COMPSEC - CompTIA Security+ (SY0-701)

CompTIA - Defensive Cybersecurity - Cyber Security

Durata:	Lingue:	Certificazione:
5 Giorni	**Italiano**	**CompTIA Security+**

Descrizione del corso

CompTIA Security+ è una certificazione internazionale che convalida le competenze di base necessarie per svolgere le funzioni di cybersecurity e perseguire una carriera nella sicurezza IT. Security+ è allineato alle ultime tendenze, coprendo le competenze tecniche più importanti nella valutazione e gestione del rischio, risposta agli incidenti, analisi forense, reti aziendali, operazioni ibride/cloud e controlli di sicurezza. Per partecipare al corso è preferibile aver conseguito la certificazione CompTIA Network+ o aver maturato due anni di esperienza in un ruolo di amministratore di sistemi/sicurezza.
Obiettivi del corso: Il corso CompTIA Security+ copre i principi fondamentali della sicurezza delle reti e la gestione del rischio IT. Argomenti trattati: – Network Security – Compliance and Operational Security – Threats and Vulnerabilities – Application, Data and Host Security – Access Control and Identity Management – Cryptography

Programma

Parte I: Concetti generali di sicurezza

– Confrontare e contrastare vari tipi di controlli di sicurezza

– Riassumere i concetti fondamentali di sicurezza

– Spiegare l'importanza dei processi di gestione del cambiamento e l`impatto sulla sicurezza

– Spiegare l'importanza di utilizzare soluzioni crittografiche appropriate

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

Parte II: Minacce, vulnerabilità e mitigazioni

– Confrontare e contrastare le motivazioni comuni delle minacce

– Spiegare i vettori di minaccia comuni e le superfici di attacco

– Spiegare i vari tipi di vulnerabilità

– Dato uno scenario, analizzare gli indicatori di attività dannose

– Spiegare lo scopo delle tecniche di mitigazione utilizzate per proteggere l'impresa

Parte III: Architettura di sicurezza

– Confrontare e contrapporre le implicazioni sulla sicurezza di Modelli di architetture diverse

– Dato uno scenario, applicare i principi di sicurezza per proteggere l'infrastruttura dell`azienda

– Confrontare e contrapporre concetti e strategie per proteggere i dati

Parte IV: Operazioni di sicurezza

– Dato uno scenario, applicare tecniche di sicurezza comuni alle risorse informatiche

– Spiegare le implicazioni sulla sicurezza di hardware e software

– Spiegare le varie attività associate alla gestione delle vulnerabilità

– Spiegare i concetti e gli strumenti di avviso e monitoraggio della sicurezza

– Dato uno scenario, modificare le capacità aziendali per migliorare la

sicurezza

– Dato uno scenario, implementare e mantenere identità e accesso gestione

– Spiegare l'importanza dell'automazione e dell'orchestrazione correlata

– Spiegare le attività appropriate di risposta agli incidenti

– Dato uno scenario, utilizzare le origini dei dati per supportare un'indagine

Parte V: Gestione e supervisione del programma di sicurezza

– Riassumere gli elementi di un'efficace governance della sicurezza

– Spiegare gli elementi del processo di gestione del rischio

– Spiegare i processi associati alla valutazione del rischio di terze parti e sua gestione

– Riepilogare gli elementi di un'efficace conformità alla sicurezza

– Spiegare i tipi e gli scopi degli audit e delle valutazioni

– Dato uno scenario, implementare pratiche di sensibilizzazione alla sicurezza