CISCO CCST Cybersecurity – Syllabus Esame di Certificazione

La **Certificazione CISCO CCST Cybersecurity** convalida le conoscenze e le competenze relative alla sicurezza informatica a livello base, per supportare e assistere attività tra cui: i principi di sicurezza, sicurezza della rete e concetti di sicurezza degli endpoint, valutazione della vulnerabilità, gestione del rischio e gestione degli incidenti.

La Certificazione **CCST Cybersecurity** è un primo passo verso altre Certificazioni CISCO, come ad esempio la Certificazione **CyberOps Associate**.

Sono disponibili risorse gratuite ONLINE per aiutare i Candidati a prepararsi per la Certificazione, al seguente link: https://skillsforall.com/careerpath/cybersecurity?userLang=en-US

Per ottenere la Certificazione **CCST Cybersecurity** si deve superare il relativo Esame, attualmente disponibile in lingua inglese. L'Esame di Certificazione è di tipo LINEAR, ovvero test a risposta multipla, multi risposta con più risposte valide, elenco, corrispondenza, drag and drop e click map. L'Esame ha una durata di circa 50 minuti ed è composto da circa 45 domande.

Gli argomenti dell'Esame di Certificazione **CCST Cybersecurity** verificano la conoscenza su cinque principali aree di skill sulla sicurezza informatica, che sono le seguenti:

1.0 PRINCIPI ESSENZIALI DI SICUREZZA

2.0 CONCETTI DI BASE SULLA SICUREZZA DI RETE

3.0 CONCETTI DI SICUREZZA DEGLI ENDPOINT

4.0 VALUTAZIONE DELLA VULNERABILITÀ E GESTIONE DEL RISCHIO

5.0 GESTIONE DEGLI INCIDENTI

Syllabus Esame di Certificazione
CISCO CCST Cybersecurity

1.0 - PRINCIPI ESSENZIALI DI SICUREZZA

1.1. - Definire i principi di sicurezza essenziali

- Vulnerabilità, minacce, exploit e rischi; vettori di attacco; rafforzare le difese; difesa in profondità; riservatezza, integrità e disponibilità (CIA); tipi di hacker; motivi degli attacchi; codice deontologico.

1.2. - Spiegare minacce e vulnerabilità comuni

- Malware, ransomware, denial of service, botnet, attacchi di social engineering (tailgating, spear phishing, phishing, vishing, smishing, ecc.), attacchi fisici, man in the middle, vulnerabilità IoT, minacce interne, Advanced Persistent Threat (APT).

1.3. - Spiegare i principi di gestione degli accessi

- Autenticazione, autorizzazione e contabilità (AAA); Protocollo RADIUS; autenticazione a più fattori (MFA); criteri password.

1.4. - Spiegare i metodi e le applicazioni di crittografia

- Tipi di crittografia, hashing, certificati, infrastruttura a chiave pubblica (PKI); algoritmi di crittografia forti e deboli; stati dei dati e crittografia appropriata (dati in transito, dati inattivi, dati in uso); protocolli che utilizzano la crittografia.

2.0 CONCETTI DI BASE SULLA SICUREZZA DI RETE

2.1. - Descrivere le vulnerabilità del protocollo

- TCP, UDP, HTTP, ARP, ICMP, DHCP, DNS

2.2. Spiegare in che modo gli indirizzi di rete incidono sulla sicurezza della rete

- Indirizzi IPv4 e IPv6, indirizzi MAC, segmentazione di rete, notazione CIDR, NAT, reti pubbliche e private.

2.3. Descrivere l'infrastruttura e le tecnologie di rete

- Architettura di sicurezza di rete, DMZ, virtualizzazione, cloud, honeypot, server proxy, IDS, IPS.

2.4. Configurazione di una rete SoHo wireless sicura

- Filtraggio degli indirizzi MAC, standard e protocolli di crittografia, SSID

2.5. Implementare tecnologie di accesso sicuro

- ACL, firewall, VPN, NAC

3.0 CONCETTI DI SICUREZZA DEGLI ENDPOINT

3.1. Descrivere i concetti di sicurezza del sistema operativo

- Windows, MacOS e Linux; funzionalità di sicurezza, inclusi Windows Defender e firewall basati su host; CLI e PowerShell; permessi di file e directory; aumento dei privilegi.

