

13 yrs

RED TEAM & BLUE TEAM,
BOTH SIDES OF THE WIRE

150+

CRITICAL VULNS & 0-DAYS
DISCLOSED TO ENTERPRISES

500+

ENDPOINTS UNDER SIEM
& DETECTION COVERAGE
BUILT

9x

CTF PODIUMS — CSAW,
BSIDES, MOD NATIONAL

PROFILE

Security engineer with **13 years on both sides of the engagement**. Red team: full-scope adversary simulations and penetration tests for **tier-1 banking groups, national oil & gas operators, telecom carriers and government bodies** — external, internal and assumed-breach, through to domain compromise. Blue team: I build the SIEM, the ATT&CK-mapped detection content and the Zero Trust perimeter those attacks get measured against, and I run the infrastructure in production. Now focused on **AI security** — red-teaming live LLM and agent deployments, and shipping LLM-assisted triage into a working SOC. CSAW MENA finalist, two-time BSides Algiers champion, 1st at the Algerian Ministry of Defense national CTF.

CORE EXPERTISE

Red Team & Adversary Emulation

AI / LLM Red-Teaming

Penetration Testing — Web · API · Mobile · Cloud

Active Directory & ADCS Attack Paths

Detection Engineering & Purple Team

Threat Hunting & DFIR

Kubernetes & Cloud Security

Zero Trust Architecture

OT / ICS Security

Exploit Development

Security Leadership (15+ engineers)

SELECTED ENGAGEMENTS

National Oil & Gas Operator — Full-Scope Red Team

ENERGY · CRITICAL INFRA

Multi-week adversary simulation across the corporate estate and the IT/OT boundary. Phishing foothold escalated through Active Directory to domain compromise; demonstrated reachability of engineering workstations and supervisory segments across a flat Purdue-model boundary. Delivered segmentation, credential-hygiene and detection-gap remediation aligned to IEC 62443 and NIS2.

Tier-1 Banking Group — Threat-Led Red Team & Assumed Breach

FINANCE · REGULATED

External perimeter and assumed-breach operations against a regulated banking environment. Chained Kerberoasting, ADCS certificate-template abuse (ESC1/ESC8) and delegation misconfigurations into privileged access; assessed segmentation around payment-processing scope. Findings reported to CVSS/CWE with executive risk narrative, remediation workshops and full retest evidence for PCI DSS 4.0 and SWIFT CSP control owners.

Telecom Carrier & Government Bodies — Offensive Assessments

TELECOM · PUBLIC SECTOR

Recurring external and internal penetration tests, web and API assessments, and social-engineering campaigns; on-call incident response and threat-hunting support during active intrusions.

Production LLM Deployments — AI Red Team

AI · EMERGING RISK

Adversarial testing of live LLM and agentic systems: direct and indirect prompt injection through RAG corpora, tool- and function-calling abuse, guardrail bypass chains, system-prompt and training-data leakage, and unbounded-consumption abuse — mapped to the OWASP LLM Top 10 and MITRE ATLAS.

EXPERIENCE

Systelium

Oct 2025 — Present · Contract

Senior Offensive Security Consultant — Infrastructure, Web & AI · West Africa

- Full-scope penetration testing across complex enterprise architectures — **Active Directory, middleware ESB platforms, cloud-hosted web applications and AI/LLM systems** — for large industrial groups operating across West Africa
- Infrastructure & Active Directory** — multi-segment enterprise networks, identity and authentication layers
- Middleware & API** — ESB platforms, Apache Karaf / JMX services, JDBC and multi-tier data layers
- Web applications** — modern stacks including Blazor / .NET, Azure App Service and OIDC / PKCE authentication flows
- AI & LLM security** — enterprise AI platforms, model and multi-tenant boundaries
- End-to-end delivery** — structured multi-phase methodology, professional reporting and remediation retesting with finding-lifecycle tracking, across sensitive multi-database estates (HR, payroll, sales) and critical infrastructure under strict confidentiality

Active Directory · Kerberos / NTLM · Apache Karaf / JMX · ESB middleware · JDBC · Blazor / .NET · Azure App Service · OIDC / PKCE · Enterprise LLM platforms

