

# SAMIR ALE

Cybersecurity Engineer

Author

samir49715@gmail.com | +33 6 50 83 84 15

## PROFESSIONAL SUMMARY

Results-driven Cybersecurity Engineer with 5+ years of hands-on experience in vulnerability management, incident response, SOC operations, and security governance. Proven track record of coordinating end-to-end vulnerability lifecycle, deploying DAST/SIEM solutions, and leading security audits aligned with ISO 27001/27002 standards. Proficient in both offensive and defensive security, with strong expertise in threat detection, risk analysis (EBIOS), and Zero Trust principles. Certified in digital forensics, and industrial systems cybersecurity.

## CORE COMPETENCIES

|                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Vulnerability Management (full lifecycle)</li><li>• Incident Response &amp; Containment</li><li>• SOC Operations &amp; SIEM Monitoring</li><li>• Penetration Testing (Web Applications)</li><li>• Security Governance &amp; Compliance</li><li>• Risk Analysis (EBIOS methodology)</li></ul> | <ul style="list-style-type: none"><li>• Cloud Security (AWS, Azure)</li><li>• Industrial Control Systems (ICS) Security</li><li>• DAST Deployment &amp; Management</li><li>• Zero Trust Architecture</li><li>• Digital Forensics &amp; Malware Analysis</li><li>• Security Awareness &amp; Training</li></ul> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## TECHNICAL TOOLBOX

|                 |                                                                    |
|-----------------|--------------------------------------------------------------------|
| SIEM / SOC      | Azure Sentinel, Splunk, QRadar, Varonis                            |
| Vuln. Scanning  | Qualys, Nessus (Nexpose), OpenVAS, Burp Suite Enterprise           |
| Offensive Tools | Nmap, Metasploit, Burp Suite, Nikto, OWASP ZAP, Wireshark          |
| Cloud Security  | Wiz, Azure Defender, AWS Security Hub                              |
| Forensics       | Autopsy, Volatility                                                |
| Frameworks      | MITRE ATT&CK, OWASP Top 10, ISO 27001/27002, EBIOS RM, NIST CSF    |
| DAST/SAST       | Burp Suite Enterprise (deployment & operations)/ Checkmarx/ Sonarq |

## PROFESSIONAL EXPERIENCE

---

### Security Expert & Coordinator

AG2R La Mondiale — Paris, France

Sep 2023 – Present

- Lead the full lifecycle of vulnerability management: monitoring, identification, prioritization, remediation coordination, and follow-up with stakeholders across multiple business units.
- Coordinate operational security involvement in risk analyses and penetration testing engagements, ensuring alignment with enterprise security strategy.
- Deploy and manage DAST (Dynamic Application Security Testing) using Burp Suite Enterprise, securing web applications in production environments.
- Respond to security incidents with timely analysis, containment, and remediation, minimizing business impact and ensuring SLA compliance.
- Drive continuous improvement of security operations (RUN activities) through process optimization and cross-team coordination.
- Produce executive-level security reports and dashboards for governance bodies, tracking KPIs on vulnerability remediation and incident response.
- Contribute to technical studies supporting the evolution and hardening of the Information Systems Security posture.

### Cybersecurity Consultant

METSYS — Paris, France

Apr 2021 – Sep 2023

- Deployed and managed the Varonis data security platform, including Datalert rule configuration and automated reporting for data access monitoring.
- Operated as SOC Analyst (L2): detected, investigated, and handled security incidents using Azure Sentinel and Varonis, correlating alerts and escalating critical threats.
- Conducted technical and organizational security audits, including penetration tests and compliance assessments aligned with Information Security Policies (ISP/PSSI).
- Managed vulnerability remediation workflows across systems and applications, coordinating with technical teams to ensure timely resolution and risk mitigation.
- Provided continuous monitoring and threat analysis, proactively identifying anomalies and potential attack vectors.

### Cybersecurity Engineer (Apprenticeship)

Xélians — Paris, France

Oct 2019 – Sep 2020

- Collaborated with the CISO on enterprise-wide risk analysis: scoping, asset identification, risk scenario mapping, and risk treatment plan development.
- Updated and enforced the Information Security Policy (ISP), ensuring alignment with ISO 27001 requirements and participating in internal audit reviews.
- Managed vulnerability lifecycle for internal solutions (SAE, GED) and infrastructure using Qualys and OpenVAS.
- Performed technical audits on web applications, delivering OWASP Top 10 training to development teams to improve secure coding practices.
- Led phishing simulation campaigns, improving security awareness metrics across the organization.
- Conducted digital forensics investigations and malware analysis on compromised endpoints.

## Cybersecurity Engineer Intern

GIE GERAP (MACIF-MAAF) — Niort, France

Mar 2019 – Jul 2019

- Coordinated the remediation action plan for web vulnerabilities identified during a penetration test engagement.
- Implemented DAST tooling (OWASP ZAP) for automated code scanning across portal and service development teams.
- Conducted live attack simulations in a lab environment to raise developer awareness on application vulnerabilities.
- Updated the Information Security Policy with recommendations based on ISO/IEC 27002 controls.
- Set up a secure workstation enabling the cybersecurity team to perform Dark Web investigations for corporate threat intelligence.
- Performed penetration tests to validate vulnerability remediation from previous audit findings.

## EDUCATION

### Master's Degree (M2) in Information Systems Risk Management

2020

Université de Poitiers, France

### Engineering Degree in Network & Telecom Security

2017

Sup'Management, Morocco

## CERTIFICATIONS

| Certification                                          | Domain             |
|--------------------------------------------------------|--------------------|
| VCPD — Varonis Certified Professional in Data Security | Data Security      |
| Autopsy Digital Forensics Certification                | Digital Forensics  |
| Incident Response with QRadar (udemy)                  | Incident Response  |
| Industrial Systems Cybersecurity (Alphorm)             | ICS Security       |
| Social Engineering Certification                       | Social Engineering |
| Information Systems Risk Analysis (OpenClassrooms)     | Risk Management    |
| Web Application Security (OpenClassrooms)              | AppSec             |

## LANGUAGES

- French — Native
- English — Professional working proficiency (read, spoken, written)