ACHRAF HACHIMI

Ingénieur en Cybersécurité | CISSP

Diplômé des Mines

+33 7 55 75 92 77 achraf-hachimi@live.fr linkedin.com/in/achraf-hachimi

PROFIL PROFESSIONNEL

Consultant en cybersécurité avec 6 ans d'expérience en infrastructures critiques à large échelle : Retail et aéronautique défense.

Réalisations clés :

— **Ingénieur Sécurité & CSIRT E.Leclerc :** Investigation incidents SOC N3, SIEM Splunk ES (SPL, Notable Events, dashboards), EDR SentinelOne (7k+ endpoints), WAF F5 ASM, Bastion Wallix. VOC & Gestion des vulnérabilités.

— **Innovation Offensive (Ghost-Hunter) :** Conception d'un agent de pentest autonome couplant Burp Suite à une architecture RAG/LLM (Llama 3) entraînée sur 13k+ rapports de Bug Bounty (10 bug report YesWeHack en 2 semaines)

— **PKI Enterprise & IAM :** Infrastructure PKI interforêts Windows Server 2025 Core, CA intermédiaire ADCS, authentification MFA YubiKey, intégration Cisco ISE AAA RADIUS pour 10k utilisateurs.

— **Designer DLP Airbus :** Refonte complète politiques Forcepoint et migration Netskope pour 147k utilisateurs. Gestion données classifiées ITAR/EAR/TOP SECRET/OTAN.

— **VOC E.Leclerc :** Pilotage du Vulnerability Operations Center avec Orange Cyber Défense (OCD). Qualification CVE, priorisation CVSS, suivi de remédiation et traitement des rapports de pentest.

— **Architecture Réseau Sécurisée Airbus :** Orchestration firewall Tufin (Palo Alto, Fortinet, Check-Point), déploiement PKI X.509 sur 10k points d'accès.

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

Sécurité & SOC

— SIEM : Splunk ES
— SOAR : Cortex
— EDR : SentinelOne
— IPS/IDS : Snort
— WAF : F5 ASM
— Scanners : Qualys
— Firewall : Palo Alto
— Bastion : Wallix
— Bug Bounty

Infrastructure

— AAA : Cisco ISE
— DLP : Forcepoint
— Netskope
— Admin : SNMP, IPv6
— PKI : ADCS, YubiKey
— Tufin
— PowerShell, Python

Systèmes & Compliance

— Windows Server
— Active Directory
— GPO, ADCS
— Kerberos, LDAP
— ANSSI, ISO 27001
— CIS Benchmarks
— ITAR, EAR, OTAN
— RGPD
— CISSP

EXPÉRIENCE PROFESSIONNELLE

Avr 2023 - Présent

2 ans 8 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 de solutions de sécurité (EDR, WAF, Bastion, CISCO ISE, MFA PKI) et conception d'architectures sécurisées conformes ANSSI pour environnements critiques.

Architecture & Intégration Sécurité

- **Stratégie & Conception :** Challenge de l'expression du besoin, conception et architecture de sécurité, benchmark de solutions et garantie de l'alignement des choix techniques avec la stratégie de sécurité globale. Rédaction des documents d'architecture (DAT), d'implémentation et d'exploitation (DEX), en étroite collaboration avec les équipes techniques.
- **Endpoint Security (EDR SentinelOne) :** Design de l'architecture de déploiement (7k+ endpoints), définition des stratégies de protection (policies) et intégration des capacités de réponse automatisée.
- **Sécurité Périmétrique (F5 ASM, Fortinet, Palo Alto) :** Conception des architectures de micro-segmentation, implémentation des règles WAF (protection OWASP Top 10, bot mitigation via Datadome) et Threat Prevention.
- **Privileged Access Management (Bastion Wallix) :** Définition de l'architecture d'accès sécurisé, gestion des élévations de privilèges et extension du périmètre de session recording (PAM).
- **Sécurité Offensive (Bug Bounty YesWeHack) :** Cadrage des programmes de Bug Bounty, coordination technique avec les chercheurs, triage des vulnérabilités et accompagnement des équipes sur les plans de remédiation.

