2023

Real World Ready

New Cyber Trends & Training in 2023

www.sans.org

Introduction

ChatGPT, Quantum Cryptography, CNAPP, AI/ML Toolchains, NFTs, Cloud Encryption, SaaS and Social Media Meltdowns.

Some say that 2023 is the beginning of the next technological revolution. The great technology experiments performed during the peak of the Covid-19 pandemic are yielding their results in 2023. Consumer behavior changed, companies adapted, and everything went digital to thrive in a new digital-driven universe.

With great successes also comes learnings from those experiments that were not so successful. We learned that virtual reality can't completely replace real-life experience. Large social networks can only sustain relevance for so long, making way for smaller, more agile ways to connect. The second dot com bust is occurring as tech companies downsize after years of rampant growth. And, with increasing geopolitical conflict, we are a cyber-attack away from damaging our world's most critical infrastructure.

The one thing that we do know about 2023 is that you must **expect the unexpected**, and SANS Institute is readying our students and partners for whatever may come. In this eBook, our cyber experts outline the skills, techniques, and training needed to be real-world ready for 2023.

"The biggest trend is AI, and that will continue through 2023. We will see changes in how people work with the continued dissolving of the traditional office workspace. Many leases up for renewal will lapse or companies will find smaller, more experiential spaces to support a hybrid workforce. The move to remote will become permanent for knowledge workers."

- Rob Lee, Chief Curriculum Officer, SANS Institute

Related Resources

SANS Webcast: Insights on Remote Access Cybersecurity and Workplace Flexibility

SANS Whitepaper: Remote Workforce Impact on Threat Defenses

2023 is the Year of Resilience

The must-haves for cybersecurity professionals

Futurists have declared 2023 the start of the 5th Industrial Revolution – the shift beyond digitization of the past two decades into one where technology and humanity are increasing intertwined. Instead of simply upgrading systems, we are continuing to evolve with them.

Artificial Intelligence has merged into our day-to-day with tools that intuitively adjust – from automating our homes to writing copy. Technology expands further into space as satellites speed connectivity and are lifelines for our physical infrastructure. Cloud centralizes information to make almost any software, platform, or experience as a service. Open-Source Intelligence (OSINT) has introduced new threats, as it exposes how much information is truly public. And science fiction is now a reality with the advent of the Metaverse.

The past few years has shown us that despite advancements in technology, the most valuable skills are the ones that are intrinsically human. The ability to connect with another person, empathize, and persuade is more important than ever. Companies must be able to change, flex, and do it swiftly, as the world speeds faster than our established processes can keep up.

We asked SANS faculty to weigh in on the must-have skills and attitudes a cyber professional or SOC team needs to be ready for what's coming. From emerging technology to hardening "soft skills," these industry insiders had one overarching theme: Today's cyber community must be willing to learn – to have a growth mindset, experiment with new modes, and be resilient as the world changes.

"The only thing certain in cyber is never-ending change. Cyber professionals need to be ready for 'what's next.' Your best bet is to follow a well-rounded curriculum teaching fundamentals like networking, scripting, and operating system security, avoiding chasing the tool or the skill of the day."

- Dr. Johannes Ullrich, Dean of Research, SANS Technology Institute

The Technical Knowledge You Need

Thinking about your next steps for training? SANS Faculty outline the technical areas that are gaining predominance in 2023.

Artificial Intelligence & Machine Learning

Cloud Identity and Access Management

Cloud as a Service (CaaS)

Core System & Network Cloud Knowledge

Incident Response

Open-Source Intelligence (OSINT)

OSI Model & Platform Testing

Satellite & Extra-Terrestrial Broadband and Infrastructure

Terraform & Infrastructure as Code

Threat Hunting

"To thrive in today's cybersecurity landscape, practitioners increasingly need skills in multi-cloud environments. Gone are the days of relying on your own in-house data centers and networks or migrating to a single cloud.

Organizations are increasingly using multiple cloud providers on both Infrastructure-as-a-Service and Software-as-a-Service modalities. Additionally, solid understanding of Identity and Access Management (IAM) architectures and infrastructures are increasingly important for modern organizations. And finally, a solid knowledge of secure deployment and operation of remote access infrastructures is vital."

- Ed Skoudis, President, SANS Technology Institute

Related Resource

SANS Webcast: How to Design a Least Privilege Architecture in AWS

"Artificial intelligence and machine learning are advancing quickly. ChatGPT showed us a glimpse of what it could mean for the future of information technology and security. Professionals must continue to learn and grow, and to adapt and work with the technology. Learning should be a lifelong endeavor."

