CompTIA CySA+ Cybersecurity Analyst

Durée: 5 Jours Réf de cours: GK5867 Version: CS0-004 Méthodes d'apprentissage: Classe à distance

Résumé:

Learn how to detect ,analyze, and protect critical infrastructures using threat-detection and threat-analysis tools.
Gain the tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate an organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. This is a comprehensive approach to security aimed toward those on the front lines of defense.
This course is designed to assist students in preparing for the CompTIA CySA+ - Cybersecurity Analyst+ (CS0-004) certification exam. CompTIA's CySA+ is a global vendor-neutral certification covering intermediate-level knowledge and skills required by information security analyst job roles. It helps identify a cybersecurity professional's ability to proactively defend an organization using secure monitoring, threat identification, incident response and teamwork. The CompTIA CySA+ CS0-004 certification exam ensures the candidate has the knowledge and skills required to:
- Identify and investigate suspicious activity across networks, endpoints, and cloud environments to uncover potential security threats.
- Identify, prioritize, and mitigate vulnerabilities using risk-based vulnerability management approaches.
- Investigate and respond to cybersecurity incidents using structured incident response processes and real-world techniques.
- Use modern security operations concepts, including threat intelligence, threat hunting, automation, and AI-assisted security operations.

Updated 30/7/2026

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

- IT Security Analyst
- Security Operations Center (SOC) Analyst
- Vulnerability Analyst
- Cybersecurity Specialist
- Threat Intelligence Analyst
- Security Engineer

Objectifs pédagogiques:

- Identify and investigate suspicious activity across networks, endpoints, and cloud environments to uncover potential security threats.
- Monitor and analyze data using industry-standard tools such as SIEM and EDR platforms.
- Identify, prioritize, and mitigate vulnerabilities using risk-based approaches.
- Investigate and respond to security incidents using structured processes and real-world techniques.
- Clearly communicate security findings and risks to stakeholders through reports and dashboards.
- Apply security practices across cloud and hybrid environments while supporting efficient and effective operations.

Pré-requis:

To ensure your success in this course, you should meet the following requirements:

- At least two years (recommended) of experience in computer

Test et certification

This course is designed to assist students preparing for the CompTIA CySA+ - Cybersecurity Analyst+ (CS0-004) certification exam. What you learn and practice in this course can be a significant part of your preparation.

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 some of the common operating systems for computing environments.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include, but are not limited to, basic authentication and authorization, resource permissions, and anti-malware mechanisms.
- Foundation-level understanding of some of the common concepts for network environments, such as routing and switching.
- Foundational knowledge of major TCP/IP networking protocols including, but not limited to, TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments. Safeguards include, but are not limited to, firewalls, intrusion prevention systems, and VPNs.

Exam details

Exam series code: CS0-004
Number of Questions: Maximum of 85 questions
Length of Test: 165 minutes
Passing Score: 750 (on a scale of 100-900)
Recommended experience: About 4 years in a SOC analyst or vulnerability analyst role

Contenu:

Course Modules

- Identifying Security Operations Fundamentals
- Applying Risk Management Strategies
- Managing System Security and Configurations
- Comparing System Architectures
- Applying Access Management
- Threat Intelligence and Threat Hunting
- Assessing Network Vulnerabilities
- Managing Incident Response and Communication
- Executing Incident Response Plans
- Analyzing Malicious Activity
- Automating Data Analysis
- Improving Processes with Automation
- Assessing Application Vulnerabilities
- Securing Applications

LABS

- Live Lab: Operate A SOC Workstation
- Applied Live Lab: Assess Attack Surface And System Hardening
- Live Lab: Deploy A CI/CD Cloud Application
- Live Lab: Deploy A CI/CD Container Application
- Live Lab: Configure Federated Authentication And PAM
- Applied Live Lab: Apply Data Protection And Endpoint Security
- Live Lab: Configure A Honeypot
- Live Lab: Implement Threat Intelligence
- Applied Live Lab: Analyze Vulnerability Scans
- Live Lab: Configure Centralized Logging
- Live Lab: Use A Playbook For Incident Response
- Live Lab: Record Case Evidence
- Live Lab: Create Log Analysis Queries
- Live Lab: Configure A Sandbox
- Applied Live Lab: Analyze Anomalous Host Activity
- Network Indicators of Compromise
- Applied Live Lab: Analyze Anomalous Network Activity
- Application and Web-based Indicators
- Live Lab: Analyze Phishing Emails
- Challenge Live Lab: Resolve Incident Response Cases
- Live Lab: Implement An Automation Solution
- Live Lab: Perform Rule Tuning
- Live Lab: Add AI To An Incident Response Playbook
- Applied Live Lab: Analyze Cloud Infrastructure Vulnerabilities
- Applied Live Lab: Analyze Web Service Vulnerabilities
- Live Lab: Integrate Security Scanning In A CI/CD Pipeline
- Challenge Live Lab: Resolve Cloud And App Vulnerabilities

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :