

ACHRAF HACHIMI

SOC N3 / CSIRT Analyst | Detection Engineering | CISSP

Cybersecurity Engineer - Mines Engineering Graduate

☎ +33 7 55 75 92 77

✉ achraf-hachimi@live.fr

in [linkedin.com/in/achraf-hachimi-33572910b](https://www.linkedin.com/in/achraf-hachimi-33572910b)

🌐 cybersec-ops.org

👤 PROFESSIONAL PROFILE

Cybersecurity engineer with **8 years of experience** in critical environments across banking / asset management, retail, and defense aerospace. SOC-oriented profile with hands-on experience in **alert qualification, incident investigation, detection engineering, SIEM rule improvement, EDR/XDR, vulnerability management, automation, and remediation.**

I currently work at **La Banque Postale Asset Management** on SOC / CSIRT run activities, alert tuning across **Defender XDR, Cybereason, Vectra, Fortinet, Barracuda, Purview, and Splunk ES**, as well as the operational migration from **Cybereason to Microsoft Defender** and log pipelines from Linux, vCenter, firewalls, and VPNs into Splunk. At **E.Leclerc**, I worked as a **SOC N3 / CSIRT analyst** on SentinelOne, Splunk ES, **Cortex XSOAR**, WAF, vulnerabilities, and advanced investigations.

Key strengths for SOC N3 roles:

- **SOC / CSIRT run:** triage, analysis, qualification, and follow-up of malware, phishing, exfiltration, suspicious endpoint behavior, DLP signals, and network / identity events.
- **EDR / XDR:** investigations and tuning on **Microsoft Defender XDR, Cybereason, SentinelOne, Vectra NDR, Fortinet, Barracuda, and Microsoft Purview.**
- **Detection engineering:** creation and improvement of **Splunk ES** rules, **SPL** searches, Notable Events, dashboards, SIEM / EDR / NDR / DLP correlation, and false-positive reduction.
- **Logs & visibility:** implementation of a **rsyslog / filebeat / logstash / kibana** chain to ingest Linux, vCenter, firewall, and VPN logs into **Splunk**.
- **SOAR & automation:** **Cortex XSOAR** playbooks for triage, IOC / CTI enrichment, Python automation, VirusTotal / MISP APIs, ticketing, N2/N3 escalation, and lessons learned.
- **Vulnerability & remediation:** CVE qualification, CVSS / business-criticality prioritization, remediation tracking, pentest report handling, and post-exploitation incident follow-up.
- **Forensics & offensive mindset:** artifact analysis, phishing email analysis, incident timelines, understanding of **MITRE ATT&CK** TTPs, and weak-signal analysis.

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

TECHNICAL SKILLS

SOC, SIEM & Detection

- Splunk ES, dashboards
- SPL, Notable Events
- KQL / Defender hunting
- Correlation rules
- Triage and qualification
- Incident response
- Threat hunting
- MITRE ATT&CK
- IOC / CTI
- RETEX and documentation

EDR, XDR & Security Tools

- 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
- VirusTotal / MISP APIs
- rsyslog, filebeat
- logstash, kibana
- Linux, Windows Server
- Active Directory, Entra ID
- VMware / vCenter
- Wallix, Zscaler
- Fortinet, Palo Alto

PROFESSIONAL EXPERIENCE

Jul 2025 - Present
1 year

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

Paris, France - Full-time

Lead Security Engineer at **La Banque Postale Asset Management**, with operational responsibility across **SOC / CSIRT, XDR / EDR / NDR / SIEM** controls, log visibility, central IAM, and Microsoft / Azure security posture.

SOC / CSIRT run and investigation

- **Alert qualification:** L2/L3 triage, analysis, and handling of **malware, phishing, exfiltration**, suspicious endpoint behavior, identity events, and DLP/Purview signals.
- **EDR/XDR:** daily investigations and remediation follow-up on **Microsoft Defender XDR, Cybereason, Vectra, Fortinet, Barracuda, Microsoft Purview**, and **Splunk ES**.
- **Cybereason to Defender migration:** contributed to the operational transition, compared alert behavior, validated detection coverage, and prepared SOC run handover.
- **Incident handling:** coordination with infrastructure, IAM, network, and production teams to qualify impact, contain risks, and track corrective actions.

