ACHRAF HACHIMI

Analyste SOC N3 / CSIRT | Detection Engineering | CISSP

Ingénieur cybersécurité - Diplômé des Mines

+33 7 55 75 92 77 achraf-hachimi@live.fr linkedin.com/in/achraf-hachimi-33572910b
cybersec-ops.org

PROFIL PROFESSIONNEL

Ingénieur cybersécurité avec **8 ans d'expérience** en environnements critiques : banque / asset management, retail et aéronautique défense. Profil orienté **SOC N3 / CSIRT**, avec expérience concrète en **qualification d'alertes**, **investigation d'incidents**, **detection engineering**, **amélioration de règles SIEM**, **EDR/XDR**, gestion des vulnérabilités, automatisation et remédiation.

J'interviens actuellement chez **La Banque Postale Asset Management** sur le RUN SOC / CSIRT, le tuning des alertes **Defender XDR**, **Cybereason**, **Vectra**, **Fortinet**, **Barracuda**, **Purview** et **Splunk ES**, ainsi que sur la migration opérationnelle **Cybereason vers Microsoft Defender** et la mise en place de pipelines de logs Linux, vCenter, firewalls et VPN vers Splunk. Chez **E.Leclerc**, j'ai travaillé comme **analyste SOC N3 / CSIRT** sur SentinelOne, Splunk ES, **Cortex XSOAR**, WAF, vulnérabilités et investigations avancées.

Réalisations clés pour une mission SOC N3 :

- **RUN SOC / CSIRT :** triage, analyse, qualification et suivi d'alertes malware, phishing, exfiltration, comportements endpoint suspects, signaux DLP et événements réseau / identité.
- **EDR / XDR :** investigations et tuning sur **Microsoft Defender XDR**, **Cybereason**, **SentinelOne**, **Vectra NDR**, **Fortinet**, **Barracuda** et **Microsoft Purview**.
- **Detection engineering :** création et amélioration de règles **Splunk ES**, recherches **SPL**, Notable Events, dashboards, corrélation SIEM / EDR / NDR / DLP, réduction des faux positifs.
- **Logs & visibilité :** implémentation d'une chaîne **rsyslog / filebeat / logstash / kibana** pour ingestion de logs Linux, vCenter, firewalls et VPN vers **Splunk**.
- **SOAR & automatisation :** playbooks de triage, enrichissement IOC / CTI, automatisation Python, APIs VirusTotal / MISP, ticketing, escalade N2/N3 et capitalisation RETEX.
- **Vulnérabilités & remédiation :** qualification CVE, priorisation CVSS / criticité métier, suivi des plans de remédiation, traitement des rapports de pentest et incidents post-exploitation.
- **Forensic & mindset offensif :** analyse d'artefacts, mails de phishing, timelines d'incident, compréhension des TTPs **MITRE ATT&CK** et exploitation des signaux faibles.

Certifications : CISSP (2026) – ISO 27001 Lead Implementer (2023) – Blue Team Level 1 (2024) – Splunk Enterprise Certified Admin (2024) – Splunk Core Certified Power User (2024)

COMPÉTENCES TECHNIQUES

SOC, SIEM & Detection
- Splunk ES, dashboards
- SPL, Notable Events
- KQL / Defender hunting
- Règles de corrélation
- Triage et qualification
- Incident response
- Threat hunting
- MITRE ATT&CK
- IOC / CTI
- RETEX et documentation

EDR, XDR & outils sécurité
- Microsoft Defender XDR
- Cybereason EDR
- SentinelOne EDR
- SentinelOne Deep Visibility
- Vectra NDR
- Fortinet IPS/IDS
- Barracuda Email Security
- Microsoft Purview / DLP
- F5 ASM / WAF
- Qualys, Rapid7

Automation & Infrastructure
- Cortex XSOAR / playbooks
- Python, PowerShell
- API VirusTotal / MISP
- rsyslog, filebeat
- logstash, kibana
- Linux, Windows Server
- Active Directory, Entra ID
- VMware / vCenter
- Wallix, Zscaler
- Fortinet, Palo Alto

EXPÉRIENCE PROFESSIONNELLE

Juil 2025 - Présent

1 an

Lead Security Engineer / SOC-CSIRT & XDR — La Banque Postale Asset Management

Paris, France - Full-time

Lead Security Engineer au sein de **La Banque Postale Asset Management**, acteur de la gestion institutionnelle et privée, avec responsabilité opérationnelle sur le **SOC / CSIRT**, les contrôles **XDR / EDR / NDR / SIEM**, la visibilité logs, l'IAM central et la posture de sécurité Microsoft / Azure.