Analyse & Réponse à Incident (SOC N3)

- **Investigation approfondie & Threat Hunting :** Analyse cross-platform (SIEM Splunk ES, dashboards custom), corrélation de logs (EDR SentinelOne Deep Visibility) et hunting proactif basé sur les TTPs du framework **MITRE ATT&CK**.
- **Detection Engineering & Splunk :** Développement de règles de corrélation complexes (SPL avancé, macros, lookups, KV Store), Notable Events customisés, réduction du bruit (False Positives) et création de cas d'usage alignés sur les risques métiers.
- **Automatisation & CTI :** Enrichissement automatisé des alertes (Python, API VirusTotal/MISP) et intégration de flux de Threat Intel pour contextualiser les menaces.
- **Forensique :** Analyse d'artefacts, analyse de mails de phising, analyse mémoire et reconstruction de timeline pour incidents majeurs.

Gestion des Vulnérabilités & Remédiation (VOC)

- **Pilotage VOC :** Interface avec Orange Cyber Défense (OCD) pour le mapping exhaustif du parc informatique (assets, versions, configurations). Collecte et centralisation des vulnérabilités identifiées sur l'ensemble du SI.
- **Qualification & Priorisation :** Requalification des CVE selon scoring CVSS, contexte métier et recommandations éditeurs. Définition des priorités de remédiation en fonction de la criticité et de l'exposition des assets.
- **Suivi de remédiation :** Proposition de workarounds ou patchs aux équipes de production. Accompagnement et suivi end-to-end jusqu'à résolution avec reporting d'avancement régulier.

Suite E.Leclerc

Suite Gestion des Vulnérabilités (VOC)

— **Traitement rapports de pentest :** Analyse des vulnérabilités identifiées par les auditeurs externes, requalification, priorisation et coordination du plan de remédiation avec les équipes de développement.

— **Remédiation post-incident :** En cas d'exploitation d'une vulnérabilité détectée par le SOC, pilotage de la remédiation d'urgence et suivi du déploiement des correctifs critiques.

— **Outils & Reporting :** Qualys, Rapid7 InsightVM, dashboards Splunk pour KPIs et pilotage VOC.

PKI & Gestion Identités

— **Infrastructure PKI Enterprise :** architecture multi-tiers Windows Server 2025 Core, CA racine offline, CA intermédiaire ADCS

— **Authentification forte MFA :** intégration YubiKey avec certificats X.509, déploiement 10k utilisateurs

— **Cisco ISE AAA :** authentification RADIUS, profilage endpoints, affectation VLAN dynamique via certificats

— **Gestion certificats avancée :** émission automatisée, révocation CRL/OCSP, renouvellement automatique, monitoring expiration

— **Sécurisation authentification :** Kerberos hardening, LDAP Secure, désactivation NTLM legacy

Pilotage & Gestion de Projet

— **Projet MFA :** Suivi et pilotage du projet d'authentification forte. Organisation des kick-off avec sponsors et parties prenantes, coordination des livrables et jalons.

— **Pilotage périmètre pilote :** Animation des points hebdomadaires avec les équipes de build. Support N3 pour débloquer les points techniques, arbitrage sur les sujets sécurité et gestion des tickets de support Microsoft.

Conformité & Gouvernance

— **Framework ANSSI :** application recommandations hardening Windows (GPO), cloisonnement SI administration

— **Documentation technique :** architecture, procédures opérationnelles

— **Audits et reporting :** rapport métriques SOC, dashboards Splunk, présentations RSSI/COMEX

Splunk ES | SPL | Notable Events | Splunk Dashboards | SentinelOne | F5 ASM | Wallix | Fortinet | Palo Alto | Cisco ISE | RADIUS | ADCS | YubiKey | Windows Server 2025 | PowerShell | ANSSI | MITRE ATT&CK | Qualys | Rapid7

Févr 2022 - Avr 2023

1 an 3 mois

Ingénieur SecOps, Designer DLP — AIRBUS

Toulouse, France - Full-time

Ingénieur SecOps DLP pour programme stratégique européen de protection des données : refonte complète des politiques DLP Forcepoint et Netskope pour 147 000 utilisateurs répartis sur 37 sites internationaux. Gestion données classifiées ITAR, EAR, TOP SECRET, CONFIDENTIEL DÉFENSE, OTAN avec conformité réglementaire export control.

