Vincent Monier

Cybersecurity Architect, Expert @ Safran.AI

- Professionnal IT/Cybersecurity operations engineer since 2013
- Stanford ACS and CEHv10 certified, plus others
- General engineering graduate (Master degree, Centrale)
- jobs@reinom.com (GPG FF9B1CE6) — https://reinom.com

Best achievements

- Detected and recovered a $1M+ financial fraud loss, found during a hunt for phishing emails (and did so again for a $200k+ one)
- Provided forensic investigations for the FBI to arrest a West-Africa based cyber crime group
- Spotted and stoped 3 insiders from exfiltrating company's intellectual property with Data Loss Prevention rules and alerts
- Reverse-engineered and cracked several thick-client software to demonstrate the business model weaknesses before losses
- Detected a crypto-mining malware working for months on company's servers, remediated it and identified its root cause
- Proved that an external threat actor could access the company's critical financial data, and got it fixed
- Made 40+ mini-games and 3 web "MMOs" for fun (and not profits)
- Contributed to Mozilla, XDebug, PHPInspectionEA, IntelliJ, Mantis, MyBB
- Found and reported vulnerabilities in well-known products, leading to published CVE (eg: Microsoft, OSTicket,...)

Career path

2022...	**Cybersecurity Architect**	Safran AI (Paris, Remote)	≥2y

- Lead incident response operations (SOC, SOAR rules, insiders/external threats...)
- Deploy and manage cybersecurity SaaS+tools (SIEM/SOAR, VPN, WAF, Anti-phishing defenses, EDR, SSO/Zero trust...)
- Audit buildings before their certification to remediate missing requirements
- Contribute to Cybersecurity governance (change management, standards, policies, work instructions, playbooks...)
- Manage MCS definition and setup for contractual engagements with clients

2021 → 2022	**Pentest Engineer**	Systancia (Mulhouse)	≤1y

- Pentest company's products to detect vulnerabilities and provide a remediation plan.
- Review third-parties (suppliers) cybersecurity posture and define enhancements guidance.

2020 → 2021	**Cyber Operations Leader**	General Electric (Belfort)	≥1y

- Manage WAF, incidents response (inc. phishing) and pentest audits for Steam business unit.
- Hunt for phishings and threats across GE Power's logs and recover from them.
- Assist and partnership with other GE units (Aviation, Gas power) during group-wide incidents.
- Pentest GE Steam applications and/or act as the "Blue team" leader during third-party audits.

2014 → 2020	**DevSecOps**	Alstom/General Electric (Belfort)	≤6y

- Analyze business needs and develop solution modules for the internal documentation and material tracking platform.
- Apply and followup group's cybersecurity policies and act as the team's main point-of-contact for cybersecurity.
- Pentest the internal platform and reverse-engineer other internal tools to find and report vulnerabilities.

2013 → 2014	**Freelance**	Lyon	1y

- Deploy CMS platforms for clients and advise their MCO/MCS.

Trainings and certificates

- Multiple CTF — 2021… (404CTF, FCSC, SpiderLabs…) Ranked top 10-50
- Offensive Security (OSCP, OSWE…) — 2021, labs only
- Certified Ethical Hacker (CEHv10) — 2020, ECC4520361897
- Stanford Advanced Computer Security — 2017, remote
- Computer engineering graduate — 2014, École Centrale de Nantes (Master2)
- TOEIC 900+ — 2013
- Bac S, Prépa PTSI/PT* — 2008

Skills

I had used/done: Chronicle, Splunk, Crowdstrike Falcon, Cyberwatch, Cloudflare WAF+WARP, Snyk, GitHub, Checkmarx, Coverity, "Kali", Hashcat, Wireshark, Metasploit, BurpSuite, SQLMap, OllyDbg, File Format Specifications (Open-Document, PDF, PNG, Targa, SVG…), Docker, OVH Cloud, IntelliJ IDEA,
Google Cloud Platform, Google Workspace, Microsoft Intune MDM (Entra), Data Forensics & Recovering (NTFS, FAT32, ext4), Reverse Engineering (ASMx86, PE/ELF), Lock Picking, NFC Access cards.

I know well enough: PHP, (My)SQL, Bash/Powershell, HTML, CSS, SVG/XSL, VanillaJS, Python, Java, C/C++/ASMx86, VBS, HTTP/0.9-2, SMTP, FTP, DNS…

Fluent (C2) in French and English, and used to know Spanish and Japanese.

Hobbyist in domotic automation, in spare parts designing and 3D printing, in tracking comets, planets and satellites, in chess and game boards playing, in planting trees, and in financial analysis of (European) companies for personal investments.

Looking for

CISO/PSO (Chief Information/Product Security Officer) in a big cap business unit
or R&D cybersecurity lab lead (internal SOC/auditing lab) in a mid-cap tech/OT company
France and nearby, on-site/remote
Short-term non-dedicated contracts (eg: project/task based) are subject to negociations.

Contact

Send a GPG encrypted email (or a regular email) to jobs@reinom.com (GPG FF9B1CE6) for hiring