen, mit denen Teams in mehreren Zimmern, Städten oder Ländern gleichzeitig arbeiten können
- Host- und Cloud-basierte Forensikdaten aus großen Umgebungen sammeln
- Best Practices zur Reaktion bei den Cloud-Plattformen Azure, M365 und AWS diskutieren
- Analysetechniken für die Reaktion bei Linux- und Mac-Betriebssystemen erlernen
- Container-Mikroservices wie z. B. Docker-Container analysieren
- Daten über mehrere Datentypen und Rechner hinweg mit unzähligen Analysetechniken korrelieren und analysieren
- Analysen von strukturierten und unstrukturierten Daten durchführen, um Angreiferverhalten zu identifizieren
- Gesammelte Daten anreichern, um zusätzliche Anzeichen für eine Kompromittierung zu identifizieren

Zielgruppe

Dieser Kurs richtet sich an Fachkräfte für Digitalforensik, Incident Response, Intrusionsdetektion und Threat Hunting in mittelgroßen bis großen Organisationen, denen die Größe und Komplexität des Unternehmens ständig Probleme bereitet.

FOR608™ ist ein fortgeschrittener Kurs, bei dem die Einführung in Host- und Netzwerk-basierte Forensik und Incident Response für Windows ausgelassen wird. Dieser Kurs ist nicht unbedingt technischer als unsere Kurse im 500er-Bereich, aber er setzt diese Kenntnisse voraus, damit Themen und Konzepte nicht wiederholt werden.

Berufliche Rollen im NICE Framework

- 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
Kursautor

Mike Pilkington
Kursautor

Tarot (Taz) Wake
Kursautor

Bei FOR608™ geht es um die Identifizierung und die Reaktion auf Vorfälle, die zu groß sind, als dass man sich auf individuelle Computer konzentrieren könnte. Unter Verwendung von Beispieltools, die auf den Betrieb auf Enterprise-Niveau ausgelegt sind, lernen die Kursteilnehmer Techniken zur Erfassung fokussierter Daten für Incident Response und Threat Hunting und beschäftigen sich näher mit Analysemethodiken. Sie lernen mehrere Ansätze zum Verständnis der Angreiferbewegung sowie Aktivitäten, die sich über Hosts mit unterschiedlichen Funktionen und Betriebssystemen hinweg erstrecken. Dabei setzen sie Timelines und Diagramme sowie Techniken zur strukturierten und unstrukturierten Analyse ein.

Geschäftsorientierte Lernergebnisse

- Durch effizienteres und präziseres Reaktionsmanagement die Auswirkungen auf Finanzen und Reputation reduzieren
- IR-Managementtechniken zur Optimierung der Ressourcennutzung während einer Ermittlung erlernen
- Plattformen für Zusammenarbeit und Analyse bereitstellen, mit denen Teams in mehreren Zimmern, Städten oder Ländern gleichzeitig arbeiten können
- Verstehen, mit welchen Techniken sich Angreifer vor EDR-Tools und Anwendungssteuertools in Windows-Systemen verstecken, und sie aufspüren
- Analysetechniken für die Reaktion bei Linux- und macOS-Systemen erlernen
- In der Lage sein, auf Container-Mikroservices wie z. B. Docker-Container zu reagieren und sie zu analysieren
- Bewährte Praktiken zur Reaktion in den beliebtesten Cloud-Umgebungen diskutieren – insbesondere Microsoft365/AzureAD und AWS

Zusammenfassung der Kursinhalte

TEIL 1: Proaktive Detektion und Reaktion

TEIL 2: Reaktion und Analyse skalieren

TEIL 3: Moderne Angriffe auf Windows und Linux DFIR

TEIL 4: macOS- und Docker-Container analysieren

TEIL 5: Cloud-Angriffe und Reaktion

TEIL 6: Abschlussübung: Incident Response auf Enterprise-Niveau

„Die flexible Arbeit war sehr beeindruckend. Ich arbeite schon seit Jahren damit, aber hier habe ich neue Methoden der Datenaufnahme erlernt, die mir in der Vergangenheit eine Menge Zeit hätten sparen können."

– Simon H., **CyberCX**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR608**

KURSFORMATE FOR608

Präsenzkurs **Live online**

FOR610: Reverse-Engineering Malware: Malware Analysis Tools & Techniques

GREM Reverse Engineering Malware
giac.org/grem
CyberLive
DoD 8140*

6	36	52
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Eine isolierte, kontrollierte Laborumgebung aufbauen, in der Code und das Verhalten schädlicher Programme analysiert werden können
- Mit Netzwerk- und System-Überwachungstools untersuchen, wie Malware mit dem Dateisystem, der Registry, dem Netzwerk und anderen Prozessen in einer Windows-Umgebung interagiert
- Schädliche, oft verschleierte JavaScript- und PowerShell-Skripts analysieren, die häufig als Teil einer Angriffskette verwendet werden
- Relevante Aspekte des Verhaltens des schädlichen Programms unter Kontrolle halten, indem der Netzwerkverkehr abgefangen und Code gepatcht wird, damit eine effektive Malware-Analyse durchgeführt werden kann
- Mit einem Disassembler und einem Debugger die innere Funktionsweise schädlicher Windows-Programmdateien untersuchen
- Verschiedene Packer und andere Verteidigungsmechanismen umgehen, die von Malware-Autoren entworfen wurden, um den Analysten in die Irre zu führen, zu verwirren oder anderweitig zu verlangsamen
- Häufige Muster auf Assembly-Ebene in schädlichem Code erkennen und verstehen, z. B. Code-Injection, C2-Interaktionen, Dropper- und Downloader-Techniken und Analyse-Gegenmaßnahmen

Zielgruppe

- Alle, die mit Vorfällen umgehen müssen, an denen Malware beteiligt ist, und die wichtige Aspekte schädlicher Programme verstehen lernen möchten
- Technologen, die Aspekte der Malware-Analyse formlos ausprobiert haben und die ihr Know-how auf diesem Gebiet formalisieren und erweitern möchten
- Forensikermittler und IT-Praktiker, die ihre Kompetenzen erweitern und lernen möchten, wie sie eine entscheidende Rolle bei der Incident Response spielen können

Berufliche Rollen im NICE Framework

- 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
Kursautor

Lenny Zeltser
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Nehmen Sie Malware unter die Lupe! Dieser beliebte Kurs beschäftigt sich detailliert mit Tools und Techniken zur Malware-Analyse. FOR610™ hat Forensikermittlern, Incident Respondern, Sicherheitsingenieuren und IT-Administratoren zu den praktischen Kompetenzen verholfen, mit denen sie Schadprogramme untersuchen, die Windows-Systeme angreifen und infizieren.

Wir müssen die Fähigkeiten von Malware verstehen, damit wir Threat Intelligence ableiten, auf Informationssicherheits-Vorfälle reagieren und die Verteidigung stärken können. Dieser Kurs legt ein solides Fundament für das Reverse-Engineering von Schadsoftware mit einer Reihe verschiedener Utilitys zur System- und Netzwerküberwachung, einem Disassembler, einem Debugger und zahlreichen anderen, gratis verfügbaren Tools.

Geschäftsorientierte Lernergebnisse

- Interne Teams befähigen, die Analyse im Haus durchzuführen, damit weniger Bedarf nach externem Know-how besteht
- Die Analysekompetenzen Ihres Teams erweitern, damit es den internen oder externen Stakeholdern mehr zu bieten hat
- Die Effizienz Ihrer Analyseaufgaben erhöhen, damit Sie wertvolle Einblicke schneller bereitstellen können
- Den Umfang und die Kosten des potenziellen Übergriffs auf ein Minimum beschränken, indem schneller auf Sicherheitsvorfälle reagiert wird

Zusammenfassung der Kursinhalte

TEIL 1: Grundlagen der Malware-Analyse

TEIL 2: Schädlichen Code reversieren

TEIL 3: Jenseits von herkömmlichen Programmdateien

TEIL 4: Eingehende Malware-Analyse

TEIL 5: Selbstverteidigende Malware untersuchen

TEIL 6: Malware-Analyseturnier

„Ich habe bei FOR610 eine Menge wertvoller Informationen erhalten, u. a. welche Bereiche ich für meine Arbeit meistern muss. Die „Capture-the-Flag"-Übung war ein Alarmsignal dafür, wie viel ich nicht weiß; dafür meinen Dank!"

– Urban M., **CNF Technologies**

„Dieser Kurs hat mir geholfen, meine Kenntnisse der Malware-Techniken zu verbessern und zu verstehen, wie ich Assets besser schützen und die Schritte zur Ausmerzung erfolgreich abschließen kann."

– Eric B., **Nestle**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR610**

KURSFORMATE FOR610

Präsenzkurs | **Live online** | **OnDemand**

FOR710: Reverse-Engineering Malware: Advanced Code Analysis™

5	36	12
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Techniken zur Codeverschleierung angehen, die eine statische Codeanalyse behindern, u. a. Steganografie
- Die wichtigsten Komponenten der Programmausführung identifizieren, um Malware im Arbeitsspeicher zu analysieren
- Entschleierten Shellcode während der Programmausführung lokalisieren und extrahieren
- Während der Malware-Analyse mit anderen Dateiformaten als Programmdateien vertraut werden
- Die Strukturen und Felder erkunden, die mit einem PE-Header verknüpft sind
- WinDBG Preview zum Debugging und zur Beurteilung wichtiger Prozessdatenstrukturen im Arbeitsspeicher heranziehen
- Verschlüsselungsalgorithmen in Ransomware identifizieren, die für Dateiverschlüsselung und Schlüsselschutz genutzt werden
- Windows-APIs erkennen, die die Verschlüsselung ermöglichen, und ihren Zweck artikulieren
- Datenverschleierung in Malware untersuchen, Algorithmusimplementierungen lokalisieren und zugrunde liegende Inhalte decodieren
- Python-Skripts zur Automatisierung der Datenextrahierung und Entschlüsselung erstellen
- Regeln zur Identifizierung von Malware-Funktionalität erstellen
- Mithilfe von DBI-Frameworks (Dynamic Binary Instrumentation) häufige Reverse-Engineering-Workflows automatisieren
- Python-Skripts in Ghidra schreiben, um die Codeanalyse zu beschleunigen

Zielgruppe

- Fachkräfte für Cybersicherheit, die Reverse-Engineering-Kompetenzen auf mittlerem Niveau haben und sie verbessern möchten
- Fachkräfte für Reverse-Engineering, die besser in der Lage sein möchten, verschleierten Code zu analysieren, die Verschlüsselungsfähigkeiten in Malware einzuschätzen und Analyseaufgaben zu automatisieren

Berufliche Rollen im NICE Framework

- 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
Kursautor

Je mehr Verteidiger ihre Analysefertigkeiten steigern und je mehr sich die Fähigkeiten der automatisierten Malware-Detektion verbessern, desto mehr bemühen sich Malware-Autoren, damit ihre Malware trotzdem im Unternehmen zur Ausführung kommt. Das Ergebnis ist eine modulare Malware mit mehreren Layern verschleierten Codes, der im Arbeitsspeicher ausgeführt wird, um unerkannt zu bleiben und die Analyse zu behindern. Malware-Analysten müssen darauf vorbereitet sein, diese fortschrittlichen Fähigkeiten zu kontern und wann immer möglich Automatisierung zu nutzen, um des Volumens, der Vielfältigkeit und der Komplexität des stetigen Stroms an Malware, der auf das Unternehmen zukommt, Herr zu werden.