- **Architecture DLP Enterprise :** Conception politiques de prévention de fuite de données, classification automatique, EDM/IDM fingerprinting
- **Migration Forcepoint vers Netskope :** Refonte 100% des règles, tests en environnement de production, rollout progressif par site
- **Gestion données sensibles :** Politiques pour données ITAR (International Traffic in Arms Regulations), EAR (Export Administration Regulations), TOP SECRET DÉFENSE, CONFIDENTIEL DÉFENSE, OTAN RESTRICTED, avec audit trails complets
- **Intégration SSE (Security Service Edge) :** Configuration Netskope CASB, DLP cloud-native, inspection SSL/TLS, politique zero-trust
- **Automatisation & orchestration :** Scripts Python pour génération règles, API Netskope/Forcepoint, dashboards monitoring temps réel
- **Formation & sensibilisation :** Support utilisateurs 147k personnes, documentation technique, formation équipes SecOps locales (37 sites)
- **Forcepoint DLP Cloud - Audit Continu :** PoC et implémentation chez Airbus Helicopters d'un outil d'audit continu des espaces de stockage cloud. Scan automatisé des fichiers, classification des données sensibles (auto-labeling) et analyse des droits d'accès associés.
- **Extension Périmètre DLP :** Déploiement DLP sur nouveaux périmètres Airbus Commercial soumis aux mêmes réglementations export control. Installation tenants Forcepoint, propagation agents via SCCM, analyse audit trail sur Splunk et activation progressive des blocages par population cible.
- **Optimisation Arbre de Règles :** Refactorisation complète pour améliorer performances et efficacité opérationnelle. Analyse Splunk des règles (règles fantômes, +80% faux positifs), consolidation par dictionnaires/classifications similaires, réorganisation de l'arbre (bypass/blocages en priorité haute, règles OCR/matching précis en fin de chaîne).

Forcepoint DLP | Netskope | CASB | Python | API REST | ITAR | EAR | Classification | EDM | Fingerprint | Auto-labeling | SCCM | Splunk

Oct 2020 - Févr 2022

1 an 5 mois

Ingénieur Réseau Sécurité — AIRBUS

Toulouse, France - Full-time

Ingénieur réseau sécurité pour infrastructure critique aéronautique : orchestration firewall multi-vendors (Tufin), déploiement PKI X.509 sur 10k points d'accès, administration Cisco ISE (authentification AAA RADIUS), et gestion infrastructure réseau sécurisée (segmentation L2/L3, VLAN, BGP, MPLS).

- **Architecture réseau :** Segmentation L2/L3, plan VLAN, matrices de flux
- **Orchestration pare-feu :** Automatisation Tufin SecureChange, Palo Alto, politiques CheckPoint, gestion changements ITIL
- **Cisco ISE NAC :** Profilage équipements, AAA RADIUS, authentification certificats, affectation VLAN dynamique
- **PKI et certificats :** Déploiement X.509 sur 10k points d'accès, gestion cycle de vie certificats, validation CRL/OCSP
- **Administration infrastructure :** Gestion parc 10k équipements, mises à jour firmware, supervision SNMP
- **Sécurité OT/IT :** Sécurisation protocoles industriels, réseaux cloisonnés, conformité normes aéronautiques

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

PROJET R&D : GHOST-HUNTER (IA OFFENSIVE)

Développement d'un agent de pentest autonome couplant Burp Suite à une architecture IA avancée (RAG/LLM) pour l'automatisation de la détection de vulnérabilités critiques.