3.2. Dimostrare familiarità con gli strumenti endpoint appropriati che raccolgono informazioni sulla valutazione della sicurezza

- netstat, nslookup, tcpdump.

3.3. Verificare che i sistemi endpoint soddisfino i criteri e gli standard di sicurezza

- Inventario hardware (gestione delle risorse), inventario software, distribuzione del programma, backup dei dati, conformità alle normative (PCI DSS, HIPAA, GDPR), BYOD (gestione dei dispositivi, crittografia dei dati, distribuzione delle app, gestione della configurazione).

3.4. Implementare aggiornamenti software e hardware

- Windows Update, aggiornamenti delle applicazioni, driver di dispositivo, firmware, patch.

3.5. Interpretare i log di sistema

- Visualizzatore eventi, registri di controllo, registri di sistema e applicazioni, syslog, identificazione delle anomalie.

3.6. Dimostrare familiarità con la rimozione del malware

- Sistemi di scansione, revisione dei registri di scansione, correzione del malware

4.0 VALUTAZIONE DELLA VULNERABILITÀ E GESTIONE DEL RISCHIO

4.1. Spiegare la gestione delle vulnerabilità

- Identificazione, gestione e mitigazione della vulnerabilità; ricognizione attiva e passiva; test (scansione delle porte, automazione).

4.2. Utilizzare tecniche di intelligence sulle minacce per identificare potenziali vulnerabilità di rete

- Usi e limitazioni dei database delle vulnerabilità; strumenti standard del settore utilizzati per valutare le vulnerabilità e formulare raccomandazioni, politiche e rapporti; Vulnerabilità ed esposizioni comuni (CVE), rapporti sulla sicurezza informatica, notizie sulla sicurezza informatica, servizi in abbonamento e intelligenza collettiva; informazioni sulle minacce ad hoc e automatizzate; l'importanza di aggiornare la documentazione e altre forme di comunicazione in modo proattivo prima, durante e dopo gli incidenti di sicurezza informatica; come proteggere, condividere e aggiornare la documentazione.

4.3. Spiegare la gestione del rischio

- Vulnerabilità vs. rischio, classificazione dei rischi, approcci alla gestione del rischio, strategie di mitigazione del rischio, livelli di rischio (basso, medio, alto, estremamente alto), rischi associati a specifiche tipologie di dati e classificazioni dei dati, valutazioni di sicurezza dei sistemi IT (sicurezza delle informazioni, gestione del cambiamento, operazioni informatiche, sicurezza delle informazioni).

4.4. Spiegare l'importanza del ripristino di emergenza e della pianificazione della continuità aziendale

- Disastri naturali e causati dall'uomo, caratteristiche dei piani di ripristino di emergenza (DRP) e dei piani di continuità operativa (BCP), backup, controlli di ripristino di emergenza (detective, preventivi e correttivi).

5.0 GESTIONE DEGLI INCIDENTI

5.1. Monitora gli eventi di sicurezza e scopri quando è necessaria l'escalation

- Ruolo di SIEM e SOAR, monitoraggio dei dati di rete per identificare incidenti di sicurezza (acquisizione di pacchetti, varie voci di file di registro, ecc.), identificazione di eventi sospetti nel momento in cui si verificano

5.2. Spiegare la digital forensics e i processi di attribuzione degli attacchi

- Cyber Kill Chain, MITRE ATT&CK Matrix e Diamond Model; Tattiche, tecniche e procedure (TTP); fonti di prova (artefatti); gestione delle prove (conservazione delle prove digitali, catena di custodia).

5.3. Spiegare l'impatto dei quadri di conformità sulla gestione degli incidenti

- Quadri di conformità (GDPR, HIPAA, PCI-DSS, FERPA, FISMA), obblighi di segnalazione e notifica.

5.4. Descrivere gli elementi della risposta agli incidenti di sicurezza informatica

- Criteri, pianificazione e procedure; fasi del ciclo di vita della risposta agli incidenti (NIST Special Publication 800-61 sezioni 2.3, 3.1-3.4.

Per maggiori informazioni sulle Certificazioni CISCO CCST, contattare TESI Automazione ai seguenti recapiti: https://www.tesiautomazione.it/it_it/contatti o accedere al sito www.tesiautomazione.it