FOR710™ schließt an FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques™ an. Der Kurs hilft Teilnehmern, die bei der Malware-Analyse bereits über Fähigkeiten auf mittlerem Niveau verfügen, und erweitert ihre Kompetenz im Reverse-Engineering. Dieser Kurs vom SANS-zertifizierten Kursleiter Anuj Soni zeigt Malware-Fachkräften, wie sie raffinierte Windows-Programmdateien sezieren – die Art von Malware, die weltweit für Schlagzeilen sorgt und Incident Response Teams in Atem hält.

Fundierte Kompetenz im Reverse-Engineering zu entwickeln, erfordert kontinuierliche Übung. Dieser Kurs umfasst nicht nur den nötigen Hintergrund und schrittweise Anleitungen, sondern bietet den Lernenden auch zahlreiche Gelegenheiten, während des Kurses reale Reverse-Engineering-Szenarien zu bearbeiten.

Zusammenfassung der Kursinhalte

TEIL 1: Code-Entschleierung und Ausführung

TEIL 2: Verschlüsselung in Malware

TEIL 3: Malware-Analyse automatisieren

TEIL 4: Malware-Analyse automatisieren (Fortsetzung)

TEIL 5: Turnier zur erweiterten Malware-Analyse (verlängerter Zugriff)

„Die Übungen zur Automatisierung waren ausgezeichnet und zeigten wirklich, was nötig ist, um RE durch Automatisierung durchzuführen."
– Daniel T., **US-amerikanisches Justizministerium**

„Dieser Kurs hat mir wirklich gut gefallen. Meiner Meinung nach war er ein guter und logischer nächster Schritt nach FOR610. Das Material ergab Sinn und war relevant für das, was ich bei der Arbeit tagtäglich zu sehen bekomme."
– Daniel R., **CrowdStrike**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/FOR710**

KURSFORMATE FOR710

Präsenzkurs | **Live online** | **OnDemand**

FOKUSBEREICH IM SANS-LEHRPLAN

Sicherheit bei ICS-Systemen

Eigentümer und Betreiber von industriellen Steuersystemen (Industrial Control Systems, ICS) sehen sich zurzeit mit einem komplexen und chaotischen Spektrum von Bedrohungen konfrontiert.

Anschläge, die physischen Schaden verursachen oder physische Prozesse beeinträchtigen, gehören nicht mehr nur in den Bereich der theoretischen Spekulation. Wir sehen nun Fälle, bei denen böswillige Akteure mit maßgeschneiderter ICS-Malware erfolgreich in Systeme eindringen, Schäden verursachen und den Betrieb stören. In Zukunft können Sie erwarten, Ihre Steuersysteme gegen zunehmend versierte Widersacher verteidigen zu müssen.

SANS-Kurse zur ICS-Sicherheit decken folgende Bereiche ab:

- Komponenten, Zwecke, Implementierungen, wichtige treibende Faktoren und Beschränkungen von ICS erkennen
- ICS-Assets identifizieren, Netzwerktopologien analysieren und kritische Hotspots auf Anomalien und Bedrohungen überwachen
- Architekturen und Techniken zur System- und Netzwerkverteidigung verstehen
- Sich bei der ICS Incident Response auf Sicherheitsoperationen konzentrieren und der Sicherheit und Betriebszuverlässigkeit Priorität einräumen
- Effektive cybertechnische und physische Kontrollmaßnahmen für den Zugang umsetzen

„Die Schulungen beginnen mit der Theorie und gehen schnell zu praktischen Interaktionen mit allen Komponenten über. Diese Erfahrung findet man nicht oft.“

– Bassem Hemida, **Deloitte**

Stellenprofil bei ICS:

- Berater für ICS-/OT-Sicherheitsbewertungen
- ICS-Sicherheitsingenieur
- ICS-Sicherheitsanalyst
- Ingenieur für Steuersysteme
- ICS-Cybersicherheitsingenieur
- ICS-/OT-Sicherheitsleiter

KURS NEU IM FOKUS

ICS310: **ICS Cybersecurity Foundations™**

1	6	3
Kurstag	CPEs	Laborübungen

Vermittelte Kompetenzen

- Die wichtigsten Sicherheitsmaßnahmen zum Schutz von Industriesystemen meistern
- Einblicke in die Frameworks IEC 62443, NIST 800-82, NIS2 und NERC CIP gewinnen
- Gemeinsame Terminologie, Systemkomponenten und digitalen/analogen Betrieb kennenlernen
- Wichtige Trends, Gerätegrundlagen und Systemein-/-ausgaben in Betriebstechnologie-Umgebungen verstehen
- Fallstudien analysieren, um zu sehen, wie die ICS-Prinzipien auf wirkliche Probleme der Branche angewendet werden

Geschäftsorientierte Lernergebnisse

- Beschäftigten zeigen, wie sie häufige ICS-Komponenten identifizieren und effektive Cybersicherheitsmaßnahmen im gesamten Betrieb implementieren
- Beschäftigte durch Einblicke aus weltweiten Fallstudien und bewährte Verteidigungsstrategien auf Kontertaktiken von Gegnern vorbereiten
- Ihr Team befähigen, anpassbare ICS-Kontrollmaßnahmen zu implementieren, die branchenspezifische und regulatorische Herausforderungen angehen und die Resilienz insgesamt verbessern

Zielgruppe

- Personen, denen ICS neu ist
- Personen, die in Zukunft mehr über ICS lernen müssen
- OT-Sicherheitsfachkräfte aus regulierten Branchen und kritischer Infrastruktur
- OT-Sicherheitsfachkräfte aus nicht regulierten Branchen
- Fachkräfte bei Anbietern/Integratoren
- Alle aus Branchen der kritischen Infrastruktur/wichtigen Ressourcen (Strom, Wasser, Nuklear, Telekom, Erdöl, Erdgas, Herstellung, Chemie, Bahn, Transport usw.), insbesondere aus den Betriebstechnologie-Umgebungen dieser Organisationen
- Personal des Verteidigungsministeriums, das an Betriebsumgebungen interessiert ist, die cyber-physische Assets nutzen oder unterstützen

Tim Conway
Kursautor

Robert M. Lee
Kursautor

Jeffrey Shearer
Kursautor

In diesem Kurs beschäftigen sich die Teilnehmer mit mechanischen und betrieblichen Systemen, um besser zu verstehen, wie die Eigentümer und Betreiber von Assets diese Umgebungen automatisiert haben. Mehrere Sektoren werden erkundet und die Gemeinsamkeiten in unterschiedlichen Prozessumgebungen aus verschiedenen Branchen und Sektoren herausgestellt. Durch ein Verständnis der gemeinsamen Bausteine und Betriebskriterien in zahlreichen Sektoren lernen die Verteidiger wichtige Fokusbereiche für risikobasierte Cybersicherheitsmaßnahmen kennen, die übergreifende Betriebsziele unterstützen.

Wir besprechen Fallstudien aus mehreren Sektoren weltweit – Cybereignisse, bei denen Gegner eine Reihe verschiedener Taktiken verfolgten, um ihre Ziele zu erreichen. Diese Fallstudien decken IT-Angriffe ab, die den Betrieb beeinträchtigten, Angriffe auf betriebliche Ziele, die sich stark auf manuelle Aktivitäten des Gegners stützten, und Angriffe auf betriebliche Ziele mithilfe ICS-fähiger Malware. Durch die Analyse dieser Fallstudien decken wir Lehren auf, die gezogen wurden, und geben Empfehlungen für erfolgreiche Verteidigungsstrategien, einschließlich Maßnahmen durch Verteidiger, die priorisiert und verfolgt werden können.

Sektoren in verschiedenen geografischen Regionen müssen jeweils andere regulatorische Anforderungen und Standards erfüllen, und mitunter fehlen solche Leitlinien überhaupt. Praktiker und Führungskräfte, die auf der Suche nach angemessenen Sicherheitskontrollmaßnahmen sind, lernen die fünf ICS Critical Controls kennen, die angepasst und in jeder Umgebung implementiert werden können.

Zusammenfassung der Kursinhalte

TEIL 1: Argumente für ICS310 und der ICS-Lehrplan

TEIL 2: ICS und Automatisierung

TEIL 3: ICS-Trends und Bedrohungen

TEIL 4: ICS-Fallstudien und weltweite Ereignisse

TEIL 5: Standards und Richtlinien des ICS für Cybersicherheit

TEIL 6: Die fünf ICS Critical Controls

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/ICS310**

KURSFORMATE ICS310

OnDemand

ICS410: **ICS/SCADA Security Essentials™**

GICSP
Global Industrial Cyber Security Professional
giac.org/gicsp

CyberLive
DoD 8140*

6	36	15
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Verschiedene industrielle Steuersysteme und ihren Zweck, ihre Anwendung, ihre Funktion und ihre Abhängigkeiten von Netzwerk-IP und industrieller Kommunikation verstehen
- Mit Steuernetzwerk-Infrastrukturdesign arbeiten (Konzepte der Netzwerkarchitektur wie Topologie, Protokolle und Komponenten) und die Beziehung zu IEC 62443 und zum Purdue-Modell kennen
- Mit Windows-Befehlszeilentools das System auf hoch riskante Elemente analysieren
- Mit Linux-Befehlszeilentools (ps, ls, netstat, ect) und einfachen Skripts die Ausführung von Programmen automatisieren, um verschiedene Tools kontinuierlich zu überwachen
- Mit Betriebssystemen arbeiten (Konzepte der Systemadministration für die Betriebssysteme Unix/Linux und/oder Windows)
- Den Sicherheitszyklus der Systeme verstehen
- Prinzipien und Grundsätze der Informationssicherung verstehen (Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung, Unbestreitbarkeit)
- Kompetenzen bei der Verteidigung eines Computernetzwerks nutzen, um mithilfe von Technologien zur Intrusionsdetektion Host- und Netzwerk-basierte Übergriffe zu erkennen
- Incident Response und Handhabungsmethodiken implementieren
- Verschiedene ICS-Technologien, Angriffe und Verteidigungsmaßnahmen den verschiedenen Cybersicherheitsstandards zuordnen, u. a. dem NIST Cybersecurity Framework, ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-53, den Critical Security Controls des Center for Internet Security und COBIT 5

