New

Introduction au SOC et aux architectures EDR/XDR

Maîtriser les mécanismes de supervision et de réponse aux cybermenaces

Présentiel ou en classe à distance

1 jour (7 h)

Prix inter : 990,00 € HT
Forfait intra : 2.850,00 € HT

Réf.: SR386

La formation **Introduction au SOC et aux architectures EDR/XDR** offre une vision claire et opérationnelle du fonctionnement d'un **Security Operations Center (SOC) moderne** et des technologies clés de détection et de réponse aux incidents. À travers un format combinant technique et démonstrations concrètes, les participants découvrent les enjeux actuels de la **cybersécurité**, l'évolution des menaces (ransomwares, espionnage industriel, attaques étatiques) et les cadres de référence tels que NIS2, RGPD, ISO 27002 et NIST CSF. La formation met en lumière les rôles respectifs des **EDR, XDR, SIEM, NDR et SOAR**, ainsi que l'apport stratégique du framework **MITRE ATT&CK** pour analyser les tactiques et techniques des attaquants et structurer une stratégie de détection efficace.

A qui s'adresse cette formation ?

Pour qui

- Administrateurs systèmes, Administrateurs réseaux, Ingénieurs infrastructure, Chefs de projet IT, Responsables informatiques, Analystes SOC juniors

Prérequis

- Aucun.

Programme

1 - Panorama des menaces et rôle du SOC

- Évolution des cybermenaces : ransomwares, espionnage industriel, opérations étatiques
- Fonctions et périmètre : CERT, CSIRT, SOC Obligations et cadres de référence : RGPD, NIS2, ISO 27002, NIST CSF
- Les trois piliers d'un SOC : collecte, détection, réponse

2 - MITRE ATT&CK, la matrice stratégique de la détection et de la réponse

- Comprendre TTPs, tactiques et techniques utilisées par les attaquants
- Pourquoi intégrer MITRE ATT&CK dans une stratégie SOC ?
- Utilisation concrète dans les opérations de sécurité
- Limites : couverture, complexité, usage en production

Atelier

Exploration de TTPs réels via la matrice MITRE ATT&CK

Présentation du serveur C2 MITRE Caldera : automatisation et simulation d'attaques

3 - Les outils au service de la Détection et Réponse

- Centralisation des Logs : Utilisation des systèmes SIEM pour la collecte et la corrélation des événements
- Corrélation Multi-Sources : Obtenir une visibilité globale avec les solutions XDR

- Analyse des Flux : Étude des protocoles et détection des comportements anormaux avec les outils NDR
- Automatisation des Réponses aux Incidents : Rôle des outils SOAR dans la gestion des incidents
- Acteurs du marché : Solutions commerciales, open source et certifiées pour chaque type d'outils
  Atelier

  Installation rapide d'un agent EDR commercial sur Windows Détection en temps réel d'un malware via la console EDR

  Passage en mode surveillance pour un suivi sans blocage

  Déploiement de l'agent Caldera pour simuler des attaques

  Exécution d'un « Malware » de scénarios réalistes (découverte, persistance, vol de credentials, chiffrement)

  Visualisation des alertes dans la console EDR

4 - Les techniques de détection utilisées par un SOC moderne

- Threat Intelligence : Enrichissement des données avec des flux externes de renseignement sur les menaces
- Indicateurs (IoA, IoC, IoV) : Signatures et indicateurs d'attaques connues
- Détection et classification des malwares à travers des règles personnalisées : YARA
- Création de règles génériques pour la corrélation des événements : SIGMA
- Intelligence artificielle : Applications de l'IA dans la détection et la réponse aux incidents
  Atelier

  Présentation d'outils et ressources gratuites incontournables pour la Cyber Threat Intelligence

5 - Internaliser ou externaliser ? SOC interne, SOCaaS, MSSP, MDR

- SOC (Security Operations Center) interne vs SOCaaS (SOC as a Service)
- MDR (Managed Detection and Response) : service géré de détection et réponse
- MSSP (Managed Security Service Provider) : surveillance et services de sécurité externalisés
- Critères techniques et organisationnels pour faire un choix rationnel

6 - Synthèse et perspectives

- Récapitulatif des points essentiels
- Évolution des menaces et transformation des SOC
- Importance de la montée en compétences continue

Les objectifs de la formation

- Comprendre le rôle, les missions et les enjeux d'un SOC moderne face aux menaces actuelles
- Identifier les apports et les limites des architectures EDR, XDR, SIEM, NDR et SOAR dans la détection et la réponse
- Observer l'usage du framework MITRE ATT&CK pour analyser les techniques d'attaque et structurer une stratégie de détection
- Découvrir les mécanismes techniques de détection (IoC/IoA/IoV, CTI, YARA, SIGMA, IA) à travers des démonstrations du formateur
- Interpréter les scénarios d'attaque et les alertes présentées lors des démonstrations EDR/XDR

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Un panorama complet des architectures de détection et de réponse
- Une formation orientée pratique et opérationnelle

Dates et villes 2026 - Référence SR386

Dernières places disponibles Session garantie

A distance

le 17 avr.	le 28 août	le 10 nov.
le 31 juil.	le 25 sept.	

Paris

le 17 avr.	le 28 août	le 10 nov.
le 31 juil.	le 25 sept.	