THE MOST TRUSTED NAME FOR INFORMATION AND SOFTWARE SECURITY TRAINING WORLDWIDE

SANS Thailand 2017

12-30 June

Venue: TISCO Tower
Level 12, Room 12G Business Lounge
48/2 North Sathorn Road
Bangrak, Bangkok, 10500 Thailand

GIAC CERTIFICATIONS
GIAC-Approved Training

Thai Language Instruction Using English Language Courseware Materials

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling

12-13, 19-20, 26-27 June | GIAC Cert: GCIH | Dr. Sorot Panichprecha

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!

FOR508
Advanced Digital Forensics, Incident Response, and Threat Hunting

15-16, 22-23, 29-30 June | GIAC Cert: GCFA | Dr. Sorot Panichprecha

Chances are very high that hidden threats already exist inside your organization's networks. Organizations 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. 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

Instructor: Dr. Sorot Panichprecha

Dr. Sorot Panichprecha is the founder of Epiphany Consulting. Epiphany, based in Bangkok, Thailand, provides both offensive and defensive services from penetration testing to digital forensic investigation and security incident response. Dr. Sorot's information security experience started in 1998, where he was responsible for managing the servers and networks for the university faculty. He started his professional career as a system administrator designing and building the first government public key infrastructure (PKI) in Thailand. Following the operationalisation of the PKI, he pursued further studies in Australia. He is now an active member of the digital forensic community in Thailand.

Dr. Sorot provides seminars on various information security topics, including digital forensics, information security fundamentals, information security risk management, and information security standards. In addition to his information security career, he is also a part-time university lecturer teaching information security subjects including digital forensics and has conducted classes for the SANS Institute in Singapore and Thailand, in addition to workshops with RSA Asia Pacific-Japan.

Dr. Sorot holds a bachelor's degree in computer science, a master's degree in information technology and a PhD, with a thesis focused on intrusion-detection systems (IDS). He has been active with SANS since 2009 and currently holds the following certifications: GSEC, GCIA, GCIH, GPEN, GWAPT, GXPN, GCFE, GCFA, GREM, and CISSP.

REGISTER AT: www.sans.org/event/thailand-2017 EMAIL: asiapacific@sans.org

Training Roadmap | Choose Your Path

Baseline Skills

SEC301 Intro to Information Security

GISF Certification — Information Security fundamentals

1 You are experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Security Techniques
Defend & Maintain

Every security professional should know the defense-in-depth techniques taught in SEC401, and SEC504 completes the "offense informs defense" preparation teaching defense specialists how attacks occur and how to respond. If you've got the core defense skills, start with SEC504.

- SEC401 Security Essentials Bootcamp Style — GSEC Certification Security Essentials
- SEC504 Hacker Tools, Techniques, Exploits and, Incident Handling — GCIH Certification Certified Incident Handler

1b You will be responsible for managing security teams or implementations, but do not require hands-on skills

Security Management

- MGT512 SANS Security Leadership Essentials For Managers with Knowledge Compression™ — GSLC Certification Security Leadership
- SEC566 Implementing and Auditing the Critical Security Controls-In-Depth — GCCC Certification Critical Security Controls

Intermediate Job Roles

2 You are experienced in security, preparing for a specialized job role or focus

Security Monitoring and Detection

- SEC503 Intrusion Detection In-Depth — GCIA Certification Certified Intrusion Analyst
- SEC511 Continuous Monitoring and Security Operations — GMON Certification Continuous Monitoring

Penetration Testing & Vulnerability Analysis

- SEC560 Network Penetration Testing and Ethical Hacking — GPEN Certification Penetration Tester
- SEC542 Web App Penetration Testing and Ethical Hacking — GWAPT Certification Web Application Penetration Tester

Incident Response and Enterprise Forensics

- FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting — GCFA Certification Forensic Analyst
- FOR572 Advanced Network Forensics and Analysis — GNFA Certification Network Forensic Analyst

MGT414 SANS Training Program for CISSP® Certification — GISP Certification Information Security Professional

Crucial Skills, Specialized Roles

SANS' comprehensive catalog enables professionals to deepen their technical skills in key practice areas. It also directly addresses other audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

3 You are a candidate for specialized or advanced training

Cyber Defense Operations

- SEC501 Advanced Security Essentials – Enterprise Defender **GCED**
- SEC505 Securing Windows and PowerShell Automation **GCWN**
- SEC506 Securing Linux/Unix | **GCUX**
- SEC579 Virtualization and Software-Defined Security

Industrial Control Systems Security

- ICS410 ICS/SCADA Security Essentials | **GICSP**
- ICS456 Essentials for NERC Critical Infrastructure Protection
- ICS515 ICS Active Defense and Incident Response

Penetration Testing and Ethical Hacking

- SEC550 Active Defense, Offensive Countermeasures and Cyber Deception
- SEC561 Immersive Hands-On Hacking Techniques
- SEC562 CyberCity Hands-on Kinetic Cyber Range Exercise
- SEC573 Automating Information Security for Python **GPYC**
- SEC575 Mobile Device Security and Ethical Hacking **GMOB**
- SEC617 Wireless Ethical Hacking, Penetration Testing, and Defenses | **GAWN**
- SEC642 Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
- SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | **GXPN**
- SEC760 Advanced Exploit Development for Penetration Testers

Digital Forensics and Incident Response

- FOR408 Windows Forensic Analysis | **GCFE**
- FOR518 Mac Forensic Analysis
- FOR526 Memory Forensics In-Depth
- FOR578 Cyber Threat Intelligence
- FOR585 Advanced Smartphone Forensics | **GASF**
- FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques | **GREM**

Software Security

- DEV522 Defending Web Applications Security Essentials **GWEB**
- DEV541 Secure Coding in Java/JEE: Developing Defensible Applications | **GSSP-JAVA**
- DEV544 Secure Coding in .NET: Developing Defensible Applications | **GSSP-.NET**

Management

- MGT514 IT Security Strategic Planning, Policy, and Leadership
- MGT517 Managing Security Operations: Detection, Response, and Intelligence
- MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep | **GCPM**

Audit | Legal

- AUD507 Auditing & Monitoring Networks, Perimeters, and Systems | **GSNA**
- LEG523 Law of Data Security and Investigations | **GLEG**