Zielgruppe

Dieser Kurs richtet sich an verschiedene Personen, die in ICS-Umgebungen arbeiten, mit ihnen interagieren oder sie beeinflussen können, u. a. Asset-Eigentümer, Anbieter, Integratoren und andere Drittanbieter. Dieses Personal stammt primär aus vier Domänen:

- IT (einschl. OT-Support)
- IT-Sicherheit (einschl. OT-Sicherheit)
- Technik
- Unternehmens-, Branchen- und Berufsstandards

Berufliche Rollen im NICE Framework

- 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
Kursautor

* DoD 8140 APPROVED
sans.org/8140

OT-Umgebungen sehen sich mit einer wachsenden Welle ausgereifter Cyberbedrohungen konfrontiert. Dennoch verlassen sich viele Organisationen auf IT-zentrische Sicherheitsmaßnahmen, die für die charakteristischen Herausforderungen von ICS- und SCADA-Systemen (Supervisory Control and Data Acquisition) schlecht geeignet sind. Da spezialisierte Kenntnisse und praktische Erfahrung auf dem Gebiet der ICS-Cybersicherheit fehlen, sind kritische Infrastrukturen Gefahren ausgesetzt. Das erhöht das Risiko von Betriebsunterbrechungen, finanziellen Verlusten und Sicherheitsvorfällen. Dieser Kurs baut auf fundamentalen Prinzipien der ICS-Cybersicherheit auf und vermittelt Fachkräften in industrieller Cybersicherheit die erweiterten Kompetenzen, die sie benötigen, um OT-Umgebungen effektiv zu sichern. Durch den Fokus auf die besonderen Anforderungen von Industriesystemen befähigt der Kurs Fachkräfte für IT- und OT-Cybersicherheit, aufkommende Bedrohungen anzugehen und so mit minimalen Auswirkungen auf den Betrieb für Sicherheit und Resilienz in der kritischen Infrastruktur zu sorgen.

Sektoren für kritische Infrastruktur und wichtige Ressourcen sehen sich einem Bedrohungsumfeld gegenüber, das sich rapide weiterentwickelt. Cyberangriffe können wesentliche Dienstleistungen unterbrechen, die Sicherheit kompromittieren und erheblichen wirtschaftlichen und betrieblichen Schaden verursachen. Fachkräfte, die Steuersysteme betreiben, managen, entwerfen, implementieren, überwachen und verteidigen, stehen hier an vorderster Linie. Dieser Kurs wurde speziell für diese Fachkräfte entworfen und vermittelt ihnen die unverzichtbaren Kompetenzen und Kenntnisse, die sie benötigen, um Steuersysteme in Umgebungen mit hohem Risiko zu sichern und zu unterstützen. Durch diesen Kurs werden Fachkräfte befähigt, die alltäglichen Sicherheitsanforderungen kritischer Infrastruktur zu erfüllen und für Resilienz, Sicherheit und Betriebskontinuität zu sorgen.

Zusammenfassung der Kursinhalte

TEIL 1: Übersicht über ICS
TEIL 2: Architekturen und Prozesse
TEIL 3: Kommunikation und Protokolle
TEIL 4: Überwachungssysteme
TEIL 5: ICS-Sicherheits-Governance
TEIL 6: „Capture-the-Flag"-Abschlussübung

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/ICS410**

KURSFORMATE ICS410

Präsenzkurs | **Live online** | **OnDemand**

ICS418: **ICS Security Essentials for Leaders**™

2 Kurstage	12 CPEs	11 Laborübungen

Vermittelte Kompetenzen

- Den Wert von ICS-Sicherheit darlegen und Cyberrisiko mit Entscheidungen zum Geschäftsrisiko verknüpfen
- Den Trend aktueller und zukünftiger Technologieänderungen nutzen, um sich geschäftlicher Anforderungen anzunehmen
- Erfolge beim Umgang mit industriellen Cyberrisiken messen und dabei u. a. Kennzahlen für Führungskräfte und Vorstand erfassen
- Mit Best Practices die Vorfallsdetektion bei der ICS-Sicherheit und Reaktionen für ihre Teams ermöglichen
- Mithilfe externer Informationen, u. a. Threat Intelligence, ein ICS-Sicherheitsprogramm anleiten
- Governance, Aufsicht, Ausführung und Unterstützung für mehrere industrielle Anlagen für ICS-Sicherheitsinitiativen und -projekte bereitstellen
- Die Unterschiede zwischen IT- und ICS-Sicherheit anwenden, um ein effektives Cybersicherheitsprogramm für Steuersysteme zu erhalten
- Sicherheitspersonal schulen, um Lücken bei Rekrutierung, Schulung und Bindung zu schließen
- Mit erweiterten Techniken bei der Gestaltung und Wandlung der Sicherheitskultur der Organisation mithelfen

Zielgruppe

ICS418 richtet sich an Führungskräfte mit Verantwortung für die Sicherung der täglichen ICS/OT-Umgebung, einschließlich DCS (Distributed Control Systems) und SCADA-Systeme. Diese Führungskräfte stammen aus diversen Hintergründen, u. a.:

- Manager mit starken Führungskompetenzen, aber begrenzten ICS-Kenntnissen
- Technische Fachkräfte, die in Führungsrollen befördert wurden, aber im Management nur minimal geschult sind
- Sicherheitsleiter, die OT- und ICS-Umgebungen organisationsweit beaufsichtigen
- Teamleiter, die für die Implementierung von Cybersicherheitsstrategien in industriellen Umgebungen verantwortlich sind

Berufliche Rollen im NICE Framework

- ICS/SCADA Security Engineer
- ICS/OT Systems Engineer
- OT SOC Operator

Jason Christopher
Kursautor

Dean Parsons
Kursautor

ICS-Sicherheit ist ein dynamisches Fachgebiet, in dem Fachkräfte ihre Verteidigungsstrategien ständig an neue Herausforderungen und Bedrohungen anpassen müssen. Das Problem wird dadurch noch erschwert, dass alle Änderungen der Sicherheit gründlich getestet werden müssen, damit Sicherheit und Zuverlässigkeit industrieller Betriebe erhalten bleiben.

Weltweit repräsentieren „kritische Infrastruktur" und „Betreiber systemrelevanter Dienstleistungen" Hunderttausende, wenn nicht Millionen von Industrieorganisationen. Einige von ihnen sind die Lebensadern der modernen Gesellschaft, z. B. Wasser, Strom, Nahrungsmittelverarbeitung und kritische Produktion. Aber jede Industrieanlage muss davon ausgehen können, dass ihre Prozesse sicher sind. Angesichts wachsender Bedrohungen, neuer Technologietrends und steigender Personalanforderungen müssen Sicherheitsmanager im Bereich der Betriebstechnologie (Operation Technology, OT) in Techniken zur Verteidigung ihrer Anlagen und Teams geschult sein.

Der zweitägige Kurs ICS418 schließt eine Kompetenzlücke, die bei Führungskräften in kritischer Infrastruktur und OT-Umgebungen identifiziert wurde. Er wendet sich an neue oder bestehende Führungskräfte, die für OT/ICS oder konvergierte IT-/OT-Cybersicherheit zuständig sind. Der Kurs vermittelt ihnen Erfahrung und Tools, mit denen sie sich dem Druck in der Branche annehmen können, Cyberrisiken zu managen und gleichzeitig dem Geschäft Priorität einzuräumen – sowie der Sicherheit und Zuverlässigkeit des Betriebs. ICS-Führungskräfte gewinnen in diesem Kurs ein solides Verständnis der treibenden Faktoren und Beschränkungen, die in diesen cyber-physischen Umgebungen bestehen, und außerdem ein nuanciertes Verständnis, wie sie Mitarbeiter, Prozesse und Technologien in der gesamten Organisation managen können.

Zusammenfassung der Kursinhalte

TEIL 1: ICS-Sicherheitsleiter – Schlüsselaspekte der Entwicklung und Zuständigkeiten

TEIL 2: Fokus auf der Entwicklung des ICS-Sicherheitsteams

„Was ich in diesem Kurs gelernt habe, hat mir geholfen, das führende Management darauf anzusprechen, dass wir Cyberverteidigung in den OT-Netzwerken benötigen."

– Vickram R., **Eastern Generating Company**

„Ich baue seit drei Jahren ein ICS-Sicherheitsteam/-programm auf und das Kursmaterial deckt wirklich die meisten, wenn nicht alle Konzepte und Bedenken ab, die integriert werden müssen."

