CTIA-7 - COMPTIA SECURITY+

Categoria: **CompTIA**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
5 Giorni	CompTIA	Docente Senior (min. 5 anni)	Professionista IT	CompTIA

OBIETTIVI

Skills you'll learn:

- Apply layered security controls, Zero Trust principles, access management, and cryptographic technologies.
- Identify threat actors, attack techniques, vulnerabilities, and indicators of malicious activity, including AI-related risks.
- Protect cloud, hybrid, on-premises, and connected environments while supporting resilience and business continuity.
- Use monitoring, vulnerability management, security tools, automation, and operational security practices to help defend modern environments.
- Manage authentication, authorization, federation, multifactor authentication, and secure access controls.
- Detect, respond to, and investigate security incidents using logs, alerts, and security data.
- Apply security policies, risk management practices, compliance requirements, audit concepts, and security awareness programs.

PREREQUISITI

Aver frequentato il corso Network+ o avere conoscenze equivalenti

CONTENUTI

Module 1: Summarize Fundamental Security Concepts

- Security Concepts
- Security Controls

Module 2: Identify Threats, Vulnerabilities, and Attacks

- Threat Actors
- Attack Vectors and Sources
- Social Engineering

Module 3: Explain Cryptographic Solutions

- Cryptographic Algorithms
- Cryptographic Solutions

-Public Key Infrastructure

Module 4: Implement Identity and Access Management

-Access Control Models
-Active Directory Overview
-Authentication
-Authorization
-Identity Management

Module 5: Secure Enterprise Network Architecture

-Enterprise Network Architecture
-Network Security Appliances
-Secure Communications

Module 6: Secure Cloud Network Architecture

-Cloud Infrastructure
-Embedded Systems and Zero Trust Architecture

Module 7: Explain Resiliency and Site Security Concepts

-Asset Management
-Physical Security
-Redundancy Strategies

Module 8: Explain Vulnerability Management

-Device and OS Vulnerabilities
-Application and Cloud Vulnerabilities
-Vulnerability Identification Methods
-Vulnerability Analysis and Remediation
-Artificial Intelligence

Module 9: Evaluate Network Security Capabilities

-Network Security Baselines
-Network Security Capability Enhancement

Module 10: Assess Endpoint Security Capabilities

-Endpoint Security
-Mobile Device Hardening

Module 11: Enhance Application Security Capabilities

-Application Protocol Security Baselines
-Cloud and Web Application Security Concepts

Module 12: Explain Incident Response and Monitoring Concepts

-Incident Response
-Digital Forensics
-Data Sources
-Alerting and Monitoring Tools

Module 13: Analyze Indicators of Malicious Activity

-Malware Attack Indicators

-Physical and Network Attack Indicators
-Application Attack Indicators

Module 14: Summarize Security Governance Concepts
-Policies, Standards, and Procedures
-Change Management
-Automation and Orchestration

Module 15: Explain Risk Management Processes
-Risk Management Processes and Concepts
-Vendor Management Concepts
-Audits and Assessments

Module 16: Summarize Data Protection and Compliance Concepts
-Data Classification and Compliance
-Personnel Policies

INFO

Esame: SY0-801 - CompTIA Security+
Materiale didattico: Materiale didattico in formato digitale
Costo materiale didattico: incluso nel prezzo del corso a Calendario
Natura del corso: Operativo (previsti lab su PC)