SANS Secure Singapore 2017

13-25 March Grand Copthorne Waterfront

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

PROTECT YOUR COMPANY AND ADVANCE YOUR CAREER
WITH HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

"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

GIAC
GIAC-Approved Training

13 courses on

- Cyber Defense
- Detection and Monitoring
- Pen Testing
- Incident Response
- Digital Forensics
- Ethical Hacking

SAVE $350 USD
for any 5-6 day course paid for by 1 Feb 2017

Also featuring:

DFIR NETWARS TOURNAMENT

REGISTER AT
www.sans.org/secure-singapore-2017

SEC301
Intro to Information Security

Hands-On | 13-17 March | Laptop Required | GISF | David R. Miller

This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cybersecurity. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

www.giac.org/gisf

SEC401
Security Essentials Bootcamp Style

Hands-On | 13-18 March | Laptop Required | GSEC | Dr. Eric Cole

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.

www.giac.org/gsec

Security is all about making sure you focus on the right areas of defense. 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 organizations. 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.

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling

Hands-On | 13-18 March | Laptop Required | GCIH | Christopher Crowley

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organization 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.

www.giac.org/gcih

This course enables you to turn the tables on computer attackers by helping you to 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. It 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.

SEC511
Continuous Monitoring and Security Operations

Hands-On | 13-18 March | Laptop Required | GMON | Mark Hofman

www.giac.org/gmon

We continue to underestimate the tenacity of our adversaries! Organizations are investing significant time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organizations 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 organizations to detect threats that will inevitably slip through their defenses.

The underlying challenge for organizations victimized by an attack is timely incident detection. Industry data suggest that most security breaches typically go undiscovered for an average of seven months. Attackers simply have to find one way into most organizations, because they know that the lack of visibility and internal security controls will then allow them to methodically carry out their mission and achieve their goals.

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 organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach would 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 utilizing the NIST framework.

SEC542
Web App Penetration Testing and Ethical Hacking

Hands-On | 13-18 March | Laptop Required | GWAPT | Pieter Danhieux

www.giac.org/gwapt

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

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications. Major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

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 organizations. Even technically gifted security geeks often struggle with helping organizations 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.

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

Hands-On | 20-24 March | Laptop Required | GCCC | Greg Porter

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization 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).

www.giac.org/gccc

As threats evolve, an organization's security should too. To enable your organization 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 prioritized, 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.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

SANS' 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.

SEC760
Advanced Exploit Development for Penetration Testers

Hands-On | 20-25 March | Laptop Required | Stephen Sims

Vulnerabilities in modern operating systems such as Microsoft Windows 7/8/10, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet these vulnerabilities could expose organizations to significant attacks, undermining their defenses when attacked by very skilled adversaries. Few security professionals have the skillset to discover let alone even understand at a fundamental level why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. SEC760 teaches the skills required to reverse-engineer 32- and 64-bit applications, perform remote user application and kernel debugging, analyze patches for one-day exploits, and write complex exploits, such as use-after-free attacks, against modern software and operating systems.

Some of the skills you will learn in SEC760 include:

- How to write modern exploits against the Windows 7/8/10 operating systems
- How to perform complex attacks such as use-after-free, Kernel exploit techniques, one-day exploitation through patch analysis, and other advanced topics
- The importance of utilizing a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modeling
- How to effectively utilize various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success and defeating determination

Not sure if you are ready for SEC760?

Take this 10 question quiz: **www.sans.org/sec760/quiz**

FOR408
Windows Forensic Analysis

Hands-On | 13-18 March | Laptop Required | GCFE | Nick Klein

www.giac.org/gcfe

All organizations must prepare for cyber crime occurring on their computer systems and within their networks. Demand has never been higher for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't understand, and understanding forensic capabilities and artifacts is a core component of information security. You'll learn to recover, analyze, and authenticate forensic data on Windows systems. You'll understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. You'll be able to use your new skills to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 7/8/10, Office and Office365, cloud storage, Sharepoint, Exchange, Outlook). Students leave the course armed with the latest tools and techniques and prepared to investigate even the most complicated systems they might encounter. Nothing is left out – attendees learn to analyze everything from legacy Windows XP systems to just-discovered Windows 10 artifacts.

FOR526
Memory Forensics In-Depth

Hands-On | 20-25 March | Laptop Required | Alissa Torres

Digital Forensics and Incident Response (DFIR) professionals need Windows memory forensics training to be at the top of their game. Investigators who do not look at volatile memory are leaving evidence at the crime scene. RAM content holds evidence of user actions, as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the smoking gun that unravels the story of what happened on a system.

FOR526 provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyze captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work. FOR526 is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

In today's forensics cases, it is just as critical to understand memory structures as it is to understand disk and registry structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand. For those investigating platforms other than Windows, this course also introduces OSX and Linux memory forensics acquisition and analysis using hands-on lab exercises.

There is an arms race between analysts and attackers. Modern malware and post-exploitation modules increasingly employ self-defense techniques that include more sophisticated rootkit and anti-memory analysis mechanisms that destroy or subvert volatile data. Examiners must have a deeper understanding of memory internals in order to discern the intentions of attackers or rogue trusted insiders. FOR526 draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images.