- Stephen Sims, SANS Fellow

Related Resource

SANS Whitepaper: The Future of AI: Human Machine Intelligence and Automating the SOC

> *"You must have the ability to prioritize defensive strategies and activities by leveraging industry frameworks (like MITRE ATT&CK for example) to understand what TTPs are most applicable to your organization. This helps the security team stay focused on what best reduces the risk of high-impact cybersecurity events."*
>
> **- John Hubbard, SANS Senior Instructor**

Related Resource

SANS Webcast: Cybersecurity Frameworks for CISOs

The Soft Skills to Strengthen

Overwhelmingly, SANS Faculty felt that soft skills were the most important areas for professionals to strengthen. Comfort in interacting face-to-face, writing compelling business cases, and gaining critical communication skills will move cybersecurity from the backroom to the boardroom.

To continue to be successful, organizations should encourage agile thinking. One-size-fits-all is for the past. Tomorrow is about being able to quickly shift focus as business needs change. This includes upskilling cyber talent in leadership and encouraging IT professionals to learn cyber. Personal adaptability will lead to organizational resilience.

Adaptability
Agility
Business Fundamentals
Collaboration
Communication
Critical Thinking
C-Suite Presentations
Data Visualization
Growth Hacking
How to Learn
Leadership
Persuasion
Problem Solving
Social Engineering
Resilience
Threat Hunting
Troubleshooting
Writing

"All of us need to strengthen how we communicate and interact with humans: collaborating, communicating, and persuading."

- Lenny Zeltser, SANS Fellow

"100% agree on communication skills. Cyber professionals need to add a little bit of social engineering to that. As in, how to get IT or other departments to do what I want and make it seem like it was their idea all along."

- Tony Turner, CEO and Founder of Opswright

"Communication, troubleshooting, persuasion, and core system, network, and cloud knowledge are top of the list."

- Stephen Mathezer, SANS Certified Instructor

"Writing."

- Katie Nickels, SANS Certified Instructor

"Communication is something everyone could use more of."

- Jonathan Kirby, SANS SROC Engineer

"Great communication skills and critical thinking skills never go out of style and are a MUST for every cybersecurity practitioner."

- Ed Skoudis, President, SANS Technology Institute

Related Resource

SANS Webcast: How to work in ways that will make your boss take notice!

The Backroom to the Boardroom

Wherever 2023 takes us, there is one path that is critical as we move further into a hybrid technology-human existence. Chief Information Security Officers (CISOs) must be part of the top level of every organization, because protecting assets, data, systems, and people is at the heart of every organization's mission. Hence, CISOs need to be driving the conversation of how not only to protect, but to push the limits of what could be.

Conversely, every executive – whether in IT, or finance, or marketing - should have a basic understanding of leading in a virtual world. Providing foundational cybersecurity knowledge to your leadership gives every member of your leadership team the same vocabulary when responding to a crisis and securing the enterprise.

The future is here. Those who seize the opportunity will quickly rise. As SANS has seen from the rapid growth of our Cybersecurity Leadership curriculum, the cyber community is ready for their seat in the boardroom. Working together, we can be stewards of our collective mission to make the world a safer place for all.

Related Resource

SANS Leadership Perspective on Ransomware: Collective thoughts from SANS Cybersecurity Leadership Instructors

New & In Development for 2023

The cyber landscape is changing every day. To meet these needs, we all need to adapt. These new and in-development courses are on the cutting edge, helping you to advance your security posture and repel or manage the threats on the horizon. Consider adding these courses to your training plans in 2023 and beyond.

