FOR572
Advanced Network Forensics and Analysis

Mon, 13 Nov - Sat, 18 Nov | Laptop Required | Instructor: Philip Hagen | GIAC Cert: GSNA

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.

www.giac.org/gnfa

FOR585
Advanced Smartphone Forensics

Mon, 13 Nov - Sat, 18 Nov | Laptop Required | Instructor: Cindy Murphy | GIAC Cert: GASF

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, accident reconstruction, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. FOR585 will teach you those skills.

This in-depth smartphone forensic course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 20 hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools, methods, and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools. Each lab is designed to teach you a lesson that can be applied to other smartphones. You will gain experience with the different data formats on multiple platforms and learn how the data are stored and encoded on each type of smart device. The labs will open your eyes to what you are missing by relying 100% on your forensic tools.

FOR585 is continuously updated to keep up with the latest malware, smartphone operating systems, third-party applications, and encryption. This intensive six-day course offers the most unique and current instruction on the planet, and it will arm you with mobile device forensic knowledge you can immediately apply to cases you're working on the day you leave the course.

www.giac.org/gasf

ICS410
ICS/SCADA Security Essentials

Mon, 13 Nov - Fri, 17 Nov | Laptop Required | Instructor: Eric Cornelius | GIAC Cert: GICSP

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410 provides a foundational set of standardised skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with:

- **An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints.**
- **Hands-on lab learning experiences to control system attack surfaces, methods, and tools**
- **Control system approaches to system and network defence architectures and techniques**
- **Incident-response skills in a control system environment**
- **Governance models and resources for industrial cybersecurity professionals.**

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

www.giac.org/gicsp

DFIR NETWARS TOURNAMENT

Thu, 16 Nov - Fri, 17 Nov

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.

REGISTER AT
www.sans.org/sydney-2017

Pay Early and Save*

	DATE	DISCOUNT	DATE	DISCOUNT
Register and pay by	**27-9-17**	**$350.00 USD**	**11-10-17**	**$200.00 USD**

*Some restrictions apply. Early bird discounts do not apply to Hosted courses.

SANS

asiapacific@sans.org | (02) 6198 3352
0402 067 768 – Steven Armitage
0477 005 908 – Tory Lane

SANS

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

SYDNEY 2017

13-25 November | Grace Hotel Sydney

"SANS takes you to places that you never thought of. To be the best you need to be – trained by the best – SANS."
-R. Vekaria, BP

Protect Your Organisation and Advance Your Career

Nine hands-on, immersion-style information security courses taught by real-world practitioners.

CYBER DEFENCE
DETECTION & MONITORING
PENETRATION TESTING
INCIDENT RESPONSE
DIGITAL FORENSICS
ETHICAL HACKING
ICS/SCADA SECURITY

GIAC CERTIFICATIONS

And featuring

DFIR NETWARS TOURNAMENT

SAVE US$350
for any 5-6 day course paid for by 27 September 2017

REGISTER AT
www.sans.org/sydney-2017

SEC401
Security Essentials Bootcamp Style

Mon, 13 Nov - Sat, 18 Nov | Laptop Required | Instructor: Tim Garcia | GIAC Cert: GSEC

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. You'll 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.

STOP and ask yourself the following questions:

- **Do you fully understand why some organisations get compromised and others do not?**
- **If there were compromised systems on your network, are you confident that you would be able to find them?**
- **Do you know the effectiveness of each security device and are you certain that they are all configured correctly?**
- **Are proper security metrics set up and communicated to your executives to drive security decisions?**

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

Security is all about making sure you focus on the right areas of defence. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need if you are given the responsibility for securing systems and/or organisations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

www.giac.org/gsec

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling

Mon, 20 Nov - Sat, 25 Nov | Laptop Required | Instructor: George Bakos | GIAC Cert: GCIH

This course enables you to turn the tables on computer attackers by helping you understand their 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. 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 for, 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, exploiting, and defending systems. This course will enable you to discover the holes in your system before the bad guys do!

The course is particularly well-suited to individuals who lead or are a part of an incident handling team. General security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

www.giac.org/gcih

SEC511
Continuous Monitoring and Security Operations

Mon, 20 Nov - Sat, 25 Nov | Laptop Required | Instructor: Mark Hofman | GIAC Cert: GMON

The Defensible Security Architecture, Network Security Monitoring (NSM)/ Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organisation or Security Operations Center (SOC) to analyse threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach will be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and this course will greatly increase your understanding and enhance your skills in implementing CM utilising the NIST framework.

SEC511 will take you on quite a journey. We start by exploring traditional security architecture to assess its current state and the attacks against it. Next, we discuss and discover modern security design that represents a new proactive approach to such architecture that can be easily understood and defended. We then transition to how to actually build the network and endpoint security, and then carefully navigate our way through automation, NSM/CDM/CSM. For timely detection of potential intrusions, the network and systems must be proactively and continuously monitored for any changes in the security posture that might increase the likelihood that attackers will succeed.

Your SEC511 journey will conclude with one last hill to climb! The final day features a Capture-the-Flag competition that challenges you to apply the skills and techniques learned in the course to detect and defend the modern security architecture that has been designed. Course authors Eric Conrad and Seth Misenar have designed the Capture-the-Flag competition to be fun, engaging, comprehensive, and challenging. You will not be disappointed!

www.giac.org/gmon

SEC555
SIEM with Tactical Analytics *NEW!*

Mon, 20 Nov - Sat, 25 Nov | Laptop Required | Instructor: Tim Garcia

This course is designed to demystify the SIEM architecture and process by navigating the student through the steps of tailoring and deploying a SIEM to full SOC integration. The material will cover many bases in the "appropriate" use of a SIEM platform to enrich readily available log data in enterprise environments and extract actionable intelligence. Once the information is collected, the student will be shown how to present the gathered input into usable formats to aid in eventual correlation. Students will then iterate through the log data and events to analyse key components that will allow them to learn how rich this information is, how to correlate the data, start investigating based on the aggregate data, and finally, how to go hunting with this newly gained knowledge. They will also learn how to deploy internal post-exploitation tripwires and breach canaries to nimbly detect sophisticated intrusions. Throughout the course, the text and labs will not only show how to manually perform these actions, but also how to automate many of the processes mentioned so students can employ these tasks the day they return to the office.

The underlying theme is to actively apply Continuous Monitoring and analysis techniques by utilising modern cyber threat attacks. Labs will involve replaying captured attack data to provide real-world results and visualisations.

SEC560
Network Penetration Testing and Ethical Hacking

Mon, 13 Nov - Sat, 18 Nov | Laptop Required | Instructor: Pieter Danhieux | GIAC Cert: GPEN

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

FOR508
Advanced Digital Forensics, Incident Response, and Threat Hunting

Mon, 20 Nov - Sat, 25 Nov | Laptop Required | Instructor: Nick Klein | GIAC Cert: GCFA

FOR508 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**

www.giac.org/gcfa

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!