- **Workflow Opérationnel :** L'outil s'intègre comme une extension **Burp Suite** agissant en observateur passif. Pendant que l'auditeur simule une utilisation légitime (couverture des processus métiers), l'agent capture le trafic, filtre par scope et orchestre les attaques en arrière-plan.
- **RAG Massif & Knowledge Base :** Indexation de 13 484 chunks de connaissances (HackTricks, Nuclei Templates, 13 000+ rapports HackerOne) et 9000+ techniques de bypass WAF.
- **Architecture de Triage Triple-Layer :**
  - *Tier 1 (Heuristique) :* Filtrage rapide du trafic via 25 règles regex-based agressives.
  - *Tier 2 (Contextuel) :* Analyse IA intermédiaire injectée avec 10 chunks de contexte pour validation.
  - *Strategist (Llama 3.3 70B) :* Moteur de déduction par *Chain-of-Thought* analysant la logique applicative pour construire des vecteurs d'attaque sur-mesure. **Exécution active :** Injection de 30 payloads distincts par endpoint qualifié via rotation d'IP résidentielles et techniques d'évasion WAF, suivie d'une classification automatique des vulnérabilités (IDOR, XSS, Injections...) selon l'analyse des réponses serveur.
- **Optimisation :** Utilisation de modèles Llama 3 quantifiés pour une exécution locale rapide, réduisant la latence et les coûts par rapport aux modèles propriétaires.
- **Next Steps & Roadmap :** Développement de l'autonomie totale via l'intégration de **GraphRAG** pour permettre à l'agent de pivoter de manière itérative sur la cible (relations entre objets) et d'adapter dynamiquement ses payloads, imitant la persévérance d'un attaquant humain.

Burp Suite Extension | Python | RAG | Residential Proxies | Llama 3 | GraphRAG | WAF Bypass

Repository privé

⚗ PROJET R&D : HTTP DESYNC SCANNER

Implémentation d'un scanner offensif basé sur les recherches avancées de James Kettle (PortSwigger) publiées lors d'une conférence DefCon, ciblant les désynchronisations HTTP et les failles de downgrade HTTP/2 vers HTTP/1 (vecteurs responsables de la compromission de PayPal et de +350k$ de bounties sur les CDN Cloudflare/Netlify).

— **Ingénierie Bas Niveau (Raw Sockets) :** Conception d'un moteur en Go utilisant `net.Dial/tls.Dial` et ALPN pour contourner la normalisation des librairies standards. Génération de payloads "byte-perfect" exploitant les incohérences de parsing (RFC 7230 vs 2616), incluant la gestion des délimiteurs non-CRLF, BufferShift et injections dans les Trailers/AbsoluteURI.

— **Moteur de Permutation (Phase 2) :** Orchestration de 690 vecteurs d'attaque par endpoint via le croisement de 5 types de désynchronisation (CL.TE, TE.CL, H2.CL, H2.TE, CL.0) et 138 gadgets de bypass WAF (variations de casse, obfuscation par espaces/tabulations, line folding).

— **Pipeline de Validation :**

  — *Phase 1 (Recon) :* Fingerprinting passif de l'infrastructure (CDN, Load Balancers) et baseline latence.

  — *Phase 3 (Confirmation) :* Validation haute confiance par Timing Differential et Request Fusion (fusion de deux requêtes en une seule réponse backend).

Go | Raw Sockets | HTTP/2 | Request Smuggling | CL.TE | TE.CL | WAF Bypass | CDN Security

Repository privé

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 : maîtrise des architectures IPv6, MPLS, et des protocoles dynamiques (RIP, OSPF, BGP). Supervision réseau avancée via SNMP
- Sécurité des systèmes : solides connaissances en cryptographie appliquée (SSL/TLS, Kerberos, PGP), conformité réglementaire (RGPD, CNIL), et pilotage de SMSI
- Approche offensive : participation à des offensive security challenges intégrés au cursus pour développer un raisonnement d'attaquant et affiner la défense proactive

CERTIFICATIONS

CISSP ISC2

Information Security Management System ISO 27001 Certified

CERTIFIED BLUE TEAM LEVEL 1

splunk> CERTIFIED Splunk Enterprise Certified Admin

splunk> CERTIFIED Splunk Core Certified Power User

À PROPOS

Événements & Conférences

- **CISSP, Barcelone 2026**
- **CBC, Toulouse 2025**
- **THCON & CTF, Toulouse 2025 :** Classement 16/182
- **Hack in Paris 2023**
- **Intervenant au Seamless event, Dubai 2023**
- **FIC, Lille 2022 & 2019**

Langues

- **Français :** Langue maternelle
- **Anglais :** Courant (C1)
- **Espagnol :** intermédiaire

Centres d'intérêt

- **CTF (Capture The Flag) :** Root-Me, HackTheBox
- **Veille technologique :** blogs sécurité (DefCon), threat intelligence feeds
- **Contribution open-source :** scripts automation sécurité, règles détection SIEM