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

View Full Course Details including Latest Schedule Online

PHOENIX TS

Cyber Security: Threat Analysis and Response Solutions Training

This four-day course addresses the most pressing issues facing cyber-security from both a national and global perspective.

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

Course Overview

Our 3-day, instructor-led Cyber Security: Threat Analysis and Response Solutions Training course covers the following topics:

- Threat identification
- Insider threat prevention
- Detection and mitigation
- Assessment of security assurance
- Information terrorism
- Information security management standards
- Public policy drivers
- The role of information security professionals

Before taking this course, you should have some knowledge of threat identification, detection and mitigation, security assurance and network security protocol.

Schedule

Currently, there are no public classes scheduled. Please contact a Phoenix TS Training Consultant to

discuss hosting a private class at 301-258-8200.

Course Outline

Digital Forensics

- Defining digital forensics
- Engaging forensics services
- Reporting crime
- Search warrant and law
- Forensic roles
- Forensic job market
- Forensic training

Cybercrime And Defenses

- Crime in a digital age
- Exploitation
- Adversaries
- Cyber law

Building A Digital Forensics Lab

- Desktop virtualization
- Installing Kali Linux
- Attack virtual machines
- Cuckoo sandbox
- Binwalk
- The sleuth kit
- Cisco snort
- Windows tools
- Physical access controls
- Storing your forensics evidence
- Jump bag

Responding To A Breach

- Why organizations fail at incident response

- Preparing for a cyber incident
- Defining incident response
- Incident response plan
- Assembling your incident response team
- Responding to an incident
- Assessing incident severity
- Following notification procedures
- Employing post-incident actions and procedures
- Identifying software used to assist in responding to a breach

Investigations

- Pre-investigation
- Opening a case
- First responder
- Device power state
- Search and seizure
- Chain of custody
- Network investigations
- Forensics reports
- Closing the case
- Critiquing the case

Collecting And Preserving Evidence

- First responder
- Evidence
- Hard drives
- Volatile data
- Duplication
- Hashing
- Data preservation

Endpoint Forensics

- File systems
- Windows registry
- Printer spools
- Log analysis
- IoT forensics

Network Forensics

- Network protocols
- Security tools
- Security logs
- Network baselines
- Symptoms of threats

Mobile Forensics

- Mobile devices
- iOS Architecture
- iTunes Forensics
- iOS Snapshots
- How to jailbreak the iPhone
- Android
- Bypass PIN
- Forensics with commercial tools
- Call logs and SMS spoofing
- Voicemail bypass
- How to find burner phones
- SIM card cloning

Email And Social Media

- Message in a bottle
- Email header
- Social media
- People search
- Google search
- Facebook search

Cisco Forensics Capabilities

- Cisco security archietcture
- Cisco open source
- Cisco firepower
- Cisco Advanced Malware Protection (AMP)
- Cisco threat grid

- Cisco web security appliance
- Cisco CTA
- Meraki
- Email security appliance
- Cisco identity services engine
- Cisco stealthwatch
- Cisco tetration
- Cisco umbrella
- Cisco cloudlock
- Cisco network technology

Forensics Case Studies

- Investigating network communication
- Using endpoint forensics
- Investigating malware
- Investigating volatile data
- Acting as first responder

Forensic Tools

- Tools
- Mobile devices
- Kali Linux tools
- Cisco tools
- Forensic software packages
- Useful websites
- Miscellaneous sites

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

Phoenix TS is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of

individual courses for CPE credit. Complaints re-garding registered sponsors may be submitted to the National Registry of CPE Sponsors through its web site: www.nasbaregistry.org

Starting at **$1,950**

ATTENTION

For GSA pricing or Contractor quotes call 301-258-8200 – Option 2.

GSA



Price Match Guarantee

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

This **Threat Analysis and Response Solutions Training** course includes:

- 3 days of instructor-led training

- Cyber Security: Threat Analysis and Response Solutions 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*