301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

View Full Course Details including Latest Schedule Online

CYBERPHOENIX

Cyber Threats Detection and Mitigation Training

Course Overview

This training course examines the fundamentals of system forensics: what forensics is, the role of computer forensics specialists, computer forensic evidence, and application of forensic analysis skills. It also gives an overview of computer crimes, forensic methods, and laboratories. Students will learn about the tools, techniques, and methods used to perform computer forensics and investigation. This course explores emerging technologies as well as future directions of this interesting and cutting-edge field.

Course Objectives

- Understand the importance of having a solid foundation for your security posture
- Understand the attack strategy using cyber security kill chain
- Enhance their defense strategy by improving security policies, hardening the network, implementing active sensors, and leveraging threat intelligence
- Perform an incident investigation
- Understand the recovery process
- Understand continuous security monitoring and how to implement a vulnerability management strategy
- Perform log analysis to identify suspicious activities

Course Outline

Security Posture

- The current threat landscape
- Cybersecurity challenges
- Enhancing your security posture
- The Red and Blue Team

Incident Response Process

- Incident response process
- Handling an incident
- Post-incident activity
- Incident response in the cloud

Understanding the Cybersecurity Kill Chain

- External reconnaissance
- Access and privilege escalation
- Exfiltration
- Sustainment
- Assault
- Obfuscation
- Threat life cycle management

Reconnaissance

- External reconnaissance
- Internal reconnaissance
- Conclusion of the reconnaissance chapter

Compromising the System

- Analyzing current trends
- Phishing
- Exploiting a vulnerability
- Zero-day
- Performing the steps to compromise a system

Chasing a User's Identity

- Identity is the new perimeter
- Strategies for compromising a user's identity
- Hacking a user's identity

Lateral Movement

- Infiltration
- Performing lateral movement

Privilege Escalation

- Infiltration
- Avoiding alerts
- Performing privilege escalation
- Conclusion and lessons learned

Security Policy

- Reviewing your security policy
- Educating the end user
- Policy enforcement
- Monitoring for compliance

Network Segmentation

- Defense in depth approach
- Physical network segmentation
- Securing remote access to the network
- Virtual network segmentation
- Hybrid cloud network security

Active Sensors

- Detection capabilities
- Intrusion detection systems
- Intrusion prevention system
- Behavior analytics on-premises
- Behavior analytics in a hybrid cloud

PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Threat Intelligence

- Introduction to threat intelligence
- Open source tools for threat intelligence
- Microsoft threat intelligence
- Leveraging threat intelligence to investigate suspicious activity

Investigating an Incident

- Scoping the issue
- Investigating a compromised system on-premises
- Investigating a compromised system in a hybrid cloud

Recovery Process

- Disaster recovery plan
- Live recovery
- Contingency planning
- Best practices for recovery

Vulnerability Management

- Creating a vulnerability management strategy
- Implementation of vulnerability management
- Best practices for vulnerability management
- Implementing vulnerability management with Nessus

Starting at **$2,500**

ATTENTION

For GSA pricing or Contractor quotes call

240.667.7757

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

Included in this **Cyber Threats Detection and Mitigation Training**

- 3 days instructor-led training
- Cyber Threats Detection and Mitigation Training training book
- Notepad, pen and highlighter
- Variety of bagels, fruits, doughnuts and cereal available at the start of class*
- Tea, coffee and soda available throughout the day*
- Freshly baked cookies every afternoon*

10420 Little Patuxent Parkway Suite 500 Columbia, MD 21044