

[View Full Course Details including Latest Schedule Online](#)

CYBER PHOENIX

Cyber Threats Detection and Mitigation Training

Due to Covid-19 safety restrictions PhoenixTS will temporarily be unable to provide food to our students who attend class at our Training Center; however, our Break Areas are **currently open** where students will find a constant supply of Coffee, Tea and Water. Students may bring their own lunch and snacks to eat in our breakrooms or at their seat in the classroom or eat out at one of the many nearby restaurants.

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.

Schedule

| DATE | LOCATION | |
|--|--|----------------------------|
| 8/08/22 - 8/10/22 (3 days) 8:30AM - 4:30PM | Tysons Corner, VA Open | Contact Us |
| 8/15/22 - 8/17/22 (3 days) 8:30AM - 4:30PM | Live Online Open | Contact Us |
| 8/15/22 - 8/17/22 (3 days) 8:30AM - 4:30PM | Live Online Open | Contact Us |
| 2/06/23 - 2/08/23 (3 days) 8:30AM - 4:30PM | Tysons Corner, VA Open | Contact Us |
| 4/03/23 - 4/05/23 (3 days) 8:30AM - 4:30PM | Tysons Corner, VA Open | Contact Us |



| DATE | LOCATION | |
|--|--|----------------------------|
| 6/05/23 - 6/07/23 (3 days) 8:30AM - 4:30PM | Tysons Corner, VA Open | Contact Us |
| 8/07/23 - 8/09/23 (3 days) 8:30AM - 4:30PM | Tysons Corner, VA Open | Contact Us |
| 10/10/23 - 10/12/23 (3 days) 8:30AM - 4:30PM | Tysons Corner, VA Open | Contact Us |
| 12/04/23 - 12/06/23 (3 days) 8:30AM - 4:30PM | Tysons Corner, VA Open | Contact Us |

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

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

Due to Covid-19 safety restrictions PhoenixTS will temporarily be unable to provide food to our students who attend class at our Training Center; however, our Break Areas are **currently open** where students will find a constant supply of Coffee, Tea and Water. Students may bring their own lunch and snacks to eat in our breakrooms or at their seat in the classroom or eat out at one of the many nearby restaurants.

Starting at **\$2,500**

ATTENTION

For GSA pricing or Contractor quotes call

[240.667.7757](tel:240.667.7757)

GSA



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*