SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

New Courses & Certifications | 2020

SEC552: Bug Bounties & Responsible Disclosure
Why This Course: The course teaches pen testers how to discover and responsibly disclose tricky, logic-based application flaws that automated scanning tools don't reveal.
Author: Hassan El Hadary
Course Days: 2
For More Info: sans.org/SEC552

SEC582: Mastering TShark Packet Analysis
Why This Course: In this course you will master performing packet analysis through TShark and learn how to solve real-world problems through 19 different labs, demos, and challenges. This is the most in-depth, hands-on packet analysis course available.
Author: Nik Alleyne
Course Days: 2
For More Info: sans.org/SEC582

SEC541: Cloud Security Monitoring and Threat Hunting
Why This Course: SEC541 will take you on a deep dive into Amazon Web Services (AWS) in order to search out and identify threats in your cloud environment and explore ways to improve the architecture of your environment.
Author: Shaun McCullough
Course Days: 1
For More Info: sans.org/SEC541

SEC403: Secrets to Successful Cybersecurity Presentation – Online Modules
Why This Course: SEC403 gives you the skills to put together an effective security briefing, secure the interest and engagement of your audience, and confidently deliver presentations to a variety of groups.
Author: Alan Paller
Course Days: .5 (4 CPE's)
Follow on course to: SEC402
For More Info: sans.org/SEC403

FOR308: Digital Forensics Essentials
Why This Course: FOR308 is an introductory course created for digital forensics practitioners who are looking to take their capabilities to a whole new level, non-technical students getting into the field, or individuals in need to understand how it all fits together.
Authors: Kathryn Hedley, Jason Jordaan and Phil Moore
Course Days: 6
For More Info: sans.org/FOR308

MGT551: Building and Leading Security Operations Centers
Why This Course: Attendees will leave with a framework for understanding where their SOC should be focusing its efforts, how to track and organize defensive capabilities, and how to drive, verify, and communicate SOC improvements.
Author: John Hubbard
Course Days: 2
For More Info: sans.org/MGT551

Continued on next page

SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

New Courses & Certifications | 2020

SEC583: Crafting Packets
Why This Course: Crafting packets is an incredibly powerful skill for any security analyst, network engineer or system administrator. It can be used to test firewalls policies, IDS/IPS rules, host/server settings, application configurations, and much more.
Author: Andy Laman
Course Days: 1
For More Info: sans.org/SEC583

SEC586: Blue Team Ops: Defensive PowerShell
Why This Course: This course teaches deep automation and defensive capabilities using PowerShell and will provide you with skills for near real-time detection and response and elevate your defenses to the next level.
Author: Josh Johnson
Course Days: 3
For More Info: sans.org/SEC586

SEC537: Practical OSINT Analysis and Automation
Why This Course: This course teaches practical open-source intelligence (OSINT) analysis and automation techniques with tradecraft tips, tactics, techniques, and procedures based on real-world examples.
Authors: Nico Dekens, David Mashburn and John TerBush
Course Days: 2
For More Info: sans.org/SEC537

MGT520: Leading Cloud Security Design and Implementation
Why This Course: MGT520 teaches students how to build, lead, and implement a cloud security transition plan and roadmap, and then execute and manage ongoing operations.
Author: Jason Lam
Course Days: 2
For More Info: sans.org/MGT520

SEC584: Defending Cloud Native Infrastructure
Why This Course: Cloud native infrastructure and service providers are enabling organizations to build and deliver modern systems faster than ever, which can be difficult to defend and monitor. Students will gain hands-on experience building, exploring, and securing real-world modern systems.
Author: Andy Martin
Course Days: 3
For More Info: sans.org/SEC584

SEC510: Multicloud Security Assessment and Defense
Why This Course: This course provides cloud security practitioners, analysts, and researchers with an in-depth understanding of the inner workings of the most popular public cloud providers: Amazon Web Services (AWS), Microsoft Azure, and the Google Cloud Platform (GCP).
Author: Brandon Evans and Eric Johnson
Course Days: 3
For More Info: sans.org/SEC510

New GIAC Certifications

GCPN (SEC588): GIAC Cloud Penetration Tester
For More Info: giag.org/gcpn

GCSA (SEC540): GIAC Cloud Security Automation
For More Info: giag.org/gcsa

GOSI (SEC487): GIAC Open Source Intelligence
For More Info: giac.org/gosi

GBFA (FOR498): GIAC Battlefield Forensics and Acquisition
For More Info: giac.org/gbfa

SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

New Courses In-Development | 2021

SEC474:Building A Healthcare Security and Compliance Program This course will teach students how to foster the security of the IT infrastructure while also building a compliance program in their organization.

