

**COMPTIA - CYSA+ (E-BOOK + ESAME)**

CORSO IN AUTOAPPRENDIMENTO

Durata	Prezzo	Orari	Calendario
	684,00€ 559,00€ + IVA		

CompTIA – CySA+ è un corso di autoformazione, creato per i professionisti della cybersecurity che svolgono funzioni lavorative relative alla protezione dei sistemi informativi assicurando la loro disponibilità, integrità, autenticazione e riservatezza. Questo corso si concentra sulla conoscenza, abilità e competenze necessarie per difendere tali sistemi informativi in un contesto di cybersecurity, compresa la protezione, rilevamento, analisi, indagine e processi di risposta. Inoltre, il corso assicura che tutti i membri di un team IT, dal personale dell'help desk al Chief Information Officer, comprendano il loro ruolo di questi processi di sicurezza.



Questo corso aiuta gli studenti nella preparazione dell'**esame di certificazione CompTIA – CySA+**.

Contenuti del corso**Module 1: Explaining the Importance of Security Controls and Security Intelligence**

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

Module 2: Utilizing Threat Data and Intelligence

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

Module 3: Analyzing Security Monitoring Data

- Analyze Network Monitoring Output
- Analyze Appliance Monitoring Output
- Analyze Endpoint Monitoring Output

MAIN PARTNERS



formazione@pipeline.it
www.pipeline.it/formazione



- Analyze Email Monitoring Output

Module 4: Collecting and Querying Security Monitoring Data

- Configure Log Review and SIEM Tools
- Analyze and Query Logs and SIEM Data

Module 5: 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

Module 6: Applying Incident Response Procedures

- Explain Incident Response Processes
- Apply Detection and Containment Processes
- Apply Eradication, Recovery, and Post-Incident Processes

Module 7: Applying Risk Mitigation and Security Frameworks

- Apply Risk Identification, Calculation, and Prioritization Processes
- Explain Frameworks, Policies, and Procedures

Module 8: Performing Vulnerability Management

- Analyze Output from Enumeration Tools
- Configure Infrastructure Vulnerability Scanning Parameters
- Analyze Output from Infrastructure Scanners
- Mitigate Vulnerability Issues

Module 9: 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

Module 10: Understanding Data Privacy and Protection

- Identify Non-Technical Data and Privacy Controls

MAIN PARTNERS





- Identify Technical Data and Privacy Controls

Module 11: Applying Security Solutions for Software Assurance

- Mitigate Software Vulnerabilities and Attacks
- Mitigate Web Application Vulnerabilities and Attacks
- Analyze Output from Application Assessments

Module 12: 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
- Compare Automation Concepts and Technologies

Partecipanti

Il corso **CompTIA – CYSA+** è pensato per i candidati che lavorano o puntano a ruoli lavorativi come analista del centro operativo di sicurezza (SOC), vulnerability analyst, specialista di cybersecurity, threat intelligence analyst, ingegnere della sicurezza e analista della sicurezza informatica.

Prerequisiti

Per partecipare con profitto al corso **CompTIA – CYSA+** i candidati dovrebbero soddisfare i seguenti requisiti:

- almeno due anni di esperienza nella tecnologia della sicurezza delle reti informatiche o in un campo correlato;
- la capacità di riconoscere le vulnerabilità e le minacce alla sicurezza delle informazioni nel contesto della gestione del rischio;
- competenze operative di livello base con i comuni sistemi operativi per PC, dispositivi mobili e server;
- comprensione a livello base di alcuni dei concetti comuni per gli ambienti di rete come il routing e la switching;
- conoscenza di base dei protocolli di rete TCP/IP, compresi IP, ARP, ICMP, TCP, UDP, DNS, DHCP, HTTP/HTTPS, SMTP e POP3/IMAP;
- conoscenza basilare dei concetti e del quadro operativo di comuni misure di sicurezza negli ambienti informatici. Le misure di sicurezza includono l'autenticazione e l'autorizzazione, i permessi delle risorse e i meccanismi anti-malware;
- conoscenza basilare dei concetti e del quadro operativo delle comuni garanzie di sicurezza comuni in ambienti di rete, come firewall, IPS, NAC e VPN.

È possibile ottenere questo livello di abilità e conoscenza frequentando i seguenti corsi ufficiali CompTIA:

- il [corso CompTIA – Network+](#)
- il [corso CompTIA – Security+](#)

Obiettivi

MAIN PARTNERS



formazione@pipeline.it
www.pipeline.it/formazione



Al termine di questo corso i partecipanti saranno in grado di:

- raccogliere e utilizzare l'intelligence della sicurezza informatica e i dati sulle minacce;
- identificare i moderni tipi di attori delle minacce alla sicurezza informatica e le tattiche, tecniche e procedure;
- analizzare i dati raccolti dai log della sicurezza e degli eventi e dalle catture dei pacchetti di rete;
- rispondere e indagare su incidenti di cybersecurity usando tecniche di analisi forense;
- valutare il rischio di sicurezza delle informazioni negli ambienti informatici e di rete;
- implementare un programma di gestione delle vulnerabilità;
- affrontare i problemi di sicurezza con l'architettura di rete di un'organizzazione;
- comprendere l'importanza dei controlli sulla governance dei dati;
- affrontare i problemi di sicurezza con il ciclo di vita dello sviluppo del software di un'organizzazione;
- affrontare i problemi di sicurezza con l'uso da parte di un'organizzazione del cloud e dell'architettura orientata ai servizi.

Lingua

Lingua utilizzata nel corso/dal docente: Italiano

Il materiale didattico e l'ambiente di laboratorio sono in lingua Inglese

Materiali e Bonus

Il corso CompTIA – CySA+ include:

- un **CertMaster Practice**, che aiuta a prepararsi all'esame di certificazione. Il practice test è valido per i 12 mesi successivi all'acquisto del corso ed è disponibile anche sui dispositivi mobili Android ed iPhone;
- e-book ufficiale **CompTIA Study Guide**, valido per 12 mesi dalla data di acquisto;
- un **exam voucher**, valido per 12 mesi.

Hai bisogno di chiarimenti o ulteriori informazioni?

Vuoi organizzare un corso personalizzato?

Chiamaci: 02/6074791 Scrivici: formazione@pipeline.it

MAIN PARTNERS



formazione@pipeline.it
www.pipeline.it/formazione