PROGRAMMA

Security manager

Corso di formazione completa per la gestione della sicurezza online

ID S.O.F.I.A. 105605

Modulo 1 | Il ruolo del Security Manager

- La figura del Security Manager
- Definizione del ruolo ed evoluzione della funzione
- Differenza tra IT Manager e Security Manager
- Ruolo nella trasformazione digitale
- Competenze tecniche e manageriali
- Sicurezza informatica, sicurezza organizzativa, sicurezza dei dati e sicurezza dei processi
- Triade CIA: riservatezza, integrità, disponibilità
- Gestione del rischio
- Relazione con management, DPO, IT e compliance
- Caso pratico: analisi di un'organizzazione, identificazione criticità e definizione priorità operative

Modulo 2 | Governance della sicurezza

- Modelli di governance centralizzati, distribuiti e ibridi
- Ruoli, responsabilità e funzioni chiave
- Separazione dei compiti
- Policy aziendali e allineamento agli obiettivi
- Pianificazione strategica
- Gestione delle credenziali e password policy
- Monitoraggio e aggiornamento
- Laboratorio IAM: password manager aziendali e sistemi MFA
- Caso pratico: costruzione di un modello di governance

Modulo 3 | Cyber risk management avanzato

• Approccio risk-based
• ISO 27005
• NIST Risk Framework
• Integrazione tra framework
• Analisi degli asset aziendali
• Identificazione di minacce, vulnerabilità ed esposizione delle reti
• Valutazione di impatto e probabilità
• Risk appetite e decision making
• Accettazione, mitigazione, trasferimento e prioritizzazione del rischio
• Strumenti di risk assessment
• Laboratorio tecnico: vulnerability scanning con strumenti come OpenVAS
• Caso pratico: costruzione di una strategia di gestione del rischio

Modulo 4 | Compliance e responsabilità avanzata

• Compliance NIS2 e GDPR
• Obblighi normativi per infrastrutture critiche e protezione dei dati
• Responsabilità del management
• Security by Design legislativo
• Audit interno ed esterno
• Pianificazione delle verifiche e raccolta evidenze
• Accountability e tracciabilità delle decisioni
• Non conformità, sanzioni, impatti legali e reputazionali
• Caso pratico: gestione di una non conformità normativa

Modulo 5 | Framework operativi avanzati

• CIS Controls v8
• I 18 controlli e Implementation Groups
• Selezione e adattamento dei controlli al contesto aziendale
• Integrazione con ISO 27001 e NIST Cybersecurity Framework
• Roadmap di implementazione
• Allocazione risorse e coinvolgimento del management
• Monitoraggio e KPI
• Laboratorio pratico: configurazione di firewall perimetrali e protezione endpoint
• Caso pratico: implementazione CIS e ISO in azienda

Modulo 6 | Incident e Crisis Management

• Incident management avanzato
• Rilevazione e identificazione delle anomalie
• Classificazione e prioritizzazione degli incidenti
• Coordinamento del team di risposta
• Crisis management
• Business continuity
• Disaster recovery e strategie di backup
• Comunicazione interna ed esterna in caso di crisi
• Gestione della reputazione del brand

• Incident response platform e automazione della risposta
• Caso pratico: simulazione di crisi end-to-end

Modulo 7 | Security operations e controllo

• SOC: struttura, ruoli e funzionamento
• Monitoraggio, logging e analisi del traffico
• Raccolta eventi e analisi dei log
• Correlazione eventi e identificazione anomalie
• Laboratorio tecnico: analisi dei pacchetti di rete con strumenti come Wireshark
• Piattaforme SIEM
• Splunk, IBM QRadar e sistemi enterprise
• Incident response avanzato
• Caso pratico: analisi di un incidente tramite log e flussi di rete

Modulo 8 | Security by design e supply chain

• Progettazione sicura di reti, sistemi e applicazioni
• Integrazione della sicurezza nei processi di sviluppo e deployment
• Prevenzione delle vulnerabilità strutturali
• Rischi derivanti da fornitori e terze parti
• Vendor risk management
• Audit dei fornitori
• Monitoraggio delle connessioni e degli accessi partner
• Verifica della compliance di filiera
• Caso pratico: valutazione del rischio supply chain

Modulo 9 | Audit e controllo

• Audit interno
• Pianificazione delle attività ispettive interne
• Esecuzione e raccolta delle evidenze tecniche e documentali
• Audit esterno e verifiche di conformità di terza parte
• Ispezioni istituzionali
• Conformità agli standard certificativi
• Non conformità e tracciamento dei rilievi
• Azioni correttive e miglioramento continuo
• Caso pratico: simulazione di audit ispettivo

Modulo 10 | Leadership e gestione del team

• Ruolo strategico del Security Manager
• Decision making in condizioni di stress
• Gestione degli stakeholder
• Comunicazione efficace con il Top Management
• Organizzazione del personale di sicurezza
• Mappatura delle competenze
• Coordinamento dei carichi di lavoro

• Security awareness per personale non tecnico
• Formazione aziendale continua
• Riduzione dell'errore umano e prevenzione del phishing
• Caso pratico: gestione di crisi organizzative ed errori umani

Modulo 11 | Strategie e scenari futuri

• Cybersecurity strategy
• Pianificazione strategica a lungo termine
• Integrazione della sicurezza nei piani di sviluppo del business
• Intelligenza Artificiale applicata alla difesa e all'attacco
• Evoluzione del cybercrime
• Trend legislativi europei e internazionali
• Strategie di compliance anticipata
• Caso pratico: definizione di una strategia cybersecurity a 3-5 anni

Modulo 12 | Laboratorio Security Manager – Capstone Project

• Assessment aziendale
• Analisi di un'infrastruttura aziendale fittizia o reale
• Identificazione delle criticità tecniche e di governance
• Piano strategico e definizione degli obiettivi di sicurezza
• Allocazione del budget
• Roadmap di intervento
• Simulazione di crisi: data breach e ransomware
• Attivazione SOC, analisi log e coordinamento del team
• Audit finale
• Verifica della compliance post-incidente
• Valutazione delle difese perimetrali e dei processi di disaster recovery
• Presentazione della gestione end-to-end del progetto