Evan SEDENO



Analyste SOC N2-N3 · réponse à incident & automatisation

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

PROFIL

Analyste SOC chez Orange Cyberdefense depuis avril 2024, aujourd'hui N2-N3 à l'Xtended-SOC de Paris. Investigation et réponse aux incidents jusqu'au rapport client : gestions de crise, coordination avec les clients et le CERT, astreintes ; automatisation de la détection et de la réponse (playbooks XSOAR, filtres, règles).

EXPÉRIENCE PROFESSIONNELLE

Analyste SOC N2-N3 & Ingénieur de production (Xtended-SOC)

Orange Cyberdefense · Paris, France · sept. 2026 – aujourd'hui

- **Investigation et réponse aux incidents N2-N3** pour 5 grands comptes de 10 000 à 50 000 postes.
- **Conception d'une dizaine de playbooks Cortex XSOAR**, de filtres anti-faux positifs et de règles de détection (XQL, Sigma, YARA) ; MCO des plateformes EDR, XDR, SIEM (Sekoia.io, Cortex XSIAM) et SOAR.

Cortex XDR · Cortex XSIAM · Cortex XSOAR · SentinelOne · CrowdStrike · HarfangLab · Sekoia.io · XQL

Analyste SOC N2 & Ingénieur de production (Micro-SOC)

Orange Cyberdefense · Marseille, France · oct. 2024 – août 2026

- **Réponse aux incidents** pour une cinquantaine de clients (500 à 1 000 postes) : confinement par isolement de postes, investigation à distance via les consoles EDR et PowerShell (live response).
- **Investigation technique lors de plusieurs gestions de crise**, en coordination avec le client et le CERT (confinement, investigation, transmission des éléments) ; astreintes.
- **Conduite de l'investigation** d'une compromission de compte par phishing AiTM (Tycoon 2FA) : analyse des e-mails émis depuis le compte, remédiation (révocation des sessions, réinitialisation du mot de passe et du MFA), recherche de règles de boîte mail.
- Rapports d'investigation présentés aux clients (FR/EN) ; formation des stagiaires, nouveaux arrivants et analystes N1.

SentinelOne · Sekoia.io · Vectra · Vade · Pradeo · PowerShell

Analyste SOC · stage de fin d'études

Orange Cyberdefense · Marseille, France · avr. 2024 – oct. 2024

Traitement d'alertes et d'incidents N2 (SIEM, EDR/XDR) et tuning des règles ; embauche en CDI à l'issue du stage.

SIEM · EDR · XDR · Tuning

Pentester · stage

TIL Technologies · Aix-en-Provence, France · avr. 2023 – juil. 2023

Audit de sécurité et tests d'intrusion d'API REST en boîte grise : recherche, qualification et exploitation de vulnérabilités web, notamment des expositions de données excessives (Burp Suite).

Pentest · API REST · Burp Suite · Web

COMPÉTENCES

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

INVESTIGATION & DÉTECTION : réponse à incident (confinement, remédiation) · analyse de logs · gestion de crise · investigation sur poste via EDR et PowerShell à distance · threat hunting · MITRE ATT&CK · XQL · KQL · Sigma · YARA · playbooks SOAR

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

SYSTÈMES & SCRIPTING : Python · PowerShell · Bash · Linux · Windows · Active Directory · Entra ID / M365 · Docker · Git

FORMATION CONTINUE

Compromission et sécurisation d'Active Directory

Formation · Orange Cyberdefense · 2025

SentinelOne : parcours fondamentaux

Formations internes, dont Cortex XSOAR

Orange Cyberdefense

Entraînement : Root-me et TryHackMe

FORMATION

Master Informatique : Fiabilité et sécurité informatique (FSI)

Aix-Marseille Université · Marseille, France · sept. 2022 – sept. 2024

Formation labellisée SecNumedu (ANSSI)

Cybersécurité · FSI · Sécurité Réseaux · Cryptographie

Licence Informatique

Université Lyon 1 · Lyon, France · sept. 2021 – juil. 2022

Réseaux · Administration Système · Sécurité · Algorithmique · Bases de données

DUT Informatique

Aix-Marseille Université · Aix-en-Provence, France · sept. 2019 – juil. 2021

Informatique · Mathématiques · Réseaux · Développement · Web · BDD

PROJETS

VyperBox : boîte à outils web auto-hébergée pour le pentest et les CTF : hébergement de payloads chiffrés, request bin, générateur de reverse shells, obfuscation de scripts et partage sécurisé de fichiers, de code et de liens (expiration, lecture unique) ; FastAPI, React, Docker.

evansedeno.fr : portfolio bilingue, conception et déploiement de bout en bout (Next.js, Docker, Coolify) ; durcissement par CSP à nonce, CI avec audit des dépendances et détection de secrets.

Homelab : Home Assistant, VPS d'applications personnelles, Docker et Coolify.

LANGUES

Français : langue maternelle · Anglais : C1 · Espagnol : C1

CENTRES D'INTÉRÊT

Musique (DJ, fondateur du collectif Minuit Cigale) · Cinéma · Cuisine · Natation