FOR578
Cyber Threat Intelligence

Hands-On | 20-24 March | Laptop Required | Jess Garcia

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.

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that is used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture.

Cyber threat intelligence thus represents a force multiplier for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats. Malware is an adversary's tool but the real threat is the human one, and cyber threat intelligence focuses on countering those flexible and persistent human threats with empowered and trained human defenders.

During a targeted attack, an organization needs a top-notch and cutting-edge threat hunting or incident response team armed with the threat intelligence necessary to understand how adversaries operate and to counter the threat. FOR578 will train you and your team in the tactical, operational, and strategic level cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organizations more aware of the evolving threat landscape.

FOR585
Advanced Smartphone Forensics

Hands-On | 20-25 March | Laptop Required | GASF | Cindy Murphy

www.giac.org/gasf

Every time the smartphone "thinks" or makes a suggestion, the data are saved. It's easy to get mixed up in what the forensic tools are reporting. Smartphone forensics is more than pressing the "find evidence" button and getting answers. Your team cannot afford to rely solely on the tools in your lab. You have to understand how to use them correctly to guide your investigation, instead of just letting the tool report what it believes happened on the device. It is impossible for commercial tools to parse everything from smartphones and understand how the data were put on the device. Examining and interpreting the data is your job, and this course will provide you and your organization with the capability to find and extract the correct evidence from smartphones with confidence.

This in-depth smartphone forensics course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features 17 hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools 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 available, and it will arm you with mobile device forensic knowledge you can apply immediately to cases you're working on the day you finish the course.

Smartphone technologies are constantly changing, and most forensic professionals are unfamiliar with the data formats for each technology. Take your skills to the next level: it's time for the good guys to get smarter and for the bad guys to know that their texts and apps can and will be used against them!

FOR610
Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Hands-On | 13-18 March | Laptop Required | GREM | Jake Williams

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 the threat intelligence it needs to respond to information security incidents and fortify defenses. The course builds a strong foundation for analyzing malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger and other tools useful for turning malware inside-out.

www.giac.org/grem

Hands-on workshop exercises are a critical aspect of this course and allow you to apply malware analysis techniques by examining malware in a lab that you control. 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.

HOSTED
Health Care Security Essentials

Hands-On | 16-17 March | Laptop Required | Greg Porter

Health Care Security Essentials is designed to provide SANS students with an introduction to current and emerging issues in health care information security and regulatory compliance. The class provides a foundational set of skills and knowledge for health care security professionals by integrating case studies, hands-on labs, and tips for securing and monitoring electronic protected health information. Administrative insights for those managing the many aspects of health care security operations will also be discussed. The goal of the course is to present a substantive overview and analysis of relevant information security subject matter that is having a direct and material impact on the U.S. health care system.

SANS Instructors

Dr. Eric Cole
Faculty Fellow
@drericcole

Christopher Crowley
Certified Instructor
@CCrowMontance

Pieter Danhieux
Principal Instructor
@PieterDanhieux

Jess Garcia
Principal Instructor

Mark Hofman
Certified Instructor

Nick Klein
Certified Instructor

David R. Miller
Certified Instructor
@DRM_CyberDude

Cindy Murphy
Certified Instructor
@cindymurph

Greg Porter
SANS Instructor

Stephen Sims
Senior Instructor
@Steph3nSims

Alissa Torres
Certified Instructor
@sibertor

Jake Williams
Certified Instructor
@MalwareJake

Complete bios for all SANS instructors can be found at www.sans.org/secure-singapore-2017/instructors

SANS Secure Singapore 2017

13-25 March Grand Copthorne Waterfront

13 courses offered:

SEC301 **Intro to Information Security**
GIAC Cert: GISF | Instructor: David R. Miller

SEC401 **Security Essentials Bootcamp Style**
GIAC Cert: GSEC | Instructor: Dr. Eric Cole

SEC504 **Hacker Tools, Techniques, Exploits, and Incident Handling**
GIAC Cert: GCIH | Instructor: Christopher Crowley

SEC511 **Continuous Monitoring and Security Operations**
GIAC Cert: GMON | Instructor: Mark Hofman

SEC542 **Web App Penetration Testing and Ethical Hacking**
GIAC Cert: GWAPT | Instructor: Pieter Danhieux

SEC566 **Implementing and Auditing the Critical Security Controls – In-Depth**
GIAC Cert: GCCC | Instructor: Greg Porter

SEC760 **Advanced Exploit Development for Penetration Testers**
Instructor: Stephen Sims

FOR408 **Windows Forensic Analysis**
GIAC Cert: GCFE | Instructor: Nick Klein

FOR526 **Memory Forensics In-Depth**
Instructor: Alissa Torres

FOR578 **Cyber Threat Intelligence**
Instructor: Jess Garcia

FOR585 **Advanced Smartphone Forensics**
GIAC Cert: GASF | Instructor: Cindy Murphy

FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques**
GIAC Cert: GREM | Instructor: Jake Williams

HOSTED **Health Care Security Essentials**
Instructor: Greg Porter

Contact Information

For further information, please contact:

Sean Georget
sgeorget@sans.org asiapacific@sans.org +65 8612 5278 +65 6933 9540

REGISTER AT
www.sans.org/secure-singapore-2017