ITSAR ISTITUTO TECNICO SUPERIORE
ANGELO RIZZOLI

Tecnico Superiore: ITS Cyber Defense Specialist

(Piano di studio 2019-2021 - Nuovo)

Milano, 2 settembre 2019

Descrizione della Figura

Il Tecnico Superiore per la Cyber Defense definisce, propone e implementa le necessarie prassi e tecniche di sicurezza delle informazioni nel rispetto degli standard e delle procedure. Contribuisce alle prassi di sicurezza, consapevolezza e conformità fornendo consulenza, supporto, informazione e formazione.
Applica le metodologie e le tecniche di hacking etico per la ricerca, individuazione e documentazione delle vulnerabilità a livello infrastrutturale ed applicativo dei sistemi informatici (Vulnerability Assessment, Penetration Testing). Riconosce un attacco informatico nelle diverse fasi che lo contraddistinguono e sa gestire le fasi di risposta a un incidente di sicurezza (Incident Response). Sa acquisire evidenze da un sistema compromesso ed effettuare alcune operazioni base di analisi forense digitale (Digital Forensics).
I suoi compiti principali sono:

- Valutare i rischi, le minacce e le conseguenze per la sicurezza delle informazioni e intraprendere le azioni appropriate
- Fornire formazione sulla sicurezza delle informazioni e istruzione
- Fornire la convalida tecnica degli strumenti di sicurezza, implementare, configurare e gestire strumenti appropriati
- Contribuire alla definizione e promuovere attivamente le informazioni standard e le procedure di sicurezza in tutto l'IT e la comunità utente
- Diffondere consapevolezza e cultura su sicurezza delle informazioni e protezione del dato
- Identificare e rimediare alle vulnerabilità della sicurezza
- Monitorare gli sviluppi della sicurezza per garantire la continua efficienza ed efficacia dei processi e controlli di sicurezza delle informazioni
- Valutare proattivamente le nuove minacce e contrastarle in base alle potenziali informazioni derivanti dagli incidenti di sicurezza
- Implementare tecniche di sicurezza su tutto o parte di un'applicazione, processo, rete o sistema all'interno dell'area di responsabilità
- Utilizzare metodologie e strumenti per l’attività automatica e valutare autonomamente la validità dei risultati forniti dagli strumenti.
- Con il supporto di specialisti senior impostare la reportistica di dettaglio utile a illustrare lo stato di sicurezza di un sistema informatico.
- Operare nel rispetto dell’etica e delle normative inerenti la sicurezza e la compliance, applicando le buone pratiche consolidate nel settore della Cyber Security.

Ambito di inserimento

Il Tecnico Superiore Specialista in CyberDefense ha una ampia preparazione che gli permette di essere collocato in svariate realtà aziendali, tra cui:

- Aziende specializzate in Cybersecurity

- Aziende di consulenza aziendale e ICT
- Centri servizi e provider che gestiscono infrastrutture ICT (NOC e SOC)
- Reparti interni di Cybersecurity o ICT/Infrastrutture & Sistemi di aziende strutturate
- In prospettiva (con adeguata esperienza) come consulente e libero professionista in ambito Cybersecurity

In sintesi, le attività principali in cui può essere proficuamente impiegato sono: monitoraggio proattivo e preventivo delle infrastrutture e dei sistemi; rilevazione, identificazione, analisi e contrasto delle minacce ai sistemi; manovre correttive post attacco e relativa documentazione; cyber intelligence e blue teaming; security assessment e penetration testing; simulazioni CTF (Capture The Flag) e Blue/Red teaming; analisi di digital forensic; formazione interna ed esterna su tematiche e best practice di Cybersecurity, sia rivolte a personale ICT che a utenti aziendali; supporto operativo al personale ICT per l'applicazione delle opportune misure di difesa e ripristino.

Organizzazione didattica del percorso

Il percorso formativo prevede due annualità, ciascuna organizzata in due semestri, per un totale di quattro semestri. La prima annualità prevede 860 ore di lezione/laboratori (integrate da project work aziendali), mentre la seconda annualità prevede 340 ore di lezione/laboratori e 800 ore di tirocinio.
Il metodo formativo che verrà utilizzato è progettato per mettere a frutto i vantaggi di più metodologie formative in modo integrato: sessioni teoriche, esercitative, laboratori scolastici, laboratori d’impresa, stage, esperienze all’estero.

UNITÀ FORMATIVE TRASVERSALI

UFT01	Industry 4.0. Basi sulle tecnologia abilitanti (Intelligenza artificiale e Big Data)	16
UFT02	Protezione dei dati e e-privacy	16
UFT03	Diritto commerciale, digitale e diritto del lavoro	48
UFT04	Economia e organizzazione aziendale	60
UFT05	Qualità, ambiente, salute e sicurezza sui luoghi di lavoro	16
UFT06	Project Management	24
UFT07	Problem solving e creatività	16
UFT08	Design thinking	16
UFT09	Comunicazione, capacità relazionali e costruzione del gruppo di lavoro	24
UFT10	Personal branding e orientamento al lavoro	16
UFT11	Team working	24
UFT12	Lingua Inglese e microlingua di settore	88
TOTALE UF TRASVERSALI		**364**

UNITÀ FORMATIVE TECNICO PROFESSIONALI

UFS01	Elementi di crittografia	40
UFS02	Networking - Fundamentals	80
UFS03	Sistemi operativi e virtualizzazione	120
UFS04	Basi di Dati	24
UFS05	Sicurezza dei sistemi e delle reti informatiche	140
UFS06	Sicurezza nei sistemi web, cloud e mobile	24
UFS07	Sicurezza IOT	16
UFS08	Elementi di sicurezza Industrial Control Systems e SCADA	24
UFS09	Introduzione all'Ethical Hacking	40
UFS10	Malware e contromisure di sicurezza	32
UFS11	Attack kill-chain e analisi di un attacco	36
UFS12	Digital Forensics Analysis	52
UFS13	Sicurezza della Posta Elettronica	32
UFS14	Sicurezza Web e cenni di aspetti legali e privacy	24
UFS15	Vulnerability Assessment e Penetration Testing	120
UFS16	Cyber Threat Intelligence	16
UFS17	Red Teaming	16
TOTALE UF TECNICO PROFESSIONALI		**836**
TOTALE GENERALE		**1.200**