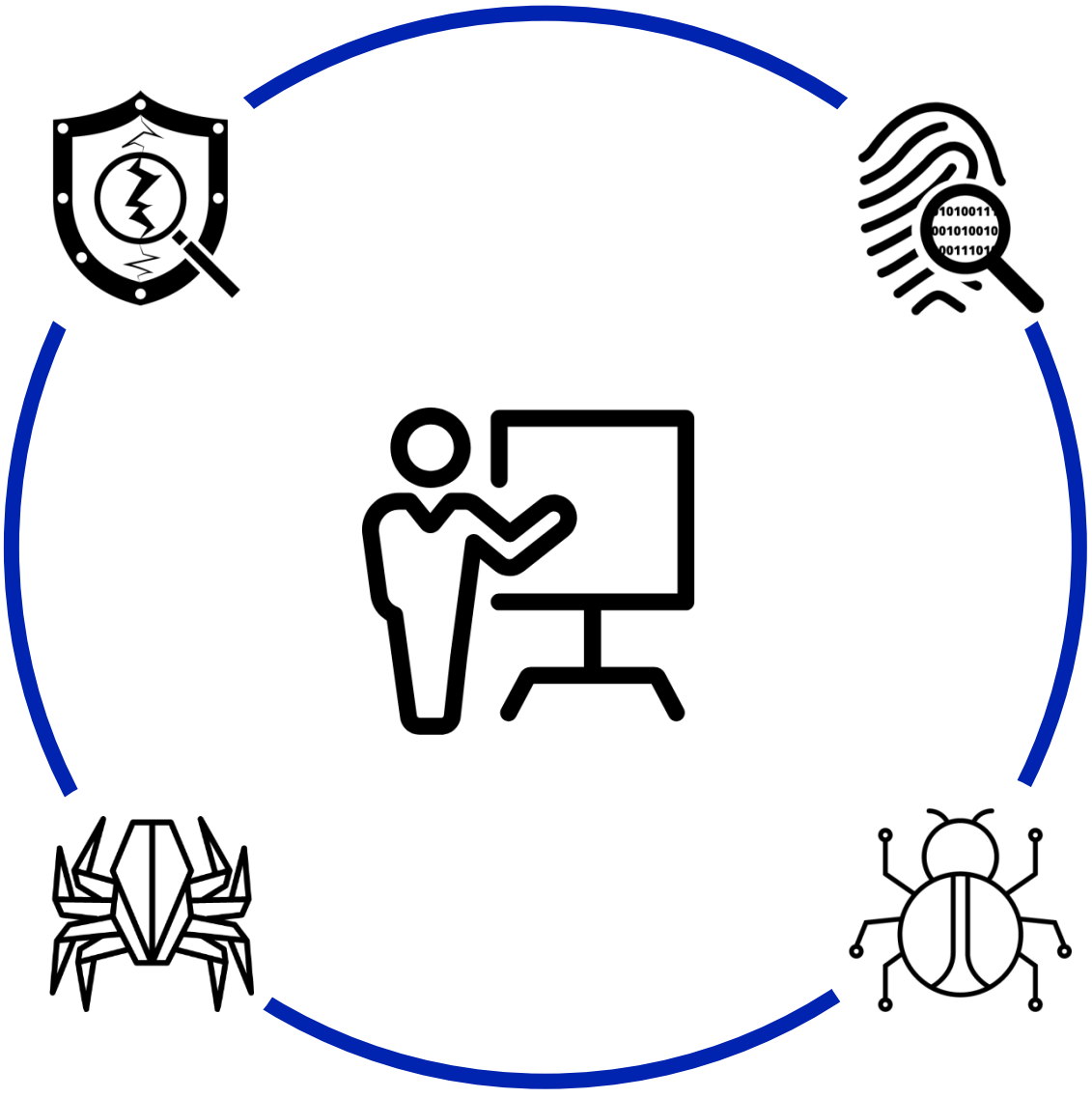
ExaTrack

Catalogue de Formations 2018



ExaTrack

Formations 2018

ExaTrack propose quatre formations, toutes ayant une liaison forte avec le système d'exploitation Microsoft Windows. Majoritairement orientées sur la réponse à incidents, ces modules permettent d'acquérir des connaissances importantes et les réflexes adéquats pour mener à bien ce type d'opérations. 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

ExaTrack

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

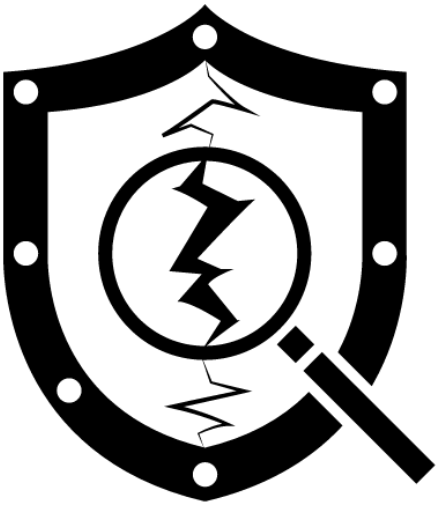
Public visé : Toute personne souhaitant mieux comprendre les fonctionnements internes de ce système d'exploitation. Elle convient aussi bien aux métiers de l'investigation numérique qu'aux auditeurs et analyste de codes malveillants.

