Global Horizon
TRAINING CENTER

Training Course:
SEC501: Advanced Security Essentials - Enterprise Defender

15 - 19 July 2024
Baku (Azerbaijan)

Training Course:
SEC501: Advanced Security Essentials - Enterprise Defender

Training Course code: IT234726 From: 15 - 19 July 2024 Venue: Baku (Azerbaijan) - Training Course Fees: 5775 Euro

Introduction

It costs enterprises worldwide billions of dollars annually to respond to malware, and particularly Ransomware, attacks. So it is increasingly necessary to understand how such software behaves. Ransomware spreads very quickly and is not stealthy; as soon as your data become inaccessible and your systems unstable, it is clear something is amiss. Beyond detection and response, when prevention has failed, understanding the nature of malware, its functional requirements, and how it achieves its goals is critical to being able to rapidly reduce the damage it can cause and the costs of eradicating it.

You Will Learn

- Core components of building a defensible network infrastructure and properly securing your routers, switches, and other network infrastructure
- Formal methods to perform vulnerability assessment and penetration testing to find weaknesses on your enterprise network
- Methods to detect advanced attacks against your network and indicators of compromise on deployed systems, including the forensically sound collection of artifacts and what you can learn from them
- How to respond to an incident using the six-step process of incident response: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned
- Approaches to analyzing malware, ranging from fully automated techniques to the manual analysis of static properties, interactive behavior, and code reversing

Course Objectives of Advanced Security Essentials - Enterprise Defender

You Will Be Able To

- Identify network security threats against infrastructure and build defensible networks that minimize the impact of attacks
- Utilize tools to analyze a network to prevent attacks and detect the adversary
- Decode and analyze packets using various tools to identify anomalies and improve network defenses
- Understand how the adversary compromises systems and how to respond to attacks using the six-step incident handling process
- Perform penetration testing against an enterprise to determine vulnerabilities and points of compromise
- Use various tools to identify and remediate malware across your enterprise

Prerequisites of Advanced Security Essentials - Enterprise Defender

While not required, it is recommended that students take SANS' SEC401: Security Essentials: Network, Endpoint, and Cloud course or have the skills taught in that class. This includes a detailed understanding of networks, protocols, and operating systems.

Course Outlines for Advanced Security Essentials - Enterprise Defender

Day 1

Definsible Network Architichuer

- Security Standards and Audit
- Authentication, Authorization, and Accounting
- Defending Network Infrastructure
- Intrusion Prevention Systems and Firewalls
- Name Resolution Attacks and Defense
- Securing Private and Public Cloud Infrastructure

Day 2

Penetration Testing

- Penetration Testing Scoping and Rules of Engagement
- Online Reconnaissance
- Social Engineering
- Network Mapping and Scanning Techniques
- Enterprise Vulnerability Scanning
- Network Exploitation Tools and Techniques
- Post-Exploitation and Pivoting
- Web Application Exploitation Tools and Techniques
- Reporting and Debriefing

Day 3

Security Operation Foundation

- Network Security Monitoring
- Advanced Packet Analysis
- Network Intrusion Detection/Prevention
- Writing Signatures for Detection
- Network Forensics and More
- Event Management Introduction
- Continuous Monitoring
- Logging and Event Collection and Analysis
- SIEM and Analytics

Day 4

Digital Forensics and Incident Response

- Active Defense
- DFIR Core Concepts: Digital Forensics
- DFIR Core Concepts: Incident Response
- Modern DFIR
- Widening the Net: Scaling and Scoping

Day 5

Malware Analysis

- Introduction to Malware Analysis
- Malware Analysis Stages: Fully Automated and Static Properties Analysis
- Malware Analysis Stages: Interactive Behavior Analysis
- Malware Analysis Stages: Manual Code Reversing

Registration form on the Training Course:
SEC501: Advanced Security Essentials - Enterprise Defender

Training Course code: IT234726 From: 15 - 19 July 2024 Venue: Baku (Azerbaijan) - Training Course Fees: 5775 Euro

Complete & Mail or fax to Global Horizon Training Center (GHTC) at the address given below

Delegate Information

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Company Information

Company Name: .....
Address: .....
City / Country: .....

Person Responsible for Training and Development

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Payment Method

- ☐ Please find enclosed a cheque made payable to Global Horizon
- ☐ Please invoice me
- ☐ Please invoice my company

Easy Ways To Register

Telephone: +201095004484 to provisionally reserve your place.	Fax your completed registration form to: +20233379764	E-mail to us : info@gh4t.com or training@gh4t.com	Complete & return the booking form with cheque to:Global Horizon 3 Oudai street, Aldouki, Giza, Giza Governorate, Egypt.