Swascan Academy

Scoprire l'invisibile:

tecniche di Threat Hunting

Ottobre '23

Se hai bisogno di maggiori informazioni, scrivi a:
formazione@swascan.com

Swascan Academy

Descrizione

La Threat Hunting è una tecnica proattiva di sicurezza informatica che mira a identificare attacchi o minacce sfuggenti che potrebbero essere presenti all'interno di un sistema o di una rete aziendale. Questa tecnica si basa sull'utilizzo di metodologie, strumenti e analisi dei dati per individuare anomalie e segnali di allarme, al fine di prevenire futuri attacchi. Il suo obiettivo è quello di fornire una visione completa e in tempo reale delle minacce alla sicurezza aziendale, permettendo così di prendere misure proattive per prevenire futuri attacchi.

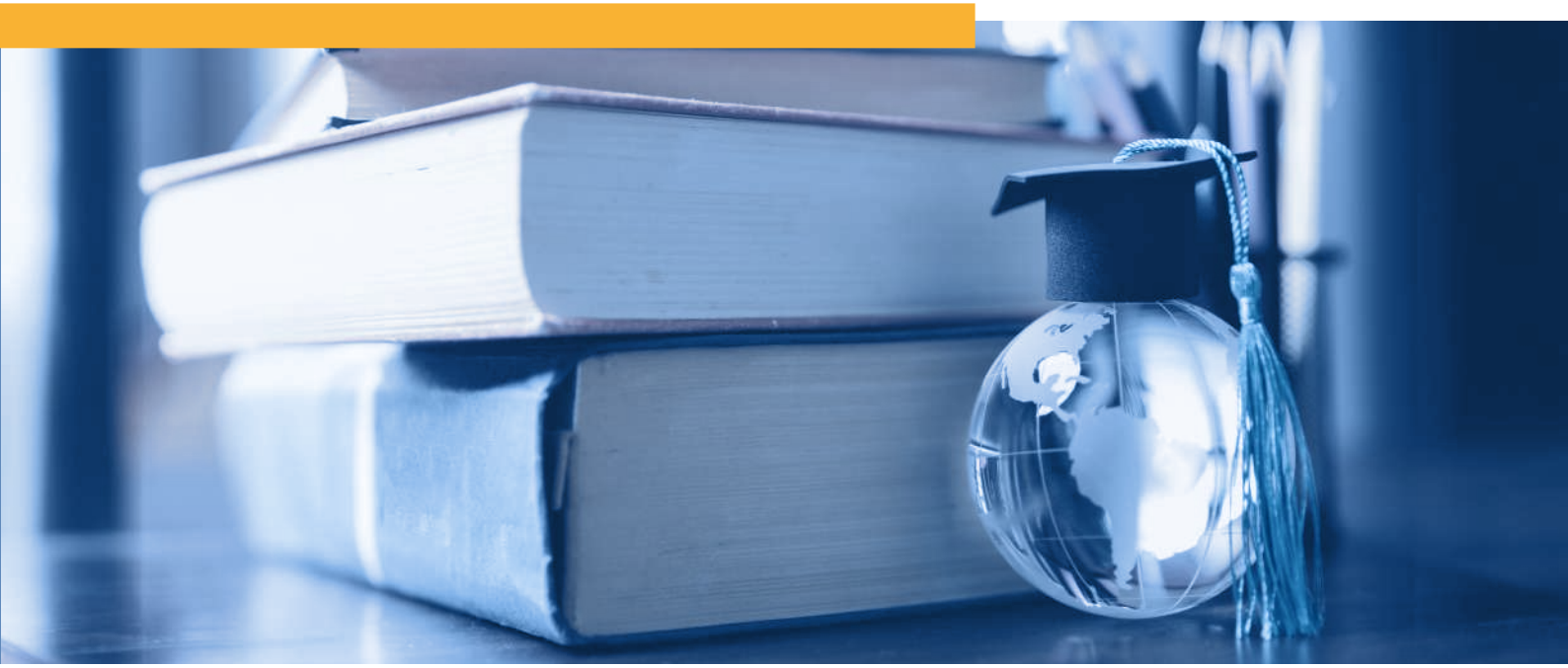
La sicurezza proattiva è la chiave per garantire la protezione dei dati e la continuità operativa!

Obiettivo

Il corso di Threat Hunting è un programma formativo progettato per fornire una conoscenza approfondita e le competenze necessarie per identificare e affrontare attacchi e minacce nascoste all'interno di un sistema o di una rete aziendale. Attraverso lezioni teoriche e sessioni pratiche, i partecipanti acquisiranno una solida comprensione dei principi fondamentali del Threat Hunting e svilupperanno abilità pratiche per applicarli efficacemente nell'ambiente di lavoro.

Programma didattico

Swascan Academy



01.

Introduzione al Threat Hunting

02.

Il Security Operations Center (SOC)

03.

Modelli e metodologie

04.

Analisi del traffico di rete con Wireshark

05.

IoC (Indicator of Compromise) e Yara Rules

06.

Inizio della caccia alle minacce

07.

Rilevamento delle minacce a diversi livelli di rete

- Esplorazione delle minacce a livello di connessione
- Identificazione delle minacce a livello IP
- Analisi delle minacce a livello di trasporto
- Caccia alle minacce a livello di applicazione

08.

Introduzione alle SandBox

09.

Laboratorio e CTF (Capture the Flag)

- Sessioni pratiche in un ambiente di laboratorio per applicare le competenze acquisite
- Discussione e analisi dei risultati delle attività pratiche

Include una copia gratuita dei materiali didattici utilizzati durante il Corso.

formazione@swascan.com

Destinatari

Il corso è dedicato al personale aziendale tecnico che possa applicare processi e procedure opportune per intervenire nelle fasi di identificazione e contenimento dell'incident response ovvero per chiunque voglia approfondire la materia.

Prerequisiti

Non sono richiesti prerequisiti mandatori, ma è consigliabile la conoscenza dei fondamenti di networking TCP/IP, la conoscenza della Cyber Kill Chain e delle nozioni sulle minacce informatiche.

formazione@swascan.com

Swascan Academy

Metodologia

Il Corso di Formazione verrà erogato in modalità sincrona attraverso la costituzione di classi virtuali.

Il Corso ha una durata di 24 ore distribuite in due appuntamenti settimanali della durata di 4 ore ciascuno nella fascia oraria pomeridiana.

Calendario

- 11-13 Ottobre
- 18-20 Ottobre
- 25-27 Ottobre

Segui il Corso da dove vuoi tu! Il corso è interamente somministrato in modalità DAD.