Evan SEDENO

L2-L3 SOC analyst · incident response & automation

Paris, France • evan@sedeno.fr • evansedeno.fr • linkedin.com/in/evan-sedeno • github.com/evansedeno



PROFILE

SOC analyst at Orange Cyberdefense since April 2024, now L2-L3 at the Paris Xtended-SOC. Incident investigation and response through to the client report: crisis responses, coordination with clients and CERT, on-call duty; automation of detection and response (XSOAR playbooks, filters, rules).

PROFESSIONAL EXPERIENCE

L2-L3 SOC Analyst & Production Engineer (Xtended-SOC)

Orange Cyberdefense · Paris, France · Sep 2026 – present

- **L2-L3 incident investigation and response** for 5 large accounts of 10,000 to 50,000 endpoints.
- **Design of around ten Cortex XSOAR playbooks**, false-positive filters and detection rules (XQL, Sigma, YARA); operational upkeep of the EDR, XDR, SIEM (Sekoia.io, Cortex XSIAM) and SOAR platforms.

L2 SOC Analyst & Production Engineer (Micro-SOC)

Orange Cyberdefense · Marseille, France · Oct 2024 – Aug 2026

- **Incident response** for about 50 clients (500 to 1,000 endpoints): containment by host isolation, remote investigation via EDR consoles and PowerShell (live response).
- **Technical investigation during several crisis responses**, in coordination with the client and CERT (containment, investigation, handover of evidence); on-call duty.
- **Led the investigation** of an AiTM phishing account takeover (Tycoon 2FA): analysis of the emails sent from the account, remediation (session revocation, password and MFA reset), mailbox rule search.
- Investigation reports presented to clients (FR/EN); trained interns, newcomers and L1 analysts.

SOC Analyst · end-of-studies internship

Orange Cyberdefense · Marseille, France · Apr 2024 – Oct 2024

L2 alert and incident handling (SIEM, EDR/XDR) and rule tuning; hired on a permanent contract at the end of the internship.

Pentester · internship

TIL Technologies · Aix-en-Provence, France · Apr 2023 – Jul 2023

Security audit and grey-box REST API penetration testing: finding, qualifying and exploiting web vulnerabilities, including excessive data exposure (Burp Suite).

PROJECTS

VyperBox: self-hosted web toolbox for pentesting and CTFs: encrypted payload hosting, request bin, reverse shell generator, script obfuscation and secure file, code and link sharing (expiry, burn after reading); FastAPI, React, Docker.

evansedeno.fr: bilingual portfolio, end-to-end design and deployment (Next.js, Docker, Coolify); hardening with a nonce-based CSP, CI with dependency audit and secret scanning.

Homelab: Home Assistant, a VPS for personal applications, Docker and Coolify.

INTERESTS

Music (DJ, founder of the Minuit Cigale collective) · Cinema · Cooking · Swimming

SKILLS

DETECTION & RESPONSE

Cortex XDR · Cortex XSIAM · Cortex XSOAR · SentinelOne · CrowdStrike · Microsoft Defender · HarfangLab · Sekoia.io · Vectra · Vade · Pradeo

INVESTIGATION & DETECTION

incident response (containment, remediation) · log analysis · crisis management · host investigation via EDR and remote PowerShell · threat hunting · MITRE ATT&CK · XQL · KQL · Sigma · YARA · SOAR playbooks

OFFENSIVE

Burp Suite · Nmap · Metasploit · NetExec · BloodHound · Responder · Mimikatz · Hashcat · Ghidra

SYSTEMS & SCRIPTING

Python · PowerShell · Bash · Linux · Windows · Active Directory · Entra ID / M365 · Docker · Git

PROFESSIONAL TRAINING

Active Directory compromise and hardening
Formation · Orange Cyberdefense · 2025

SentinelOne: core track

Internal training, incl. Cortex XSOAR
Orange Cyberdefense

Practice: Root-me and TryHackMe

EDUCATION

Master's Degree in Computer Science: IT Reliability and Security
Aix-Marseille Université
Sep 2022 – Sep 2024
SecNumedu-labelled programme (ANSSI)

Bachelor's Degree in Computer Science
Université Lyon 1
Sep 2021 – Jul 2022

Two-year University Degree in Computer Science (DUT)
Aix-Marseille Université
Sep 2019 – Jul 2021

LANGUAGES

French: native · English: C1 · Spanish: C1