– David B., **Pernod Ricard**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/ICS418**

KURSFORMATE ICS418

Präsenzkurs | **Live online** | **OnDemand**

ICS456: Essentials for NERC Critical Infrastructure Protection™

GRUNDLEGEND ÜBERARBEITET

GCIP
Critical Infrastructure Protection
giac.org/gcip

5	31	23
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Die Cybersicherheitsziele der NERC-CIP-Standards verstehen
- Den NERC-Regulierungsrahmen, die Quelle seiner Autorität und den Entwicklungsprozess der CIP-Normen verstehen, sowie die Beziehung zu anderen BES-Zuverlässigkeitsstandards
- Die Sprache von NERC CIP fließend sprechen und verstehen, wie scheinbar ähnliche Begriffe erheblich unterschiedliche Bedeutungen haben können und welche Auswirkungen das auf Ihr Compliance-Programm hat
- Die Komplexität aufschlüsseln, um BES-Cyber-Assets und -Systeme leichter zu identifizieren und zu kategorisieren
- Bessere Kontrollmaßnahmen für das Sicherheitsmanagement entwickeln, indem Sie verstehen, was effektive Richtlinien und Verfahren in der Cybersicherheit ausmacht
- Physische und logische Kontrollmaßnahmen und Überwachungsanforderungen verstehen
- Die CIP-007-Systemmanagement-Anforderungen und ihre Beziehung zu den CIP-010-Konfigurationsmanagement-Anforderungen verstehen, sowie die verschiedenen Zeitrahmen für Beurteilung und Behebung von Schwachstellen
- Herausfinden, was ein nachhaltiges Programm zur Personalschulung und Risikobeurteilung ausmacht

Zielgruppe

- IT- und OT-Cybersicherheit (ICS)
- Supportpersonal im Außendienst
- Sicherheitsbetriebspersonal
- Incident-Response-Personal
- Compliance-Personal
- Teamleiter
- Personen, die an Governance beteiligt sind
- Anbieter/Integratoren
- Auditoren

Berufliche Rollen im NICE Framework

- 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
Kursautor

Ted Gutierrez
Kursautor

Stephen Sims
Kursautor

Angesichts des dynamischen Umfelds der Cybersicherheitsbedrohungen und des Drucks neuer Vorschriften ist Compliance mit den NERC-CIP-Standards (North American Electric Reliability Corporation Critical Infrastructure Protection) mehr als eine Pro-forma-Übung, sondern eine komplexe, wichtige Herausforderung für Organisationen im Bereich der Stromversorgung in Nordamerika. ICS456™ klärt die Verwirrung und bietet praktische Anleitungen, die Regulierungspolitik in Aktion umsetzen. Der Kurs ist für Fachkräfte in Betrieb, IT-/OT-Sicherheit und Compliance vorgesehen und entmystifiziert die NERC-CIP-Anforderungen, setzt sie zu realen ICS-Umgebungen (Industrial Control System, industrielles Steuersystem) in Bezug und befähigt Teams, Risiken zu managen, Verstöße zu vermeiden und eine Kultur der Cyberresilienz aufzubauen. Wenn Ihre Aufgabe darin besteht, Audits einen Schritt voraus zu sein und gleichzeitig die kritische Infrastruktur zu verteidigen, gibt Ihnen ICS456™ die Kenntnisse und Tools an die Hand, die Sie benötigen, um diese Aufgabe zuversichtlich zu erfüllen.

ICS456™ geht über die Grundlagen von NERC CIP hinaus und bietet umsetzbare Strategien für Compliance und Sicherheit. Sie entwickeln ein gründliches Verständnis der Rolle, die FERC (Federal Energy Regulatory Commission), NERC (North American Electric Reliability Corporation) und regionale Organisationen bei der Durchsetzung von Zuverlässigkeitsstandards spielen. Der Kurs bietet mehrere Ansätze zur Identifizierung und Kategorisierung von BES-Cybersystemen (Bulk Electric System), die sicherstellen, dass Anlageneigentümer die Anforderungen ihrer individuellen Umgebungen korrekt ausarbeiten und anwenden können. ICS456™ ist mehr als nur ein Compliance-Kurs: Er schließt die Lücke zwischen regulatorischen Anforderungen und der Umsetzung von Sicherheit in der wirklichen Welt. Sie erkunden praktische Strategien zur Sicherung von industriellen Steuersystemen und Betriebstechnologie und finden dabei einen Ausgleich zwischen bewährten Praktiken der Cybersicherheit und den Realitäten der Compliance.

Zusammenfassung der Kursinhalte

TEIL 1: Anlagenidentifikation und Governance
TEIL 2: Zugriffskontrolle und -überwachung
TEIL 3: Systemmanagement
TEIL 4: Informationsschutz und Reaktion
TEIL 5: Der CIP-Prozess

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/ICS456**

KURSFORMATE ICS456

Präsenzkurs | **Live online** | **OnDemand**

ICS515: ICS Visibility, Detection, and Response™

GRID
Response and Industrial Defense
giac.org/grid
DoD 8140*

6	36	22
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- ICS-Netzwerke untersuchen und die Assets und ihre Datenflüsse identifizieren, um festzustellen, welche Netzwerkinformationen zur Identifizierung ausgeklügelter Bedrohungen benötigt werden
- Das ICS mit Konzepten der aktiven Verteidigung schützen, z. B. Verarbeitung von Threat Intelligence, Überwachung der Netzwerksicherheit, Malware-Analyse und Incident Response
- Mit dem SANS ICS515 Student Kit, den Sie nach dem Kurs behalten dürfen, eine eigene speicherprogrammierbare Steuerung erstellen
- Detaillierte Kenntnisse von gezielten Bedrohungen für ICS und Malware gewinnen, u. a. STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, TRISIS/TRITON, FROSTYGOOP, EKANS und PIPEDREAM
- Technische Tools wie Shodan, Wireshark, Zeek, Suricata, Volatility, FTK Imager, PDF-Analyseprogramme, PLC-Programmierungssoftware und mehr ausnutzen
- IOCs (Kompromittierungsanzeichen) in YARA erstellen
- Mithilfe verschiedener Modelle, z. B. Sliding Scale of Cybersecurity, Active Cyber Defense Cycle, Collection Management Framework und ICS Cyber Kill Chain Informationen aus Bedrohungen extrahieren und sie für den langfristigen Erfolg der ICS-Netzwerksicherheit nutzen

Zielgruppe

- Leiter und Mitglieder von ICS Incident Response Teams
- ICS- und OT-Sicherheitspersonal
- IT-Sicherheitsfachkräfte
- Teamleiter und Analysten im Security Operations Center
- ICS Red Team und Penetrationstester
- Aktive Verteidiger

Berufliche Rollen im NICE Framework

- Cyber Defense Incident Responder (OPM 531)
- ICS/SCADA Security Engineer
- ICS/OT Systems Engineer
- OT SOC Operator

Robert M. Lee
Kursautor

* DoD 8140 APPROVED
sans.org/8140

Die Schulung ICS515 hilft Ihnen, die Transparenz und die Asset-Identifizierung in Ihren ICS-/OT-Netzwerken zu verbessern. Sie lernen, wie Sie Cyberbedrohungen überwachen und erkennen, ICS-Cyberangriffe dekonstruieren und Lehren daraus ziehen und Incident Response durchführen. Sie erfahren, wie Sie ein weltweit führendes ICS-Cybersicherheitsprogramm mithilfe eines informationsbasierten Ansatzes umsetzen, damit für einen sicheren und zuverlässigen Betrieb gesorgt wird.

Der Kurs vermittelt den Teilnehmern ein Verständnis ihrer vernetzten ICS-Umgebung und befähigt sie, diese auf Bedrohungen zu überwachen, mit Incident Response zu reagieren, wenn eine Bedrohung identifiziert wird, und aus Interaktionen mit dem Angreifer zu lernen, um die Netzwerksicherheit zu verbessern. Dieser Ansatz ist wichtig, damit ausgefeilte Bedrohungen gekontert werden können, z. B. mit Malware wie STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, TRISIS/TRITON und mit Ransomware. Außerdem sind diese Bemühungen unerlässlich zum Verständnis und zur Ausführung einer modernen, komplexen Automatisierungsumgebung und für Ursachenanalysen bei Ereignissen, die eigentlich keine Cyber-Incidents sind, sich aber über das Netzwerk manifestieren. Den Kursteilnehmern werden in diesem Kurs die Kernkompetenzen für jedes ICS-Cybersicherheitsprogramm vermittelt.

Der Kurs verwendet einen praktischen Ansatz mit zahlreichen technischen Datenmengen aus ICS Ranges, Geräten mit emulierten Angriffen und Malware aus der wirklichen Welt in den Ranges. Damit wird eine hoch simulierte Erfahrung bei der Erkennung von Bedrohungen und der Reaktion darauf geschaffen. Die Teilnehmer interagieren außerdem mit einem PLC (Programmable Logic Controller), den sie behalten dürfen, einem physischen Kit, der den Betrieb elektrischer Systeme auf der Ebene der Stromerzeugung, Übertragung und Verteilung emuliert, und virtuellen Maschinen, die als HMI (Human Machine Interface) und EWS (Engineering Workstation) eingerichtet sind.

Zusammenfassung der Kursinhalte

TEIL 1: ICS Cyber Threat Intelligence
TEIL 2: Transparenz und Asset-Identifizierung
TEIL 3: ICS-Bedrohungsdetektion
TEIL 4: Incident Response
TEIL 5: Bedrohungs- und Umgebungsmanipulation
TEIL 6: Abschlussübung

„Dieser Kurs war ein Augenöffner. Er hat nicht nur meine Kenntnisse über die Bedrohungen geschärft, denen ICS-Umgebungen ausgesetzt sind, und mir einen Rahmen für die aktive Verteidigung gegen diese Bedrohungen zur Verfügung gestellt, sondern mich auch inspiriert, mehr zu lernen.“

– Srinath Kannan, **Accenture**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/ICS515**

KURSFORMATE ICS515

Präsenzkurs | **Live online** | **OnDemand**

ICS612: **ICS Cybersecurity In-Depth™**

5	30	31
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

- Aktive und passive Methoden erlernen, mit denen Sie Informationen über eine ICS-Umgebung auf sichere Weise sammeln
- Schwachstellen in ICS-Umgebungen identifizieren
- Herausfinden, wie Angreifer Prozesse in böswilliger Absicht unterbrechen und steuern können und wie Sie sich dagegen verteidigen
- Proaktive Maßnahmen zur Verhinderung, Erkennung, Verlangsamung und Unterbindung von Angriffen implementieren
- ICS-Operationen verstehen und wissen, wie „normal" aussieht
- Drosselpunkte in eine Architektur einbauen und herausfinden, wie mit ihnen Sicherheitsvorfälle erkannt werden können und darauf reagiert werden kann
- Komplexe ICS-Umgebungen managen und die Fähigkeit entwickeln, ICS-Sicherheitsereignisse zu erkennen und darauf zu reagieren

Zielgruppe

- Erfolgreiche Absolventen des Kurses ICS410: ICS/SCADA Security Essentials haben die Grundkenntnisse, die als Voraussetzungen für diesen Kurs betrachtet werden
- Prozesssteuerungsingenieure
- System- oder Sicherheitssystemingenieure
- Aktive Verteidiger bei ICS
- Alle mit umfangreicher Erfahrung in Steuersystemen, die die Prozesse und Methoden zur Sicherung der ICS-Umgebung verstehen möchten

Berufliche Rollen im NICE Framework

- Process Control Engineer/Instrument & Control Engineer
- ICS/OT Systems Engineer

Tim Conway
Kursautor

Jason Dely
Kursautor

Christopher Robinson
Kursautor

Jeffrey Shearer
Kursautor

Bei der Perspektive und beim Ansatz zur Sicherung von OT-Umgebungen einerseits und IT-Umgebungen andererseits gibt es Unterschiede. Da jedes OT-System individuell auf die spezifischen Betriebsanforderungen einer Organisation zugeschnitten ist, stellt sich die Frage, wie diese Systeme gesichert werden können. Der fünftägige Kurs ICS612 führt Sie in unserer immersiven Betriebsumgebung von der Theorie zum praktischen Lernen. Sie erlernen Methodiken zur Identifizierung betrieblicher Schwachstellen und bauen Verteidigungsmaßnahmen durch die Rollen von Technik, Betrieb, Red Team und Blue Team auf. Sie navigieren vom grundlegenden PLC- und HMI-Betrieb zu den Komplexitäten einer erweiterten IT- und OT-Sicherheitsarchitektur und -Überwachung. Dabei gewinnen Sie Einblicke, wie Akteure den Betrieb durch ICS-Systeme und Personal angreifen. Sie festigen diese Kompetenzen in praktischen Laborübungen und schließen den Kurs mit einem Incident-Response-Szenario ab, bei dem Sie den Betrieb der Kursumgebung untersuchen und wiederherstellen. Nach Abschluss dieses Kurses wissen Sie, wie Sie ein unbekanntes System analysieren, um die Betriebsresilienz zu sichern und aufrechtzuerhalten.

