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

View Full Course Details including Latest Schedule Online

PHOENIX TS

Network Security Monitoring with Security Onion

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

This 4 day, instructor led course will provide the basic concepts of Security Onion and it's use as a Network Security Monitoring (NSM) suite. Participants will install Security Onion, then use component tools to collect and visualize network data. Participants will also learn toolset service verification and troubleshooting in this course. You will benefit most from this course if you want to accomplish basic monitoring tasks in Security Onion, or if you want to have a solid foundation for advancing to become a Network Security Monitoring Expert. If you intend to work with Security Onion in depth this course is a good place to start, but you will need to engage in additional courses to be fully prepared to work with the toolset in production.

After taking this course, participants will know:

- About the Security Onion toolset
- How the tools support Network Security Monitoring.
- How to locate Security Onion requirements, OS image, and documentation.
- How to install and configure Security Onion on a virtual machine.
- How to verify services and troubleshoot Security Onion.
- Which tools help you visualize the network in terms of sensors and data feeds.
- How to apply Security Onion to the collection, detection and analysis activities of Network Security Monitoring

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

Day 1: Overview and Install

- Module A: What is Network Security Monitoring?
- Define Network Security Monitoring 7
- Compare Network Monitoring with Firewalls, Network Monitoring, and Continuous Monitoring 8
- Learn how Network Security Monitoring Works 9
- Discuss Advantages to NSM 9
- Determine when NSM is Not Possible 10
- Learn NSM Lexicon 10
- Examine NSM Operational Cycle 12
- Discuss NSM Data 13
- Module B: Security Onion Installation 16
- Learn about Security Onion 16
- Examine Security Onion Tools 17
- Prepare for Installation 17
- Install Security Onion 18
- Configure Security Onion 18
- Daily Summary: NSM Overview and SO Installation 21

Day 2: Network Traffic and Alerts 22

- Module A: Replay Network Traffic 23
- Network Traffic: FPC- PCAP 23
- Replay sample PCAP Files 24
- Running Packet Analysis Tools 25
- Examine packet data in Squil 25
- Module B: Alerts 28
- Detection Mechanisms 28
- Alert Interfaces 28
- Analyzing Alerts in Squert 29
- Daily Summary: Network Traffic and Alerts 32

Day 3: Kibana and BRO 33

- Module A: Log Analysis with Kibana 34

- Determining the Value of Log Data 34
- Working with Kibana 34
- Pivoting from Kibana 36
- SSO to Squert from Kibana 36
- PIVOT from Squert to Kibana 36
- Module B: BRO 38
- Work with BRO 38
- Learning about the BRO Intel Framework 39
- Daily Summary: Kibana and BRO 41

Day 4: Production Implementation & Troubleshooting 42

- Module A: Network Security Monitoring in Production 43
- Distributed Deployment Requirements 44
- CPU 44
- Monitoring is CPU Intensive. All the SO IDS tools (can you name them) are incredibly CPU intensive. The more traffic you are monitoring, the more CPU cores you'll need. 44
- RAM 44
- Install Order 44
- Using OnionSalt 45
- Air-gapped Networks 45
- Module B: Troubleshooting Security Onion 47
- Status 47
- Updates 48
- Screen Askew 48
- Adding Analyst Accounts 48
- Reboot, No Services 48
- Ruleset Options 48
- Snort Community Ruleset 48
- Viewing with Rule Categories 49
- Start and Stop Services 49
- Disable Services 49
- Disable Snorby 49
- SGUIL 50
- Sguil Days To Keep 50
- Day 4 Summary: SO Production & Troubleshooting 52
- Resources 53
- Security Onion 53
- External PCAP Files 53

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

Security Onion Training Facts FAQs

Who should take this course?

This course is designed for Security Analysts, Team Leads and Network and Information Security Managers.

What is the recommended experience for this course?

The course assumes that you're familiar with basic networking and security principles.

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 **$3,250**

ATTENTION

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

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.