Formation « Détection des incidents de sécurité »

Réf : SECUSOC

Tous les attaquants laissent des traces ! Le SOC est la brique indispensable pour les détecter et limiter les impacts d'une compromission. Détecter est impératif face au niveau de menace actuel et ce sont l'efficacité des analystes et l'intelligence des règles qui font la différence. Vous disposez d'un SOC, ce SOC dispose d'une vision unique sur le Si grâce aux sources d'information qu'il collecte, il est en première ligne pour détecter. De nouvelles techniques de recherche d'attaquant, dont la chasse aux menaces (hunting), doivent également être mis en place pour être proactif vis à vis des nouvelles techniques et outils d'attaque.

Objectifs

- **Former les analystes SOC à la détection et aux spécificités de la détection système, en s'appuyant principalement sur l'environnement Windows. À l'issue de la formation, les stagiaires seront capables de :**
  - **Décrire l'écosystème de la détection système : chaîne de détection (événement → signal → alerte → incident), sources de données à collecter, normalisation, cycle de vie des signatures, tableaux de bord**
  - **Mobiliser les méthodologies de création d'alertes : Kill Chain, MITRE ATT&CK, pyramide de la douleur, hiérarchisation des alertes.**
  - **Détecter les techniques d'attaque spécifiques à Windows : authentifications (Kerberos, NTLM, LSASS), vol d'identifiants, PowerShell, règles Sysmon, latéralisation (RDP, SMB, PSRemoting, WMI), persistance, élévations de privilèges, et traces des outils des attaquants.**
  - **Identifier les moyens de détection sur d'autres environnements : Linux, réseau, cloud.**
  - **Mettre en œuvre le processus métier de l'analyste : investigation d'une alerte, chasse (hunting), SOAR.**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Analystes SOC N2 et N3**

Pré-requis

- **Avoir de bonnes bases en cybersécurité ou avoir suivi la formation SECUCYBER**
- **Connaissance d'un SIEM (ELK, Logpoint, Prelude, Qradar, Splunk, etc) ou avoir suivi une formation SPLUNK ou ELASTICSEARCH**
- **Avoir un SOC dans son organisation**

Méthode pédagogique

- **Cours magistral illustré par des travaux pratiques à chaque module**

Supports

- **Support de cours en français au format papier en présentiel et au format numérique en distanciel**
- **Machine virtuelle contenant l'ensemble des exercices**
- **Ordinateur portable mis à disposition des stagiaires qui ne disposerait pas du leur**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM de savoir-faire, pas un simple test de connaissance, dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUSOC par HS2.**

Programme

Panorama de la détection système

- Chaîne de détection et terminologie
- Organisation des équipes
- Sources de données
- Quoi collecter ?
- Normalisation et standardisation des données
- Connaissance du SI supervisé et des pratiques d'administration
- Cycle de vie des signatures
- Tableaux de bord
- Environnement, contexte de détection, interaction avec les autres acteurs de la sécurité opérationnelle

Méthodologies

- Kill chain / Mitre attack
- "Pyramide of pain" et détection de menace connue vs inconnue
- Démarche de création et de hiérarchisation des nouvelles alertes
- Comprendre les agents IA
- Apports de l'apprentissage automatique
- Usage des agents dans le SOC
- Limites et risques des agents

Techniques de détection pour Windows

- Détection grâce aux journaux d'authentification :
  - ActiveDirectory, Kerberos, NTLM, lsass, ntds, sam
  - moyens de détection des outils et techniques de vol d'authentifiant dont mimikatz
- Techniques d'attaque et de détection Powershell
- Pré-requis et création de règles Sysmon
- Détection des techniques de latéralisation : RDP, SMB, PSRemoting, WMI
- Détection de la persistance : création de services, tâches planifiées, clés de registres, dossiers startup
- Repérage des traces générées par les outils communément utilisés par les attaquants : Cobalt Strike, Empire, Lolbins
- Fonctionnement et détection des élévations de privilège : SID, Niveau d'intégrité, token
- Détection en amont la reconnaissance faite par l'attaquant au sein du SI : adfind, bloodhoud, LOLBins

Techniques de détection de compromission d'autres environnements

- Linux : auditd, wazuh, ossec
- Réseau : scans, flux, beaconning, trafic HTTP/HTTPS sortant, trafic DNS
- Infonuagique (Cloud) : API et services

Processus métier des analystes

- Processus d'investigation d'une alerte
- Processus de chasse (hunting)
- SOAR (ochestration, automatisation et réponse aux incidents de sécurité)

Examen de certification