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

Nombre de participants : 10 maximum

Plan :

- Fonctionnement global de Windows
- Processus
  - Gestion de la mémoire
  - Format PE
  - Structures internes
  - Isolations
  - Communications inter-processus
- Système de fichier
  - Organisation
  - Accès aux données
- Bases de registres
  - Organisation
  - Types de données
- Windbg
- Noyau
  - Processus de boot
  - Architecture du noyau
  - Interactions entre les drivers
  - Object manager
  - Gestion des entrées / sorties
  - Protections
  - Analyse de crash dumps



ExaTrack

Windows Forensics

Cette formation porte sur l'analyse des données brutes. Une explication détaillée de la structure des données est présentée pour le système de fichier, la mémoire, les processus et les fichiers spécifiques à Windows. Cette analyse approfondie apportera les capacités pour extraire et interpréter des informations précieuses lors d'investigations.

Durée de la formation : 5 jours

Public visé : Ce cours est principalement orienté pour la réponse à incident et l'investigation légale.

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

Nombre de participants : 10 maximum

Plan :

- Méthodologie d'analyse
- Acquisition des données et préservation de la preuve
- Analyse d'exécutables
- Processus
  - Organisation de la mémoire
  - Interactions avec le système
- Système de fichier
  - Organisation
  - Stockage des données
  - Exploitation de traces d'activités
  - Analyse fine du format NTFS
- Bases de registres
  - Organisation
  - Stockage des données
  - Exploitation de traces d'activités
  - Analyse fine du format
- Fichiers spécifiques
  - Analyse de formats de fichiers spécifiques à Windows
  - Identification d'activités suspectes
  - Apprendre à appréhender un format de données inconnu
- Mémoire
  - Analyse de dumps mémoire
  - Analyses avec un dump corrompu

Analyse de Malwares

Cette formation vous permettra d'appréhender l'analyse de codes malveillants. La création d'un environnement isolé ainsi qu'une méthodologie d'analyse qui permettront de commencer une investigation dans de bonnes conditions seront aussi abordé. L'assembleur et le reverse-engineering seront étudiés pour permettre à un analyste de travailler sur un exécutable malveillant de la façon la plus efficace possible.

Ces notions seront mises en pratiques à travers de nombreux exercices offrant une expérience tirée de cas réels.

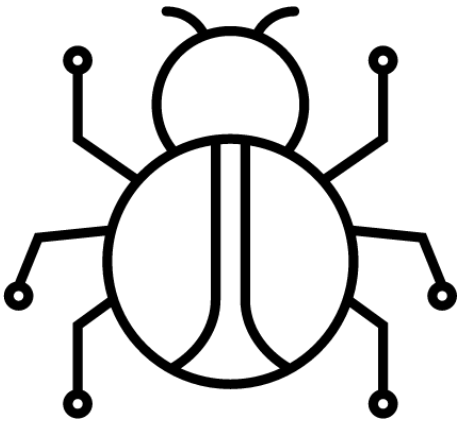
Durée de la formation : 5 jours

Public visé : Cette formation s'adresse aux analystes des CERT, CSIRT et structures ayant besoin d'analyser des codes malveillants.

Prérequis : Bonne connaissance de Windows, savoir ce qu'est un processus, un malware, avoir des notions de Python ou Ruby.

Nombre de participants : 10 maximum

Plan :



- Mise en place d'un environnement d'analyse
  - Création d'une machine virtuelle orientée analyse
  - Cloisonnement d'un code malveillant
  - Exploitation des traces générées
- Reverse Engineering et Assembleur x86 (32/64)
  - Instructions / Registres / Mémoire
  - Structure des fonctions
  - Analyse statique de code exécutable
- Analyse dynamique
  - Debug d'exécutables
  - Instrumentation d'un programme pour en extraire les actions
- Analyse de malwares
  - Méthode d'analyse
  - Modification de l'environnement par le malware
  - Techniques d'anti-analyse courantes
  - Packing / Unpacking
- Automatisation
  - Développement d'outils de pré-analyse
  - Extraction de configuration de malware
  - Développement d'un faux C&C

Analyse de Malwares - Avancé

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, 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

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