Cyber Defense & Blue Team

New Courses

SEC673: Advanced Information Security Automation with Python	SEC673 is designed as the logical progression point for students who have completed SEC573: Automating Information Security with Python, or for those who already familiar with basic Python programming concepts. We jump immediately into advanced concepts. SEC673 looks at coding techniques used by popular open-source information security packages and how to apply them to your own Python cybersecurity projects.	**Author:** Mark Baggett **Course Sections:** 6 **For More Info:** sans.org/sec673
SEC586: Security Automation with PowerShell	SEC586: Security Automation with PowerShell: Defensive PowerShell teaches deep automation and defensive tactics using PowerShell. Learn how to automate everything from regular hardening and auditing tasks to advanced defenses. This course will provide you with skills for near real-time detection and response and elevate your defenses to the next level. **Refreshed case studies, examples, and labs**	**Author:** Josh Johnson **Course Sections:** 6 **For More Info:** sans.org/sec586
SEC595: Applied Data Science and Machine Learning for Cybersecurity Professionals	SEC595 provides students with a crash-course introduction to practical data science, statistics, probability, and machine learning. The course is structured as a series of short discussions with extensive hands-on labs that help students to develop useful intuitive understandings of how these concepts relate and can be used to solve real-world problems. If you've never done anything with data science or machine learning but want to use these techniques, this is the course for you.	**Author:** David Hoelzer **Course Sections:** 6 **For More Info:** sans.org/sec595
SEC497: Practical Open-Source Intelligence (OSINT)	SEC497 provides practical, real-world tools and techniques to help individuals perform OSINT research safely and effectively. SEC497 is an action-oriented course on OSINT, providing real-world examples, hands-on labs, and techniques that can be applied immediately. **Updated course content and labs**	**Author:** Matt Edmondson **Course Sections:** 6 **For More Info:** sans.org/sec497

In Development

SEC406: Essential Linux Skills for the Security Professional	Whether red, blue, forensics, ICS, mobile - it doesn’t matter what area you work in or vertical you support, you must know Linux. But if you have only lived in a “Windows” world until now, that can pose a real challenge. This course is for you. We will break it all down to get you up and running on Linux in no time. **Beta – Winter 2023**	**Author:** Mark Baggett **Course Sections:** 6
SEC547: Defending Product Supply Chains	The threat landscape has changed, and gone are the days when erecting a strong perimeter is sufficient to keep adversaries at bay. Supply chain attacks are effective in bypassing traditional defenses because they act as a sort of “Maginot Line”, circumventing traditional controls and often inviting the adversary inside through the use of “trusted” technologies. SEC547 covers the overarching threat landscape and provides real-world examples of how these attacks work and why they are effective and outlines actionable takeaways for students to bring back to their own environments.	**Author:** Tony Turner **Course Sections:** 3

Industrial Control Systems

New Courses

ICS418: ICS Security Essentials for Managers	ICS418 empowers leaders responsible for securing critical infrastructure and operational technology environments. The course addresses the need for dedicated ICS security programs, the teams that run them, and the skills required to map industrial cyber risk to business objectives to prioritize safety. ICS418 will help you manage the people, processes, and technologies necessary to create and sustain lasting ICS cyber risk programs while promoting a culture of safety, reliability, and security.	**Author:** Dean Parsons & Jason D. Christopher **Course Sections:** 2 **For More Info:** sans.org/ics418

Cloud Security

New Courses

SEC388: Introduction to Cloud Computing and Security	This course steps through the many facets of cloud: from establishing your very own cloud account in which you will explore the "Big Three" cloud vendor of your choice (Amazon Web Services, Azure, and Google Cloud Platform), and learn about services to enhance operations, maintenance, and security.	**Author:** Serge Borso **Course Sections:** 3 **For More Info:** sans.org/sec388
SEC549: Enterprise Cloud Security Architecture	A shift to the cloud requires cybersecurity professionals to reorient their security goals around a new threat model to enable business requirements while improving their organization's security posture. SEC549 takes an architectural lens to enterprise-scale, cloud infrastructure challenges, addressing the security considerations architects need to address when tasked with business expansion into the cloud, from the secure usage of shared cloud-hosted data to the centralization of workforce identity.	**Author:** Kat Traxler & Eric Johnson **Course Sections:** 5 **For More Info:** sans.org/sec549

