SANS

Melbourne 2017

22-27 May | Venue: Jasper Hotel

GIAC CERTIFICATIONS

GIAC-Approved Training

REGISTER AT: **www.sans.org/melbourne-2017**   EMAIL: **asiapacific@sans.org**

SEC401
Security Essentials Bootcamp Style

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.

SEC542
Web App Penetration Testing and Ethical Hacking

GIAC Cert: GWAPT

SEC542 enables students to assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations. 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.

SEC550
Active Defense, Offensive Countermeasures and Cyber Deception

The current threat landscape is shifting. Traditional defenses 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 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).

FOR508
Advanced Digital Forensics, Incident Response, and Threat Hunting

GIAC Cert: GCFA

This course 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

ADVANCED THREATS ARE IN YOUR NETWORK - IT'S TIME TO GO HUNTING!

FUTURE SANS TRAINING EVENTS			
Cyber Defence Canberra	27 June – 8 July	**www.sans.org/cyber-defence-canberra-2017**
Adelaide	21-26 August	**www.sans.org/adelaide-2017**
Sydney	13-25 November	**www.sans.org/sydney-2017**

Training Roadmap | Choose Your Path

SANS

Baseline Skills

New to Cybersecurity?

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 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

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

SEC566 Implementing and Auditing the Critical Security Controls – In-Depth — **GCCC** Certification Critical Security Controls

---

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

Intermediate Job Roles

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

---

3
You are a candidate for specialized or advanced training

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.

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

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
FOR500 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**

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**

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**

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**

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**

PMP® is a registered trademark of the Project Management Institute, Inc.