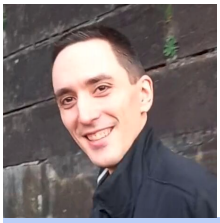

Vincent Monier

SOC & Incident Response Lead

jobs@reinom.com
+33625185493
🇫🇷 / 🇺🇸

10y XP — Centralien — CEH, OSCP/OSWE, Stanford ACS
Ethical hacker — CSIRT — Bug bounty hunter — ANSSI reporter
Avail. for: IR/SOC Lead, CISO Jr (big/medium caps)

SOC & Pentest Lead — Preligens — Paris — ≧ 1 an ½

… ↑ 2022

- Approve IT architect diagrams and review some infra-as-code (Terraform) before production release
- Whitebox code review, hunting for security issues in company's products
- Internal IT security audits as compliance pre-audits, including physical security checks
- Phishing and other general trainings company-wide for awareness, including definition of KPIs for followups
- Plan, architect and setup the company-wide security tools (SIEM, SOAR, EDR, VPN, Firewall, MDM, DNS, …)
- Define rules and configuration for these tools, and both implement them and manage the third-party implementation teams
- SOC Lead: automate resolution of simplest security event, manage SOC engineer for L2 incidents, and resolve & report to C-levels for L3s
- Create standards and policies to align the company with the NIST800-53 standards
- Guide the company's security posture with risk-driven management

Cybersecurity Pentester Engineer — Systancia — Mulhouse — ≦1 an

2022 ↑ 2021

- Hunt for Zero-day vulnerabilities in company produts, advise and followup with dev teams for the patching process
- Verify third parties security (vendor assessment) to strengthen the supply chain
- Contain and recover assets during incidents, and investigate logs for root cause (including insider threats)

Cybersecurity Engineer SOC Lead — General Electric — Belfort — 1 an ½

2021 ↑ 2020

- Incident response SOC lead to prevent M$ financial losses for the Steam Power (GE) business unit
- Apply "lessons-learnt" by enhancing the security rules to prevent new incidents
- Followup and resolve supply-chain incidents (Solarwinds) and CVEs patching (Ghostcat)
- Forensics (logs-based) during post-incidents and case opening with the appropriate authorities (FBI)
- Pentest GE SPS internal applications & infrastructure to hunt for vulnerabilities and weaknesses
- Setup and manage the WAF (Web Application Firewall) and firewall rules
- Review architectures and assist business to ensure compliance with security policies and best practices

DevOps Security Champion — General Electric — Belfort — 5 ans ½

2020 ↑ 2014

- DevSecOps for powerplant projects management internal web application (PHP/Java/SQL, 10k users, 30M hits/an, 10TB de données)
- Help preventing, detecting and resolving application attacks from actual threat actors & audit pentests
- Internal pentesting (purple teaming) the web modules developed by other engineers
- Train and support the 40+ engineers team for secured development processes and methods

Trainees & freelance — Lyon Nantes Liège — 1 an ½

2014 ↑ 2012

- Install and configure internet facing websites for clients
- Keeping these websites operationnal
- Web security audits and pentests
- Develop 3D simplification and labeling algorithms for city buildings and museums

Trainings & certificates

2021	**Offensive Security**	OSCP OSCE OSWE… classes & labs
2020	**Certified Ethical Hacker**	Certified CEHv10 (ECC4520361897) Verify
2017	**Stanford Advanced Computer Security**	Professional certificate (remote)
2014+	**CTF, labs & online trainings**	OVH Cloud CTF, FCSC (28e/1347), 404CTF (10e/2460), Hacking et sécurité, expertise (HAC2018) ↗ Portswigger's Burp Suite labs

2014	**Computer engineering at École Centrale**	Centrale Nantes
2013	**TOEIC 900+**	
—	**BAC S, Prépa PTSI/PT***	

Skills

SOC Tools	Chronicle, Splunk, Crowdstrike Falcon, Cyberwatch, Cloudflare WAF+WARP, Google Workspace, Intune MDM…
Whitebox SAST	Checkmarx, Coverity, custom IntelliJ (IDE) token analyzer…
Attack tools	"Kali", Hashcat, Wireshark, Metasploit, BurpSuite, SQLMap, OllyDbg…
TTPs	SQLi, XSS, XSRF, LFI, RCE, Auth-bypass, Data-leak, LLM injections …
Standards	OWASP Top 10, NIST800-53, SP800-171 CUI…
Web game development	40+ mini games and 3 web MMOs ↗
Technical Watch	Replays from Blackhat, Defcon, HITB, CodeBlue… Whitepapers for Spectre, Meltdown, Foreshadow, Heartbleed
File Format Specifications	Open-Document, PDF, PNG, Targa, SVG…
IT Tools	Google Workspace, Intune MDM
DevOps Tools	Docker, OVH, IDEA, Google Cloud Platform
Pentest	Web, network, IT systems/OS, (LLM)
Zero-day report writing	ANSSI, Stanford, OSTicket
Data Forensics & Recovering	NTFS, FAT32, ext4
Cracking & Reverse Engineering	ASMx86, PE/ELF
(Open source) contributions	Mozilla, XDebug, PHPInspectionEA, IntelliJ, Mantis, MyBB
BIOS & OS	Windows XP-7-10, Ubuntu/XUbuntu, Kali, UEFI/Secure boot
Community Management	JeuWeb, Furry Stars
Physical Pentest	Lock Picking, NFC Access cards

Languages

French + English	C2, Fluent
Coding Languages	PHP SQL Bash/Powershell HTML/CSS/SVG/XSL JS Python Java C/C++/ASMx86 VBS…
Network Protocols	HTTP/0.9-2, SMTP, FTP, DNS…
Japanese, Spanish	~A1 (like, very basic, because it has been such a while)

Hobbies

Electronic & domotic	Using Raspberry Pis for home automation including speech recognition
3D Printing	Designing and printing spare parts for reparing stuff, to save planet and costs
Astronomy	Tracking comets, planets and satellites
Chess & game boards	Playing real physical games together
Gardening	Planting trees and vegetables, caring for birds and insects
Financial analysis	Checking on some company's P/L accounts, investing in stock markets

Contacts

Mail	jobs@reinom.com	PGP 1E59A10C932970A90D10BF7CCD2FBF56FF9B1CE6 ↗
Phone	+33625185493	
Sites	Dev Blog: https://reinom.com ↗ LinkedIn ↗, Twitter (MonierFr) ↗	
Others	"Xenos" in HackerOne ↗, NewbieContest ↗, InfoSec Exchange ↗, Stack Overflow ↗	

Looking for

Jobs title	CSIRT Cyber Security Indicent Response/SOC Lead, Red/Purple team lead, CISO Junior
Locations	France (all), Belgium, Luxembourg, Germany, Switzerland