RUN SOC / CSIRT et investigation

- **Qualification d'alertes :** triage L2/L3, analyse et traitement d'alertes **malware**, **phishing**, **exfiltration**, comportements endpoint suspects, événements identité et signaux DLP/Purview.
- **EDR/XDR :** investigations quotidiennes et suivi de remédiation sur **Microsoft Defender XDR**, **Cybereason**, **Vectra**, **Fortinet**, **Barracuda**, **Microsoft Purview** et **Splunk ES**.
- **Migration Cybereason vers Defender :** contribution à la transition opérationnelle, comparaison des comportements d'alertes, validation de couverture et handover vers le run SOC.
- **Gestion d'incidents :** coordination avec les équipes infrastructure, IAM, réseau et production pour qualifier l'impact, contenir les risques et suivre les actions correctives.

Detection engineering, règles et pipeline logs

- **Création et amélioration de règles :** conception de scénarios de détection SOC, tuning des règles existantes, réduction des faux positifs et documentation du fonctionnement des use cases.
- **Splunk & visibilité :** mise en place d'une chaîne **rsyslog / filebeat / logstash / kibana** pour collecter et normaliser les logs **Linux**, **vCenter**, **firewalls** et **VPN** avant ingestion dans **Splunk**.
- **Corrélation et dashboards :** exploitation des logs endpoint, réseau, identité, DLP et infrastructure pour produire des dashboards, accélérer la qualification et alimenter les indicateurs SOC.
- **Capitalisation :** production de consignes de triage, documentation de règles, reporting, RETEX et supports de transfert vers les analystes / équipes opérationnelles.

Defender XDR | Cybereason | Splunk ES | SPL | KQL | Vectra | Fortinet | Barracuda | Purview | Detection Engineering | rsyslog | filebeat | logstash | kibana

Avr 2022 - Juin 2025

3 ans 3 mois

Ingénieur Cybersécurité & Analyste SOC N3 — E.Leclerc

Toulouse, France - Full-time

Ingénieur sécurité et CSIRT SOC N3 spécialisé en réponse à incident avancée, intégration d'outils de sécurité et amélioration continue des capacités SOC : EDR, SIEM, SOAR, WAF, bastion, PKI/MFA et gestion des vulnérabilités.

Analyse SOC N3, EDR et réponse à incident

- **Investigation approfondie :** analyse cross-platform avec **Splunk ES**, corrélation de logs endpoint / réseau / identité, exploitation **SentinelOne Deep Visibility** et hunting basé sur **MITRE ATT&CK**.
- **SentinelOne EDR :** design de l'architecture de déploiement sur **7k+ endpoints**, définition des policies, suivi de couverture agent et investigation des problèmes de performance / compatibilité lors du rollout.
- **Détection Splunk :** développement de règles de corrélation complexes, recherches **SPL**, macros, lookups, KV Store, Notable Events, dashboards et réduction des faux positifs.
- **Forensic et phishing :** analyse d'artefacts, analyse de mails suspects, reconstruction de timelines et qualification d'incidents applicatifs / endpoint.

SOAR, automatisation et capitalisation

- **Automatisation SOAR / Cortex XSOAR :** mise en place de playbooks de triage, enrichissement IOC / CTI, qualification d'alertes web et SI interne, ticketing et escalade vers les niveaux N2/N3.
- **Enrichissement automatisé :** scripts **Python**, APIs **VirusTotal / MISP**, contextualisation des menaces et réduction du temps de qualification.
- **Documentation opérationnelle :** rédaction de DAT/DEX, procédures d'exploitation, consignes de triage et supports de handover pour les équipes SOC / support.

Vulnérabilités, WAF et remédiation

- **VOC :** interface avec Orange Cyber Défense, cartographie des assets, qualification CVE, priorisation CVSS / criticité métier et suivi de remédiation.
- **Post-incident et pentest :** traitement de vulnérabilités exploitées ou issues de rapports d'audit, coordination des plans correctifs avec les équipes de production et développement.
- **WAF / anti-bot :** exploitation des signaux **F5 ASM**, Fortinet, Palo Alto et Datadome pour qualification d'alertes applicatives et amélioration des règles de protection web.

Splunk ES | SPL | SentinelOne | Deep Visibility | Cortex XSOAR | SOAR | Playbooks | Python | VirusTotal | MISP | F5 ASM | Datadome | Qualys | Rapid7 | MITRE ATT&CK

Suite

E.Leclerc

Identité, accès et architecture défensive utiles au SOC

— **PKI / MFA :** infrastructure multi-tiers **Windows Server / ADCS**, CA racine offline, CA intermédiaire, YubiKey avec certificats X.509 et intégration Cisco ISE AAA/RADIUS.

— **Accès privilégiés :** bastion **Wallix**, élévation de privilèges, session recording, contrôle des accès administratifs et contribution aux investigations sur usages sensibles.

— **Hardening authentification :** Kerberos hardening, LDAP Secure, désactivation NTLM legacy et application de recommandations ANSSI / GPO.

