Surveiller, détecter et répondre aux incidents

Il existe des mesures simples sur le plan technique ou organisationnel pour prévenir les risques. La surveillance et la détection sont préconisées pour toute organisation et sont primordiales pour la prise en compte des enjeux de la sécurité de l'information.

Compétences visées

- Identifier les indicateurs de compromission (IOC)
- Mettre en œuvre les différents moyens de surveillance et de détection
- Gérer les incidents de cybersécurité

Objectifs pédagogiques

- Identifier les menaces et les attaques sur votre SSI
- Identifier les indicateurs de compromission (IOC)
- Mettre en œuvre les différents moyens de surveillance et de détection
- Anticiper et limiter l'impact des attaques
- Maîtriser les différentes étapes de gestion des incidents de sécurité

Public

Personne travaillant au sein d'une équipe de sécurité opérationnelle ou d'une équipe de réponse aux incidents, administrateur, RSSI, chef de projet

Prérequis

Avoir des connaissances informatiques est nécessaire.

Programme

Introduction

- Identifier les menaces en 2018
- Lister les familles d'attaques répertoriées
- Identifier les phases du processus d'attaque : Cyber Kill chain
- Comparer les Red Team, Blue Team et Hunt Team
- Définir le principe de compromission préalable

Surveiller et détecter

- Identifier une reconnaissance passive et active
- Détecter des fuites d'informations
- Scanner un réseau
- Mettre en place des pare-feux
- Mettre en place des sondes de sécurité IDS/IPS
- Mettre en place une défense active "honeypot"
- Attaquer pour mieux se défendre

Gérer les failles de sécurité

- Se mettre à jour sur les vulnérabilités du SI
- Corriger les failles web
- Mettre à jour ses applications
- Sensibiliser l'humain avec de la prévention
- Mettre en place une supervision sécurité continue
- Faire de la Security by design

Gérer les incidents

- Identifier les objectifs de l'attaquant
- Déterminer les points d'entrée
- Analyser la timeline de l'incident

Détecter la persistance

- Nettoyer une infrastructure Windows
- Identifier la persistance UNIX/Linux
- Lister les moyens employés

Durée
5 jours - 35 heures

Prix inter
3500 €HT

Prochaines dates
24 au 28 septembre 2018
26 au 30 novembre 2018

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le domaine de la Cybersécurité et de la détection d'attaques.

Après cette formation, vous pouvez suivre la formation S'initier à l'analyse inforensique.