



ROSSELL GAEL

CYBERSECURITY MANAGER SECURITY OPERATIONS & PROJECT LEADERSHIP

CONTACT

+41 79 884 74 47
gael.rossell@gmail.com
linkedin.com/in/gael-rossell
https://github.com/galoxplz
Bussigny, Vaud - Permit B

SKILLS

Security Operations Center (SOC)
Management
Project management
Incident Response & Crisis Management
SIEM Expertise (Kibana/ELK, Microsoft
Sentinel)
EDR/XDR (CrowdStrike, Microsoft
Defender for Endpoint)
Threat Intelligence & OSINT
Data Loss Prevention (Symantec DLP,
Microsoft Purview)
Cloud Security (Azure AD, O365, Defender
Suite)
Leadership & Mentoring
Metrics & SOC KPIs

EDUCATION

CISSP Certification
On going
Master
EXIA Cesi - Toulouse, France

LANGUAGES

French **Native**
English **B2**

PROFILE

IT & Cybersecurity professional with **9 years of experience** leading technical initiatives across infrastructure, project delivery and information security, including **3 years focused on cybersecurity** and security operations.
Experienced in building and maturing SOC and InfoSec capabilities within a regulated financial environment, from defining operating models and security processes to coordinating technical implementations, incident response and cross-functional remediation programmes.
Combines hands-on technical expertise with project leadership, stakeholder management and team development across **SOC, SIEM, DLP, threat intelligence**, GRC, audits and infrastructure security. Continued technical development through independent software engineering, AI automation and cybersecurity projects. Native French speaker with professional working proficiency in English.

WORK EXPERIENCE

Independent IT Projects – Software, AI & Cybersecurity

Switzerland 2026-Present

Community projects: Project T.A.H.I.T.I. – Marvel Heroes Omega → mhtahiti.com

- Developed a C#/ .NET server-side feature for an existing multiplayer game platform, covering scaling, persistence, multiplayer logic, rewards and automated testing.
- Used OpenAI Codex for AI-assisted software engineering, including architecture, codebase analysis, implementation, debugging, testing and technical documentation.

Independent AI projects: Majordomo

- Designed and built a functional AI-powered voice assistant POC, integrating Home Assistant, OpenAI LLM/STT/TTS, presence detection and smart-home automation.

Community projects: TERA Europe Classic+ → tera-europe-classic.com

- Conducted authorized server, network and security investigations on a gaming infrastructure, including stability, database load, DDoS and vulnerability assessment.

SOC Manager - Associate Director

Swissquote Bank - Switzerland, Gland 2022-2026

- Established and led the SOC (3 analysts, 2 incident responders)
- Built a 24/7 on-call structure (PagerDuty) and JIRA-based incident tracking
- Directed response to phishing and fraud-related incidents, with ~4–6 incidents/month and hundreds of alerts
- Mentored analysts on SIEM (Sentinel, ELK), Defender, and IR processes
- Reported bi-weekly to the CISO and supported executive communication
- Designed dashboards and KPIs/KRIs for SOC performance (alert breakdown, FP ratio, coverage)
- Managed recruitment and onboarding of SOC team members
- Coordinated SOC activities and reporting with the CISO
- Managed projects: DLP upgrades, migration from CrowdStrike to Microsoft Defender for Endpoint
- Led phishing simulation campaigns and internal awareness programs
- Supported ISO 27001 audits and PCI-DSS compliance
- Developed SOC coverage roadmap and optimized processes

Information Security and Risk Analyst

- Conducted SIEM monitoring in ELK before SOC structure was established
- Performed daily checks on Symantec DLP and other security control tools
- Rebuilt and applied the annual control plan, including privileged account and admin rights reviews
- Designed and implemented the first processes for phishing monitoring, tracking, and takedowns (impersonation, typosquatting)
- Collaborated on Business Impact Analyses (BIAs) for continuity and risk management
- Administered and maintained endpoint protection (CrowdStrike)
- Automated blacklist analysis with n8n for phishing email investigations

