SANS

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

OCTOBER SINGAPORE 2017

9-28 October | Grand Copthorne Waterfront Hotel

Protect Your Business and Advance Your Career

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

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

GIAC CERTIFICATIONS

"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

CORE NETWARS EXPERIENCE

CYBER DEFENCE NETWARS TOURNAMENT

SAVE US$350
for any 5-6 day course paid for by 30 August

www.sans.org/october-singapore-2017

SEC401

GSEC Certification
Security Essentials

www.giac.org/gsec

Security Essentials Bootcamp Style

Mon, 16 Oct - Sat, 21 Oct
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Paul A. Henry

This course will teach you the most effective steps to prevent attacks and detect adversaries with actionable techniques you can directly apply when you get back to work. You'll learn tips and tricks from the experts so you can win the battle against the wide range of cyber adversaries that want to harm your environment.

SEC401: Security Essentials Bootcamp Style 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 in the *Wall Street Journal*!

Prevention Is Ideal but Detection Is a Must

With the rise in advanced persistent threats, it is almost inevitable that organisations will be targeted. Whether the attacker is successful in penetrating an organisation's network depends on the effectiveness of the organisation's defence. Defending against attacks is an ongoing challenge, with new threats emerging all of the time, including the next generation of threats. Organisations need to understand what really works in cybersecurity. What has worked, and will always work, is taking a risk-based approach to cyber defence. Before your organisation spends a dollar of its IT budget or allocates any resources or time to anything in the name of cybersecurity, three questions must be answered:

> What is the risk? > Is it the highest priority risk? > What is the most cost-effective way to reduce the risk?

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.

SEC501

GCED Certification
Certified Enterprise Defender

www.giac.org/gced

Advanced Security Essentials – Enterprise Defender

Mon, 23 Oct - Sat, 28 Oct
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Paul A. Henry

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. SEC501: Advanced Security Essentials – Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

"The hands-on lab approach is a great way to make sense of what is being taught, and working with other classmates helped expand our knowledge and brought cohesion." -Rachel Weiss, UPS Inc.

Despite an organisation's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organisations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organisation to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

SEC503

Intrusion Detection In-Depth

GCIA Certification
Certified Intrusion Analyst

www.giac.org/gcia

Mon, 16 Oct - Sat, 21 Oct
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Dr. Johannes Ullrich

Reports of prominent organisations being hacked and suffering irreparable reputational damage have become all too common. How can you prevent your company from becoming the next victim of a major cyber attack?

Preserving the security of your site in today's threat environment is more challenging than ever before. The security landscape is continually changing from what was once only perimeter protection to protecting exposed and mobile systems that are almost always connected and sometimes vulnerable. Security-savvy employees who can help detect and prevent intrusions are therefore in great demand. Our goal in SEC503 is to acquaint you with the core knowledge, tools, and techniques to defend your networks with insight and awareness. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

Mark Twain said, "It is easier to fool people than to convince them that they've been fooled." Too many IDS/IPS solutions provide a simplistic red/green, good/bad assessment of traffic and too many untrained analysts accept that feedback as the absolute truth. This course emphasises the theory that a properly trained analyst uses an IDS alert as a starting point for examination of traffic, not as a final assessment. SEC503 imparts the philosophy that the analyst must have access and the ability to examine the alerts to give them meaning and context. You will learn to investigate and reconstruct activity to deem if it is noteworthy or a false indication.

SEC503: Intrusion Detection In-Depth delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open-source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution. Basic exercises include assistive hints while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material.

SEC504

Hacker Tools, Techniques, Exploits, and Incident Handling

GCIH Certification
Incident Handler

www.giac.org/gcih

Mon, 23 Oct - Sat, 28 Oct
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
Laptop Required
(If your laptop supports only wireless, please bring a USB Ethernet adapter.)
Instructor: Bryce Galbraith

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organisation has an Internet connection or one or two disgruntled employees (and whose does not!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

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 those attacks. Additionally, 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.

