



As attackers have learned to evade traditional signature-based solutions such as firewalls, an analytics-based approach within the IT security industry is increasingly important for most organizations. The behavioral analytics skills covered by the CompTIA Cybersecurity Analyst (CSA+) exam identify and combat malware and advanced persistent threats, resulting in enhanced threat visibility across a broad attack surface.

Learn to: Configure and use threat detection tools  
Perform Data analysis  
Interpret the results to identify vulnerabilities, threats, and risks to an organization.

The new CompTIA CySA+ CS0-002 exam is available as of April 21, 2020

**Our unique model follows a streamlined approach to workforce development and skills attainment**

**Assess:** Assess each student to determine existing skill sets

**Educate:** Deliver goal-specific training utilizing all delivery modalities

**Mentor:** Expose students to instructors and mentors with front-line IT and cybersecurity experience

**Certify:** Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

**Validate:** Validate student abilities through performance analytics and real-world exercises hosted on a cyber range

## Course Outline:

Chapter 1: The Importance of Threat Data and Intelligence

Chapter 2: Threat Intelligence in Support of Organizational Security

Chapter 3: Vulnerability Management Activities

Chapter 4: Vulnerability Assessment Tools

Chapter 5: Threats and Vulnerabilities Associated with Specialized Technologies

Chapter 6: Threats and Vulnerabilities Associated with Operating in the Cloud

Chapter 7: Mitigating Controls for Attacks and Software Vulnerabilities

Chapter 8: Security Solutions for Infrastructure Management

Chapter 9: Software Assurance Best Practices

Chapter 10: Hardware Assurance Best Practices

Chapter 11: Data Analysis in Security Monitoring Activities

Chapter 12: Implement Configuration Changes to Existing Controls to Improve Security

Chapter 13: The Importance of Proactive Threat Hunting

Chapter 14: Automation Concepts and Technologies

Chapter 15: The Importance of the Incident Response Policy

Chapter 16: Appropriate Incident Response Procedures

Chapter 17: Analyze Potential Indicators of Compromise

Chapter 18: Utilize Basic Digital Forensics Techniques

Chapter 19: The Importance of Data Privacy and Protection

Chapter 20: Security Concepts in Support of Organizational Risk Mitigation

Chapter 21: The Importance of Frameworks, Policies, Procedures, and Controls

## Included

40 hours of instructor-led training sessions

CompTIA authorized textbook and class materials

Practice questions and exam study tips