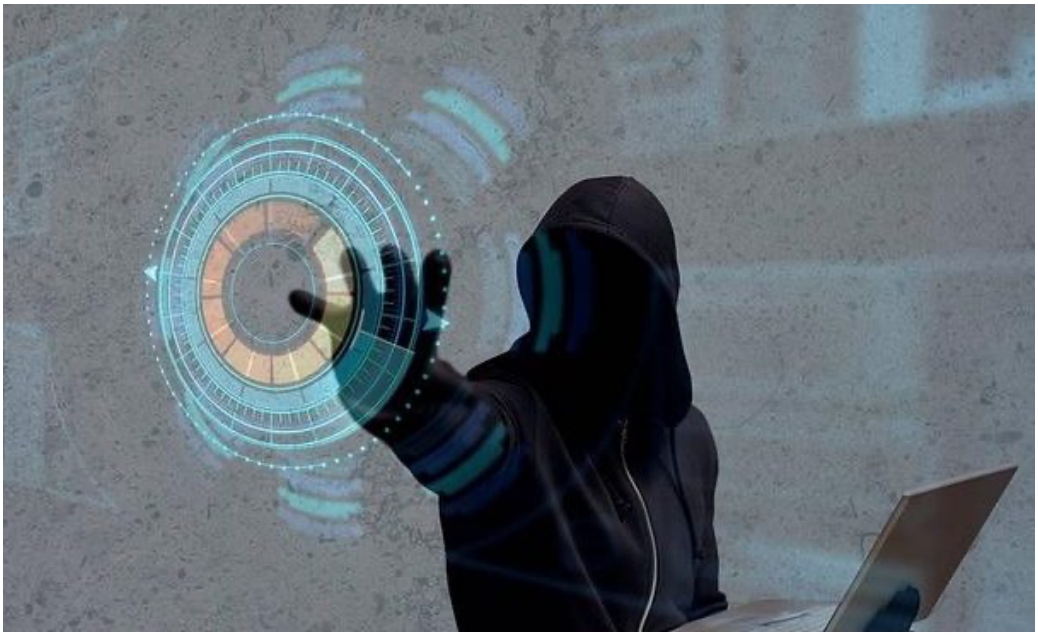
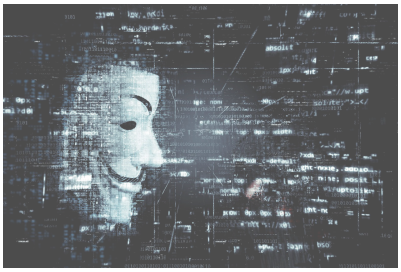
CORSO CYBER SECURITY

CONTESTO

Il 2020 ha aperto una nuova fase nel mondo della sicurezza informatica: la crisi globale scaturita dalla pandemia ha portato ad un vertiginoso aumento del numero di attacchi informatici, rendendo ancor più necessario formare talenti in grado di contrastare questo fenomeno. Per questo è importante creare solide competenze nell'ambito della Cybersecurity per aumentare il livello di sicurezza delle organizzazioni italiane pubbliche e private, la competitività, l'occupazione e l'economia. Infatti, la richiesta di esperti di cyber security è in continuo aumento nel mercato globale, rendendo il mondo della sicurezza informatica uno dei campi più sicuri e remunerativi a cui puntare.



OBIETTIVO



In tale contesto il CERT di Poste Italiane ha istituito un percorso formativo qualificante, di livello tecnico-teorico che mira ad approfondire gli aspetti tecnici e tecnologici relativi alle minacce informatiche e prevenire e rispondere correttamente in tempi brevi agli attacchi informatici.

Il corso in Cyber Security prenderà il via il prossimo 10 ottobre 2023 e si concluderà nel mese di gennaio 2024.

ARTICOLAZIONE DEL CORSO

L'iniziativa, voluta da Poste Italiane e realizzata con il patrocinio del Dipartimento di Ingegneria Informatica, Modellistica, Elettronica e Sistemistica (DIMES) dell'Università della Calabria, risponde all'esigenza di creare un ecosistema di competenza in cyber security adeguata ad aumentare il livello di sicurezza delle organizzazioni italiane pubbliche e private, la competitività, l'occupazione e l'economia.

Le attività didattiche del Corso, di livello tecnico operativo con esercitazioni pratiche e utilizzo di tool e piattaforme, saranno svolte da docenti qualificati ed esperti in materia provenienti dalle principali organizzazioni di spicco del settore.

L'iter didattico sarà articolato nei seguenti 4 moduli:

- MOULO I: Malicious email and malware analysis - Poste Italiane
- MODULO II: Investigation and Network Security - Palo Alto Networks
- MODULO III: Threat Hunting & Capture the Flag challenge - SentinelOne
- MODULO IV: Incident Management e DFIR gennaio 2024 - Yoroi

MODULO I MALICIOUS EMAIL AND MALWARE ANALYSIS

Il Modulo sarà erogato dai docenti di *Poste Italiane* (16 ore)

DESCRIZIONE

La prima parte del modulo propone di aumentare la comprensione di come è fatta una comunicazione elettronica, cosiddetta e-mail, con il fine di lavorare in sicurezza con questo strumento.

