Analyse forensic et réponse aux incidents de sécurité

Date et durée

Code formation : CYBER001FR
Durée : 3 jours
Nombre d'heures : 21 heures

Description

Maîtrisez la double compétence essentielle face aux cyberattaques : la réponse aux incidents pour contenir la menace et l'analyse forensic pour **mener une investigation numérique rigoureuse**. Cette formation vous apprend à collecter et préserver des preuves numériques de manière méthodique pour comprendre chaque étape d'une attaque et renforcer durablement votre sécurité.
Notre **programme de 3 jours** est conçu pour être une immersion pratique dans les techniques d'enquête modernes. Vous maîtriserez le cycle de vie complet de la réponse aux incidents, de la préparation à la remédiation. Au-delà des processus, vous appliquerez des **méthodologies de collecte** avancées sur les systèmes Windows et Linux, en explorant des artéfacts complexes, comme ceux issus de la mémoire vive (RAM) ou des navigateurs web. L'ensemble des cours s'appuie sur la **manipulation d'outils d'investigation** reconnus, vous préparant ainsi aux réalités du terrain.
Cette formation vous dote de compétences directement opérationnelles, validées par une **simulation d'attaque finale**. Vous saurez mener une enquête technique complète et la synthétiser dans un **rapport d'analyse forensic** clair et percutant. Cette double expertise, à la fois technique et rédactionnelle, est un atout majeur pour **accélérer votre carrière en cybersécurité** et vous spécialiser en gestion de crise.

Objectifs

À l'issue de cette formation en analyse forensic et réponse aux incidents*, vous atteindrez les objectifs de compétences suivants :*

- structurer et piloter un plan de réponse aux incidents en maîtrisant chaque étape du cycle de vie (de la préparation et la détection jusqu'à l'éradication de la menace et la reprise d'activité) ;
- mettre en œuvre les bonnes pratiques de collecte des preuves numériques (duplication de disque, capture de mémoire vive) en garantissant leur intégrité pour une future analyse ;
- conduire une analyse forensic sur des systèmes Windows et Linux en examinant les journaux d'événements, les navigateurs web et d'autres artéfacts pour identifier les traces d'une compromission ;
- rédiger un rapport d'analyse technique clair et structuré, présentant les conclusions de l'investigation de manière factuelle et exploitable.

Points forts

- **Une expertise directe du terrain :** apprenez directement auprès d'un consultant spécialiste de la réponse aux incidents et de l'analyse forensic, qui partage son expérience concrète issue de véritables enquêtes sur des cyberattaques.
- **Une immersion pratique et concrète :** ici, la théorie est immédiatement mise en pratique. Chaque concept est exploré à travers des ateliers, des études de cas réalistes et la manipulation des outils du

métier (open source et professionnels).
- **Une simulation d'attaque "Grandeur Nature" :** pour valider vos compétences, vous serez plongé au cœur d'une simulation d'attaque complète. Vous mènerez l'enquête de A à Z dans un environnement de laboratoire sécurisé, comme lors d'une véritable investigation.
- **Des compétences directement opérationnelles :** vous ne repartez pas seulement avec des connaissances, mais avec des méthodologies, des procédures et des réflexes que vous pourrez appliquer dès le lendemain pour analyser et répondre efficacement aux incidents de sécurité.

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- **Solides connaissances des fondamentaux systèmes et réseaux :** compréhension de l'architecture d'un système d'exploitation (processus, gestion mémoire et systèmes de fichiers) et des protocoles clés (TCP/IP, DNS et HTTP).
- **Culture générale en cybersécurité :** familiarité avec les principaux types de menaces et de vulnérabilités (malwares, phishing, failles web courantes, etc.).
- **Expérience pratique en administration système :** aisance avec l'utilisation de la ligne de commande sur Windows et Linux, et connaissance de la gestion des services et des permissions.

Public

Cette formation s'adresse aux publics suivants :

- **les analystes et ingénieurs en cybersécurité (équipes SOC, CSIRT, etc.)** qui cherchent à maîtriser les méthodologies d'investigation post-incident pour analyser en profondeur les alertes et les compromissions ;
- **les professionnels de la réponse aux incidents** qui veulent structurer leur approche, maîtriser de nouveaux outils et se conformer aux meilleures pratiques du secteur ;
- **les administrateurs systèmes et réseaux confirmés** qui, souvent en première ligne lors d'une alerte, désirent acquérir les bons réflexes pour préserver les preuves, mener les premières analyses et collaborer efficacement à l'enquête.

Programme

Jour 1 : maîtriser les fondamentaux de la réponse aux incidents

- Stratégie de réponse aux incidents : préparation des équipes, des outils et des procédures.
- Identification et qualification des incidents : techniques de détection, d'analyse initiale et de priorisation des menaces.
- Confinement de la menace : méthodes d'isolement des systèmes compromis pour limiter l'impact.
- Communication de crise : procédures de notification internes et externes.
- Éradication et récupération : processus pour éliminer la cause racine de l'attaque et restaurer les services en toute sécurité.

Jour 2 : appliquer les fondamentaux de l’analyse forensic

- Acquisition des preuves et chaîne de conservation : techniques de duplication de disque (imaging) et collecte de données volatiles.
- Récupération de données (File Carving) : principes et mise en œuvre pour reconstituer des fichiers supprimés.
- Analyse des journaux système : exploitation des logs (Windows, Linux et applicatifs) pour retracer une activité suspecte.
- Analyse des communications réseau : identification des traces d'une attaque dans les captures de trafic (PCAP).

Jour 3 : approfondir l’analyse forensic avec des concepts avancés

- Techniques d'investigation à grande échelle : utilisation des outils d'indexation pour accélérer les recherches.
- Analyse des navigateurs web : investigation des artéfacts liés à l'activité de l'utilisateur (historique, cache, sessions).
- Analyse de la mémoire vive (RAM) : recherche de preuves éphémères non présentes sur le disque (processus, malwares, etc.).
- Analyse des e-mails malveillants : techniques pour décortiquer les en-têtes et pièces jointes (phishing, malware).
- Rapport d'analyse forensic : structure, bonnes pratiques de rédaction et présentation claire des conclusions.