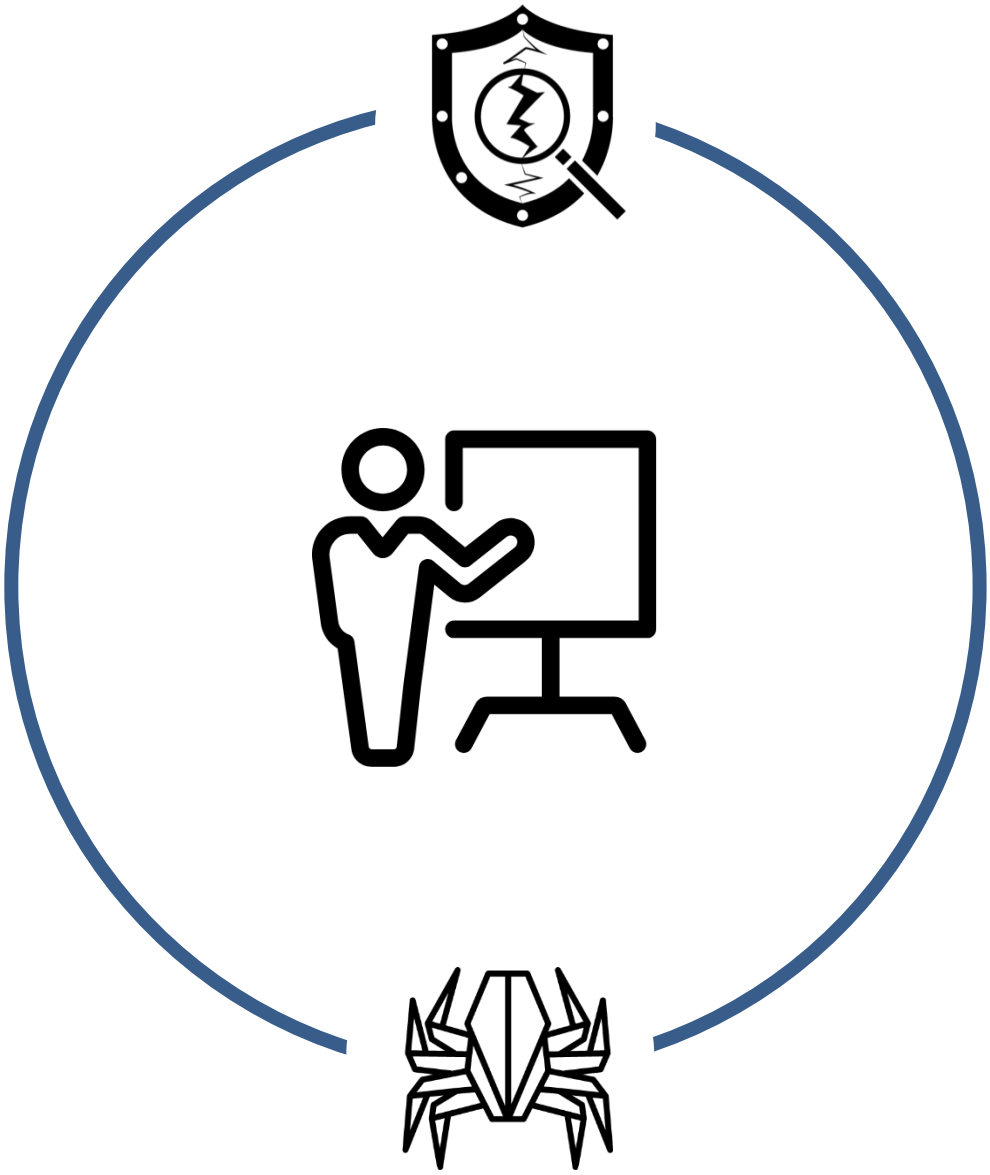
ExaTrack

Catalogue de Formations 2020



ExaTrack

Formations 2020

ExaTrack propose deux formations ayant une liaison forte avec le système d'exploitation Microsoft Windows, ces modules permettent d'acquérir des connaissances importantes et les réflexes adéquats pour mener à bien des analyses poussées. Des cas concrets d'attaques seront étudiés pour une immersion complète et une mise en situation réelle. Chacune de ces formations comporte une part de travaux pratiques qui permettront aux stagiaires de concrétiser et valider l'acquisition des compétences.