Die Konzepte und Lernziele des Kurses werden primär durch praktische Laborübungen vermittelt. Die Laboreinrichtung für die Kursübungen soll eine reale Umgebung simulieren, in der ein Controller im Einsatz befindliche Geräte überwacht/steuert und ein HMI (Human Machine Interface) zur Verfügung steht, auf der Personal vor Ort die nötigen Prozessänderungen vornehmen kann. Mithilfe der Operator-Workstations in einem remoten Steuerzentrum können Systemoperatoren mit einem SCADA-System die Geräte vor Ort überwachen und steuern. Die Übungseinrichtung ist repräsentativ für eine reale ICS-Umgebung und umfasst eine Verbindung zum Unternehmen, die Datentransfers (z. B. Historian), Fernzugriff und andere typische Unternehmensfunktionen erlaubt.

Zusammenfassung der Kursinhalte

TEIL 1: Der lokale Prozess
TEIL 2: System der Systeme
TEIL 3: ICS-Netzwerkinfrastruktur
TEIL 4: ICS-Systemmanagement
TEIL 5: Abschlussübung

„Ich fand es gut, dass der Kurs so viele Laborübungen umfasste. Ich fühle mich bei OT-Ausrüstung jetzt 100 % sicherer. Das sagt eine Menge aus, weil mein Hintergrund und meine Erfahrung strikt auf IT beschränkt waren."

– Jim J., **Pilot Flying J**

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/ICS612**

KURSFORMATE ICS612

Präsenzkurs

KURS NEU IM FOKUS

ICS613: ICS/OT Penetration Testing & Assessments™

5	30	25
Tage Programm	CPEs	Laborübungen

Vermittelte Kompetenzen

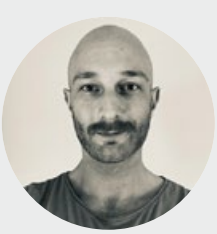
- Sichere, effektive und wertbringende Penetrationstests und Sicherheitsbewertungen mit passiven und aktiven Techniken planen und ausführen, um die betriebliche Resilienz in ICS-Umgebungen zu beurteilen
- ICS-Penetrationstests und Sicherheitsbewertungen so abstimmen, dass sie den organisatorischen und betrieblichen Sicherheitszielen des Kunden dienlich sind
- In Zusammenarbeit mit Kunden realistische ICS-Angriffsszenarien für besonders wertvolle Assets identifizieren
- Mit Stakeholdern kommunizieren und koordinieren, um Erwartungen, Ziele und Ergebnisse für ICS-Sicherheitsbewertungen zu definieren
- Die Vorteile der beiden Ansätze für aktive Tests verstehen und wissen, wie die Orientierung der Penetrationstestmethoden an der ICS-Cyber-Kill-Kette einen angemessenen Kontext in Bezug auf den Gegner für Einsatzaktivitäten, Erkenntnisse und Empfehlungen bereitstellt
- Die Effektivität und Sicherheit von Tools und Techniken bewerten, bevor sie auf ICS-Geräte und -Netzwerke angewendet werden
- Relevante Ziele identifizieren und anwendbare Gegner-TTPs auswählen, um effektive Angriffsszenarien in ICS-Penetrationstests und Sicherheitsbewertungen unabhängig vom Industriesektor zu entwickeln
- Termingerechte Statusaktualisierungen und korrekte, umsetzbare Berichte verfassen und bereitstellen, die die Ziele und Ergebnisse des Kunden unterstützen

Zielgruppe

- Fachkräfte für Cybersicherheit, deren Aufgabe es ist, industrielle Umgebungen zu beurteilen
- Fachkräfte für Cybersicherheit, die Cyberbewertungen und Penetrationstests für regulatorische Compliance durchführen müssen
- Mitglieder von Team Red, Team Blue oder Hunt-Team, Incident Responder und Penetrationstester bei ICS, die ihre eigenen Kompetenzen und die ihres Teams verbessern möchten
- Teams, die Bewertungen bei industriellen Anlagen oder Waffensystemen des US-Verteidigungsministeriums oder des Bundes durchführen
- Fachkräfte für Cybersicherheit, die Erfahrung bei der sicheren Arbeit mit industriellen Geräten und Distributed Control Systems sammeln möchten
- Erfahrene Penetrationstester und Cyberfachkräfte, die ihre Kompetenzen in Bezug auf die ICS-Domäne verbessern möchten

Jason Dely
Kursautor

Don Weber
Kursautor



Tyler Webb
Kursautor

Fachkräfte in Technik, Betrieb und Sicherheit, die weltweit in industriellen Umgebungen und Sektoren für kritische Infrastruktur arbeiten, müssen zunehmend Penetrationstests und Sicherheitsbewertungen für wichtige Systeme und Geräte durchführen. In diesem Kurs lernen die Teilnehmer die erforderlichen Kenntnisse und Kompetenzen, um diese Aufgaben sicher durchzuführen und gleichzeitig für einen zuverlässigen und robusten Betrieb zu sorgen und effektive Ergebnisse im Bereich der Cybersicherheit zu erzielen.

ICS613™ geht auf die besonderen treibenden Faktoren und Beschränkungen von ICS-Umgebungen ein und bietet eine direkte, praktische Schulung, in der Kompetenzen für Penetrationstests und die Bewertung von Geräten, Anwendungen, Architekturen, Kommunikation und Prozessumgebungen für ICS entwickelt werden. Nach Abschluss dieses Kurses sind die Teilnehmer in der Lage, in der wirklichen Welt Penetrationstests und Sicherheitsbewertungen voll einsatzfähiger Umgebungen durchzuführen.

Zusammenfassung der Kursinhalte

TEIL 1: Bewertungstypen und -konzepte

TEIL 2: Bewertungseinsätze

TEIL 3: Aktive Methode – von oben nach unten

TEIL 4: Passive Methode – von unten nach oben

TEIL 5: Aktive Bewertung und „Capture-the-Flag“-Übung

Eine detaillierte Kursbeschreibung finden Sie auf **SANS.ORG/ICS613**

KURSFORMATE ICS613

Präsenzkurs

STAY SHARP

Hoch wirksame Schulungen zur Cybersicherheit

Stay Sharp: 1- bis 3-tägige Kurzkurse

Das Kurzkursangebot von SANS Stay Sharp:

- Schulungen mit weltweit führenden Fachkräften in Cybersicherheit als Kursleiter
- Gezielte Kurzkurse, mit denen Sie spezifische technische Kenntnisse und Kompetenzen aufbauen
- Hochwertige Schulungen mit weniger Zeitverlust im Büro und zu Hause
- Praktische Schulungen, bei denen Sie das Gelernte noch in derselben Woche anwenden können
- Virtuelle Livestream-Schulungen über Live Online

Kurzkurse von SANS Stay Sharp:

ICS418: ICS Security Essentials for Leaders™

ICS418™ stattet Führungskräfte mit den Kompetenzen aus, die sie benötigen, um ein ausgereiftes ICS-Sicherheitsprogramm aufzubauen und zu pflegen. Sie lernen, Teams, Prozesse und Technologien effektiv zu managen und gleichzeitig industrielle Cyberrisiken in Bezug zu den Geschäftszielen zu setzen und so für Sicherheit und Zuverlässigkeit zu sorgen.

LDR419: Performing a Cybersecurity Risk Assessment™

LDR419™ zeigt den Teilnehmern, auf welche Risiken sie in ihrem spezifischen Organisationskontext achten müssen, wie sie diese Risiken effektiv aufdecken und wie sie der Unternehmensführung die Ergebnisse präsentieren, damit sie aktiv umgesetzt werden.

LDR433: Managing Human Risk™

LDR433™ befähigt Organisationen, den Risikofaktor Mensch zu messen und durch Verhaltensänderung und Aufbau einer starken Sicherheitskultur effektiv zu managen.

„Diese Schulung stärkt die Kompetenzen, die ich in meiner Position benötige. Anstatt drei Monate lang bei der Arbeit zu lernen, kann ich einen SANS-Kurs belegen und bin sofort bereit für meine Aufgaben.“
– Bryan G., **US-Notenbank**

SEC467: Social Engineering for Security Professionals™

SEC467™ vermittelt Ihnen die Kompetenzen, die Sie benötigen, um Ihre Sicherheitsstrategie in Bezug auf Social Engineering zu erweitern.

SEC535: Offensive AI – Attack Tools & Techniques™ NEU

Bei SEC535™ lernen Sie, KI zur Erkundung, Toolanpassung, Malware-Entwicklung und Simulation ausgereifterer Angriffe zu nutzen, um sich gegen moderne KI-gestützte Bedrohungen zu verteidigen.

SEC547: Defending Product Supply Chains™ NEU

SEC547™ vermittelt den Teilnehmern, wie sie das Risiko von Lieferkettenangriffen durch eingehende Strategien und Taktiken zum Risikomanagement in der Lieferkette auf ein Minimum beschränken.

SEC556: IoT Penetration Testing™

SEC556™ ermöglicht eine Untersuchung des gesamten IoT-Ökosystems (Internet of Things, Internet der Dinge) und vermittelt Ihnen entscheidende Fähigkeiten, die Sie benötigen, um einfache und komplexe Sicherheitsmechanismen in IoT-Geräten zu identifizieren, zu bewerten und auszunutzen.