Kyo Conseil

Jul 2019 – Present

CISO — Chief Information Security Officer · Algiers, Algeria

- Own the company's **security strategy, architecture and technical direction** as CISO; direct a team of **15+ engineers** across offensive security, DevSecOps, infrastructure and software
- Stood up the **SOC capability from zero**: SIEM across **500+ endpoints**, ATT&CK-mapped detection content and Sigma rules, alert triage workflow and incident response runbooks
- Replaced legacy VPN with **Zero Trust network access** — identity-aware per-application authorization, device posture checks and mTLS for internal systems
- Design and operate a **multi-datacenter virtualization estate** with ZFS storage, immutable backups and tested disaster recovery
- Built and run a production **multi-tenant SaaS platform with OS-level tenant isolation** across thousands of accounts, hardened against cross-tenant compromise
- Own vendor security review, client-facing security assurance and audit readiness (ISO 27001 / NIST CSF aligned)

Wazuh · Elastic · Sigma · MITRE ATT&CK · Cloudflare Zero Trust · Proxmox VE · ZFS · Docker · Terraform · Ansible · Nginx · MySQL · GitLab CI/CD

Synack

Jun 2021 – Present

Security Researcher · Remote (Synack Red Team platform)

- Discovered and disclosed **150+ critical and high-severity vulnerabilities, including zero-days**, across enterprise web, API, mobile and cloud-native targets on the vetted Synack Red Team researcher platform
- AI/ML attack surface research** — prompt injection, indirect injection via retrieval, agent tool abuse, model behaviour manipulation and data leakage against production LLM deployments
- Assessed **Kubernetes clusters, serverless stacks and microservice estates** for IAM privilege escalation, container escape, exposed control planes and CI/CD supply-chain exposure
- Built custom recon, fuzzing and exploitation tooling in **Python, Go and Rust** for targets where off-the-shelf scanners stop short — auth bypass, deserialisation, business-logic abuse
- Authored reproducible, developer-ready reports with working PoCs; supported client remediation and retest cycles

Burp Suite Pro · Nuclei · Impacket · BloodHound · Sliver · Semgrep · Python / Go / Rust · AWS · Azure · GCP · Kubernetes · OWASP LLM Top 10 · MITRE ATLAS

Kyo Conseil

Sep 2017 – Jul 2019

Senior Cybersecurity Specialist — Red Team · Algiers, Algeria

- Led red team and penetration test delivery** for banking, oil & gas, telecom and government clients — external, internal, assumed-breach, phishing and physical/social engineering
- Mapped and exploited **Active Directory attack paths** to domain compromise, then ran **purple team** replays with client blue teams to build and validate detections
- Designed **Zero Trust and micro-segmented network architectures** for enterprise and regulated deployments
- Embedded security into delivery: **SAST, DAST, dependency and secret scanning in CI/CD**, plus SIEM detection libraries and threat-hunting playbooks
- Wrote executive and technical reports and presented findings to **C-level stakeholders and regulators**

Cobalt Strike · Metasploit · Impacket · BloodHound · Responder · Nmap · Burp Suite · Wazuh · Zero Trust · DevSecOps · Incident Response

Dalil Technology

Jan 2013 – Present

Co-Founder / CTO · Algiers, Algeria

- Grew the company from **two people to 50+**; won **Best Startup Algeria 2016** at Seedstars
- Architected a cloud-native SaaS platform serving **10,000+ users** — event-driven microservices on AWS and GCP, built secure-by-design with threat modelling and least-privilege IAM
- Shipped AI/ML product features (NLP, computer vision, recommendation) and led blockchain R&D including audited Ethereum smart contracts

Next.js · FastAPI · PostgreSQL · Redis · Kubernetes · AWS · GCP · Terraform · Solidity

Eprint

Dec 2015 – Aug 2017

IT Manager · Algiers, Algeria

- Owned the full IT estate — Windows Server, Active Directory, Linux, Cisco networking, VPN, backup and DR
- Hardened the perimeter, managed firewall policy and ran company-wide security awareness and phishing simulations

Windows Server · Active Directory · VMware · Cisco · Linux

ShieldCheck — Security & Compliance Scanner LIVE [compliance.bellounis.com](#)

Passive, non-intrusive assessment platform running **six scan modules** against any domain or IP — network recon (DNS, ports, geo), SSL/TLS certificate chain and validity, server security headers, software version and **CVE exposure**, plus **GDPR and PCI DSS** control checks — exported as PDF or HTML reports. Safe against third-party estates, so it doubles as a **vendor and supply-chain due-diligence** tool.

