THE MOST TRUSTED NAME FOR INFORMATION AND SOFTWARE SECURITY TRAINING WORLDWIDE

SANS Adelaide 2017

21-26 August | Venue: Adelaide Convention Centre

REGISTER AT: **www.sans.org/adelaide-2017** EMAIL: **asiapacific@sans.org** PHONE: **02 6198 3352**

SEC401
Security Essentials Bootcamp Style

Instructor: Dave Shackleford | 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.

SEC401: Security Essentials Bootcamp Style is focused on teaching you the essential information security skills and techniques you need to protect and secure your organization's critical information assets and business systems.

SEC503
Intrusion Detection In-Depth

Instructor: Jonathan Ham | GIAC Cert: GCIA

Reports of prominent organizations 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: Intrusion Detection In-Depth 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.

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling

Instructor: Chris Pizor | GIAC Cert: GCIH

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.

FOR500 (Formerly FOR408)
Windows Forensic Analysis

Instructor: Nick Klein | GIAC Cert: GCFE

FOR500 focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. Learn to recover, analyze, and authenticate forensic data on Windows systems. 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. Use your new skills for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR500 teaches you how to mine this mountain of data.

FUTURE SANS TRAINING EVENTS

Melbourne	22-27 May	**www.sans.org/melbourne-2017**
Cyber Defence Canberra	27 June – 8 July	**www.sans.org/cyber-defence-canberra-2017**
Sydney	13-25 November	**www.sans.org/sydney-2017**

Training Roadmap | Choose Your Path

Baseline Skills

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 that teaches 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 you 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

New to Cybersecurity?

- **SEC301** Intro to Information Security — **GISF** Certification Information Security Fundamentals

Intermediate Job Roles

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

Security Monitoring & 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 course offerings enable professionals to deepen their technical skills in key practice areas. The courses also address other topics and 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**
- **SEC566** Implementing and Auditing the Critical Security Controls – In-Depth | **GCCC**
- **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 | **GIAD**

Penetration Testing & 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 with 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**
- **SEC566** Implementing and Auditing the Critical Security Controls – In-Depth | **GCCC**
- **LEG523** Law of Data Security and Investigations | **GLEG**