SEC580: Metasploit for Enterprise Penetration Testing™

SEC580™ vermittelt Ihnen, wie sie die erstaunlichen Fähigkeiten des Metasploit-Frameworks in einem umfassenden Regime für Penetrationstests und Schwachstellenbeurteilung anwenden.

sans.org/mlp/stay-sharp

Live Online

SANS

CYBER RANGES

Erweitern Sie Ihre praktischen Cyberfähigkeiten durch Aufgaben wie in der wirklichen Welt. Sammeln Sie praktische Erfahrungen in sicheren, realistischen Umgebungen, damit Sie bereit sind, wenn der Ernstfall eintritt.

SANS CYBER RANGES DECKEN EIN BREITES SPEKTRUM VON DISZIPLINEN UND EINE REIHE VON SCHWIERIGKEITSSTUFEN VON EINSTEIGERN BIS ZU EXPERTEN AB

Finden Sie unsere praktischen Schulungslösungen bei unseren SANS-Schulungsveranstaltungen oder kontaktieren Sie uns, wenn Sie an einer privaten und maßgeschneiderten Lösung interessiert sind.

CYBER RANGE BOOTUP CTF

BootUp CTF

Testen Sie Ihre Cybersicherheitskompetenzen mit BootUp CTF, einem „Capture-the-Flag"-Event mit über 125 multidisziplinären Aufgaben. Beschäftigen Sie sich mit realistischen Szenarien, bei denen Sie praktische Kompetenzen und Tools anwenden, um authentische Ziele und Memory Captures in Angriff zu nehmen.

CYBER RANGE CYBER CITY

CyberCity

CyberCity ist eine Miniaturstadt im Maßstab 1:87, die durch Anlagen wie in der wirklichen Welt gesteuert wird. Gewinnen Sie praktische Erfahrung mit SCADA-gesteuerten Systemen wie Strom, Wasser, Verkehr und mehr und bereiten Sie sich auf die Herausforderungen vor, die sich in Umgebungen mit kritischer Infrastruktur an die Cybersicherheit stellen.

CYBER RANGE NETWARS

NetWars-Turnier

SANS NetWars bietet eine Suite mit sechs fortschrittlichen Ranges für alle Kompetenzniveaus, mit einer packenden Storyline für interaktives Lernen. Die facettenreichen, realistischen Aufgaben betonen die eingehende praktische Anwendung und die Bewertung wesentlicher Cybersicherheitskompetenzen des jeweiligen Fokusbereichs.

CYBER RANGE SANS SKILLS QUEST BY NETWARS

Skills Quest by NetWars

Erweitern Sie Ihre Cybersicherheitskompetenzen jederzeit und überall mit Herausforderungen im individuellen Lerntempo und (bei Bedarf) mit Anleitungstipps, die auf eine kontinuierliche Weiterentwicklung Ihrer Kompetenzen abgestimmt sind. Dieser Cyber Range ist sechs Monate lang rund um die Uhr und sieben Tage in der Woche verfügbar, so dass Sie in Ihrem eigenen Tempo lernen können.

PRAKTISCHE CYBERSCHULUNGSLÖSUNG

Von einer der vertrauenswürdigsten Ressourcen für Cybersicherheitsschulungen

Cybertalente entdecken
Identifizieren und rekrutieren Sie Personal mit Talent und Begabung für eine Rolle in der Cybersicherheit.

Branchenführende Inhalte
Bleiben Sie mit den neuesten Kenntnissen und Taktiken für Cybersicherheit stets einen Schritt voraus.

Schutz stärken
Stärken Sie den Sicherheitsstatus Ihrer Organisation durch praktische Übungen.

CPE-Punkte verdienen
Lassen Sie sich Ihre Schulungen für die berufliche Weiterbildung anerkennen.

Klare Roadmap
Folgen Sie einem strukturierten Lernpfad, um wichtige Kompetenzen auf dem Gebiet der Cybersicherheit zu meistern.

Leaderboard
Verfolgen Sie Ihren Fortschritt und messen Sie sich an Ihren Kollegen, um kontinuierliche Verbesserung voranzutreiben.

Weitere Informationen über Cyber Ranges

sans.org/cyber-ranges

SANS

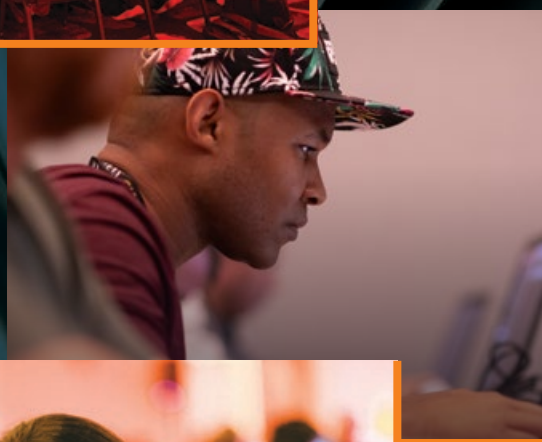
CYBER RANGES

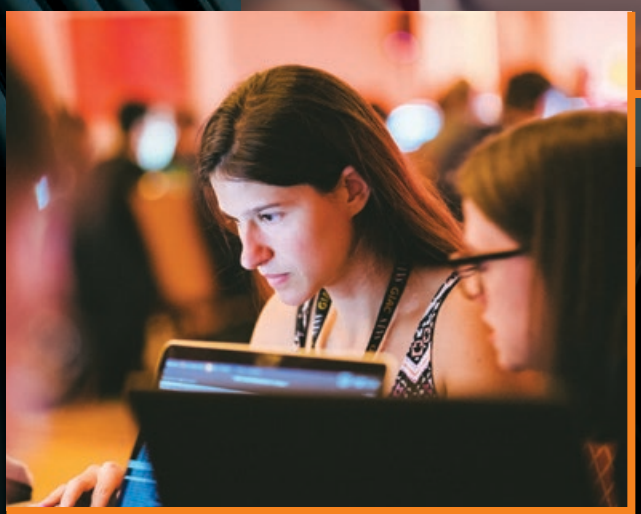
SANS Cyber Ranges bieten praktische Schulungen und Kompetenzbewertungen, mit denen Sie und Ihr Team realistische Einblicke in Stärken und verbesserungfähige Bereiche erhalten.

Range-Teilnehmer lösen Probleme und entwickeln Kompetenzen durch interaktive, narrative Übungen, die Problemstellungen in einen realistischen Kontext setzen. SANS Cyber Ranges decken ein breites Spektrum von Disziplinen und umfassende Schwierigkeitsstufen ab, von Einsteigern bis zu Experten.

Cyber Ranges werden von SANS-Kursleitern entwickelt, die für ihre Erfahrung bekannt sind, und spiegeln realistische Host- und Netzwerkinfrastrukturen wieder. Diese Ranges präsentieren Szenarien, die kontinuierlich aktualisiert werden, um die neueste Bedrohungslandschaft zu reflektieren. So stellen sie sicher, dass Lernende sich mit aktuellen und praktischen Herausforderungen beschäftigen.

> SANS bietet das Beste auf dem Gebiet der Cybersicherheitsschulungen, ob bei Schulungskursen, CTF-Veranstaltungen oder Studienabschlüssen. Ich bin froh über meine Verbindung zu SANS.
>
> – J. D., Lenovo





Core

Dieser ultimative, multidisziplinäre Cyber Range ist der umfassendste der NetWars Ranges und fördert die vielfältigsten Cyberkompetenzen in einer kooperativen Umgebung.

Cyberverteidigung

Cyber Defense NetWars konzentriert sich auf die Verhinderung, Analyse und Verteidigung gegen komplexe Angriffsszenarien aus der wirklichen Welt, u. a. Brute-Force-Angriffe und Ransomware-Kampagnen.

DFIR

Bei diesem Tool-unabhängigen Ansatz geht es um digitale Forensik, Incident Response, Threat Hunting und Malware-Analyse. Von Artefakten im Kleinen bis zu Verhaltensbeobachtungen im Großen wird alles abgedeckt.

Grid

Hier liegt der Fokus auf Technologien, die bei Systemen zur Stromerzeugung und -verteilung genutzt werden. Bei den Aufgaben geht es um Szenarien, Protokolle und Architekturen für Stromsysteme.

Healthcare

Hier liegt der Fokus auf der Sicherung von Medizintechnologie. Bei den Aufgaben geht es darum, Geräteschwachstellen aufzuspüren, Web-Anwendungen zu beurteilen und auf Ransomware-Bedrohungen zu reagieren.

ICS

Hier liegt der Fokus auf dem Betrieb von Fabrikmaschinen. Die Teilnehmer spielen in einer Werkshalle, wo sie Cyberangriffe gegen physische Geräte und Herstellungskomponenten erkennen und abwehren müssen.

SANS NETWARS BIETET EINE SUITE MIT SECHS FORTSCHRITTLICHEN RANGES FÜR ALLE KOMPETENZNIVEAUS

Verfügbar bei jeder unserer Präsenzschulungen oder als individuell angepasste Lösung in einem Cyber Range speziell für Ihr Team. Kontaktieren Sie uns, wenn Sie Informationen über individuell angepasste Ranges wünschen.

PRAKTISCHE CYBERSCHULUNGSLÖSUNG

Von einer der vertrauenswürdigsten Ressourcen für Cybersicherheitsschulungen

Cybertalente entdecken

Identifizieren und rekrutieren Sie Personal mit Talent und Begabung für eine Rolle in der Cybersicherheit.

Schutz stärken

Stärken Sie den Sicherheitsstatus Ihrer Organisation durch praktische Übungen.

Klare Roadmap

Folgen Sie einem strukturierten Pfad, um wichtige Kompetenzen auf dem Gebiet der Cybersicherheit zu meistern.

Branchenführende Inhalte

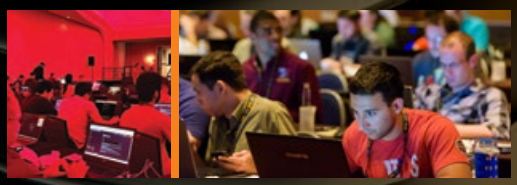
Bleiben Sie mit den neuesten Kenntnissen und Taktiken für Cybersicherheit stets einen Schritt voraus.

CPE-Punkte verdienen

Lassen Sie sich Ihre Schulungen für die berufliche Weiterbildung anerkennen.

Leaderboard

Verfolgen Sie Ihren Fortschritt und messen Sie sich an Ihren Kollegen, um kontinuierliche Verbesserung voranzutreiben.



