Ref : DNDASECUBLUE	**Durée :** 5 Jours	**Tarif :** 3 600 €HT

Formation Détection et réponse aux incidents de sécurité

Objectifs de la formation Détection et réponse aux incidents de sécurité:

- Mettre en place une architecture de détection
- Appliquer la notion de "prévention détective"
- Limiter l'impact d'une compromission
- Prioriser les mesures de surveillance à implémenter
- Maitriser le processus de réponse à incident

Programme de la formation Détection et réponse aux incidents de sécurité:

Module 1 : État des lieux
- Pourquoi la détection
  - Défense en profondeur
  - Tous compromis
- Évolution de la menace
- Principes de défense
- CTI et renseignement
  - IOC, Yara, MISP

Module 2 : Comprendre l'attaque
- Objectifs de l'attaquant
- Phases d'une attaque
- Plusieurs champs de bataille
  - Réseau
  - Applications
  - Systèmes d’exploitation
  - Active Directory
  - Utilisateurs et Cloud
- Portrait d'une attaque réussie

Module 3 : Architecture de détection
- Architecture sécurisée
- Détection : les classiques
  - IDS/IPS
  - SIEM
  - SandBox
  - Capture réseau
  - WAF
- Valoriser les "endpoints"

  Whitelisting
  Sysmon
  Protections mémoire
  Mesures complémentaires de Windows 10
- Les outsiders
  "Self-defense" applicative
   Honey-*
   Données DNS
- Focus : Journalisation

Module 4 : Blue Team vs. attaquant

- Gérer les priorités
- Outils & techniques
  Wireshark / Tshark
  Bro / Zeek Recherche d'entropie
  Analyse longue traîne
- Détection et kill chain
  Focus: Détecter Bloodhound Exploitation
  C&C
  Mouvements latéraux
  Focus : Attaques utilisant Powershell
  Elévation de privilèges
  Persistance
- Focus: détecter et défendre dans le Cloud

Module 5 : Réponse à incident et Hunting
- Le SOC & CSIRT
- Triage
- Outils de réponse
    Linux
    Windows
    Kansa
    GRR
- Partons à la chasse
    Principes de base
- Attaquer pour mieux se défendre
    Audit "Purple team"

Public

Membres d'un SOC ou d'un CSIRT , Administrateurs , Responsables sécurité.

Pré-requis

Avoir suivi au préalable la formation fondamentaux techniques de la cybersécurité (et/ou) avoir de solides bases en sécurité des systèmes d'information.

Méthodes pédagogiques

Cours magistral avec travaux pratiques et échanges interactifs.