Malware Analysis

CODICE	**DT0191**
DURATA	**5 gg**
PREZZO	**2.490,00 €**
EXAM	

DESCRIZIONE

Questo corso insegnerà al partecipante le basi sull'identificazione dei malware, sul loro isolamento, sull'analisi statica e dinamica, nonchè sulle tecniche di offuscamento del codice. Sarà inoltre presentata una panoramica sulle principali tecniche di deploy attraverso exploit lato client.

TARGET

Security professional, Security operation

PREREQUISTI

Fondamenti di informatica e di programmazione

CONTENUTI

Modulo 1: Fondamenti

- Cybersecurity
- Analisi di un attacco
- Classificazione dei malware
- Dannosita, ambiente operativo, modalità di infezione

Modulo 2: Analisi statica

- Gli antivirus scanner
- Hashing
- Le stringe
- Il malware compresso
- DLL e funzioni

Modulo 3: Analisi dinamica

- Le sandbox
- L’esecuzione del Malware
- Il monitoraggio dei processi
- Il monitoraggio dei registri
- Simulare una rete
- Packet sniffing

Modulo 4: Offuscamento

- Livello di rete
- Livello di contenuto
- Livello applicativo
- Livello eseguibile

Modulo 5: IoC e tecniche di deploy

- Indicatori di compromissione
- Deploy di malware attraverso la rete
- Exploit lato clie