Detection engineering, rules and log pipeline

- **Detection use cases:** design of SOC detection scenarios, tuning of existing rules, false-positive reduction, and documentation of use-case logic.
- **Splunk & visibility:** implementation of a **rsyslog / filebeat / logstash / kibana** chain to collect and normalize **Linux, vCenter, firewall**, and **VPN** logs before ingestion into **Splunk**.
- **Correlation and dashboards:** use of endpoint, network, identity, DLP, and infrastructure logs to build dashboards, speed up qualification, and feed SOC metrics.
- **Knowledge base:** triage guidance, detection rule documentation, reporting, lessons learned, and handover material for analysts and operations teams.

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

Apr 2022 - Jun 2025
3 years 3 months

Cybersecurity Engineer & SOC N3 Analyst — E.Leclerc

Toulouse, France - Full-time

Security engineer and SOC N3 / CSIRT analyst focused on advanced incident response, security tooling integration, and continuous improvement of SOC capabilities: EDR, SIEM, SOAR, WAF, bastion, PKI/MFA, and vulnerability management.

SOC N3 analysis, EDR and incident response

- **Deep investigation:** cross-platform analysis with **Splunk ES**, endpoint / network / identity log correlation, **SentinelOne Deep Visibility**, and **MITRE ATT&CK**-based hunting.
- **SentinelOne EDR:** deployment architecture design across **7k+ endpoints**, policy definition, agent coverage tracking, and investigation of performance / compatibility issues during rollout.
- **Splunk detection:** development of complex correlation rules, **SPL** searches, macros, lookups, KV Store, Notable Events, dashboards, and false-positive reduction.
- **Forensics and phishing:** artifact analysis, suspicious email analysis, timeline reconstruction, and qualification of application / endpoint incidents.

SOAR, automation and knowledge capitalization

- **SOAR / Cortex XSOAR automation:** implementation of triage playbooks, IOC / CTI enrichment, web and internal IT alert qualification, ticketing, and escalation to N2/N3 teams.
- **Automated enrichment:** **Python** scripts, **VirusTotal** / **MISP** APIs, threat contextualization, and reduction of qualification time.
- **Operational documentation:** DAT/DEX, operating procedures, triage guidance, and handover material for SOC and support teams.

Vulnerabilities, WAF and remediation

- **VOC:** interface with Orange Cyberdefense, asset mapping, CVE qualification, CVSS / business-criticality prioritization, and remediation tracking.
- **Post-incident and pentest follow-up:** handling of exploited vulnerabilities or audit findings, coordination of corrective plans with production and development teams.
- **WAF / anti-bot:** use of **F5 ASM**, Fortinet, Palo Alto, and Datadome signals to qualify application alerts and improve web protection rules.

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

Continued
E.Leclerc

Identity, access and defensive architecture supporting the SOC

- **PKI / MFA:** multi-tier **Windows Server** / **ADCS** infrastructure, offline Root CA, intermediate CA, YubiKey with X.509 certificates, and Cisco ISE AAA/RADIUS integration.
- **Privileged access:** **Wallix** bastion, privilege elevation, session recording, administrative access control, and investigation support on sensitive usage.
- **Authentication hardening:** Kerberos hardening, LDAP Secure, NTLM legacy reduction, and ANSSI / GPO recommendations.
- **Operational steering:** weekly technical meetings, N3 support for complex incidents, security arbitration, and SOC / CISO reporting.

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

Jul 2020 - Mar
2022
1 year 9 months

SecOps Engineer, DLP Designer — AIRBUS

Toulouse, France - Full-time

DLP SecOps engineer on a strategic European data protection program: re-design of **Forcepoint** policies and **Netskope** migration for **147,000 users** across **37 international sites**. Experience focused on investigation, log analysis, rule tuning, and false-positive reduction for data leakage incidents.