SEC550

Active Defense, Offensive Countermeasures and Cyber Deception

Mon, 16 Oct - Fri, 20 Oct
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Bryce Galbraith

The current threat landscape is shifting. Traditional defences are failing us. We need to develop new strategies to defend ourselves. Even more importantly, we need to better understand who is attacking us and why. You may be able to immediately implement some of the measures we discuss in this course, while others may take a while. Either way, consider what we discuss as a collection of tools that will be at your disposal when you need them to annoy attackers, determine who is attacking you, and, finally, attack the attackers.

SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception is based on the Active Defense Harbinger Distribution live Linux environment funded by the Defense Advanced Research Projects Agency (DARPA). This virtual machine is built from the ground up for defenders to quickly implement Active Defences in their environments. The course is very heavy with hands-on activities – we won't just talk about Active Defences, we will work through labs that will enable you to quickly and easily implement what you learn in your own working environment.

You Will Learn:

- **How to force an attacker to take more moves to attack your network – moves that in turn may increase your ability to detect that attacker**
- **How to gain better attribution as to who is attacking you and why**
- **How to gain access to a bad guy's system**
- **Most importantly, you will find out how to do the above legally**

SEC560

GPEN Certification
Penetration Tester

www.giac.org/gpen

Network Penetration Testing and Ethical Hacking

Mon, 9 Oct - Sat, 14 Oct
9:00am - 7:15pm (Day 1)
9:00am - 5:00pm (Days 2-6)
37 CPEs
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? SANS SEC560, our flagship course for penetration testing, fully arms you to address this task 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 more than 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.

You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasise the importance of defence in depth.

SEC575

GMOB Certification

Mobile Device Security Analyst

www.giac.org/gmob

Mobile Device Security and Ethical Hacking

Mon, 23 Oct - Sat, 28 Oct
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Tim Medin

Mobile devices are no longer a convenience technology: they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores throughout the world. Users rely on mobile devices more today than ever before – we know it, and the bad guys do too.

This course is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS, Android, and wearable devices including Apple Watch and Android Wear. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you'll exploit lost or stolen devices to harvest sensitive mobile application data.

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you'll review the ways in which we can effectively communicate threats to key stakeholders. You'll leverage tools including Mobile App Report Cards to characterise threats for management and decision makers, while identifying sample code and libraries that developers can use to address risks for in-house applications as well.

Mobile device deployments introduce new threats to organisations including advanced malware, data leakage, and the disclosure of enterprise secrets, intellectual property, and personally identifiable information assets to attackers. Further complicating matters, there simply are not enough people with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you'll be able to differentiate yourself as being prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test – all critical skills to protect and defend mobile device deployments.

SEC660

GXPN Certification

Exploit Researcher and Advanced Penetration Tester

www.giac.org/gxpn

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Mon, 16 Oct - Sat, 21 Oct
9:00am - 7:00pm (Days 1-5)
9:00am - 5:00pm (Day 6)
46 CPEs
Laptop Required
Instructor: Tim Medin

This course is designed as a logical progression point for those who have completed **SEC560: Network Penetration Testing and Ethical Hacking**, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponising Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

"SEC660 was hands-on, packed with content, and current to today's technology!" -Michael Horken, Rockwell Automation

Attackers are becoming more clever and their attacks more complex. In order to keep up with the latest attack methods, you need a strong desire to learn, the support of others, and the opportunity to practice and build experience. SEC660 provides attendees with in-depth knowledge of the most prominent and powerful attack vectors and an environment to perform these attacks in numerous hands-on scenarios. This course goes far beyond simple scanning for low-hanging fruit, and shows penetration testers how to model the abilities of an advanced attacker to find significant flaws in a target environment and demonstrate the business risk associated with these flaws.

FOR508

GCFA Certification
Forensic Analyst

www.giac.org/gcfa

Advanced Digital Forensics, Incident Response, and Threat Hunting

Mon, 16 Oct - Sat, 21 Oct
9:00am - 5:00pm
36 CPEs
Laptop Required
Instructor: Chad Tilbury

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

DAY 0: A 3-letter government agency contacts you to say an advanced threat group is targeting organisations like yours, and that your organisation is likely a target. They won't tell how they know, but they suspect that there are already several breached systems within your enterprise. An advanced persistent threat, aka an APT, is likely involved. This is the most sophisticated threat that you are likely to face in your efforts to defend your systems and data, and these adversaries may have been actively rummaging through your network undetected for months or even years.

