CompTIA Cybersecurity Analyst (CySA+)

Course code: CTCA

This five-day course is intended for administrators, especially network administrators and security administrators who are responsible for security or are interested in seeing beneath the surface through the eyes of a security analyst. The course is ideal for anyone who works as a threat and risk analyst, security specialist, member of the SOC team. The course is also intended for anyone who is interested in obtaining the globally recognized CompTIA CySA + certification.

Who is the course for

This course is primarily designed for students who are seeking the CompTIA CySA+ certification and who want to prepare for the CompTIA CySA+ CS0-002 certification exam. The course more generally supports candidates working in or aiming for job roles such as security operations center (SOC) analyst, vulnerability analyst, cybersecurity specialist, threat intelligence analyst, security engineer, and cybersecurity analyst.

What we teach you

- Assess and respond to security threats and operate a systems and network security analysis platform
- Identify modern cybersecurity threat actors types and tactics, techniques, and procedures
- Analyze data collected from security and event logs and network packet captures
- Respond to and investigate cybersecurity incidents using forensic analysis techniques
- Assess information security risk in computing and network environments
- Implement a vulnerability management program
- Address security issues with an organization's network architecture
- Understand the importance of data governance controls
- Address security issues with an organization's software development life cycle
- Address security issues with an organization's use of cloud and service-oriented architecture

Required skills

- At least two years' experience in computer network security technology or a related field
- The ability to recognize information security vulnerabilities and threats in the context of risk management
- Foundation-level operational skills with the common operating systems for PCs, mobile devices, and servers
- Foundation-level understanding of some of the common concepts for network environments, such as routing and switching
- Foundational knowledge of TCP/IP networking protocols, including IP, ARP, ICMP, TCP, UDP, DNS, DHCP, HTTP/HTTPS, SMTP, and POP3/IMAP
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include authentication and authorization, resource permissions, and antimalware mechanisms
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments, such as firewalls, IPS, NAC, and VPNs You can obtain this level of skill and knowledge by taking the following courses:
- The Official CompTIA Network+ (Exam N10-007)
- CompTIA Security+
- (Exam SY0-501)

Course outline

Module1: Explaining the Importance of Security Controls and Security Intelligence

- Identify Security Control Types
- Explain the Importance of Threat Data and Intelligence

Module2: Utilizing Threat Data and Intelligence

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Copyright © 2020 GOPAS, a.s.,
All rights reserved

- Classify Threats and Threat Actor Types
- Utilize Attack Frameworks and Indicator Management
- Utilize Threat Modeling and Hunting Methodologies

Module3: Analyzing Security Monitoring Data
- Analyze Network Monitoring Output
- Analyze Appliance Monitoring Output
- Analyze Endpoint Monitoring Output
- Analyze Email Monitoring Output

Module4: Collecting and Querying Security Monitoring Data
- Configure Log Review and SIEM Tools
- Analyze and Query Logs and SIEM Data

Module5: Utilizing Digital Forensics and Indicator Analysis Techniques
- Identify Digital Forensics Techniques
- Analyze Network-related IoCs
- Analyze Host-related IoCs
- Analyze Application-Related IoCs
- Analyze Lateral Movement and Pivot IoCs

Module6: Applying Incident Response Procedures
- Explain Incident Response Processes
- Apply Detection and Containment Processes
- Apply Eradication, Recovery, and Post-Incident Processes

Module7 Applying Risk Mitigation and Security Frameworks
- Apply Risk Identification, Calculation, and Prioritization Processes
- Explain Frameworks, Policies, and Procedures

Module8: Performing Vulnerability Management
- Analyze Output from Enumeration Tools
- Configure Infrastructure Vulnerability Scanning Parameters
- Analyze Output from Infrastructure Vulnerability Scanners
- Mitigate Vulnerability Issues

Module9: Applying Security Solutions for Infrastructure Management
- Apply Identity and Access Management Security Solutions
- Apply Network Architecture and Segmentation Security Solutions
- Explain Hardware Assurance Best Practices
- Explain Vulnerabilities Associated with Specialized Technology

Module10: Understanding Data Privacy and Protection
- Identify Technical Data and Privacy Controls

Module11: Applying Security Solutions for Software Assurance
- Mitigate Software Vulnerabilities and Attacks
- Mitigate Web Application Vulnerabilities and Attacks
- Analyze Output from Application Assessments

Module12: Applying Security Solutions for Cloud and Automation
- Identify Cloud Service and Deployment Model Vulnerabilities
- Explain Service-Oriented Architecture
- Analyze Output from Cloud Infrastructure Assessment Tools

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Copyright © 2020 GOPAS, a.s.,
All rights reserved

- Compare Automation Concepts and Technologies

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Copyright © 2020 GOPAS, a.s.,
All rights reserved