CYSA (COMPTIA CYBERSECURITY ANALYST) 1.0

Objetivo

CompTIA Cybersecurity Analyst CySA+ Certification Training Course Objectives: â□¢ Prepare for and pass the Cybersecurity Analyst (CySA+) exam; â□¢ Threat and Vulnerability Management; â□¢ Software and Systems Security; â□¢ Security Operations and Monitoring; â□¢ Incident Response; â□¢ Compliance and Assessment.

PÃºblico Alvo

IT Security Professionals must have 3-4 years of hands-on information security or related experience for preparation to CompTIA Cybersecurity Analyst CySA+ Certification exam (CS0-002 CySA+).

PrÃ©-Requisitos

It is recommended that you have the following skills and knowledge before starting this course: â□¢ Knowledge of basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers); â□¢ Understanding of TCP/IP addressing, core protocols, and troubleshooting tools; â□¢ Network attack strategies and defenses; â□¢ Knowledge of the technologies and uses of cryptographic standards and products; â□¢ Network- and host-based security technologies and practices; â□¢ Standards and products used to enforce security on web and communications technologies.

Carga HorÃiria

40 horas (5 dias).

ConteÃºdo ProgramÃitico

Cybersecurity Analyst
Cybersecurity Objectives
Privacy vs. Security
Evaluating Security Risks
Building a Secure Network
Secure Endpoint Management
Penetration Testing
Reverse Engineering
The Future of Cybersecurity Analytics

Using Threat Intelligence
Threat Data and Intelligence
Threat Classification
Attack Frameworks
Applying Threat Intelligence Organizationwide

Reconnaissance and Intelligence Gathering
Mapping and Enumeration
Passive Footprinting
Gathering Organizational Intelligence
Detecting, Preventing, and Responding to Reconnaissance

Designing a Vulnerability Management Program
Identifying Vulnerability Management Requirements
Configuring and Executing Vulnerability Scans
Developing a Remediation Workflow
Overcoming Risks of Vulnerability Scanning
Vulnerability Scanning Tools

Analyzing Vulnerability Scans
Reviewing and Interpreting Scan Reports
Validating Scan Results
Common Vulnerabilities

Cloud Security
Understanding Cloud Environments
Operating in the Cloud
Cloud Infrastructure Security

Infrastructure Security and Controls
Understanding Defense-in-Depth
Improving Security by Improving Controls
Analyzing Security Architecture

Identity and Access Management Security
Understanding Identity
Threats to Identity and Access
Identity as a Security Layer
Federation and Single Sign-On

Software and Hardware Development Security
Software Assurance Best Practices
Designing and Coding for Security
Software Security Testing
Hardware Assurance Best Practices

Security Operations and Monitoring
Security Monitoring

Building an Incident Response Program
Security Incidents
Phases of Incident Response
Building the Foundation for Incident Response
Creating an Incident Response Team

Coordination and Information Sharing
Classifying Incidents

Analyzing Indicators of Compromise
Analyzing Network Events
Investigating Host-Related Issues
Investigating Service and Application-Related Issues

Performing Forensic Analysis and Techniques
Building a Forensics Capability
Understanding Forensic Software
Conducting Endpoint Forensics
Network Forensics
Cloud, Virtual, and Container Forensics
Conducting a Forensic Investigation
Forensic Investigation: An Example

Containment, Eradication, and Recovery
Containing the Damage
Incident Eradication and Recovery
Wrapping Up the Response

Risk Management
Analyzing Risk
Managing Risk
Security Controls

Policy and Compliance
Understanding Policy Documents
Complying with Laws and Regulations
Adopting a Standard Framework
Implementing Policy-Based Controls
Security Control Verification and Quality Control

Labs:
Lab 1: Analyzing Output from Network Security Monitoring Tools
Lab 2: Analyzing Output from Security Appliance Logs
Lab 3: Analyzing Output from Endpoint Security Monitoring Tools
Lab 4: Analyzing Email Headers
Lab 5: Configuring SIEM Agents and Collectors
Lab 6: Analyzing, Filtering, and Searching Event Log and syslog Output
Lab 7: Collecting and Validating Digital Evidence
Lab 8: Analyzing Network-related IoCs
Lab 9: Analyzing Host and Application IoCs
Lab 10: Observing IoCs during a Security Incident
Lab 11: Analyzing Output from Topology and Host Enumeration Tools
Lab 12: Testing Credential Security
Lab 13: Configuring Vulnerability Scanning and Analyzing Outputs

Lab 14: Assessing Vulnerability Scan Outputs
Lab 15: Assessing the Impact of Regulation on Vulnerability Management
Lab 16: Performing Account and Permissions Audits
Lab 17: Configuring Network Segmentation and Security
Lab 18: Configuring and Analyzing Share Permissions
Lab 19: Assessing the Impact of Web Application Vulnerabilities
Lab 20: Analyzing Output from Web Application Assessment Tools
Lab 21: Analyzing Output from Cloud Infrastructure Assessment Tools