Nome del corso e codice: **Cyber Threat Intelligence | MOD.2: Modello MITRE ATT&CK**

Date delle sessioni: 26 gennaio 2027

Orari: 9.00-16.00

Sede: CEIDA, Via Palestro 24, Roma | Possibile collegamento da remoto

Competence Center: Digital & AI Transformation

Prezzo: €500,00 + IVA (quota esente se corrisposta da Enti Pubblici)

Docente	**Francesco Schifilliti**
Info di contatto	Mail: segreteria@ceida.com
Orario ricevimento	Appuntamento da concordare via mail

Descrizione del corso

Questo corso è stato progettato per fornire ai partecipanti una solida conoscenza dei modelli fondamentali di Cyber Threat Intelligence sia con riferimento alle procedure di gara che di gestione del contratto e dei sistemi integrati di sicurezza.

Attraverso la realizzazione di analisi complesse di Cyber Threat Intelligence, descrivendole utilizzando anche la versione aggiornata del framework MITRE ATT&CK, si rappresenteranno le primarie competenze necessarie per la redazione di un capitolato di appalto che consentirà la gestione autonoma o affidata a terzi della sicurezza dei sistemi informativi, tenendo presente la necessità di ricostruire un team integrato di professionalità tecniche amministrative e legali che riescano a far sposare i linguaggi e le necessità delle amministrazione con l'innesto delle competenze del DPO e il registro del trattamento dei dati e cyber manager e relativo registro .

Comprendere il loro impiego a seconda delle necessità operative e utilizzarli in maniera cooperativa. Inoltre, nel corso sarà mostrato come analizzare le informazioni di intelligence utilizzando tecniche analitiche, come progettare e produrre le diverse tipologie di report fondamentali per una corretta gestione dei sistemi informativi tutti all'epoca della NIS 2.

Si procederà altresì alla ricostruzione della normativa dedicata attraverso le disposizioni di ACN e AGID che in fase di abilitazione, gara, gestione del contratto condizionano queste tipologie di contratti e conseguentemente sistemi operativi.

La trattazione degli argomenti sarà approfondita attraverso lo studio di Use Case con esempi pratici e con lo svolgimento di esercizi.

Destinatari del corso

RUP, RUP fase progettazione ed esecuzione, RUP fase di gara, Direttore dell'esecuzione, Responsabili dei CED, Responsabile del Piano dell'informatica, DPO, Cybermaneger Security Analyst Cyber Threat Intelligence Analyst, Cyber Security Engineer/Analyst, Cyber Incident Responder, SOC/CERT/CSIRT Analyst Cyber Security Manager, Cyber Security Team Leader, Chief Technology Officer (CTO).

Programma e Contenuti

Modulo 2: [Modello MITRE ATT&CK]

In questo modulo si fornisce una panoramica completa del framework ATT&CK e delle sue estensioni, illustrando come utilizzarlo praticamente e in modalità avanzata nella Cyber Threat Intelligence. Partendo dai concetti fondamentali e arrivando fino ai modelli di scoring più evoluti, i partecipanti acquisiranno gli strumenti teorici e pratici per mappare, analizzare e prioritizzare le minacce in base alle tecniche reali osservate nel panorama attuale.

Risorse di apprendimento

Durante il corso saranno utilizzati diversi strumenti didattici:

a. Dispense delle lezioni;
b. Use Case e report tecnici prodotti da organizzazioni e aziende di Cyber Threat Intelligence;
c. Esercizi teorici e pratici per consolidare le conoscenze apprese nei vari moduli.

Metodologia di apprendimento

Il corso adotta un approccio didattico operativo e partecipativo, che integra lezioni frontali con analisi di casi concreti e approfondimenti sulle tecniche di analisi affrontate nei vari moduli.

Sintesi del percorso di apprendimento

Sessione	Data	Orario	Docente
2	26 gennaio 2027	9.00-16.00	**Dott. Francesco Schifilliti**

Letture consigliate

- Recorded Future - The Threat Intelligence Handbook
- Aaron Roberts – Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers

Profilo docenti

Dott. Francesco Schifilliti

Consulente di Cybersecurity con una solida esperienza in Cyber Threat Intelligence, Digital Forensics e Incident Response, a supporto di Boards, Legal and Compliance e delle forze dell'ordine durante incidenti informatici ad alto impatto e indagini delicate.

Opera nell'intersezione tra tecnologia, indagini e governance, traducendo complesse evidenze tecniche in informazioni chiare, difendibili e fruibili per executives e decision-maker.

RACCOMANDAZIONE IMPORTANTE

Si informa che l'attivazione del corso avverrà esclusivamente a seguito di comunicazione scritta da parte del CEIDA.
Pertanto, si sconsiglia vivamente di effettuare prenotazioni o acquisti di titoli di viaggio, pernottamenti o altri servizi connessi, prima di aver ricevuto tale conferma ufficiale, comprensiva della modalità di erogazione del corso (in presenza o a distanza).
CEIDA declina ogni responsabilità per eventuali spese sostenute anticipatamente e non potrà essere ritenuto in alcun modo tenuto a rimborsi o compensazioni di natura economica o altra.