CTIA-8 - COMPTIA CYBERSECURITY ANALYST (CYSA+)

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:

- -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.

PREREQUISITI

Aver frequentato il corso CompTIA Security+ o avere conoscenze equivalenti

CONTENUTI

Module 1: Identifying Security Operations Fundamentals

- -Cybersecurity Foundations
- -Governance, Policies, and Controls
- -Introduction to Incident Response in the SOC

Module 2: Applying Risk Management Strategies

- -Risk Concepts
- -Threat Modeling Frameworks

Module 3: Managing System Security and Configurations

- -Attack Surface Management
- -System Hardening

Module 4: Comparing System Architectures

- -Infrastructure and System Architecture
- -Modern Network Architectures

-Critical Infrastructure and Industrial Controls

Module 5: Applying Access Management

-Identity and Access Management
-Device and Endpoint Management
-Data Protection and Cryptography

Module 6: Threat Intelligence and Threat Hunting

-Threat Actor Concepts
-Threat Intelligence Sources
-Threat Hunting

Module 7: Assessing Network Vulnerabilities

-Vulnerability Scanning Foundations
-Vulnerability Scan Types
-Select Vulnerability Tools
-Vulnerability Analysis and Prioritization
-Vulnerability and Incident Reporting

Module 8: Mana7ging Incident Response and Communication

-Manage Logs
-Incident Escalation
-Post-Incident Actions
-Incident Response Metrics

Module 9: Executing Incident Response Plans

-Attack Methodology Frameworks
-The Incident Response Process
-Incident Response Techniques

Module 10: Analyzing Malicious Activity

-Threat Detection and Analysis Tools
-Host Indicators of Compromise
-Network Indicators of Compromise
-Application and Web-based Indicators

Module 11: Automating Data Analysis

-Scripting Fundamentals
-Scripting Languages
-Security Analytics and Pattern Recognition
-Technology and Tool Integration

Module 12: Improving Processes with Automation

-Standardization and Team Coordination
-Automation, Orchestration, and Enrichment
-AI Risks and Governance
-AI in Security Operations

Module 13: Assessing Application Vulnerabilities

-Web and Application Vulnerability Analysis
-Cloud Vulnerability Assessment

Module 14: Securing Applications
-Secure Software Development and Testing
-Application Attack Identification and Mitigation

INFO

Esame: CS0-004 - CompTIA Cybersecurity Analyst (CySA+)
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)