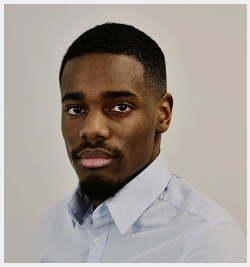

PROFIL

Analyste Cyber Threat Intelligence Junior , formé en cybersécurité et expérimenté en veille OSINT/dark web, collecte d'IoCs, analyse SIEM et gestion d'incidents. Motivé à renforcer la détection des menaces et la sécurité des systèmes d'information.

CONTACT

Sucy-en-Brie, 94

cmervilon@gmail.com

+33 7 81 59 37 43

https://www.linkedin.com/in/christopher-mervilon-b14668221/

FORMATIONS

Master Cybersecurité
Nexa Digital School | 2023 - 2025

Licence - Chef de Projet Logiciel & Réseaux
ESGI Paris | 2022 - 2023

CENTRES D'INTÉRÊT

- Football, Boxe
- Veille active sur les cybermenaces et vulnérabilités (CVE, actualités sécurité, hacktivisme)

Christopher MERVILON

Analyste Threat Intelligence & Threat Hunting

PROJETS

PROJET EN CYBER THREAT INTELLIGENCE - 2025

- Analyse de groupes APT via sources OSINT (X, Telegram, dark web), extraction d'IoC (IP, hash, URL), veille sur vulnérabilités critiques (CVE, CVSS), et simulation d'attaques en lab virtualisé (MITRE ATT&CK, Metasploit, Wireshark).
- Déploiement d'un environnement de threat hunting (MISP, Elastic, Sigma, YARA), avec intégration de flux TI (Anomali ThreatStream, Intel471, RecordedFuture, KELA) pour la détection de fuites, accès compromis et surveillance cybercriminelle.

Rédaction de livrables CTI orientés décision stratégique et réponse opérationnelle.

EXPERIENCES

ANALYSTE CYBER THREAT INTELLIGENCE & THREAT HUNTER

THREAT HUNTERS | 03/24 - 09/25 (ALTERNANCE + STAGE)

- Réalisation d'une veille OSINT et dark web (SpiderFoot, Shodan, OnionScan, Onyphe) sur les menaces ciblant les secteurs sensibles et sur les données compromises (identifiants, cartes bancaires, adresses).
- Extraction et analyse d'IoC (IP, domaines, hash, adresses e-mail frauduleuses) via VirusTotal, AbuseIPDB et EmailRep, avec intégration et enrichissement dans MISP et OpenCTI pour faciliter leur exploitation et partage.
- Corrélation avancée des IoC collectés avec les logs internes via SIEM pour identifier les expositions et comportements suspects, et alimenter les playbooks SOC pour automatiser le suivi des menaces.
- Participation active au Threat Hunting proactif : recherche de menaces latentes, simulation de scénarios MITRE ATT&CK et identification de nouvelles tactiques et techniques adverses.
- Gestion et suivi des incidents critiques et activités d'anti-fraude : coordination avec les équipes techniques pour remédier aux vulnérabilités et fuites de données, détection et remontée des fuites susceptibles d'alimenter des campagnes malveillantes, et production de rapports clairs avec recommandations pour renforcer les contrôles préventifs.

COMPÉTENCES

Cybersécurité & Threat Intelligence

Collecte IOC (MISP/OPENCTI, VirusTotal, AbuseIPDB et EmailRep) - SIEM (Splunk) - TTPs (MITRE ATT&CK) - Veille darkweb (Intel471/KELA, RecordedFuture, OnionScan, Onyphe) - OSINT (Maltego, TheHarvester, Shodan, SpiderFoot) - EDR (CrowdStrike Falcon) - Gestion incidents (TheHive, Cortex SOAR) - Règle de détection d'alerte (Sigma/YARA) - Scan de vulnérabilités (Nessus) - Analyse du trafic réseau (Wireshark, tcpdump)

CERTIFICATIONS

- Fortinet Certified Fundamentals Cybersecurity – Introduction to the Threat Landscape 3.0