Next.js · TypeScript · TLS / X.509 analysis · DNS & port recon · CVE correlation · GDPR & PCI DSS mappings · PDF / HTML reporting

DZ Compliance Wizard — Data Protection Law 18-07 & 25-11 LIVE [18-07.site](#)

Trilingual (FR / EN / AR, full RTL) guided self-assessment for Algeria's data protection regime — the regional counterpart to GDPR. Eight-stage audit covering **DPO governance and ANPDP notification**, processing inventory, data subject rights, technical and organisational security measures, and **cross-border transfer legality**, ending in a regulator-ready compliance report. **Privacy by design**: every answer stays in browser local storage and is never transmitted to a server.

Next.js · TypeScript · i18n with RTL · client-side persistence · scored control framework · PDF / HTML report generation

ComposeLab — Visual Docker Compose Builder LIVE [composelab.app](#)

Free and open-source DevSecOps tool: drag services onto a canvas, draw dependency edges, and export production-ready YAML with **healthchecks, named volumes, network isolation and resource limits. 50+ preconfigured services**, live validation for port conflicts and broken dependencies, and YAML import that reverse-engineers an existing stack onto the canvas. **Bring-your-own-key AI stack generation** (OpenAI, Anthropic, Groq, Ollama) runs entirely client-side — **API keys never leave the browser; zero backend, zero telemetry**.

Next.js 15 · React 19 · React Flow v12 · Zustand · Monaco Editor · js-yaml · Tailwind · TypeScript

TraceLess RUNTIME SECRET EXPOSURE · OPEN SOURCE [github.com/0x890/TraceLess](#)

Go scanner answering the question no port or CVE scanner does: **what could a low-privileged attacker harvest from this host right now?** Read-only /proc introspection with 30+ rules for credentials leaked in process environments and command lines (DB, AWS/Azure/GCP, JWT signing keys, OAuth, SMTP, GitHub/Slack/Stripe tokens), needless root, and services bound to 0.0.0.0. Severity-scored with remediation, JSON output for CI/CD, single static binary, non-destructive and authorization-gated.

Go 1.21 · /proc introspection · regex rule engine · JSON · Docker · MIT

AI-Powered SOC DETECTION ENGINEERING

Security operations pipeline where LLMs correlate SIEM alerts, enrich with threat intelligence, map activity to MITRE ATT&CK and draft incident response playbooks — cutting L1 triage load on repetitive alerts.

Python · Claude API · LangChain · Elasticsearch · Wazuh · FastAPI

Uptiq INCIDENT AUTOMATION · OPEN SOURCE [github.com/0x890/uptiq](#)

Self-hosted status page and incident-management platform that **closes the detection-to-resolution loop**: a processor engine evaluates alert rules every 30s, auto-creates incidents on threshold breach, deduplicates, and auto-resolves on recovery. Agent telemetry, real-time SSE, public/private incident visibility, and Discord/Slack/email/webhook dispatch. JWT admin auth with separate service-key metric ingestion.

Next.js 14 · Express · TypeScript · PostgreSQL 16 · Docker Compose · SSE · bash agent

ServerScope ATTACK SURFACE MANAGEMENT

Agentless asset and attack-surface discovery across Linux (SSH), Windows (WinRM), Active Directory (LDAP), VMware, Proxmox and AWS/Azure/GCP — surfaces shadow IT, abandoned and unpatched hosts and risk-scores each asset.

Python 3.14 · Pydantic · SSH / WinRM · LDAP · Proxmox API · AWS / Azure / GCP · pytest

ProxmoxGuru INFRASTRUCTURE CLIENT · OPEN SOURCE [github.com/0x890/ProxmoxGuru](#)

Cross-platform desktop client for Proxmox VE — multi-cluster management of nodes, VMs, LXC, storage, networking, backups and live task and log streams. **Built security-first**: credentials encrypted at rest through OS-level storage and never exposed to the renderer, scoped API-token auth, contextIsolation on with nodeIntegration off, per-server TLS verification. Shipped for macOS (universal), Windows and Linux.

