Formation Malwares, Détection, identification et éradication

Présentation

Les logiciels malveillants (ou malwares) représentent une menace sérieuse pour les organisations. Conçus pour des objectifs spécifiques, comme exploiter les ressources d'un système pour miner des crypto-monnaies ou chiffrer des données pour exiger une rançon, ils nécessitent une réponse rapide et efficace. Cette formation de 3 jours permet aux participants de comprendre les différentes familles de malwares, leurs techniques d'infection, de propagation et de persistance. Ils apprendront également à réaliser des analyses approfondies pour les détecter, s'en protéger et les éradiquer.

Durée : 21,00 heures (3 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

Face à la montée en puissance des cyberattaques par malwares (ransomwares, spywares, botnets), cette formation intensive vise à doter les participants des compétences nécessaires pour :

- Détecter efficacement les infections sur des systèmes Windows ;
- Analyser le comportement des malwares, même sophistiqués ;
- Mettre en œuvre des stratégies d'éradication et de remédiation adaptées ;
- Automatiser certaines réponses aux incidents pour améliorer la résilience opérationnelle.

Prérequis

- Bonne maîtrise de l'environnement Windows (poste de travail et serveur)
- Connaissances fondamentales en cybersécurité et réseaux

Public

- Responsables de la gestion des incidents
- Techniciens en réponse aux incidents
- Auditeurs techniques
- Analystes en sécurité

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

DOCAPOSTE Institute

Programme de la formation

Fondamentaux des malwares

- Panorama des menaces : virus, vers, ransomwares, spyware, botnets
- Techniques avancées : rootkits (userland / kernel) et bootkits
- Mécanismes d'infection, escalade de privilèges et persistance

Détection et investigation

- Limites des antivirus traditionnels
- Détection avancée avec EDR, NIDS/HIDS
- Collecte et interprétation des IOC (hash, signatures, comportements)
- Déploiement d'outils de monitoring et d'analyse

Techniques d'analyse

- Analyse dynamique (sandboxing, comportement en environnement contrôlé)
- Analyse mémoire avec Volatility : extraction d'artefacts malveillants
- Introduction à la rétro-ingénierie : lecture de code assembleur simple

Analyse et éradication

- Étapes d'analyse d'un système compromis
- Évaluation de la portée de l'infection
- Techniques d'éradication manuelle et assistée
- Protocoles de nettoyage et validation post-incident

Réponse automatisée aux incidents

- Scripts d'automatisation et playbooks SOAR
- Intégration avec des solutions EDR / SIEM
- Cas pratiques : déclenchement d'actions en réponse à des IOC détectés
- Stratégies d'orchestration pour réduire le temps de réponse

Organisation

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France