# **CyberSA-D-25 -** PNRR 1.5 - Cybersecurity: aspetti tecnici.

## Durata

4 ore

## Modalità

Aula Virtuale

## Programma

Il Corso si inquadra nelle iniziative di Formazione e Security Awareness finanziate con risorse PNRR, Missione 1, Componente 1, Investimento 1.5 Cybersecurity". Il Corso è destinato alle figure professionali tecnico/informatiche e anche ad altri soggetti che hanno il compito di attuare e/o supportare il rafforzamento della sicurezza informatica nell'ambito dell'Amministrazione.

Modulo 1: Network Security

- Apparati NGFW e funzionalità avanzate delle nuove tecnologie
- Rilevanza ed approcci per la segmentazione delle reti
- La network security in ambito Cloud
- Modalità di controllo del traffico di rete e soluzioni per identificazione minacce

Modulo 2: Data security

- Come la data security permette di indirizzare i requisiti GDPR
- Crittografia
- Cancellazione dei dati
- Mascheramento dei dati
- Anonimizzazione
- Strumenti di data discovery
- Strumenti di classificazione dei dati
- IAM - Logging e monitoraggio di accesso ai dati

Modulo 3: Endpoint security

- Evoluzione dei sistemi di protezione degli endpoint: dall'antivirus alle nuove tecnologie
- Endpoint Detection and Reporting (EDR)
- DLP e protezione delle informazioni gestire tramite gli endpoint
- MDM e gestione degli endpoint
- Gestione delle utenze locali e controllo degli accessi privilegiati
- Shadow IT

Modulo 4: Risk Management

- Approcci al rischio
- La gestione del rischio
- Risk assessment
- Trattamento del rischio
- Eventi indesiderati ed eventi accidentali
- Security by design
- Rischio della supply chain
- Scenari di rischio

Modulo 5: Vulnerability management

- Vulnerability Scanning, assessment e management
    - Remediation
    - Reporting and Metrics
    - Categorizzazione e prioritizzazione
    - CVE
    - Reporting
- Threat Intelligence: come può coadiuvare l'effettivo vulnerability management
- Soluzione e tecnologie per vulnerability scanning e management

Modulo 6: Incident Reporting

- MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – tecniche di attacco MITRE
- SOC
    - Security Information and Event Management (SIEM)
    - Security Orchestration, Automation and Reporting (SOAR)
- CERT e l'approccio ENISA
- Ruoli e responsabilità gestione incidenti di sicurezza e crisi
- Best practice per la gestione dei gravi incidenti e forensics
- Requisiti regolamentari: Comunicazione con le autorità di controllo
- Data breach, GDPR e punti di attenzione

Modulo 7: Misure minime di sicurezza ICT

- Gestione del rischio
- Protezione delle reti e dei sistemi
- Gestione delle identità e degli accessi
- Protezione dei dati
- Sensibilizzazione e formazione
- Gestione degli incidenti
- Vantaggi dell'implementazione delle misure minime:
    - Riduzione del rischio di attacchi informatici
    - Protezione dei dati
    - Miglioramento della conformità normativa
    - Aumento della fiducia dei cittadini

Quiz di verifica dell'apprendimento

Il Programma è suscettibile di integrazioni e/o variazioni volte a potenziare l'efficacia dell'intervento e ad approfondire tematiche prioritarie per l'Amministrazione.