Electron · React 18 · TypeScript · Vite · Tailwind · Recharts · electron-store · GitHub Actions

ClaudeMon EMBEDDED / HARDWARE

Flipper Zero application (C, FAP SDK) mirroring live AI agent session events over USB serial, with D-pad approval of privileged tool calls — out-of-band human-in-the-loop control for autonomous agents.

C · Flipper Zero FAP SDK · Python · USB serial · ufbt

Offensive

Red Teaming & Adversary Emulation · Web / API / Mobile / Cloud Pentesting · Active Directory & ADCS Attack Paths · Exploit Development · Social Engineering & Phishing · C2 (Cobalt Strike, Sliver, Mythic) · Burp Suite Pro · Impacket · BloodHound · Metasploit · Nuclei · Ghidra

	AI Security	LLM & Agent Red-Teaming · Direct & Indirect Prompt Injection · RAG Poisoning · Tool / Function-Calling Abuse · Model Extraction & Data Leakage · Guardrail Evaluation · OWASP LLM Top 10 · MITRE ATLAS · NIST AI RMF · EU AI Act readiness · PyRIT · Garak
	Defensive	SIEM / SOAR (Wazuh, Elastic) · Detection Engineering (Sigma, MITRE ATT&CK) · Threat Hunting · DFIR & Incident Response · EDR Tuning · Purple Teaming · Atomic Red Team · Caldera · Threat Intelligence
	Cloud & Infra	AWS · Azure · GCP · Kubernetes · Docker · Terraform · Ansible · Proxmox VE · ZFS · Cloudflare Zero Trust · Istio · Nginx · GitLab CI/CD · SBOM & supply-chain security
	OT / ICS	IEC 62443 · Purdue Model segmentation · SCADA / DCS exposure review · Modbus & DNP3 · IT/OT boundary assessment
	Engineering	Python · Go · Rust · TypeScript · Bash · PowerShell · FastAPI · Next.js · Node.js · Solidity · PostgreSQL · Redis
	Networking	BGP · OSPF · WireGuard · IPSec · Palo Alto · Fortinet · Cisco · 802.11 wireless security · SDN · micro-segmentation
	Frameworks	MITRE ATT&CK · NIST CSF & 800-53 · ISO 27001 · CIS Controls · NIS2 · DORA · TIBER-EU · PCI DSS 4.0 · SWIFT CSP · SOC 2 · GDPR · HIPAA

CERTIFICATIONS & TRAINING	Security	Cybrary career-path training , 2019 — CISSP · CCSP · SSCP · CompTIA Security+ · CISO (exam-preparation coursework)
	Agile	Scrum Fundamentals Certified — SCRUMstudy / VMedu, 2019 (expired 2022)
	Development	Zend PHP Certified Engineer — Zend Technologies, 2011 (expired 2013)

COMPETITIVE SECURITY	1st	SICA CTF — Algerian Ministry of National Defense (<i>national</i>)	2018
	2nd	CSAW MENA Finals — NYU Abu Dhabi	2018
	1st	CSAW Qualification — NYU Tandon, New York	2017
	2nd	CSAW Qualification — NYU Tandon, New York	2016
	3rd	CSAW Finals — NYU Abu Dhabi	2016
	1st	BSides Algiers CTF — back-to-back champion	2015 & 2016
	1st	Hack.INI CTF — ESI Algiers	2014
	2nd	BSides Algiers CTF	2014
	1st	Best Startup Algeria — Seedstars (<i>entrepreneurship</i>)	2016

EDUCATION & COMMUNITY	BSc, Architecture & Urban Arts — University of Chlef, Algeria	2012 — 2015
	Security career is self-taught and competition-forged: CTF circuit 2014–2018, then professional red team delivery.	
	Mozilla Foundation — Mozilla Representative	2015 — 2019
	Reps Alumni · Google Developer Groups — Member & Speaker, 2011 — 2014	