**Mathieu M – Analyste Cybersécurité**

**Points forts**

* Identifier les causes profondes des incidents détectés.
* Évaluer l'impact de l'incident sur le plan technique et pour les différents secteurs d'activité.
* Fournir une analyse détaillée des actions menées par l'attaquant sur le périmètre compromis.
* Gérer les projets
* Établir une timeline forensique pour suivre l'évolution des menaces et des contre-mesures.
* Assurer une surveillance continue et une enquête numérique sur tous les systèmes d'exploitation.
* Repérer les vulnérabilités du système d'information ou de son application.

**Niveaux d’Intervention**

* Qualifier les incidents remontés par le SIEM (levée de doutes, sévérité des incidents, impacts).
* Répondre aux incidents (CSIRT) lors d’incidents avérés
* Faire de l'investigation légale lorsque nécessaire (forensiques)
* Administrer les outils du CSIRT (Antivirus, EDR, plateforme CTI, sandbox,)
* Prise en charge des alertes escaladées par les autres niveaux du SOC (investigation depuis le SIEM et de nombreuses solutions de sécurité : anti DDOS, FW, antivirus, bastion traçant, solution EDR, métiers…)
* Faire la veille des menaces, traitement des vulnérabilités, analyse et traitement des IOC
* Évaluer la sécurité des services et des applications (Test d’intrusion, test de vulnérabilité)
* Analyse et exploitation des vulnérabilités
* Production des rapports d’audits (Searching and reporting)
* Pentesting des applications et serveurs web
* La détection d'intrusions, le ' reverse engineering ' et gestion des vulnérabilités
* OSINT : Exploitation des informations issues de sources libres

**Formation et certifications**

**2022 Ingénieur spécialité Cybersécurité** ESAIP, Angers, France

**2022 Microsoft Certified :** Azure AI Fundamentals

**Connaissances**

**Technologie** Qradar, Splunk, bastion (wallix), SentinelOne, Pingcastle, qualys, Palo Alto, Proofpoint

**Normes et standards** ISO 27001, 27002, 27005, EBIOS

**Réglementations** GDPR, LPM, CNIL

**Outils / IDE**  Atom/ Bash / Visual Studio / Visual Code

**Gestion de projet** Agile (Scrum), Gouvernance SSI

**Langages**  Android Apps développent / HTML5, CSS3 / C, C++, PHP, SQL, Python, YAML (Ansible), Latex

**Réseaux** Sécurité SI, Pile TCP/IP, Architecture et routage IP, Adressage, Modèle OSI, Protocoles réseaux, Fortinet, Zscaler,

**Systèmes d’exploitation** Linux User (Ubuntu / Debian/ Kali/ Fedora/ CentOS/ Mageia), Windows

**Hobbies & Divers**

**Langues** Anglais (professionnel), Français (maternelle)

**Hobbies** Manga, Tennis, Football, voyage, Actualité, Vulnhub

**Expériences Professionnelles**

**Avril 2023 – Avril 2024 Consultant Cyber sécurité – Unilabs France (Paris)**

**Contexte :** Ingénierie en Cyber Sécurité

**Responsabilité :** Analyste SOC

**Réalisations**

* Piloter le scan d’équipements et remédiation des vulnérabilités remontées via Qualys (VMDR + WAS)
* Analyse et traitement des mails
* Threat hunting via splunk et SentinelOne
* Répondre aux incidents en cas d’attaques ou intrusions (SIRT TEAM)
* Traiter les demandes de ticketings sur la cybersécurité
* Audit active directory via Pingcastle.
* Faire évoluer le SI en matière de cybersécurité.
* Créer des règles de détection selon le besoin
* S’occuper de tous les lots de travaux techniques pour la cybersécurité (firewalling, reverse proxy, Serveurs, virtualisation, antivirus)
* Analyse et traitement des incidents de sécurité
* Veille sécuritaire sur les nouvelles attaques/menaces au monde
* Suivi des incidents de bout en bout et gestion de cycle de vie des tickets d'incident
* Proposition de l'intégration des solutions pour renforcer le niveau de sécurité
* Mise en place des campagnes de sensibilisation face aux enjeux de la cybersécurité
* Gestions des mots de passe, des comptes privilégiés, contrôle et supervision des sessions.

**Environnement : SentinelOne, Splunk, QUALYS, RSA, Bastion (wallix), Pingcastle, Proofpoint, F5, Palo Alto, ServiceNow**

**Février. 2022- Mars 2023 Consultant Cyber sécurité – Banque Postale**

**Contexte :** Analyste Cybersécurité

**Responsabilités :** Analyste SOC

**Réalisations**

Analyste SOC

* Qualifier les incidents remontés par le SIEM (levée de doutes, sévérité des incidents, impacts)
* Répondre aux incidents (CSIRT) lors d’incidents avérés
* Faire de l'investigation légale lorsque nécessaire (forensiques)
* Gérer les alertes DLP (fuite de données) en suivant le processus défini
* Administrer les outils du CSIRT (Antivirus, EDR, plateforme CTI, sandbox,)
* Prendre en charge les alertes escaladées par les autres niveaux du SOC (investigation depuis le SIEM et de nombreuses solutions de sécurité : anti DDOS, FW, antivirus, bastion traçant, solution EDR, métiers…)
* Réaliser des analyses de logs/paquets en profondeur,
* Participer et piloter la réponse à incident ;
* Faire la veille des menaces, traitement des vulnérabilités, analyse et traitement des IOC
* Identifier et gérer les incidents de sécurité
* Contribuer au renforcement de la cybersécurité
* Effectuer des analyses techniques détaillées sur des équipements systèmes, réseaux ou sécurité
* Mettre en place des KPI SOC
* Participer à l’amélioration des règles de détection existante
* Participer aux projets d’amélioration SOC
* Effectuer une veille sur les vulnérabilités, les nouvelles menaces et les Iocs

Analyse des vulnérabilités

* Analyser et qualifier les vulnérabilités
* Orienter les équipes techniques quant aux correctifs ou palliatifs à mettre en œuvre
* Documenter les bases de connaissances et procédures de traitement

**Environnements : Splunk, ServiceNow, SentinelOne, Qradar, Bastion(wallix), Qualys, Nessus, Palo Alto, F5 (ASM), Pingcastle, Bloodhound, Barracuda Email Security, DLP (Symantec)**