CYSA - CompTIA CySA+ - Cybersecurity Analyst (CS0-003)

CompTIA - Defensive Cybersecurity - Cyber Security

Durata:	Lingue:	Certificazione:
5 Giorni	**Italiano**	**CompTIA Cybersecurity Analyst (CySA+) (CS0-003)**

Descrizione del corso

CompTIA Cybersecurity Analyst (CySA+) è una certificazione internazionale per professionisti IT che applica analisi comportamentali a reti e dispositivi per prevenire, rilevare e combattere le minacce alla sicurezza informatica attraverso il monitoraggio continuo della sicurezza.
CySA+ si concentra sulla capacità dei candidati non solo di acquisire, monitorare e rispondere in modo proattivo ai risultati del traffico di rete, ma sottolinea anche la sicurezza di software e applicazioni, l'automazione, la caccia alle minacce e la conformità alle normative IT, che influiscono sul lavoro quotidiano degli analisti della sicurezza.
CySA+ copre le competenze di base più aggiornate dell'analista della sicurezza e le competenze lavorative imminenti utilizzate da analisti di intelligence delle minacce, analisti della sicurezza delle applicazioni, analisti della conformità, risponditori/gestori di incidenti e cacciatori di minacce, introducendo nuove tecniche per combattere le minacce all'interno e all'esterno del Centro operativo di sicurezza (SOC).

Il corso include:
- Slide del corso
- Guida ufficiale CompTIA in formato digitale in lingua inglese
- DB online con gli esercizi ufficiali CompTIA di pratica d'esame
- Ricco set di laboratori online su piattaforma CompTIA funzionali all'applicazione pratica dei concetti

Il voucher di esame è acquistabile separatamente al costo di 350,00 € + IVA

Programma

Module 1: Threat Management

- Cybersecurity Analysts
- Cybersecurity Roles and Responsibilities
- Frameworks and Security Controls
- Risk Evaluation
- Penetration Testing Processes
- Reconnaissance Techniques
- The Kill Chain
- Open Source Intelligence
- Social Engineering
- Topology Discovery
- Service Discovery
- OS Fingerprinting

Module 2: Threat Management

- Security Appliances
- Configuring Firewalls
- Intrusion Detection and Prevention
- Configuring IDS
- Malware Threats
- Configuring AntiVirus Software
- Sysinternals
- Enhanced Mitigation Experience Toolkit
- Logging and Analysis
- Packet Capture
- Packet Capture and Monitoring Tools
- Log Review and SIEM
- SIEM Data Outputs
- SIEM Data Analysis
- Pointintime Data Analysis

Module 3: Vulnerability Management

- Managing Vulnerabilities
- Vulnerability Management Requirements
- Asset Inventory
- Data Classification
- Vulnerability Management Processes
- Vulnerability Scanners
- Microsoft Baseline Security Analyser
- Vulnerability Feeds and SCAP
- Configuring Vulnerability Scans
- Vulnerability Scanning Criteria
- Exploit Frameworks
- Remediating Vulnerabilities
- Analysing Vulnerability Scans
- Remediation and Change Control
- Remediating Host Vulnerabilities
- Remediating Network Vulnerabilities
- Remediating Virtual Infrastructure Vulnerabilities
- Secure Software Development
- Software Development Life Cycle
- Software Vulnerabilities
- Software Security Testing
- Interception Proxies
- Web Application Firewalls
- Source Authenticity
- Reverse Engineering

Module 4: Cyber Incident Response

- Incident Response
- Incident Response Processes
- Threat Classification
- Incident Severity and Prioritisation
- Types of Data
- Forensics Tools
- Digital Forensics Investigations
- Documentation and Forms
- Digital Forensics Crime Scenes

- Digital Forensics Kits
- Image Acquisition
- Password Cracking
- Analysis Utilities
- Incident Analysis and Recovery
- Analysis and Recovery Frameworks
- Analysing Network Symptoms
- Analysing Host Symptoms
- Analysing Data Exfiltration
- Analysing Application Symptoms
- Using Sysinternals
- Containment, Eradication, and Validation Techniques
- Corrective Actions

Module 5: Security Architecture

- Secure Network Design
- Network Segmentation
- Blackholes, Sinkholes, and Honeypots
- System Hardening
- Group Policies and MAC
- Endpoint Security
- Managing Identities and Access
- Network Access Control
- Identity Management
- Identity Security Issues
- Identity Repositories
- Contextbased Authentication
- Single SignOn and Federation
- Exploiting Identities
- Exploiting Web Browsers and Applications
- Security Frameworks and Policies
- Frameworks and Compliance
- Reviewing Security Architecture
- Procedures and Compensating Controls
- Verifications and Quality Control
- Security Policies and Procedures

- Personnel Policies and Training

ITCore Group

Via Balestra, 12
6900 Lugano (CH)
+41.091.9760019
www.itcoregroup.com

Via Lanino, 36
21047 Saronno (VA)
+39.02.84108669
www.itcoregroup.com