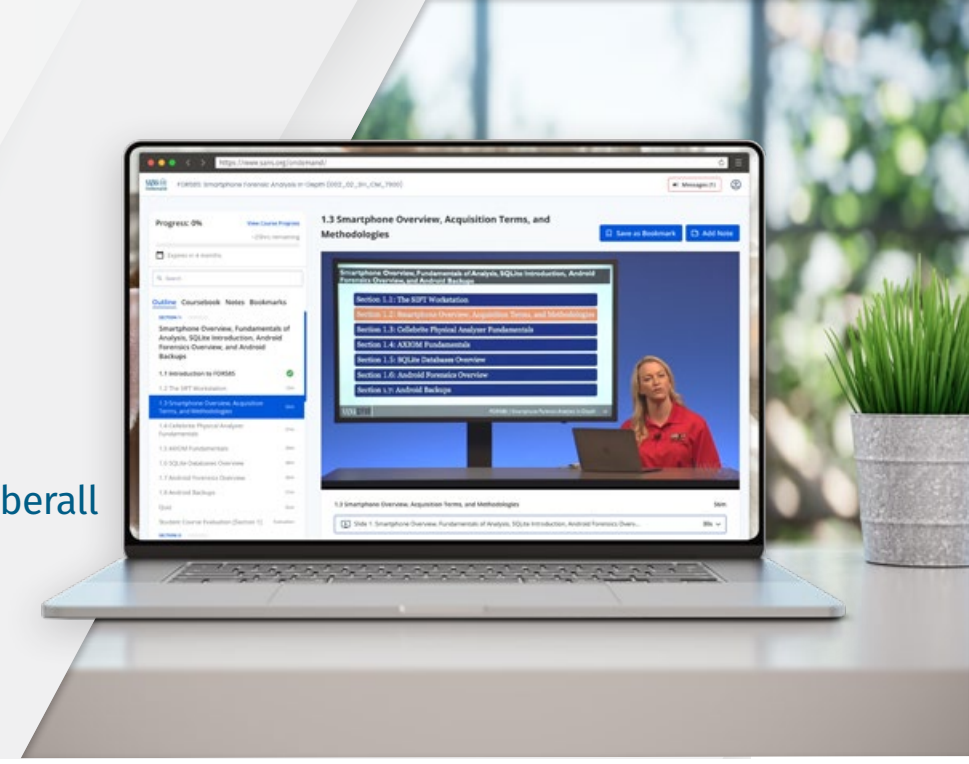
Weitere Informationen über Cyber Ranges

sans.org/cyber-ranges

SANS OnDemand

Lernen Sie mit SANS OnDemand im eigenen Tempo, jederzeit und überall

sans.org/ondemand



Mit **SANS OnDemand** können Sie unsere erstklassigen Kurse zur Cybersicherheit als Online-Schulungen im eigenen Lerntempo absolvieren. Vier Monate lang haben Sie erweiterten Zugriff auf Ihren Kurs und die Laborübungen. OnDemand bedeutet ultimative Flexibilität beim Lernen, denn Sie können die Schulungsinhalte wiederholt durcharbeiten, um das Gelernte zu vertiefen und langfristig zu festigen.

Durch das flexible Lerntempo eignet sich SANS OnDemand für jeden Lernstil.

- **Flexible SANS-Schulungen im individuellen Lerntempo**
- **Vier Monate lang Zugang zu Kursmaterialien und Laborübungen, jederzeit und überall**
- **Live-Support von GIAC-zertifizierten Fachexperten**

> „Der Kurs würde mir wohl nicht so viel nutzen, wenn ich das Kursmaterial nicht über die OnDemand-Plattform erhielte. Dort kann ich mir den Inhalt und entscheidende Themen wiederholt ansehen."
>
> – Kenneth Huss, **Cisco**

Neue Schulungs-App für SANS OnDemand

Schulungen zur Cybersicherheit **jederzeit und überall.**

Privatschulungen zur Cybersicherheit

Praktische Fähigkeiten meistern und Bedrohungen einen Schritt voraus bleiben

SANS-Privatschulungen sind von Experten geführte, praktische Cybersicherheitsschulungen, die ganz auf die Anforderungen Ihrer Organisation zugeschnitten werden. Ob Sie sich an internen Zielen orientieren, die Reisekosten senken oder die Vertraulichkeit wahren müssen – unsere flexiblen Schulungslösungen bieten maximale Wirkung.

Argumente für SANS-Privatschulungen

Exklusiv und individuell anpassbar
Eine Schulung spezifisch für Ihr Team, in einer privaten, sicheren Umgebung, fokussiert auf Themen, die für Ihr Unternehmen relevant sind

Flexibler Zeitplan
Schulungstermine, die den Anforderungen Ihrer Organisation entsprechen

Branchenspezifische Einblicke
Maßgeschneiderte Diskussionen und praktische Lerninhalte, die für Ihren Sektor relevant sind

Bequem und kostengünstig
Geringere Reisekosten und Schulung in einer kontrollierten Umgebung

Mehrere Bereitstellungsoptionen
Präsenzschulung, Live online oder Hybridformat

Erweiterte Lernoptionen
Schulungen können um Cyber Ranges, OnDemand-Inhalte zum Lernen im individuellen Tempo und GIAC-Zertifizierungen erweitert werden

Was unsere Kunden sagen

„SANS bietet die besten Schulungen zur Informationssicherheit, die Sie finden werden: praktische, realistische Kompetenzen, die sofort anwendbar sind."
– Jeff Stebelton, NetJets Inc.

„Die Privatschulung war von unschätzbarem Wert. Kollegen, die gemeinsame Zuständigkeiten haben, lernen zusammen, was die Erfahrung noch relevanter macht."
– Tonya Henderson, Health & Human Services

WEITERE INFORMATIONEN

SANS TECHNOLOGY INSTITUTE

Center of Academic Excellence in Cyber Defense (CAE-CD) laut National Security Agency (NSA)*

ENTDECKEN SIE DAS BESTE COLLEGE FÜR CYBERSICHERHEIT

BACHELOR- UND MASTER-ABSCHLÜSSE | UNDERGRADUATE- UND GRADUATE-ZERTIFIKATE

EINER DER TOP-10-INNOVATOREN BEI CYBERSICHERHEITSSCHULUNGEN LAUT *HELP NET SECURITY*

* Das SANS Technology Institute (SANS.edu) wurde aufgrund seines Beitrags zur Stärkung der nationalen Cybersicherheit von der US-amerikanischen NSA als CAE-CD eingestuft. Damit wird der Einsatz von SANS für die Entwicklung hoch qualifizierter Fachkräfte auf dem Gebiet der Cybersicherheit anerkannt, und Studierende erhalten branchenweit führende Schulungen, die sich an den nationalen Standards für Cybersicherheit orientieren und ihnen einen Wettbewerbsvorteil auf dem Arbeitsmarkt gewähren.

SANS TECHNOLOGY INSTITUTE

Erkundigen Sie sich, ob der SANS-Kurs, an dem Sie interessiert sind, für ein Zertifikat oder einen Abschluss zählt.

E-Mail **info@sans.edu** oder Telefon +1 301 241 7665

sans.edu

Bei 68 % aller Verstöße ist der Mensch ein Faktor.* Dieses kritische Risiko muss effektiv gemanagt werden.

SANS SECURITY AWARENESS

Den Risikofaktor Mensch durch Schulungen zum Sicherheitsbewusstsein managen

SANS-Schulungen zum Sicherheitsbewusstsein sind eindrucksvoll und lassen sich leicht in bestehende Rahmenwerke integrieren. Die Inhalte vertiefen das Gelernte und lassen sich skalieren, wenn der Bedarf der Organisation wächst. So erhalten Sie eine cyberresiliente Belegschaft.

Endbenutzerschulung

Maßgeschneiderte, von Experten erstellte Schulungen zum Sicherheitsbewusstsein mit messbaren Erfolg

Über 50 Module | 6 Themenbereiche | In 34 Sprachen lokalisiert

Phishing-Simulation

Von führenden Experten geschaffene Vorlagen identifizieren Risikobereiche, fördern sichere E-Mail-Praktiken und bieten kontextspezifische Schulungen.

5 Schwierigkeitsstufen | In 34 Sprachen lokalisiert | Erweiterte Detektion von Menschen

WEITERE INFORMATIONEN sans.org/security-awareness-training

*Verizon DBIR

Den Risikofaktor Mensch durch rollenbasierte Schulungen managen

Rollenbasierte SANS-Schulungsmodule sind auf optimales Teilnehmerengagement und langfristigen Lernerfolg ausgelegt, mit relevanten Inhalten zu aktuellen Cyberbedrohungen.

Grundlagen der KI-Sicherheit für geschäftliche Führungskräfte – Enterprise Edition

Diese Schulung deckt kritische Bereiche der sicheren Programmierung ab, u. a. die 10 wichtigsten Schwachstellen von OWASP und die Sicherheit von Smartphone-Apps. **8 Module** | **75 Minuten**

Schulung für Entwickler

Diese Schulung für sichere Programmierung deckt kritische Bereiche ab, z. B. die 10 wichtigsten Schwachstellen von OWASP und die Sicherheit von Smartphone-Apps. **70 Module** | **270 Minuten**

Schulung zu Grundlagen der Sicherheit – Geschäftliche Führungskräfte und Manager

Befähigt Führungskräfte, eine sichere Umgebung zu schaffen und aufrechtzuerhalten, die für den betrieblichen und strategischen Erfolg unabdingbar ist. **10 Module** | **60 Minuten**

Schulung zu Grundlagen der Sicherheit – IT-Administratoren

Eine immersive Schulung für IT-Fachkräfte mit realistischen Szenarien, die Kompetenzen durch Aufgaben mit zunehmendem Schwierigkeitsgrad verbessert. **12 Module** | **90 Minuten**

Schulung zur industriellen Steuersystemen

Vermittelt grundlegende Techniken zum Schutz von industriellen Steuersystemen und kritischer Infrastruktur. **22 Module** | **144 Minuten**

Rollenbasierte PCI-DSS-Schulung

Eine rollenspezifische Schulung zur Sicherung von Zahlungsumgebungen und zur Orientierung an PCI-DSS-Standards. **6 Lernpfade** | **28 Minuten**

GIAC
CERTIFICATIONS

GIAC-Zertifizierungen

Cybersicherheitszertifizierung auf höchstem Niveau

CYBERLIVE

Praktische Kompetenztests mit CyberLive

Die Messlatte bei den GIAC-Zertifizierungen liegt nun noch höher

CyberLive stellt realistische Tests direkt für Cybersicherheits-Fachkräfte zur Verfügung und hilft ihnen so, Fertigkeiten, Fähigkeiten und Verständnis unter Beweis zu stellen.

