Vendor-Neutral Global IT Certifications

Star Security Cyber Analytics

PRODUCE PROACTIVE SECURITY MEASURES

WITH NEW APPROACH OF CYBER SECURITY

SSCA

Star Secuirty Cyber Analytics

Exam Code: S09-013

LEARN + EXAM = CERTIFIED

www.starcertification.org

info@starcertification.org

Star Security Cyber Analytics

The world has converged today, especially with everything and everyone connected across the cyber space. Every day, massive data is exchanged across the cyber world, a lot of which is highly sensitive information that needs to be protected from all sorts of cybercrimes. Cybersecurity is a must-have for information security and IT professionals, in order to safeguard their business interests.Monitoring and threat detection are crucial if businesses are to stay ahead of the curve. Security Analytics is an approach to cybersecurity focused on the analysis of data to produce proactive security measures.

Star Security Cyber Analyticsis a thorough training program that will teach learners to spot vulnerabilities, fend off attacks, and immediately respond to emergencies. The program explains the use of various security analytics tools to implement real-time monitoring of servers, endpoints and network traffic, consolidate and coordinate diverse event data from application and network logs, and perform forensic analysis to better understand attack methods and system vulnerabilities.

Audience: Star Security Cyber Analytics assumes that the learner has a minimum of 2-3 years of experience in the information security domain with equivalent knowledge of Networking and Cyber Security.

Course Objectives:

In this course, you will learn about:

- Fundamentals of Cybersecurity
- Threats associated with network security
- Reconnaissance techniques and incident response process
- Vulnerability management and scanning result analysis
- Evaluating and mending the incident
- How to secure your organization environment from common vulnerabilities
- How to analyse the threats and take appropriate action to mitigate the threats
- Access management and compensating Controls
- How to implement secure software development life cycle

Course Outcome :

After completing this course, you will be able to:

- Explain cybersecurity analytics concepts
- Use techniques to manage threats and deal with incidents
- Fetch login credentials by exploiting vulnerabilities
- Protect systems against vulnerabilities and threats by investigating and applying the appropriate countermeasures
- Recover deleted files by analysing the forensic image
- Deploy security measures for secure software development
- Investigate live systems and crack passwords

Course Outline :

1. Fundamentals of Cybersecurity
2. Preventing Networks from Cybersecurity Threats
3. Managing Threats Using Reconnaissance Techniques
4. Understanding Vulnerability Management
5. Analysing Results of Vulnerability Scans
6. Understanding Incident Response Process
7. Dealing with Incidents
8. Understanding Forensic Investigations
9. Exploring Principles and Concepts of Security Architecture
10. Exploring Security Issues Encountered in Identity and Access Management
11. Supporting Defence-in-Depth Security Architecture with Compensating Controls
12. Securing Software Development
13. Labs

Lab Session 1 - Using Microsoft Baseline Security Analyzer for Scanning a Computer
Lab Session 2 - Verifying Drive/Image Using FTK Imager
Lab Session 3 - Fetching Login Credentials by Exploiting Vulnerabilities in a Website Using Burp Suite
Lab Session 4 - Recovering Deleted Files by Analysing the Forensic Image Using Autopsy
Lab Session 5 - Discovering Vulnerabilities in a System Using Nessus
Lab Session 6 - Preventing Malware Using Enhanced Mitigation Experience Toolkit (EMET)
Lab Session 7 - Investigating a Live System Using Helix3
Lab Session 8 - Using Wireshark to Capture and Analyse the Flow of Packets in a Network
Lab Session 9 - Scanning Open Ports on a Kali Linux System Using Nmap
Lab Session 10 - Cracking Passwords from its Hash Form Using John the Ripper

Exam Information:

Exam Code	:	S09-013	Exam Pattern	:	Multiple Choice
Exam Duration	:	2 Hrs	Exam Delivery	:	AEPTC (ACADEMIC EDUCATION & PROFESSIONAL TESTING CENTER)
Passing Score	:	70%			

Course Duration : 48 Hrs