Contenu

Windows Internals

Cette formation a pour but d'expliquer une grande partie des fonctionnements internes du système d'exploitation Microsoft Windows. Les mécanismes de gestion des processus, des fichiers, de la base de registre et les communications avec le matériel sont autant de sujets abordés.

Durée de la formation : 5 jours

Public visé : Toute personne souhaitant mieux comprendre les fonctionnements internes de ce système d'exploitation. Elle convient aussi bien aux métiers de l'investigation numérique qu'aux auditeurs et analystes de codes malveillants.

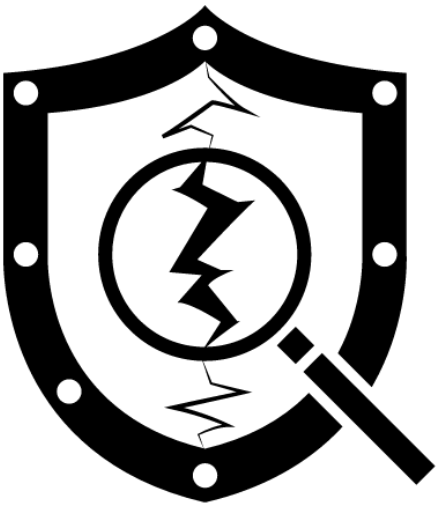
Prérequis : Bonne connaissance de Windows, savoir ce qu'est un processus, un fichier EXE/DLL/SYS.

Nombre de participants : 10 maximum

Prix : 3800 € HT par personne

Plan :

- Fonctionnement global de Windows
- Processus
  - Gestion de la mémoire
  - Structures internes
  - Format PE
  - Isolations
  - Représentation noyau
- WinDBG
- Noyau
  - Structures internes
  - Appels système
  - Object manager
  - IoManager
  - IRQL / APC / DPC
- Modèle de contrôle d'accès
  - Token
  - Security descriptor
  - Privilèges
- Autres technologies
  - WoW64
  - Windows Management Instrumentation (WMI)
  - Event Tracing for Windows (ETW)
  - Communications inter-processus



Analyse de Malwares - Avancée

Cette formation aborde l'analyse de codes malveillants complexes ayant des interactions avancées avec le système d'exploitation. Les malwares analysés mettent tout en œuvre pour ne pas être détectés et encore moins compris. Deux bootkits (codes malveillants infectant le processus de démarrage du système) seront analysés durant la session.

Durée de la formation : 5 jours

Public visé : Cette formation s'adresse aux analystes des CERT, CSIRT, SOC, structures possédant une expérience dans l'analyse de malware ayant besoin d'analyser des codes malveillants complexes.

Prérequis : Très bonne connaissance de Windows, savoir faire du Reverse Engineering, savoir développer en Python ou Ruby, bien connaître les API Windows et avoir déjà analysé des malwares.

Nombre de participants : 10 maximum

Prix : 3800 € HT par personne

Plan :

- Windbg
- Analyse d'un malware utilisé lors d'APT
  - Persistance non documentée
  - Dissimulation du code
  - Détection des anomalies
  - Machines virtuelles
- Reverse Engineering avancé
  - Communications interprocessus
  - Techniques d'anti-débug et d'anti-Analyse
  - Packers et obfuscation avancée
  - Implémentation de CPU exotique
- Automatisation
  - Désobfuscation
  - Unpacking
- Noyau
  - Processus de boot
  - Infection du processus de boot
  - Modifications de l'espace noyau
  - PatchGuard
  - Identification de la présence de rootkit
  - Emulation du code exécutable
  - Analyse de deux bootkits 64b