Weitere Informationen auf **giac.org/cyberlive**

„Ich weiß zu schätzen, dass GIAC-Fachkräften sofort Respekt und Vertrauen entgegengebracht wird. Andere wissen, dass harte Arbeit in der Zertifizierung steckt, und erkennen die Kompetenzen und Kenntnisse an, die sie mit sich bringt."

– Ben Boyle, GXPN, GDAT, GWAPT

Umfragen zufolge bevorzugen 82 % der Organisationen bei der Einstellung zertifizierte Personen, und GIAC-Zertifizierungen werden weltweit in Tausenden von Stellenangeboten für Cybersicherheit als bevorzugte Qualifizierungen angegeben.

Mit einer GIAC-Zertifizierung beweisen Sie, dass Sie die spezifischen Kompetenzen haben, die Arbeitgeber für die Sicherheit ihres Unternehmens benötigen. Unsere praktischen CyberLive-Tests führen die Kompetenzverifizierung noch weiter und signalisieren Arbeitgebern, dass Sie kritische Kompetenzen gemeistert haben.

VORTEILE FÜR ORGANISATIONEN

81 % der Kandidaten leisten qualitativ höherwertige Arbeit.

VORTEILE FÜR STUDIERENDE

92 % haben mehr Vertrauen in ihre Fähigkeiten.

MEHR INFO

giac.org

Weitere Informationen auf GIAC.ORG

Vorbereitung Ihres Führungsteams

Immersive Übung zur Vorbereitung Ihres Führungsteams

SANS Executive Cyber Exercises (ECE) sind Cyberübungen, in denen Ihr Führungsteam durch eine simulierte Krise geleitet wird. Unsere Branchenexperten führen einen Sicherheitsvorfall durch und coachen gleichzeitig Ihre Stakeholder zu Best Practices bei der Krisenreaktion.

Organisationen, die mit unserer Schulung eine Krisenreaktion üben, können:

- Die Krisenbereitschaft der Organisation auf Vorstandsebene beurteilen
- Strategien zur Schadensbegrenzung anwenden
- Best Practices der Branche in den Bereichen Cybersicherheit, Organisationsstruktur und Krisenkommunikation anwenden
- Regulatorische Anforderungen und Governance-Auflagen erfüllen

SANS | EXECUTIVE CYBER EXERCISES

PREPARE | PRACTICE | PREVAIL

SANS Summits

BRANDNEUE INHALTE

NIE ZUVOR GESEHENE FORSCHUNG

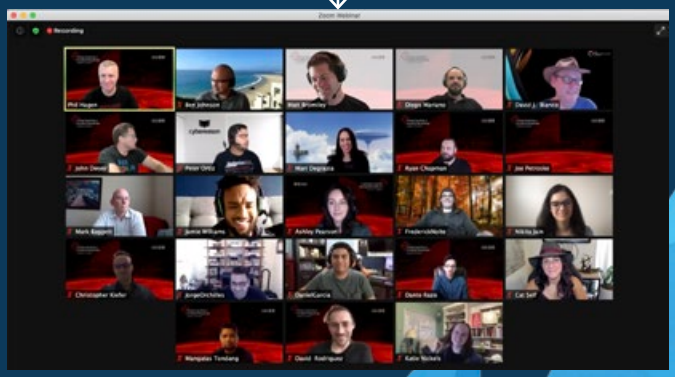
ANWENDBARE LÖSUNGEN

IHRE Community arbeitet GEMEINSAM und SCHNELL an Lösungen für Cybersicherheit

Als Präsenzveranstaltung mit exklusiven Vorteilen

ODER

Online kostenlos für die globale Community



5 gute Gründe für eine Teilnahme an SANS Summits

1. Detaillierte technische Vorträge zu Kompetenzen und Techniken für „First Release“ oder „Zero-Day“
2. Interaktive Podiumsdiskussionen mit Branchenfachleuten
3. Networking mit führenden Fachleuten und Peers, die mit den gleichen schwierigen Problemen konfrontiert sind wie Sie
4. Zugang zu Aufzeichnungen und Präsentationen des Summit
5. Als Teilnehmer profitieren Sie von einer frischen Perspektive, besseren Verbindungen zur Community und neuen Tools, die Sie bei Ihrer Arbeit sofort nutzen können

„In fast jeder Sitzung habe ich etwas erfahren, was ich noch nicht wusste, und zusätzliche Tools und Methoden kennengelernt, die mir helfen werden.“

– Dallas M., **PepsiCo**

Kommende Cybersecurity Summits

- **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**

Weitere Informationen

Gratisressourcen zur Cybersicherheit sans.org/free

Kostenlose Schulungen und Veranstaltungen

SANS-Kurse zur Probe
In einer kostenlosen, einstündigen Kursvorschau erkunden Sie Themen und Kompetenzniveaus und finden so den richtigen Kurs.
sans.org/course-preview

Summit-Präsentationen
Präsentationen zu aktuellen Themen
sans.org/presentations

SANS Cyber Aces Online
Dieser kostenlose Online-Kurs vermittelt die Kernkonzepte zur Beurteilung und zum Schutz von Informationssicherheitssystemen
cyberaces.org

SANS-Workshops
Praktische, virtuelle Schulungen als Gelegenheit, sich intensiv mit dem Kursmaterial zu beschäftigen
sans.org/workshops

NetWars-Turniere
Gratisteilnahme an einem NetWars Cyber Range bei der Anmeldung zu einer 4- bis 6-tägigen Liveschulung
sans.org/cyber-ranges/upcoming-netwars-tournament

Soziale Medien

Finden Sie uns unter **@SANSInstitute** und nehmen Sie Kontakt mit uns auf, damit Sie stets über die neuesten SANS-Ressourcen informiert sind

New2Cyber
Cyberverteidigung
Offensivoperationen
DFIR
Führung
Cloud
ICS
Sicherheitsbewusstsein
Cyber Ranges
https://x.com/sansinstitute

Webcasts

sans.org/webcasts

Blogs

sans.org/blog

Podcasts

Blueprint
Fortgeschrittene Kompetenzen zur Cyberverteidigung

Cloud Ace
Die Zukunft der Cloud-Sicherheit

GIAC: Trust Me, I'm Certified
Führend in der Cybersicherheitsbranche

Internet Storm Center
Tägliche Updates zu InfoSec-Bedrohungen

sans.org/podcasts

SANS Cyber Academies

VetSuccess Academy
Women's Immersion Academy
Cyber Workforce Academy
Cyber Diversity Academy
HBCU Academy
sans.org/scholarship-academies

Newsletter

NewsBites
Eine halbwöchentlich erscheinende Zusammenfassung der wichtigsten aktuellen Nachrichtenartikel zum Thema Cybersicherheit

@Risk
Eine wöchentliche Zusammenfassung neu entdeckter Angriffsvektoren, Schwachstellen mit aktiven neuen Exploits und anderer wertvoller Daten

OUCH!
Ein kostenloser monatlicher Newsletter zum Sicherheitsbewusstsein für allgemeine Computernutzer in mehr als 20 Sprachen

sans.org/newsletters

Gratisressourcen zur Cybersicherheit

Internet Storm Center
Kostenloser Analyse- und Warndienst
isc.sans.edu

Gratistools
Über 150 Open-Source-Tools von SANS-Lehrkräften
sans.org/tools

Whitepaper
Beiträge zu aktuellen Themen
sans.org/white-papers

Poster und Cheatsheets
sans.org/posters

Vorlagen für Sicherheitsrichtlinien
Vorlagen für Sicherheitsrichtlinien von Fachexperten und führenden Köpfen der Informationssicherheit für Ihre Nutzung
sans.org/information-security-policy

CIS Controls v8
Die CIS Controls sind empfohlene Maßnahmen zur Cyberverteidigung mit spezifischen und umsetzbaren Methoden, die heute am stärksten verbreiteten und gefährlichsten Angriffe zu stoppen.
sans.org/blog/cis-controls-v8

Jährlicher Bericht zum Sicherheitsbewusstsein
Nutzen Sie datenorientierte Maßnahmen zum Umgang mit dem Risikofaktor Mensch und bringen Sie Ihr Programm in die Zukunft des Sicherheitsbewusstseins
https://www.sans.org/mlp/ssa-2024-security-awareness-report/

NICE Framework
Nutzen Sie das NICE Framework mit anerkannten Cybersicherheits-Zertifizierungen von GIAC als Leitfaden für Ihre Karriere
giac.org/workforce-development/government/niceframework

Treten Sie kostenlos der SANS.org-Community bei

Durch Mitgliedschaft in der SANS.org-Community erhalten Sie Zugang zu aktuellen Ressourcen, die unsere fachkundigen Lehrkräfte täglich beitragen und die sonst nirgends zu finden sind, u. a. Nachrichten zur Cybersicherheit, Schulungen und Gratistools.

Erstellen Sie auf sans.org/account/create noch heute Ihr Gratiskonto und erhalten Sie Zugang zu den oben erwähnten Ressourcen und noch mehr!

Zentral für alles, was wir tun, ist das Ziel, das SANS verfolgt: Cybersicherheits-Fachkräfte mit praktischen Kompetenzen und Kenntnissen zu befähigen, damit die Welt sicherer wird.

Unserer Überzeugung nach muss man Führung vorleben. Deshalb gehen wir Partnerschaften mit den führenden Praktikern der Branche ein, um Schulungs-, Zertifizierungs- und Studienprogramme auf dem neuesten Stand zu entwickeln und bereitzustellen. Unsere Absolventen lernen von Menschen, die heute vor Ort aktiv sind und an der Front neue Wege zur Sicherung unserer Cyberdomäne testen, ausprobieren und entwerfen.

Wenn Sie sich für SANS entscheiden, machen Sie nicht nur einen Kurs – Sie werden Teil unserer Community. Ob Sie neu bei Cyber sind oder zu den Führungskräften gehören, wir werden Sie auf Ihrem Weg unterstützen. Dazu bieten wir eine Reihe von Karrierepfaden, Gratisressourcen, Summits und verschiedene Modalitäten zum Schulungszugriff an. Eine Investition in SANS ist eine Investition in Ihre Karriere, Ihre Organisation und Ihre Zukunft.

Das SANS-Versprechen: Alle, die eine SANS-Schulung abschließen, können die gelernten Kompetenzen und Kenntnisse bei der Rückkehr zur Arbeit noch am selben Tag anwenden.

Den aktuellen Schulungskalender finden Sie auf
www.sans.org/events

SANS | GIAC CERTIFICATIONS