AVANCÉ

SÉCURITÉ DÉFENSIVE

MISE EN PLACE DE SONDES DE DÉTECTION D'INTRUSION

Détectez et déjouez les tentatives d'intrusion sur votre système d'information.

Code : SDI

Les attaquants sont de plus en plus motivés et outillés pour s'introduire dans votre système d'information.

Comprendre leurs techniques d'attaque et être en mesure de les détecter est aujourd'hui essentiel !

À travers cette formation vous apprendrez à mettre en place des règles de détection efficaces face aux cyberattaques actuelles et cela avec des sondes de détection open source.

Ces détections portent aussi bien sur les parties système et réseau que la partie applicative.

PROGRAMME

Méthodes mobilisées : cette formati on est construite avec une alternance de cours théoriques et de cas pratiques afi n de favoriser l'acquisiti on des savoirs du programme (cf. Ressources).

Modalités d'évaluation : En amont de la formation, une évaluation des compétences de l'apprenant est effectuée.

Puis, les objectifs sont régulièrement évalués tout au long de la formation (50% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

- Introduction aux menaces cyber actuelles
- Enjeux de la supervision et détection dans les systèmes d'information
- Outils de supervision et de détection
- La gestion d'incident
- Présentation IDS/IPS, EDR, XDR, etc.
- Présentation de la sonde Suricata
- Installation et configuration de Suricata
- Détection d'attaques réseau

JOUR 2

- Présentation de la sonde Wazuh
- Mise en place de Wazuh
- Scans de vulnérabilités avec Wazuh
- Blocage d'une attaque par force brute SSH via Wazuh
- Introduction aux attaques Web
- Détection d'attaques Web via Suricata
- Contournement de règles de détection d'attaques Web

JOUR 3

Détection d'exploitation d'une faille récente avec Suricata

- Intégration de VirusTotal dans Wazuh
- Étude de cas : Détection d'une tentative de compromission par logiciel malveillant :
  - Détection via la réseau et méthodes de contournements
  - Détection via le système hôte

PROCHAINES DATES

5 février 2025
12 mai 2025
22 septembre 2025
17 novembre 2025

OBJECTIFS

- Comprendre les méthodes utilisées pour détecter les attaques
- Savoir créer ses propres règles de détection sur des outils open source
- Comprendre comment les attaquants contournent les systèmes de détection d'intrusion
- Savoir mettre en place les règles adéquats contre des attaques sur le réseau et sur les machines hôtes

INFORMATIONS GÉNÉRALES

Code : SDI

Durée : 3 jours

Prix : 2 460 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Administrateurs réseau / système
- Techniciens réseau / système
- Ingénieurs sécurité

PRÉ-REQUIS

- Avoir des notions de sécurité informatiques
- Maîtriser les modèles OSI et TCP/IP
- Savoir utiliser un environnement Linux

RESSOURCES

- Support de cours
- 80% d'exercices pratiques
- 1 PC par personne avec un environnement dédié sur notre plateforme MALICE