Formation Sécurité des postes & systèmes (EDR, durcissement)

Informations

Durée : 2 jours (14h.)

Tarif* : Nous consulter

Réf : SPSY

Niveau : Moyen

intra

Mise à jour le 30/12/25

*tarif valable jusqu'au 31/12/2026

Prochaines sessions

Contactez-nous pour connaitre nos futures sessions.

Pré-requis

- Connaissances de base en systèmes (Windows et/ou Linux)
- Compréhension générale des environnements IT
- Notions de cybersécurité recommandées

Objectifs

Objectifs pédagogiques :

- Comprendre les menaces ciblant les postes et systèmes
- Connaître les principes du durcissement des systèmes
- Comprendre le rôle et le fonctionnement d'un EDR
- Identifier les bonnes pratiques de sécurisation des endpoints
- Appréhender la détection et la réponse aux comportements anormaux

Objectifs opérationnels :

- Appliquer des règles de durcissement sur postes et serveurs
- Réduire la surface d'attaque des systèmes
- Comprendre et exploiter les alertes d'un EDR
- Réagir face à une activité suspecte sur un endpoint
- Contribuer à une stratégie globale de sécurité des systèmes

Programme

Jour 1 – Sécurisation et durcissement des postes & systèmes

Menaces ciblant les endpoints

Panorama des attaques ciblant postes et serveurs
Malware, ransomware, exploitation de vulnérabilités
Attaques internes et mouvements latéraux
Importance des endpoints dans la chaîne d'attaque

Principes du durcissement des systèmes

Qu'est-ce que le hardening ?
Réduction de la surface d'attaque
Configuration sécurisée par défaut
Principe du moindre privilège

Durcissement des postes et serveurs

Gestion des services et processus
Politiques de mots de passe et d'accès
Mises à jour et correctifs
Sécurisation des accès locaux et distants

Atelier pratique

Analyse d'un système mal configuré
Identification des failles de configuration
Proposition de mesures de durcissement

Jour 2 – EDR, détection et réponse sur les endpoints

Introduction aux solutions EDR

Antivirus vs EDR : différences et complémentarités
Fonctionnement d'un EDR

Formation Sécurité des postes & systèmes (EDR, durcissement)

Collecte des événements et comportements
Détection basée sur les comportements

Supervision et analyse des alertes

Typologies d’alertes EDR
Qualification des événements suspects
Faux positifs vs incidents réels
Corrélation avec d’autres sources

Réponse à incident sur les endpoints

Isolement d’un poste compromis
Analyse et containment
Remédiation et restauration
Documentation et retour d’expérience

Atelier pratique

Analyse d’alertes EDR simulées
Qualification d’un incident endpoint
Élaboration d’un plan de réponse