Saranno presi in considerazione gli elementi costitutivi di una e-mail: header, body, attachment e link. Durante la lezione saranno forniti gli strumenti per ispezionare ed analizzare in modo sicuro una e-mail e identificare gli elementi "a rischio".

La seconda parte del modulo ha l'obbiettivo di capire come l'attaccante utilizza le proprie conoscenze, al fine di ostacolare l'analisi del proprio codice e perché, non sempre è utile esplodere un codice malevolo in una "sandbox".

Il corsista sarà messo in grado di trattare tali software senza compromettere la postazione in cui lavoreranno, apprendendo i rudimenti per deoffuscare codice e come estrarre indicatori di compromissione (IOC) dai malware reali che saranno analizzati. Sarà, inoltre, accennato come sfruttare le attuali intelligenze artificiali (AI come ChatGPT), per semplificare la fase di analisi.

Tutto il software supplementare e necessario per il laboratorio sarà fornito in classe.

MODULO II INVESTIGATION AND NETWORK SECURITY

Il Modulo sarà erogato dagli esperti di *Palo Alto Networks* (10 ore)

DESCRIZIONE

I principali temi saranno:

- Il viaggio del SOC nel futuro
- Laboratorio di Investigation & Threat Hunting Lab
- Viaggio nell'AI-Powered Security
- Laboratorio Network Security

MODULO III THREAT HUNTING & CAPTURE THE FLAG CHALLENGE

Il Modulo sarà erogato dagli esperti di *SentinelOne* (16 ore)

DESCRIZIONE

Il Threat Hunting è un'attività cruciale all'interno delle strategie di sicurezza informatica di un'organizzazione, un approccio proattivo per migliorare la resilienza ad attacchi avanzati che porta, se correttamente implementato, benefici come la rilevazione anticipata

delle minacce, una riduzione dei tempi di permanenza (dwell time) della minaccia, il rafforzamento delle capacità di risposta e l'integrazione di intelligence sugli agenti di minaccia e le rispettive tattiche, tecniche e procedure (TTP) di attacco.

La corretta strutturazione, implementazione ed integrazione delle mission di Threat Hunting all'interno dei processi di sicurezza rappresenta una sfida importante, che richiede il supporto di una piattaforma predisposta a tali attività e comprovata da professionisti nel settore della Digital Forensics & Incident Response (DFIR).

In questo modulo, si analizzeranno alcune possibili metodologie di threat hunting, gli strumenti comunemente utilizzati, e come creare e validare ipotesi di threat hunting; argomenti principali del workshop includeranno le differenze tra threat hunting e searching, l'utilizzo del framework MITRE ATT&CK, l'uso di indicatori di compromissione (IoC) atomici e comportamentali e l'interpretazione dei risultati delle attività di hunting.

Il modulo si concluderà la seconda giornata con un'esperienza immersiva di tipo 'Capture the Flag', una simulazione di attacco che incorporerà vettori e metodologie di attacco avanzate e persistenti, in cui i partecipanti saranno chiamati ad indagare diversi scenari con livelli di difficoltà crescenti, utilizzando la piattaforma SentinelOne Singularity XDR.

MODULO IV INCIDENT MANAGEMENT E DFIR

Il Modulo sarà erogato dagli esperti di Yoroi (10 ore)

DESCRIZIONE

Il modulo di Incident Management e DFIR ha l'obiettivo di approfondire due aspetti fondamentali nel mondo della Cyber Security: identificare correttamente un incidente ed esser pronti ad attuare le corrette misure di contenimento e Remediation. Si inizierà con lo studio della metodologia di gestione dell'incidente a partire dalla definizione del perimetro di analisi, per spostarci poi sulla parte di Incident Response, imparando quali azioni compiere in seguito ad un attacco andato a buon fine. Il modulo si concluderà con esercitazioni pratiche su scenari realistici utilizzando tool specifici e con qualche cenno alla reportistica Post-Incident.

PERCORSO FORMATIVO

Il percorso ha una durata complessiva di 52 ore.

Le attività di ciascun modulo, si svolgeranno in due giornate consecutive al mese e si concluderà nel mese di gennaio 2024.

SEDE DI SVOLGIMENTO

Il corso si svolgerà presso la sede di Poste Italiane sita in via August Von Platen 9.

DESTINATARI

20-25 studenti/lavoratori.

REQUISITI MINIMI

- programmazione di base (qualunque linguaggio);
- conoscenze minime di networking;
- conoscenze di linguaggi di programmazione (GNU/Linux, Html, Java Script, Power Shell, Python);
- conoscenze sistemi operativi di base;
- Pc personale con sistema di virtualizzazione preinstallato (es: VirtualBox).

ISCRIZIONE

Per candidarsi inviare il proprio CV alla seguente casella mail: **dcs@posteitaliane.it**

SCADENZA

La scadenza della richiesta di ammissione è prevista per il 5 ottobre, il corso è GRATUITO.