Digital Forensics & Incident Response

New Courses

FOR509: Enterprise Cloud Forensics and Incident Response	The world is changing and so is the data we need to conduct our investigations. Cloud platforms change how data is stored and accessed. They remove the examiner's ability to put their hands directly on the data. Many examiners are trying to force old methods for on-premises examination onto cloud hosted platforms. Rather than resisting change, examiners must learn to embrace the new opportunities presented to them in the form of new evidence sources. FOR509: Enterprise Cloud Forensics addresses today's need to bring examiners up to speed with the rapidly changing world of enterprise cloud environments by uncovering the new evidence sources that only exist in the cloud.	**Author:** David Cowen, Pierre Lidome, Josh Lemon & Megan Roddie **Course Sections:** 6 **For More Info:** sans.org/for509
FOR608: Enterprise-Class Incident Response & Threat Hunting	Enterprises today have thousands - maybe even hundreds of thousands - of systems ranging from desktops to servers, from on-site to the cloud. Although geographic location and network size have not deterred attackers in breaching their victims, these factors present unique challenges in how organizations can successfully detect and respond to security incidents. When sizeable organizations suffer a breach, the attackers seldom compromise one or two systems. Without the proper tools and methodologies, security teams will always find themselves playing catch-up, and the attacker will continue to achieve success. FOR608: Enterprise-Class Incident Response & Threat Hunting focuses on identifying and responding to incidents too large to focus on individual machines.	**Author:** Mathias Fuchs, Mike Pilkington & Tarot (Taz) Wake **Course Sections:** 6 **For More Info:** sans.org/for608
FOR710: Reverse-Engineering Malware: Advanced Code Analysis	Developing deep reverse-engineering skills requires consistent practice. FOR710: Reverse-Engineering Malware - Advanced Code Analysis prepares malware specialists to dissect sophisticated Windows executables, such as those that dominate the headlines and preoccupy incident response teams across the globe. This course not only includes the necessary background and instructor-led walk throughs, but also provides students with numerous opportunities to tackle real-world reverse engineering scenarios during class. Includes extended CTF.	**Author:** Anuj Soni **Course Sections:** 5 **For More Info:** sans.org/for710
FOR532: Enterprise Memory Forensics In-Depth	Replacement to FOR526 - Memory forensics ties into many disciplines in cyber investigations. From the classical law enforcement investigations that focus on user artifacts via malware analysis to large-scale hunting, memory forensic has numerous applications that for many teams are still terra incognita. The FOR532 Enterprise Memory Forensics In-Depth course strives to change that and significantly speed up your incident response, threat hunting and malware analysis.	**Author:** Mathias Fuchs **Course Sections:** 4 **For More Info:** sans.org/for532

FOR528: Ransomware for Incident Responders	FOR528 provides the hands-on training required for those who may need to respond to ransomware incidents. The term “ransomware” no longer refers to a simple encryptor that locks down resources. The advent of Human-Operated Ransomware (HumOR), along with the evolution of Ransomware-as-a-Service (RaaS), have created an entire ecosystem that thrives on hands-on-the-keyboard, well-planned attack campaigns. Our course uses deftly devised, real-world attacks and their subsequent forensic artifacts to provide you, the analyst, with all that you need to respond when the threat becomes a reality.	**Author:** Ryan Chapman **Course Sections:** 4 **For More Info:** sans.org/for528
FOR498: Data Acquisitions and Rapid Triage	A digital forensic acquisition training course, FOR498 provides the necessary skills to identify the many and varied data storage mediums in use today, and how to collect and preserve this data in a forensically sound manner despite how and where it may be stored. It covers digital acquisition from computers, portable devices, networks, and the cloud. It then teaches the student Battlefield Forensics, or the art and science of identifying and starting to extract actionable intelligence from a hard drive in 90 minutes or less. **New course name**	**Author:** Kevin Ripa & Eric Zimmerman **Course Sections:** 6 **For More Info:** sans.org/for498

In Development

FOR577: LINUX Incident Response & Analysis	LINUX powers a vast range of business-critical systems across the globe. From webservers to database platforms, to network hardware to security appliances, LINUX can often be found “under the hood” making sure the system just keeps working. This course gives incident responders and forensic investigators the knowledge they need to understand how the systems work, how attackers compromise environments and how to respond and investigate in an effective manner. **Beta - Late 2023**	**Author:** Tarot (Taz) Wake **Course Sections:** 6
FOR589: Cybercrime Intelligence	FOR589 teaches students how to hunt for Criminal Intelligence (CRIMINT) on the Dark Web and how to infiltrate adversary infrastructure through covert sock puppet accounts using advanced Human Intelligence (HUMINT) tradecraft. Learn to analyze criminal “on-chain” financial transactions using Blockchain Intelligence (BLOCKINT) tools and how to identify, analyze, and extract cryptocurrency artifacts from criminal devices in computer and mobile forensics investigations. **Beta - Late 2023**	**Author:** Sean O’Connor, Will Thomas & Trevor Giffen **Course Sections:** 5