EXPERTISE

- SOC and SIEM: Kibana/ELK, Microsoft Sentinel (use case development, tuning, dashboards)
- EDR and Endpoint: CrowdStrike (deployment, administration), Microsoft Defender for Endpoint (migration project)
- DLP and Data Security: Symantec DLP (incident handling), Microsoft Purview (implementation project)
- Threat Intelligence and OSINT: SecurityTrails, VirusTotal, IPQS, OpenCTI, NCSC Switzerland; phishing takedowns, fraud/darknet monitoring
- Incident Response: phishing, fraud, intrusion attempts, DDoS investigations, playbook authoring
- Cloud Security: Entra ID, O365, CRM 365; Microsoft Defender suite (MDI, MDO, Defender for Cloud)
- Governance and Compliance: ISO 27001 audits, PCI-DSS compliance, password & conditional access policy
- Automation and Scripting: n8n workflows, incident response playbooks, API integrations
- Management: recruitment (7 hires across SOC, GRC, Security Engineering), mentoring, onboarding, awareness campaigns
- Metrics and Reporting: SOC KPIs/KRIs (alert breakdown, EDR/DLP coverage, false positives)
- Infrastructure: VMware vSphere, Windows Server

HOBBIES

- CTF Sqiddies
- PlaidCTF 2025, ranking 248
 - SwampCTF 2025, ranking 19
 - RITSEC CTF 2025, ranking 7
 - Cyber Apocalypse CTF 2025, ranking 3833
 - Black Alps 2024
 - Insomnihack 2024
 - Insomnihack 2025

Fitness, Running, Gaming, Japanese Learning

REFERENCE

Swissquote Bank

Career break

- Switzerland - France2018-2022
- Active volunteer in two nonprofit associations
 - Hacker Without Borders
 - CyberPeace Institute
 - Focused on personal circumstances while maintaining self-study and preparation for a career in cybersecurity

Infrastructure & Security Project Manage

- Sopra Steria - Toulouse, France2015-2018
- Managed a VMware-based infrastructure supporting CNES development teams, coordinating provisioning, availability, performance and operational priorities.
 - Led infrastructure security improvements, including risk assessment, integrity monitoring with Tripwire, SSL/TLS certificate management and remediation tracking.
 - Coordinated technical activities with development and application teams to ensure infrastructure readiness and secure service delivery.
 - Supported Orange production environments, deployments and incident resolution, while automating recurring operational tasks with Bash.

Infrastructure Architecte

- Koncept - Toulouse, France2013-2015
- CNES (main scope): Sole administrator of an infrastructure of 4 physical servers running VMware vSphere
 - Managed dozens of VMs used by development teams for CNES applications
 - Implemented infrastructure security controls: created risk matrix, deployed Tripwire for log integrity, configured SSL/TLS certificates for web apps
 - Oversaw provisioning, monitoring, and troubleshooting of VMs to ensure availability and performance
 - Orange (secondary scope):
 - Supported application servers and production deployments during night shifts
 - Wrote and maintained Bash scripts to automate recurring administrative tasks
 - Assisted in production rollouts and operational support

ACHIEVEMENTS

- Built and managed a SOC from the ground up for a financial institution with 1200 employees
- Established 24/7 on-call structure using PagerDuty and JIRA for incident and task tracking
- Recruited 3 SOC analysts, 2 GRC specialists, and 2 Security Engineers, effectively building the InfoSec team
 - Directed response to large-scale phishing campaigns targeting clients with dozens of malicious domains
 - Investigated multi-vector intrusion attempts combined with DDoS, coordinating across WAF, BIG-IP, and application logs
- Reported bi-weekly to the CISO and contributed to ISO 27001 audits and PCI-DSS compliance
- Defined and tracked SOC KPIs: alert breakdown, EDR/DLP coverage, false positive reduction
- Authored onboarding paths and playbooks, and delivered phishing simulations and awareness campaigns