— **Pilotage opérationnel :** animation de points techniques, support N3 pour débloquer les incidents complexes, arbitrage sécurité et reporting SOC / RSSI.

Wallix | ADCS | YubiKey | Cisco ISE | RADIUS | Kerberos | LDAP Secure | Windows Server | ANSSI | GPO

Juil 2020 - Mars 2022

1 an 9 mois

Ingénieur SecOps, Designer DLP — AIRBUS

Toulouse, France - Full-time

Ingénieur SecOps DLP sur un programme stratégique européen de protection des données : refonte des politiques **Forcepoint** et migration **Netskope** pour **147 000 utilisateurs** répartis sur **37 sites internationaux**. Expérience centrée sur l'investigation, l'analyse de logs, le tuning de règles et la réduction des faux positifs sur incidents de fuite de données.

— **Investigation DLP :** analyse d'événements de fuite de données, qualification des incidents, audit trails et suivi des remédiations.

— **Règles et faux positifs :** refonte des règles Forcepoint / Netskope, tests en production, rollout progressif, analyse Splunk des règles fantômes et consolidation des règles bruitées.

— **Automatisation :** scripts Python, APIs Netskope / Forcepoint, génération de règles, dashboards de monitoring et reporting opérationnel.

— **Déploiement agents :** propagation via SCCM, analyse des logs d'audit dans Splunk et activation progressive des blocages par population.

— **Contexte réglementé :** politiques adaptées aux données **ITAR**, **EAR**, **TOP SECRET**, **CONFIDENTIEL DÉFENSE** et **OTAN**.

Forcepoint DLP | Netskope | CASB | Splunk | Python | API REST | SCCM | ITAR | EAR | Classification

Juil 2018 - Juin 2020

2 ans

Ingénieur Réseau Sécurité — AIRBUS

Toulouse, France - Full-time

Ingénieur réseau sécurité sur infrastructure critique aéronautique : orchestration firewall multi-vendors, segmentation, PKI X.509, Cisco ISE, AAA RADIUS et supervision. Expérience utile pour l'analyse SOC des flux, événements réseau, accès et causes racines.

- **Segmentation et filtrage :** matrices de flux, VLAN, politiques firewall et gestion de changements via **Tufin SecureChange**.
- **Contrôle d'accès :** administration **Cisco ISE**, profilage endpoints, AAA RADIUS, authentification certificats et affectation VLAN dynamique.
- **PKI / certificats :** déploiement X.509 sur 10k points d'accès, cycle de vie certificats, validation CRL/OCSP.
- **Troubleshooting :** analyse d'incidents réseau, supervision SNMP, coordination avec équipes infrastructure et remédiation de configurations à risque.

Tufin | Palo Alto | Fortinet | CheckPoint | Cisco ISE | RADIUS | TACACS+ | X.509 | SNMP | ITIL

PROJETS SOC, AUTOMATION & OFFENSIVE

ThePhishAnalyzer / phishing.cybersec-ops.org — Workbench d'investigation phishing pour analystes SOC

- Accélération du triage de mails suspects : parsing EML/RFC822, SPF/DKIM/DMARC, extraction d'URL, détection d'incohérences, scoring de risque et synthèse analyste.
- Enrichissement Barracuda LinkProtect, Cortex, OSINT/réputation, analyse de pièces jointes et préparation de preuves pour investigation.

SOC Automation | Phishing Analysis | EML Parsing | Barracuda | Cortex | OSINT | TypeScript

Ghost-Hunter — Prototype RAG/LLM pour triage sécurité applicative

- Extension Burp Suite assistée par IA pour capturer le trafic, filtrer par scope et proposer des scénarios de test contextualisés depuis une base de connaissance AppSec.
- Apport SOC : meilleure compréhension des attaques web, enrichissement des scénarios de détection et qualification plus fine des alertes applicatives.

Burp Suite | Python | RAG | Llama 3 | WAF Bypass | AppSec

FORMATION

2014 - 2020

Diplôme d'Ingénieur - ECOLE NATIONALE SUPÉRIEURE DES MINES-TÉLÉCOMS DE LILLE

Sciences et Technologies de l'Informatique et des Télécommunications | Lille, France

— Spécialisation en cybersécurité et administration des réseaux.

— Réseaux & protocoles : IPv6, MPLS, RIP, OSPF, BGP, supervision SNMP.

— Sécurité des systèmes : SSL/TLS, Kerberos, PGP, RGPD/CNIL et SMSI.

CERTIFICATIONS

À PROPOS

— **Langues :** Français natif, anglais courant (C1), espagnol intermédiaire.

— **Événements :** CISSP Barcelone 2026, CBC Toulouse 2025, THCON & CTF Toulouse 2025 (16/182), Hack in Paris 2023, FIC Lille 2022 & 2019.

— **Centres d'intérêt :** CTF, Root-Me, HackTheBox, veille menace, scripts d'automatisation sécurité et règles SIEM.