



Ayoub EL OUADI

Cybersecurity Consultant

FREELANCE • AVAILABLE
IMMEDIATELY

+33 6 68 62 07 29

contact@ayoubelouadi.com

ayoubelouadi.com

linkedin.com/in/elouadi-ayoub

Paris, Île-de-France

01 Profile

A network and telecommunications engineer by training (École Mohammadia d'Ingénieurs), I started in the field: systems/network administration, Linux/Windows hardening, NOC/SOC implementation, before moving into banking audit and regulatory compliance, then operational security at AXA GIE.

Now an independent consultant, I operate where governance meets operations: GRC and risk analysis (EBIOS, ISO 27005), SecOps, LPM/NIS compliance, patch management at global scale, and cross-functional security project leadership.

Rigorous and results-driven, I structure security processes, coordinate multidisciplinary teams and roll out operational controls at scale, for reliable, measurable and lasting frameworks.

8+

YEARS OF EXPERIENCE

14

SIGNIFICANT ENGAGEMENTS

03

MAJOR GROUPS (CAC 40 /
BANKING)

04

REGULATORY FRAMEWORKS
(LPM • NIS • GDPR • ISO
27001)

INDUSTRIES SERVED

Insurance

Banking & Finance

Luxury & Cosmetics

Press & Media

Public Research

Telecoms

02 Career Highlights

01 Group-wide EDR deployment

Integration and full rollout of Cybereason across AXA GIE's asset base — 1,800 workstations and Windows / Linux servers — including detection use cases and response processes.

02 MTSB security baseline v2 & v3

Steering of the minimum technical baseline across all AXA assets: annual compliance targets, KPIs per control and remediation plans, with the SOC and local entities.

03 Ransomware cyber-crisis response

Forensic investigation, IOC identification, containment, network architecture redesign and hardening, followed by a crisis report and executive summary for management.

04 LPM compliance and system accreditation

Compliance programme for a banking group (5 subsidiaries): CISO workshops, risk analyses, access-rights reviews and preparation of accreditation files for strategic and vital information systems.

03 Skills & Education

TOOLS & ENVIRONMENTS

- Cybereason (EDR)
- Digital Guardian (DLP)
- SIEM
- ServiceNow
- Wireshark
- PingCastle
- Checkmarx
- pfSense
- Active Directory
- Windows / Linux
- Citrix
- Cloud

EDUCATION & TRAINING

05/2025

Operational Project Management

Actinium

05/2020

Project Stakeholders Management

Actinium

2015 – 2018

State Engineering Degree in Networks and Telecommunications

École Mohammadia d'Ingénieurs
— Rabat, Morocco

2012 – 2015

CPGE — PSI Track (French preparatory classes)

Lycée Moulay Youssef — Rabat, Morocco

LANGUAGES

French	BILINGUAL
English	FLUENT
Arabic	NATIVE

AREAS OF EXPERTISE

■ Governance & Compliance (GRC)

- Risk analysis (EBIOS, ISO 27005)
- Regulatory compliance (LPM, NIS, GDPR, ISO 27001)
- Definition of security policies and continuous controls
- Accreditation of sensitive information systems (SIS / SIV)
- Leading security workshops with CISOs and business/IT teams

■ Endpoint, Server & Data Protection

- Deployment and management of EDR solutions (Cybereason)
- Administration of DLP policies (Digital Guardian)
- Hardening of Windows / Linux environments
- Active Directory security
- Patch management and access control

■ Application Security & Security by Design

- Implementation of Security by Design practices
- Code audits and SAST / DAST analysis
- Definition of secure development best practices
- Support for development teams

■ Cybersecurity Project Management

- End-to-end security project management
- Cross-functional coordination (IT, security, business)
- KPI tracking and reporting to governance bodies
- Continuous improvement of security posture

■ Operational Security (SecOps)

- Security monitoring and incident management
- SIEM / EDR / DLP alert analysis
- Incident investigation and response
- Continuous improvement of security controls
- Coordination with SOC and IT teams

■ Vulnerability Management & Security Audits

- Management of penetration testing and vulnerability scan campaigns
- Analysis and prioritisation of vulnerabilities
- Follow-up of remediation plans
- Technical and application security audits

