FLN

CONSULTANT SSI/ SOC (N2)

DOMAINES DE COMPÉTENCES

Savoir-faire	**Cybersécurité et SOC** • Gestion d'alertes • Analyse de logs (Splunk, SEKOIA.IO) • Forensique et analyse de malware (Volatility, FTK Imager) • Gestion des vulnérabilités (Qualys, Crowdstrike) • Veille et Renseignements (CTI) **Sécurité Offensive** • Tests d'intrusion (Burp, Metasploit) • Recherche et publication de CVE • Sensibilisation & Documentation **Documentations techniques** • Fiche Reflexes, Tableau de bord et KPI
Outils	• Langages : Python, C, C++, Java SE/EE, SQL, NoSQL • Programmation web : HTML, CSS, PHP, Spring MVC • Réseau : Mise en réseau d'appareils, Cisco, Wireshark, eSight NMS • Cloud : Microsoft Azure
Cybersécurité	• Outils : Hashcat, Graylog, TheHive, Mantis, Sekoia, Splunk, XSOAR, Crowdstrike, Qualys, CyberArk, MISP, LogPoint • Red team : Burp, Metasploit • Blue team : IDA, Volatility, PhotoRec, Zimmermann tools, FTK imager
OS	• Windows • Linux

DIPLÔMES

- **2019 :** Diplôme d'ingénieur informatique, majeure cybersécurité
- **2016 :** DUT informatique

FORMATIONS PROFESSIONNELLES & CERTIFICATIONS

- **2022** : Certification Security Analyst SEKOIA.IO, C301
- **2021** : Certification SPLUNK Fundamentals Level 2
- **2020** : Certification SPLUNK Fundamentals Level 1

LANGUES

- **Anglais :** Courant

EXPÉRIENCES PROFESSIONNELLES

CONSULTANT SSI (SOC) I Intrinsec

Depuis Mars 2020 (4 ans et 10 mois)

Contexte : Au sein de l'équipe MSSP SOC, composée de 12 analystes, j'avais la charge de la gestion des alertes de sécurité pour divers clients.

Mon rôle comprenait la qualification des alertes remontées par les SIEM, grâce à des règles corrélées via l'outil XSOAR de Cortex, ainsi que le dispatch hebdomadaire des tickets d'alertes, effectué en rotation et basé sur le calendrier des équipes, les compétences disponibles et la criticité des actifs.

Mission SOC (Security Operation Center)

Dans le cadre de la gestion des incidents de sécurité pour plusieurs clients, mon rôle consistait à analyser et traiter les alertes de sécurité tout en garantissant le respect des SLA et en proposant des améliorations continues des règles et processus.

Gestion des alertes :

- Analyse complète des alertes à partir de Cortex XSOAR (SIEM), Splunk, et Sekoia pour déterminer si elles constituaient des incidents avérés.
- Traitement de tickets de toutes criticités (faible à critique) au sein d'une équipe de 12 analystes.
- Investigation des signes de compromission (IOC) dans les logs corrélés pour valider les incidents, tels que des comportements malveillants ou légitimes :
    - Comportement légitime : Documentation dans XSOAR, clôture du ticket, et historisation pour un éventuel suivi dans le cadre d'une APT.
    - Comportement malveillant : Rédaction d'un rapport d'investigation détaillé pour le client, incluant des recommandations et un plan d'action pour évaluer l'impact sur le SI.

Astreinte SOC :

- Traitement des évènements en horaires non ouvrés (HNO) pour garantir une couverture 24/7 sur un périmètre réduit.

Amélioration continue :

- Proposition d'ajustements des règles SIEM et d'exclusions des comportements légitimes identifiés lors de l'exécution des playbooks, afin de réduire les faux positifs.
- Suivi des KPI, incluant la charge des analystes et les efforts d'amélioration continue.

Rôle de dispatch :

- Répartition hebdomadaire des tickets en fonction des priorités, des compétences des équipes, et des SLA.
- Suivi des actions prises et des demandes spécifiques des clients.

Exemples d'incidents avérés traités :

- Confidentialité : Usurpation d'identité détectée et traitée avec plan d'action.
- Intégrité : Compromission du SI par exploitation d'une vulnérabilité Ivanti.

Mission CTI (Cyber Threat Intelligence)

Dans le cadre des activités de renseignement sur les menaces, j'ai contribué à la collecte et à la gestion des informations sur les indicateurs de compromission (IOC) et à leur analyse pour améliorer la réponse aux incidents.