- **DLP investigation:** analysis of data leakage events, incident qualification, audit trails, and remediation follow-up.
- **Rules and false positives:** Forcepoint / Netskope rule redesign, production testing, progressive rollout, Splunk analysis of unused rules, and consolidation of noisy rules.
- **Automation:** Python scripts, Netskope / Forcepoint APIs, rule generation, monitoring dashboards, and operational reporting.
- **Agent deployment:** deployment through SCCM, audit log analysis in Splunk, and progressive activation of blocking policies by user population.
- **Regulated context:** policies adapted to **ITAR**, **EAR**, **TOP SECRET**, **CONFIDENTIAL DEFENSE**, and **NATO** data.

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

Jul 2018 - Jun 2020
2 years

Network Security Engineer — AIRBUS

Toulouse, France - Full-time

Network security engineer on critical aerospace infrastructure: multi-vendor firewall orchestration, segmentation, X.509 PKI, Cisco ISE, AAA RADIUS, and monitoring. This background supports SOC analysis of flows, network events, access issues, and root causes.

- **Segmentation and filtering:** flow matrices, VLANs, firewall policies, and change management through **Tufin SecureChange**.
- **Access control:** **Cisco ISE** administration, endpoint profiling, AAA RADIUS, certificate authentication, and dynamic VLAN assignment.
- **PKI / certificates:** X.509 deployment across 10k access points, certificate lifecycle, and CRL/OCSP validation.
- **Troubleshooting:** network incident analysis, SNMP monitoring, coordination with infrastructure teams, and remediation of risky configurations.

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

🔗 SOC, AUTOMATION & OFFENSIVE PROJECTS

ThePhishAnalyzer / phishing.cybersec-ops.org — Phishing investigation workbench for SOC analysts

- Faster suspicious email triage: EML/RFC822 parsing, SPF/DKIM/DMARC, URL extraction, inconsistency detection, risk scoring, and analyst summary.
- Barracuda LinkProtect, Cortex, OSINT/reputation enrichment, attachment analysis, and evidence preparation for investigation.

SOC Automation Phishing Analysis EML Parsing Barracuda Cortex OSINT TypeScript

Ghost-Hunter — RAG/LLM prototype for application security triage

- AI-assisted Burp Suite extension to capture traffic, filter by scope, and suggest contextualized test scenarios from an AppSec knowledge base.
- SOC value: better understanding of web attacks, richer detection scenarios, and more precise qualification of application alerts.

Burp Suite Python RAG Llama 3 WAF Bypass AppSec

EDUCATION

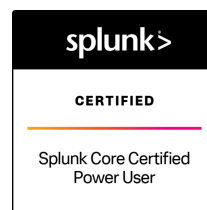
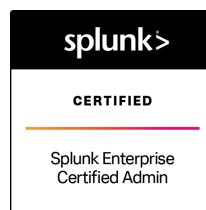
2014 - 2020

Engineering Degree - École Nationale Supérieure des Mines-Télécoms de Lille

Computer Science and Telecommunications Engineering / Lille, France

- Specialized in cybersecurity and network administration.
- Networks & protocols: IPv6, MPLS, RIP, OSPF, BGP, and SNMP monitoring.
- Systems security: SSL/TLS, Kerberos, PGP, GDPR/CNIL, and ISMS fundamentals.

CERTIFICATIONS



ABOUT

- **Languages:** French native, English fluent (C1), Spanish intermediate.
- **Events:** CISSP Barcelona 2026, CBC Toulouse 2025, THCON & CTF Toulouse 2025 (ranked 16/182), Hack in Paris 2023, FIC Lille 2022 & 2019.
- **Interests:** CTF, Root-Me, HackTheBox, threat intelligence, security automation scripts, and SIEM detection rules.