SEC513: Modern Linux Security for the Enterprise and Cloud The concept for this class is to expand from securing a limited number of Linux-based systems, often done manually one system at a time, to securing hundreds or thousands of Linux-based systems and containers, commonly found in today's enterprise and cloud-based environments.

SEC595: Data Science and Machine Learning for Security Professionals This course teaches how to use data science techniques to quickly write scripts to manipulate and analyze network and security data.

FOR608: Enterprise-Class Incident Response & Threat Hunting This course focuses on building critical and in-depth knowledge of collecting, analyzing, and correlating host- and network-based forensic artifacts from enterprise-scale networks.

SEC587: Advanced Open Source Intelligence Gathering & Analysis (SEC537 2-day) This class is for those that already have a firm foundation in the world of OSINT and are looking to go deeper into many of its technical collection areas.

SEC556: IoT Pen Testing will immerse students into the interfaces commonly observed in IoT devices and provide a process and testing framework (IoTA) to evaluate these devices within many layers of the OSI model.

SEC565: Red Team Operations prepares operators to emulate adversaries and threats in a professional manner to test a target organization's people, process, and technology from a holistic perspective. Red Team operators must understand how adversaries and threats operate to emulate them effectively.

FOR710: Reverse-Engineering Malware: Advanced Code Analysis continues where FOR610 leaves off, helping students who have already attained intermediate-level malware analysis capabilities take their reversing skills to the next level.

MGT416: Vendor Risk Management & Data Privacy This course will provide an overview of the key elements that are required to properly implement and deliver a successful Vendor Risk and Data Privacy program.

SEC405: Business Financial Essentials There are few disciplines more critical than financial stewardship. This course will take the info sec leader on a journey to help them understand and navigate their organization's financial status.

SEC554: Blockchain and Smart Contract Security This course teaches how to interact with and get data from public blockchains, exploit several classes of smart contract vulnerabilities, test and exploit weak cryptography/entropy, discover and recreate private keys, how to trace/track movements on a blockchain.

CLOUD SECURITY

SEC388: Intro to Cloud Computing & Sec steps through the many facets of cloud: from establishing your very own cloud account in which you will explore the "Big Three" (Amazon Web Services, Azure, and Google Cloud Platform) cloud vendor of your choice, to exploring services to enhance operations, maintenance, and security.

FOR509: Cloud Forensics & Incident Response This course focuses on understanding forensic data in the cloud, best practices and how to conduct proper evidence preservation and memory acquisition in the cloud.

SEC557: Security Audit Compliance Automation Essentials (Cloud & Enterprise) This course teaches auditors, engineers, and managers how to audit modern technologies and provide audit info at in both the enterprise and cloud environment.

SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

New Courses & Certifications | 2019

MGT521: Driving Cybersecurity Change - Establishing a Culture of Protect, Detect and Respond

This course will teach leaders how to leverage the principles of organizational change, enabling them to develop, maintain and measure a security driven culture. Through hands-on, real-world instruction and a series of interactive labs and exercises in which you will apply the concepts of organizational change to a variety of different security initiatives, you will quickly learn how to embed cybersecurity into your organizational culture.

Author: Lance Spitzner

For More Info: sans.org/MGT521

FOR498: Battlefield Forensics & Data Acquisition

This in-depth digital acquisition and data handling course will provide first responders and investigators alike with the advanced skills necessary to properly respond to, identify, collect, and preserve data from a wide range of storage devices and repositories.. Constantly updated, FOR498 addresses today's need for widespread knowledge and understanding of the challenges and techniques that investigators require when addressing real-world cases.

Authors: Eric Zimmerman & Kevin Ripa

New GIAC Certification in 2020: GBFA GIAC Battlefield Forensics and Acquisition

For More Info: sans.org/FOR498

SEC402: Cybersecurity Writing: Hack the Reader

Want to write better? Learn to hack the reader! Discover how to find an opening, break down your readers' defenses, and capture their attention to deliver your message--even if they're too busy or indifferent to others' writing. This unique course, built exclusively for cybersecurity professionals, will strengthen your writing skills and boost your security career.

Author: Lenny Zeltser

For More Info: sans.org/SEC402

SEC488: Cloud Security Essentials

Why This Course: More businesses than ever are shifting mission-critical workloads to the cloud. And not just one cloud - research shows that most enterprises are using up to five different cloud providers. SEC488 provides hands-on tools, techniques, and patterns to shore up organization's cloud security weaknesses.

Authors: Kenneth G. Hartman, Kyle Dickinson, and Ryan Nicholson

Course Days: 5

For More Info: sans.org/SEC488

SEC699: Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection

This advanced purple team course focuses on adversary emulation for data breach prevention and detection, and how real-life threat actors can be emulated in an enterprise environment and how adversarial techniques can be emulated and detected.

Authors: Erik Van Buggenhout and Jim Shewmaker

For More Info: sans.org/sec699