■ Incident Response & Cyber Crisis Management

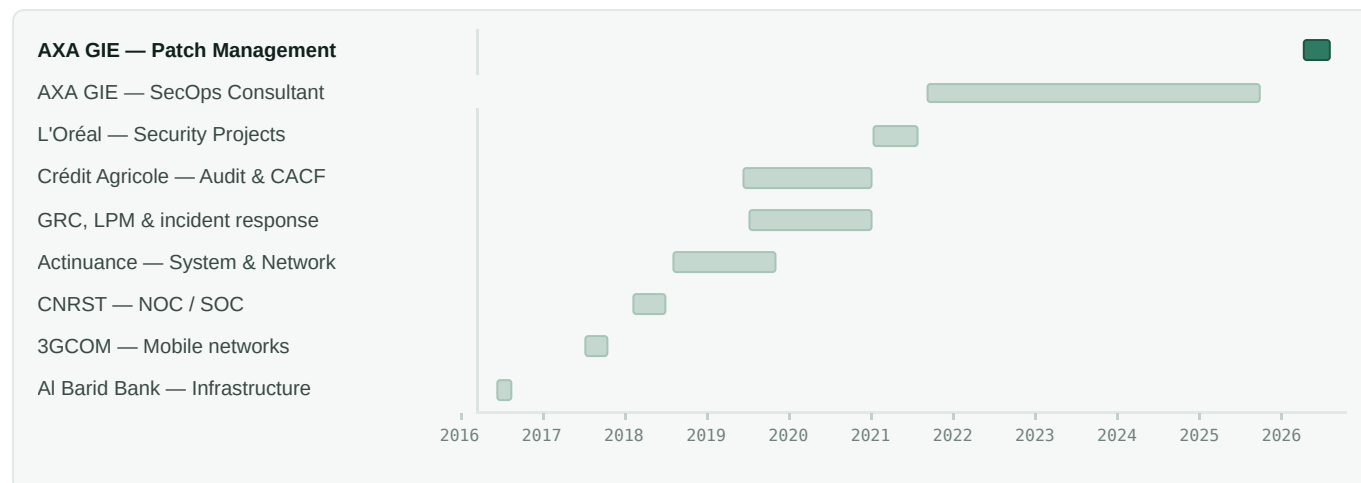
- Forensic investigation, log and network traffic analysis
- Identification of Indicators of Compromise (IOC)
- Containment and remediation (ransomware attacks)
- Participation in crisis cells and incident reporting

■ Awareness & Security Culture

- Creation of awareness materials
- Delivery of user training sessions
- Promotion of security best practices

04 Key Engagements

ENGAGEMENT TIMELINE • 2016 – 2026



AXA GIE

Patch Management — CSO Team

04/2026 → Present

● ONGOING

Leading global patch management within AXA GIE's CSO team, as part of a critical-vulnerability reduction programme.

PATCH MANAGEMENT

VULNERABILITY MGMT

PILOTAGE

GLOBAL PATCH MANAGEMENT – CRITICAL VULNERABILITY REDUCTION

- Led and coordinated global patch management across the entire AXA GIE asset base, directly addressing critical vulnerabilities identified across the IS.
- Managed patching across workstations (Windows, macOS) as well as servers and VMs (Windows, Linux, Citrix).
- Defined and prioritised patch deployment campaigns based on vulnerability criticality and risk exposure.
- Coordinated cross-functionally with Infrastructure, Cloud, Operations and Support teams to ensure a consistent, controlled patch rollout.
- Monitored and validated patch cycles (test, pilot, general rollout) to minimise production impact.

KPIS, REPORTING AND PROJECT STEERING

- Defined and tracked dedicated KPIs: number of open / resolved vulnerabilities, patch coverage rate by asset type, average remediation time.
- Built a tracking dashboard providing a consolidated, near real-time view of asset status (workstations, servers, VMs) against identified risks.
- Steered the overall project: prioritisation, trade-offs, and status reporting to security governance bodies.
- Produced regular reporting on patching campaign progress and evolving risk exposure.
- Identified and escalated non-compliant or exempted assets in coordination with the relevant technical teams.



