Are you one of the top Information Security Professionals in Singapore?

Prove your knowledge and skills at the

SANS Singapore 2016 NetWars Championship!

9 April

HOSTED BY:

Bryce Galbraith

FREE OF CHARGE TO ALL STUDENTS AT SANS SECURE SINGAPORE 2016

We are pleased to invite you to join the SANS Singapore 2016 NetWars Championship! SANS is conducting its first-ever open NetWars Tournament in Singapore – come and join this exciting event to test your skills in a challenging and fun learning environment with the chance to win exciting prizes for the top 3 finishers.

Winner receives an Apple Watch!

NEW! ICS515:

ICS Active Defense and Incident Response

28 March - 1 April | Robert M. Lee

ICS515: ICS Active Defense and Incident Response will empower students to understand their networked industrial control system (ICS) environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This process of monitoring, responding to, and learning from threats is known as "active defense." It is the approach needed to appropriately counter advanced adversaries targeting ICS, as has been seen with malware such as Stuxnet, HAVEX, and BlackEnergy2. Students can expect to come out of this course fully understanding how to to deconstruct targeted ICS attacks, with a focus on delivery methods and observable attributes. This knowledge demystifies adversary capabilities and gives actionable recommendations to defenders. The course uses a hands-on approach that shows real-world malware and breaks down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of concepts such as generating and using threat intelligence, performing network security monitoring, and executing threat triage and incident response to ensure the safety and reliability of operations. The strategy presented in the course serves as a basis for ICS organizations looking to show that defense is doable.

NEW! FOR578: **Cyber Threat Intelligence**

4-8 April | Robert M. Lee

THERE IS NO TEACHER BUT THE ENEMY!

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

During a targeted attack, an organization needs a top-notch and cutting-edge incident response armed with the critical intelligence necessary to understand how adversaries operate and to combat the threat. **FOR578: Cyber Threat Intelligence** will train you and your team to detect, scope, and select resilient courses of action in response to such intrusions and data breaches.

FOR408: Windows Forensic Analysis

28 March - 2 April | GIAC Cert: GCFE | Chad Tilbury

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.

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques

28 March - 2 April | GIAC Cert: GREM | Jess Garcia

This popular malware analysis course helps forensic investigators, incident responders, security engineers and IT administrators acquire practical skills for examining 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.

SANS Secure Singapore 2016

The Most Trusted Name for Information and Software Security Training Worldwide

Singapore | 28 March - 8 April

Location: Grand Copthorne Waterfront

Choose from these popular courses:

FOR578: **Cyber Threat Intelligence NEW!**

ICS515: **ICS Active Defense and Incident Response NEW!**

SEC550: **Active Defense, Offensive Countermeasures, and Cyber Deception NEW!**

SEC504: **Hacker Tools, Techniques, Exploits & Incident Handling**

FOR408: **Windows Forensic Analysis**

SEC542: **Web App Penetration Testing and Ethical Hacking**

FOR610: **Reverse-Engineering Malware: Malware Analysis Tools and Techniques**

AUD507: **Auditing & Monitoring Networks, Perimeters, and Systems**

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

SEC511: **Continuous Monitoring and Security Operations**

Also featuring:

NETWARS

REGISTER AT

sans.org/event/secure-singapore-2016

CONTACT

+65 6933 9540 | AsiaPacific@sans.org

GIAC Approved Training

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

28 March - 2 April | GIAC Cert: GCIH | BJ Gleason

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.

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 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!

SEC511: Continuous Monitoring and Security Operations

28 March - 2 April | GIAC Cert: GMON | Mark Hofman

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.

You Will Be Able To

- Analyze a security architecture for deficiencies
- Apply the principles learned in the course to design a defensible security architecture
- Understand the importance of a detection-dominant security architecture and Security Operations Center (SOC)
- Identify the key components of Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Monitoring (CM)
- Determine appropriate security monitoring needs for organizations of all sizes
- Implement robust Network Security Monitoring/Continuous Security Monitoring (NSM/CSM)
- Determine requisite monitoring capabilities for a SOC environment
- Determine capabilities required to support continuous monitoring of key Critical Security Controls
- Utilize tools to support implementation of Continuous Monitoring per NIST guidelines SP 800-137

AUD507: Auditing & Monitoring Networks, Perimeters, and Systems

28 March - 2 April | GIAC Cert: GSNA | David Hoelzer

One of the most significant obstacles facing many auditors today is how exactly to go about auditing the security of an enterprise. What systems really matter? How should the firewall and routers be configured? What settings should be checked on the various systems under scrutiny? Is there a set of processes that can be put into place to allow an auditor to focus on the business processes rather than the security settings? All of these questions and more will be answered by the material covered in this course.

This course is specifically organized to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practices, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation are taken from real-world examples.

A great audit is more than marks on a checklist; it is the understanding of what the underlying controls are, what the best practices are, and why. Sign up for this course and gain the mix of theoretical, hands-on, and practical knowledge to conduct a great audit.

SEC542: Web App Penetration Testing and Ethical Hacking

28 March - 2 April | GIAC Cert: GWAPT | Micah Hoffman

Web applications play a vital role in every modern organization. But, if your organization does not 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, so 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.

In addition to more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS NetWars Cyber Range. This Capture-the-Flag event on the final day brings students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way to hammer home lessons learned.

NEW! SEC550: Active Defense, Offensive Countermeasures and Cyber Deception

4-8 April | Bryce Galbraith

The current threat landscape is shifting. Traditional defenses are 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 at your disposal when you need them to annoy attackers, determine who is attacking you, and, finally, attack the attackers.

SEC550 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 Defenses in their environments. The course is very heavy with hands-on activities – we won't just talk about Active Defenses, we will work through labs that will enable you to quickly and easily implement what you learn in your own working environment.

You Will Be Able To

- 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

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

4-8 April | GIAC Cert: GCCC | Randy Marchany

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.

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.

You Will Be Able To

- Apply a security framework based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organizations' important information and systems
- Understand the importance of each Control, how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of networks and systems
- Identify and utilize tools that implement Controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each Control
- Employ specific metrics to establish a baseline and measure the effectiveness of the Controls
- Understand how the Critical Controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
- Audit each of the Critical Controls with specific, proven templates, checklists, and scripts provided to facilitate the audit process