- Gestion des IOC dans la base interne MISP (ajout/suppression).
- Recherche d'indicateurs de compromission via des outils spécialisés tels que Sekoia, MISP, VirusTotal et divers outils open source…
- Contribution à la contextualisation des menaces et à l'amélioration des processus de

détection en intégrant les IOC pertinents dans les outils SOC.

Exemples de recherche liée aux menaces :

- Recherche d'IOC concernant diverses failles, tout aussi bien pour une 0 day (log4j), que pour un cas avéré (ivanti), afin de pouvoir investiguer, et vérifier s'il y pu avoir, ou non, exploitation de la faille.

Mission VOC (Vulnerability Operation Center)

Dans le cadre de la gestion des vulnérabilités pour plusieurs clients, mon rôle consistait à identifier, analyser et prioriser les failles de sécurité tout en proposant des recommandations adaptées pour réduire les risques.

- Gestion proactive des vulnérabilités identifiées via l'outil Qualys, en se concentrant sur celles de sévérité haute à critique.
- Analyse approfondie des résultats et traitement des vulnérabilités élevées et critiques en fonction du scoring CVSS.
- Réalisation de tests de vérification sur demande pour confirmer la validité des vulnérabilités détectées via des actions manuelles (scan…)
- Création de rapports détaillés pour les clients, comprenant :
  - Des commentaires sur les vérifications effectuées.
  - La priorisation des actions à mener.
  - Des recommandations sur les remédiations à mettre en place.
- Transmission des informations et recommandations aux Service Delivery Managers (SDM), qui se chargeaient de présenter et défendre ces préconisations auprès des clients.

Environnement Technique : Cortex XSOAR, Splunk, Sekoia, Crowdstrike, Qualys

Ingénieur SSI (CTI) I Alter Solutions

Octobre 2019 à mars 2020 (6 mois)

Contexte : Au sein de l'équipe de sécurité opérationnelle interne, mon rôle consistait à apporter un soutien technique et stratégique dans leurs missions quotidiennes. J'intervenais dans le cadre d'activités de veille et de sensibilisation pour renforcer la posture de cybersécurité interne.

Missions

- **Veille et renseignement en cybersécurité**
  - Réalisation d'une veille active sur les menaces émergentes, notamment sur les vulnérabilités critiques et les exploits zero-day.
  - Identification et contextualisation des indicateurs de compromission (IOC) via des outils tel que MISP.

- **Sensibilisation et formation**
  - Conception et animation d'une présentation détaillée du Top 10 OWASP, accompagnée d'une démonstration pratique via l'environnement DVWA, pour sensibiliser les équipes de développement aux principales failles de sécurité applicative.

- **Publication d'une CVE et recherche en sécurité**
  - Création d'un environnement de test sécurisé en bac à sable pour l'analyse de vulnérabilités (Machine virtuelle Windows avec PyInstaller).
  - Développement d'un Proof of Concept (PoC) pour l'exploitation d'une faille zero-day.
  - Publication de la CVE-2019-16784, mettant en lumière une vulnérabilité critique et son exploitation.
    https://github.com/advisories/GHSA-7fcj-pq9j-wh2r

Consultant SSI (SOC N1) I CGI

Mars 2019 à août 2019

Contexte : Au sein du SOC de CGI, entreprise de services et conseils en technologies de l'information, d'intégration de systèmes et de solutions

Missions :

- Gestion des alertes :
  - Analyse complète des évènements
  - Investigation des signes de compromission
  - Rédaction de documentation
- Configuration de LogPoint afin de réaliser un POC (Syslog & Nessus).
  - Création de tableaux de bords avec les données récupérées.

Environnement Technique : TheHive, Graylog, MantisBT, LogPoint

Ingénieur Réseau et Sécurité I SCC France (Stage)

Avril 2018 à septembre 2018

Contexte : En tant que stagiaire au sein de l'équipe Réseau & Communication, mon rôle consistait à contribuer à la sécurisation des infrastructures réseau et à la mise en place de solutions techniques pour garantir la disponibilité, la performance et la sécurité des systèmes.

Missions :

- Mise en place d'un VPN avec accès sécurisé sur une surface Cloud (Microsoft Azure)
- Configuration d'un outil de supervision d'équipement réseau (eSight NMS)

Environnement Technique : Microsoft Azure, eSight NMS

Développeur Web Fullstack I ISTA (Stage)

Avril 2016 à juin 2016

Contexte : En tant que stagiaire au sein de l'équipe web d'Ista, j'ai contribué au développement d'une plateforme administrative destinée à optimiser la gestion des données internes.

Missions :

- Développement et mise en place d'une plateforme administrative, permettant la récupération et affichage de données contenues dans leur base de données

Environnement Technique : HTML, CSS, PHP, Spring MVC