Incident management, security project leadership and continuous improvement of controls.

SECOPS

EDR / DLP

MTSB

ISO 27001

MTSB PROJECT (MINIMUM TECHNICAL SECURITY BASELINE) – V2 & V3

- Led and managed the MTSB programme, ensuring a minimum level of security across AXA's entire asset base: workstations, Windows/Linux servers, databases, business applications and mobile devices.
- Coordinated technical and security teams (SOC, IT Infrastructure, Cloud, Networks, Endpoints) to bring assets into compliance with baseline requirements.
- Supervised the controls defined by the baseline: patch management, secure configuration, encryption, antivirus, EDR, system hardening, account and access management.
- Annual compliance targets per scope, KPIs per control (compliance rate, asset coverage, pending remediations), gap identification and action-plan steering, with quarterly reporting to security management.

SECURITY INCIDENT MANAGEMENT AND INVESTIGATIONS

- Real-time supervision of security alerts across various tools (SIEM, DLP, EDR).
- In-depth analysis of reports from Digital Guardian (DLP) and Cybereason (EDR) to identify threats and anomalous behaviours.
- Applied escalation procedures with SOC, IT and business teams, then drafted and distributed incident communications: reports, post-mortems, recommendations.

INTEGRATION AND LEADERSHIP OF THE EDR SOLUTION – CYBEREASON

- Led the global integration and deployment of Cybereason EDR within AXA GIE, covering workstations, Windows and Linux servers.
- Designed and prioritised detection and response use cases with the SOC and Threat Intelligence teams, then defined the operational processes for EDR incident management.
- Tracked the agent rollout across the asset base and the associated KPIs: EDR coverage, detection quality, response reactivity.

DLP POLICY MANAGEMENT AND OPTIMISATION

- Implementation, configuration and administration of DLP policies in Digital Guardian.
- Continuous improvement of rules: filter refinement, alert-noise reduction, coordination with business teams.
- Developed specific policies reducing data-leakage risk and strengthening regulatory compliance (GDPR, ISO 27001).

USER REQUESTS AND DEROGATION MANAGEMENT

- Processed and analysed end-user security requests: specific tools, privilege elevation, exceptional access, DLP/EDR derogations.
- Assessed request compliance against AXA Group policies; drafted and harmonised the associated procedures (workflow, roles, acceptance criteria).
- Daily use of ServiceNow and tracking of process performance KPIs (SLA compliance, rejection rate, average handling time).

Embedding security into projects and supporting business / IT teams.

SECURITY BY DESIGN

ISO 27005

EBIOS

GOUVERNANCE

INTEGRATION OF SECURITY INTO PROJECTS

- Supported business and IT teams in implementing the security process throughout the project lifecycle (from design to production).
- Participated in security tenders: drafted requirements, analysed vendor proposals and managed compliance audits (internal and external).
- Managed vulnerabilities on application and infrastructure projects, coordinating with technical teams on remediation and patch follow-up.
- Conducted project risk analyses according to Group standards and the ISO 27005 / EBIOS frameworks, defining and monitoring associated action plans.
- Contributed to security governance through dashboards, monthly reporting and support to the security department's steering.
- Collaborated closely with Infrastructure, Cloud, Network and Compliance teams to ensure consistency of security requirements across the project portfolio.
- Raised awareness among project managers and application owners of cybersecurity best practices and internal compliance requirements.



Crédit Agricole

Security Analyst — Internal Audit Team · Cyber CheckUp

10/2020 → 12/2020

Continuous controls and security posture assessment across the Group's subsidiaries.

CONTRÔLE CONTINU

KPI

AUDIT INTERNE

CONTINUOUS CONTROLS

- Monitoring and analysis of security indicators across Group subsidiaries as part of the CyberCheck-UP campaign (compliance, maturity, risk exposure).
- Facilitated coordination workshops with local security managers (CISOs, internal controllers, IT teams) to collect information, clarify requirements and support entities in understanding the controls.
- Created consolidated dashboards (KPIs, compliance rates, gaps by subsidiary, critical-control summary) giving security management a global, up-to-date view.
- Reviewed and analysed deliverables submitted by subsidiaries: validated evidence, identified gaps, issued improvement recommendations and prioritised actions.
- Contributed to improving the continuous-control process by ensuring consistency, quality and traceability of collected data.
- Prepared summary reports for security management, facilitating campaign steering and strategic decision-making.