Offensive Operations

New Courses

SEC598: Security Automation for Offense, Defense, and Cloud	SEC598: Security Automation for Offense, Defense, and Cloud will equip you with the expertise to apply automated solutions to prevent, detect, and respond to security incidents. Students first train to understand the concept of automation, then learn how existing technologies can be best leveraged to build automation stories that translate repeatable problems to automated scripts.	**Author:** Jeroen Vandeleur **Course Sections:** 6 **For More Info:** sans.org/sec598
SEC565: Red Team Operations and Adversary Emulation	Develop and improve Red Team operations for security controls in SEC565 through adversary emulation, cyber threat intelligence, Red Team tradecraft, and engagement planning. Learn how to execute consistent and repeatable Red Team engagements that are focused on the effectiveness of the people, processes, and technology used to defend environments.	**Author:** Jean-Francois Maes & Jorge Orchilles **Course Sections:** 6 **For More Info:** sans.org/sec565
SEC554: Blockchain and Smart Contract Security	SEC554 will teach you all topics relevant to securing, hacking, and using blockchain and smart contract technology. The course takes a detailed look at the technology that underpins multiple implementations of blockchain, the cryptography and transactions behind them, the various smart contract languages like Solidity and Rust, and the protocols built with them like NFTs, DeFi, and Web3. The labs in the course provide the hands-on training and tools needed to deploy, audit, scan, and exploit blockchain and smart contract assets, as well as actively learn how to defend them and identify threats and threat actors using them for malicious purposes.	**Author:** Steven Walbroehl **Course Sections:** 5 **For More Info:** sans.org/sec554
SEC556: IoT Penetration Testing	SEC556 facilitates examining the entire IoT ecosystem, helping you build the vital skills needed to identify, assess, and exploit basic and complex security mechanisms in IoT devices. This course gives you tools and hands-on techniques necessary to evaluate the ever-expanding IoT attack surface.	**Author:** Larry Pesce, James Leyte-Vidal & Steven Walbroehl **Course Sections:** 3 **For More Info:** sans.org/sec556
SEC661: ARM Exploit Development	SEC661 is designed to break down the complexity of exploit development and the difficulties with analyzing software that runs on IoT devices. Students will learn how to interact with software running in ARM environments and write custom exploits against known IoT vulnerabilities.	**Author:** John deGruyter **Course Sections:** 2 **For More Info:** sans.org/sec661

SEC467: Social Engineering for Security Professionals	SEC467 will prepare you to add social engineering skills to your security strategy. In this course, you will learn how to perform reconnaissance on targets using a wide variety of sites and tools, create and track phishing campaigns, and develop media payloads that effectively demonstrate compromise scenarios. You will also learn how to conduct pretexting exercises, and you will put what you have learned into practice with a fun Capture-the-Human exercise. SEC467 will open up new attack possibilities, help you better understand the human vulnerability in attacks, and provide you with hands-on practice with snares that have been proven effective.	**Author:** James Leyte-Vidal & Dave Shackleford **Course Sections:** 2 **For More Info:** sans.org/sec467
SEC670: Red Teaming Tools – Developing Windows Implants, Shellcode, Command and Control	SEC670 prepares you to create custom compiled programs specifically for Windows and introduces students to techniques that real nation-state malware authors are currently using. You will learn the essential building blocks for developing custom offensive tools through required programming, APIs used, and mitigations for techniques covering privilege escalation, persistence, and collection.	**Author:** Jonathan Reiter **Course Sections:** 6 **For More Info:** sans.org/sec670

In Development

SEC446: Hardware Assisted Hacking	Tightly packed with tips, techniques, and hands-on procedures, this course teaches the foundations of both hardware theory and hardware practice, as well as how they relate to hardware and software security. **Beta 2023**	**Author:** Monta Elkins **Course Sections:** 5
SEC568: Combating Supply Chain Attacks with Product Security Testing	Think Red, Act Blue – Attackers are using new methods of compromising software supply chains that bypass traditional security controls on products spanning multiple attack surfaces. SEC568 is a complete training program designed to equip you with the skills and knowledge necessary to execute product security assessments through deeply technical risk analysis.	**Author:** Douglas McKee & Ismael Valenzuela **Course Sections:** 5