This is a hypothetical situation, but the chances are very high that hidden threats already exist inside your organisation's networks. Organisations can't afford to believe that their security measures are perfect and impenetrable, no matter how thorough their security precautions might be. Prevention systems alone are insufficient to counter focused human adversaries who know how to get around most security and monitoring tools.

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: Advanced Digital Forensics, Incident Response, and Threat Hunting** 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.

MGT517

Managing Security Operations: Detection, Response, and Intelligence *NEW!*

Mon, 23 Oct - Fri, 27 Oct
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Christopher Crowley

Managing Security Operations covers the design, operation, and ongoing growth of all facets of the security operations capabilities in an organisation. An effective Security Operations Center (SOC) has many moving parts and must be designed with the ability to adjust and work within the constraints of the organisation. To run a successful SOC, managers need to provide tactical and strategic direction and inform staff of the changing threat environment as well as provide guidance and training for employees. This course covers design, deployment, and operation of the security program to empower leadership through technical excellence.

The course covers the functional areas of Communications, Network Security Monitoring, Threat Intelligence, Incident Response, Forensics, and Self-Assessment. We discuss establishing Security Operations governance for:

- Business alignment and ongoing adjustment of capabilities and objectives
- Designing the SOC and the associated objectives of functional areas
- Software and hardware technology required for performance of functions
- Knowledge, skills, and abilities of staff as well as staff hiring and training
- Execution of ongoing operations

You will walk out of this course armed with a roadmap to design and operate an effective SOC tailored to the needs of your organisation.

"SANS coursework is the most thorough learning available, anywhere. What you learn is not only conceptual, but also hands-on, showing you what to do, why you do it, and how you can apply solutions that you learn to real-world problems."

-Duane Tucker, Barmark Partners

FOR572

Advanced Network Forensics and Analysis

GNFA Certification
Network Forensic Analyst

www.giac.org/gnfa

Mon, 16 Oct - Sat, 21 Oct
9:00am - 5:00pm
36 CPEs
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.

It is exceedingly rare to work any forensic investigation that doesn't have a network component. Endpoint forensics will always be a critical and foundational skill for this career, but overlooking network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or prove useful even in definitively proving a crime actually occurred.

FOR572: Advanced Network Forensics and Analysis 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.

ICS410

ICS/SCADA Security Essentials

GICSP Certification
Industrial Cyber Security Professional

www.giac.org/gicsp

Mon, 23 Oct - Fri, 27 Oct
9:00am - 5:00pm
30 CPEs
Laptop Required
Instructor: Eric Cornelius

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: ICS/SCADA Security Essentials** 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.

CORE NETWARS EXPERIENCE

19-20 October | Hosted by Bryce Galbraith

CYBER DEFENCE NETWARS TOURNAMENT

26-27 October | Hosted by Paul A. Henry

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 October Singapore 2017 (NON-STUDENT ENTRANCE FEE IS $1,610 USD).

www.sans.org/october-singapore-2017

OCTOBER SINGAPORE 2017

9-28 October | Grand Copthorne Waterfront Hotel

SEC401: Security Essentials Bootcamp Style | GSEC

SEC501: Advanced Security Essentials – Enterprise Defender | GCED

SEC503: Intrusion Detection In-Depth | GCIA

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling | GCIH

SEC550: Active Defense, Offensive Countermeasures and Cyber Deception

SEC560: Network Penetration Testing and Ethical Hacking | GPEN

SEC575: Mobile Device Security and Ethical Hacking | GMOB

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | GXPN

FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting | GCFA

FOR572: Advanced Network Forensics and Analysis | GNFA

MGT517: Managing Security Operations: Detection, Response, and Intelligence

ICS410: ICS/SCADA Security Essentials | GICSP

SAVE US$350
for any 5-6 day course paid for by 30 August

Core NetWars Experience | Cyber Defence NetWars Tournament

For more information, contact the SANS team in Singapore

Sean Georget
sgeorget@sans.org | +65 8612 5278 | +63 908 886 5722
asiapacific@sans.org | +65 6933 9540