Security reinforcement, CISO workshop facilitation and LPM control monitoring.

LPM

PKI

PINGCASTLE

CHECKMARX

SIS / SIV

COMPLIANCE – FRENCH MILITARY PROGRAMMING LAW (LPM)

- Managed and monitored the security reinforcement programme in line with LPM requirements.
- Led workshops and coordinated regularly with the CISOs of the Group's entities to ensure alignment with LPM controls and security best practices.
- Prepared, consolidated and presented key indicators to steering and security committees: compliance level, residual risks, action-plan progress.
- Organised and facilitated specialised technical workshops: secure administration of sensitive environments, PKI / CARIOCA management, password robustness policy, Active Directory auditing with PingCastle, code auditing with Checkmarx (SAST analysis).
- Conducted access-rights reviews and risk analyses, including impact modelling and definition of the required security measures.
- Analysed compliance deliverables from technical and business teams, verified evidence quality, diagnosed gaps and recommended corrective measures.
- Participated in the accreditation process for Strategic and Vital Information Systems (SIS / SIV): LPM compliance verification, risk assessment and preparation of accreditation dossiers.

Implementation of a Security by Design process and code auditing.

OWASP

SAST / DAST

AUDIT DE CODE

SECURE DEVELOPMENT OF AN APPLICATION

- Designed and drafted a complete Security by Design process embedding security requirements from the earliest development phases (scoping, design, development, testing, deployment).
- Definition of secure development best practices.
- Performed vulnerability scans on the application under development (SAST / DAST analysis) to identify potential weaknesses.
- Manual and automated code audits to verify compliance with security standards (OWASP, internal best practices) and identify application risks.
- Wrote remediation recommendations for developers: fixes, hardening, input validation, error handling, authentication.

Creation of educational content and facilitation of training sessions.

SENSIBILISATION

CULTURE SÉCURITÉ

EMPLOYEE CYBERSECURITY AWARENESS

- Wrote awareness articles on cybersecurity best practices: phishing, password management, workstation security, mobility.
- Created educational infographics to simplify technical concepts and strengthen employees' understanding of cyber risks.
- Facilitated training and knowledge-sharing sessions on information security, tailored to user levels and focused on preventing risky behaviours.

Investigation, containment, remediation and post-incident secure redesign.

FORENSICS

RANSOMWARE

GESTION DE CRISE

IOC

INVESTIGATION, FORENSIC ANALYSIS AND EVIDENCE COLLECTION

- Full forensic analysis of compromised servers and workstations to identify the attack vector, attacker actions and malware propagation.
- In-depth analysis of infrastructure logs (Windows/Linux servers, firewalls, proxies, antivirus) to reconstruct the incident timeline.
- Network traffic analysis with Wireshark to identify lateral movements, suspicious connections and exfiltration attempts.
- Identified the entry point, exploited vulnerabilities, compromised accounts and techniques used; extracted and documented Indicators of Compromise (IOC).

CONTAINMENT AND EMERGENCY HARDENING

- Immediate isolation of compromised systems and halting of ransomware propagation.
- Emergency hardening of Internet access and external entry points: VPN, exposed ports, vulnerable services.
- Disabled compromised accounts, reset sensitive access and applied critical patches on vulnerable servers.

NETWORK ARCHITECTURE REDESIGN AND HARDENING

- Partial reorganisation of the network architecture and stricter segmentation between servers, users and sensitive zones.
- Strengthened firewall rules and ACLs following least-privilege and defence-in-depth principles.
- Active Directory hardening: GPOs, privileged accounts, password policies, RDP restrictions.

CRISIS MANAGEMENT, COMMUNICATION AND POST-INCIDENT

- Participation in crisis cells with executive management, IT and security teams.
- Wrote a comprehensive crisis report (timeline, evidence analysis, extent of compromise, recommendations) and an executive summary for top management.
- Verified system restoration from clean backups and strengthened detection and prevention mechanisms (antivirus, EDR, alert rules).

