FOR572
Advanced Network Forensics and Analysis

Mon, 23 Oct - Sat, 28 Oct | Laptop Required | Instructor: Philip Hagen

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

FOR572 was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we'll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is already under way.

GIAC NETWORK FORENSIC ANALYST GNFA

www.giac.org/gnfa

FOR610
Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Mon, 23 Oct - Sat, 28 Oct | Laptop Required | Instructor: Hal Pomeranz

Learn to turn malware inside out! This popular course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems.

Understanding the capabilities of malware is critical to an organization's ability to derive threat intelligence, respond to information security incidents, and fortify defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and many other freely available tools.

Hands-on workshop exercises are a critical aspect of this course. They enable you to apply malware analysis techniques by examining malicious software in a controlled and systemic manner. When performing the exercises, you will study the supplied specimens' behavioral patterns and examine key portions of their code. To support these activities, you will receive pre-built Windows and Linux virtual machines that include tools for examining and interacting with malware.

GIAC REVERSE ENGINEERING MALWARE GREM

www.giac.org/grem

FOR578
Cyber Threat Intelligence

Mon, 16 Oct - Fri, 20 Oct | Laptop Required | Instructor: Jess Garcia

THERE IS NO TEACHER BUT THE ENEMY!

Make no mistake: current network defense, threat hunting, and incident response practices contain a strong element of intelligence and counterintelligence that cyber analysts must understand and leverage in order to defend their networks, proprietary data, and organizations.

FOR578: Cyber Threat Intelligence will help network defenders, threat hunting teams, and incident responders to:

- Understand and develop skills in tactical, operational, and strategic level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)
- Validate information received from other organizations to minimize resource expenditures on bad intelligence
- Leverage open-source intelligence to complement a security team of any size
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX

GIAC CYBER THREAT INTELLIGENCE GCTI

www.giac.org/gcti

CORE NETWARS EXPERIENCE

26-27 October | Hosted by Pieter Danhieux

NetWars is a computer and network security challenge designed to test a participant's experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars to help identify skilled personnel and as part of extensive hands-on training. With NetWars, you'll build a wide variety of skills while having a great time.

REGISTRATION IS LIMITED AND FREE

for students attending any long course at SANS Tokyo Autumn 2017 (NON-STUDENT ENTRANCE FEE IS $1,610 USD).

REGISTER AT

www.sans.org/tokyo-autumn-2017

SANS

asiapacific@sans.org | +81 3 3242 6276
Yoshihiro Sekitori | ysekitori@sans.org | +81 3 3242 6276
Shuji Koyanagi | skoyanagi@sans.org | +81 80 6538 6030

SANS

The Most Trusted Source for Information Security Training, Certification, and Research

INFORMATION SECURITY TRAINING

TOKYO AUTUMN 2018

16-28 October

Protect your organisation. Advance your career.

Ten hands-on, immersion-style courses taught by SANS's real-world practitioners.

Featuring training in:

CYBER DEFENCE	SEC401 | SEC566
INCIDENT HANDLING	SEC504
PENETRATION TESTING	SEC542 | SEC560
SECURITY OPERATIONS	SEC511
DIGITAL FORENSICS	FOR508 | FOR572 | FOR610
CYBER THREAT INTELLIGENCE	FOR578

Core NETWARS EXPERIENCE

GIAC CERTIFICATIONS

REGISTER AT

www.sans.org/tokyo-autumn-2017

SEC401 WILL BE TAUGHT IN JAPANESE

SEC401
Security Essentials Bootcamp Style

Mon, 16 Oct - Sat, 21 Oct | Laptop Required | Instructors: Satoshi Hayashi, Masafumi Negishi

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment. SEC401 is focused on teaching you the essential information security skills and techniques you need to protect and secure your organisation's critical information assets and business systems. Our course will show you how to prevent your organisation's security problems from being headline news!

www.giac.org/gsec

SEC504 WILL BE TAUGHT IN JAPANESE

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling

Mon, 23 Oct - Sat, 28 Oct | Laptop Required | Instructor: Zachary Mathis

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, this course helps you turn the tables on computer attackers. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning for, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!

www.giac.org/gcih

SEC511
Continuous Monitoring & Security Operations

Mon, 16 Oct - Sat, 21 Oct | Laptop Required | Instructor: Christopher Crowley

We continue to underestimate the tenacity of our adversaries! Organisations are investing a significant amount of time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organisations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organisations to detect threats that will inevitably slip through their defences. **SEC511: Continuous Monitoring and Security Operations** will teach you how to strengthen your skills to undertake that proactive approach.

www.giac.org/gmon

SEC542
Web App Penetration Testing and Ethical Hacking

Mon, 16 Oct - Sat, 21 Oct | Laptop Required | Instructor: Pieter Danhieux

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.

Web applications play a vital role in every modern organisation. But, if your organisation does not properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organisations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

Students will come to understand major web application flaws and their exploitation and, most importantly, learn a field-tested and repeatable process to consistently find these flaws and convey what they have learned to their organisations. Even technically gifted security geeks often struggle with helping organisations understand risk in terms relatable to business. Much of the art of penetration testing has less to do with learning how adversaries are breaking in than it does with convincing an organization to take the risk seriously and employ appropriate countermeasures. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help you demonstrate the true impact of web application flaws through exploitation.

www.giac.org/gpen

SEC560
Network Penetration Testing and Ethical Hacking

Mon, 23 Oct - Sat, 28 Oct | Laptop Required | Instructor: Pieter Danhieux

As a cybersecurity professional, you have a unique responsibility to find and understand your organisation's vulnerabilities and to work diligently to mitigate them before the bad guys pounce. Are you ready? SEC560, the flagship SANS course for penetration testing, fully arms you to address this duty head-on. With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, SEC560 truly prepares you to conduct high-value penetration testing projects step-by-step and end-to-end. Every organisation needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specially designed to get you ready for that role. The course starts with proper planning, scoping and recon, then dives deep into scanning, target exploitation, password attacks, and web app manipulation, with over 30 detailed hands-on labs throughout. The course is chock full of practical, real-world tips from some of the world's best penetration testers to help you do your job safely, efficiently...and masterfully. SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test – and on the last day of the course, you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organisation, demonstrating the knowledge you've mastered in this course.

www.giac.org/gpen

SEC566
Implementing and Auditing the Critical Security Controls – In-Depth

Mon, 23 Oct - Fri, 27 Oct | Laptop Required | Instructor: Randy Marchany

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organisation have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organisation's security should too. To enable your organisation to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Critical Security Controls, a prioritised, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

SANS's in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

www.giac.org/gccc

FOR508
Advanced Digital Forensics, Incident Response, and Threat Hunting

Mon, 23 Oct - Sat, 28 Oct | Laptop Required | Instructor: Nick Klein

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting will help you to:

- Detect how and when a breach occurred
- Identify compromised and affected systems
- Determine what attackers took or changed
- Contain and remediate incidents
- Develop key sources of threat intelligence
- Hunt down additional breaches using knowledge of the adversary

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organised crime syndicates, and hactivism. Constantly updated, FOR508 addresses today's incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

GATHER YOUR INCIDENT RESPONSE TEAM –
IT'S TIME TO GO HUNTING!

www.giac.org/gcfa