Leadership

New Courses

AUD507: Auditing Systems, Applications, and the Cloud	Performing IT security audits at the enterprise level can be an overwhelming task. It is difficult to know where to start and which controls should be audited first. Audits often focus on things that are not as important, wasting precious time and resources. Management is left in the dark about the real risk to the organization's mission. Operations staff can't use the audit report to reproduce or remediate findings. AUD507 gives the student the tools, techniques and thought processes required to perform meaningful risk assessments and audits. Learn to use risk assessments to recommend which controls should be used and where they should be placed. Know which tools will help you focus your efforts and learn how to automate those tools for maximum effectiveness. 20 Hands-On Exercises.	**Author:** Clay Risenhoover **Course Sections:** 6 **For More Info:** sans.org/aud507
MGT433: Managing Human Risk	This intense three-day course enables you to build, manage, and measure a mature awareness program that proactively engages your workforce and effectively manages your human risk.	**Author:** Lance Spitzner **Course Sections:** 3 **For More Info:** sans.org/mgt433
MGT516: Building and Leading Vulnerability Management Programs	Vulnerability, patch, and configuration management are not new security topics. In fact, they are some of the oldest security functions. Yet, we still struggle to manage these capabilities effectively. The quantity of outstanding vulnerabilities for most large organizations is overwhelming, and all organizations struggle to keep up with the never-ending onslaught of new vulnerabilities in their infrastructure and applications. When you add in the cloud and the increasing speed at which all organizations must deliver systems, applications, and features to both their internal and external customers, security may seem unachievable. This course will show you the most effective ways to mature your vulnerability management program and move from identifying vulnerabilities to successfully treating them. **New course name**	**Author:** Johnathan Risto & David Hazar **Course Sections:** 5 **For More Info:** sans.org/mgt516

MGT553: Cyber Incident Management	Incident Response (IR) is the technical analysis and response activities that stem from a cyber breach, compromise, or attack. Incident Management (IM) is the layer above the IR activities, and it is responsible for the coordination and liaison with the rest of the organization, external third parties and law enforcement to enable the team to detect, understand, and remediate the attacker. IM is usually less hands-on than IR, as its role is steering the IR team's activities in line with business priorities to understand and mitigate business impacts. Good IM requires agile and decisive actions across numerous areas of an organization supported by fast technical analysis of systems, data, networks, and user activity. **Expanding to a 5-day course late 2023**	**Author:** Steve Armstrong-Godwin **Course Sections:** 2 **For More Info:** sans.org/mgt553

In Development

MGT520: Leading Cloud Security Design and Implementation	While the cloud environment may appear similar to running a traditional IT environment on the premises, the cloud solutions protection requirements are in fact very different because the traditional network perimeter is no longer the best line of defense, and the threat vectors are not the same. Effective defense of the organization's cloud environment requires significant planning and governance by a well-informed management team. This course provides the information security leader's need to drive a secure cloud model and leapfrog on security to leverage the security capabilities in the cloud. We will walk through the key aspects of managing cloud security programs in the continuous operations post-migration that are common across organizations on the same journey. Nine scenario-based labs are included. **Existing 3-day course expanding to 5 days in late 2023.**	**Author:** Clay Risenhoover **Course Sections:** 5

GIAC Certifications

New Certifications

GIAC Cloud Forensics Responder (GCFR) FOR509	The GCFR certification validates a practitioner's ability to track and respond to incidents across the three major cloud providers. GCFR-certified professionals are well-versed in the log collection and interpretation skills needed to manage rapidly changing enterprise cloud environments.	giac.org/gcfr
GIAC iOS and MacOS Examiner (GIME) FOR518	The GIME certification validates a practitioner's knowledge of Mac and iOS computer forensic analysis and incident response skills. GIME-certified professionals are well-versed in traditional investigations as well as intrusion analysis scenarios for compromised Apple devices.	giac.org/gime
GIAC Security Operations Manager (GSOM) MGT551	The GSOM certification validates a professional's ability to run an effective security operations center. GSOM-certified professionals are well-versed in the management skills and process frameworks needed to strategically operate and improve a SOC and its team.	giac.org/gsom
GIAC Cloud Threat Detection (GCTD) SEC541	The GCTD certification validates a practitioner's ability to detect and investigate suspicious activity in cloud infrastructure. GCTD-certified professionals are experienced in cyber threat intelligence, secure cloud configuration, and other practices needed to defend cloud solutions and services.	giac.org/gctd

Security Awareness Training

SANS Security Awareness training is designed to educate your enterprise on cyber risk. These digital products are quick, informative, and engaging for a general audience, with interactive and gamified content that reinforces cyber safe behaviors. SSA's specialized products meet the varied needs of your general workforce (end users), developers, and IT administrators.

For more information or a demo, contact the SANS Security Awareness team at **SSAinfo@sans.org**.

New Releases

Security Essentials for IT Administrators	Security Essentials for IT Administrators is a short form, computer-based technical training course providing advanced-level training on the unique threats and mitigation techniques required in Information Technology roles. Designed to address and prevent misconfiguration errors, this 12-module interactive course covers real-world attack scenarios and mitigation strategies. **New – Winter 2023**	sans.org/security-awareness-training

SANS | GIAC CERTIFICATIONS