Identification of Essential Systems, gap analysis and NIS compliance implementation.

NIS

GAP ANALYSIS

POLITIQUES SSI

NIS DIRECTIVE COMPLIANCE

- Identification and classification of Essential Information Systems (EIS) in line with NIS Directive requirements, in collaboration with business and IT teams.
- Gap analysis between existing practices and NIS regulatory requirements, producing a complete compliance matrix.
- Drafting and updating of NIS-compliant security policies: incident management, business continuity, access control, vulnerability management, logging, hardening and governance.
- Identification of priority workstreams and construction of a scoping action plan covering the required technical, organisational and documentary measures.
- Drafting of the final compliance report for management and competent authorities: compliance status, residual risks, remediation plan, operational recommendations.
- Vulnerability scans and code audits as part of the technical assessment of Essential Information Systems, to identify priority weaknesses.



Crédit Agricole Consumer Finance

Management of Internal and External Security Audits

06/2019 → 12/2019

Technical audit follow-up, action-plan management and security reporting.

PENTESTS

VULNERABILITY MGMT

REPORTING COPILOT

MANAGEMENT OF PENETRATION TESTS AND VULNERABILITY TESTS

- Collection and formalisation of penetration-testing and vulnerability-testing requirements from business, IT and security teams.
- Operational management of testing campaigns: scoping, coordination with providers, scope definition, execution monitoring and validation of test conditions.
- Analysis, reporting and follow-up of remediation of identified vulnerabilities, coordinating with technical teams (infrastructure, network, development).
- Production of risk, performance and coverage indicators: vulnerability criticality, remediation timelines, correction rate.
- Preparation of materials and minutes for Steering Committees and other decision-making bodies, enabling informed decisions on application and technical risks.
- Development of the annual test plan, integrating compliance requirements, business priorities, IS evolutions and the history of detected vulnerabilities.



Actiniance

System & Network Administrator

08/2018 → 10/2019

Infrastructure management, system hardening and flow-matrix design.

PFSense

DURCISSEMENT

ACTIVE DIRECTORY

NETWORK AND SECURITY ADMINISTRATION

- Creation of a network flow matrix under pfSense: analysis of internal / external communications, mapping of critical services and definition of associated firewall rules.
- Design and drafting of Linux hardening guides (Debian, Red Hat): secure system configuration, user and rights management, SSH hardening, logging, update and patching policies.
- Drafting of Windows Server hardening guides: role and service configuration, Active Directory strengthening, security-oriented GPOs, password and authentication policies, audit and log management.
- Contribution to the overall strengthening of the company's security posture through standardised, documented best practices.



CNRST — Rabat

Engineering Intern — Network & Security Administration

02/2018 → 06/2018

Contribution to the operational implementation of a NOC / SOC for the MARWAN 4 infrastructure.

NOC / SOC

SUPERVISION

IMPLEMENTATION OF A MARWAN 4 NOC / SOC

- Contribution to the implementation of a NOC / SOC centre dedicated to the MARWAN 4 national academic network.
- Participation in defining operational needs, supervision tools and security indicators.
- Initial configuration of monitoring, incident-management and network-supervision tools.
- Development of operating, alert-management and escalation procedures.



3GCOM — Rabat

Engineering Intern — Mobile Network Optimisation

07/2017 → 09/2017

Network performance analysis and optimisation recommendations.

RÉSEAUX MOBILES

3G / 4G

MOBILE NETWORK OPTIMISATION

- Analysis of mobile network performance (3G / 4G) using operator internal tools.
- Identification of areas with low coverage or degraded service.
- Proposals for optimisation actions on radio parameters: handover, power, resource allocation.



Al Barid Bank — Rabat

Network Administrator Intern

06/2016 → 07/2016

Analysis and optimisation of the IT network, redesign and hardening of infrastructures.

SWITCHING

INFRASTRUCTURE

REDESIGN OF A CENTRAL SWITCHING SOLUTION

- Analysis of the bank's former central switching architecture.
- Participation in the redesign of the solution to improve performance, resilience and security.
- Update of network configurations under engineer supervision and drafting of technical documentation.