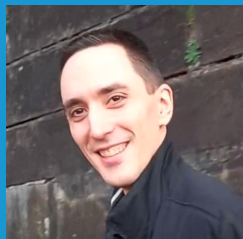


Vincent Monier



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.

Cybersecurity Architect @ Safran.AI

10y Engineering exp. – CEH, OSCP/OSWE, Stanford ACS

Looking for (IT operations) CISO or CERT/SOC Manager offer in FR/CH/BE/LU
jobs@reinom.com (GPG FF9B1CE6) – +33625185493 – <https://cv.reinom.com>

Career path

2022...	Cybersecurity Architect	Safran AI (Paris, Remote)	≥2y
<ul style="list-style-type: none">• Lead the incidents detection (eg: SOAR rules) and remediation (SOC), against both external threats and insiders• 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• Define processes and governance (change management, standards, policies, work instructions, incidents playbooks, trainings...)			
2021 → 2022	Pentest Engineer	Systancia (Mulhouse)	≤1y
<ul style="list-style-type: none">• 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
<ul style="list-style-type: none">• 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
<ul style="list-style-type: none">• 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
<ul style="list-style-type: none">• Deploy CMS platforms for clients and advise their MCO/MCS.			

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
- Prevented data leak by creating DLP rules that spotted 3 insiders exfiltrating company's data and files
- Reverse-engineered and cracked some thick-client software to demonstrate that a SaaS solution should be developed instead
- Detected a crypto-mining malware working for months on company's server, 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, OpenTicket,...)

Trainings and certificates

2021...	404CTF & FCSC (+other CTFs)	Remote, ranked top 10-50
2021	Offensive Security (OSCP, OSWE...)	Classes & labs only
2020	Certified Ethical Hacker	Verified (ECC4520361897)
2017	Stanford Advanced Computer Security	Professional certificate, remote
2014	Computer engineering	École Centrale de Nantes, on-site
2013	TOEIC 900+	on-site
–	BAC S, Prépa PTSI/PT*	on-site