Benoit Gagnon-Perrault

Sainte-Julie, QC • 514.909.0773 • benoitgperrault@gmail.com • benoitgperrault.github.io • linkedin.com/in/bgperrault

SUMMARY

Cybersecurity Analyst who is fully bilingual, with experience in security operations and remote IT support. Skilled in alert monitoring and analysis, incident investigation, and SIEM/EDR solutions. Experience with Microsoft Sentinel, ArcSight, Splunk and Microsoft Defender for Endpoint. Strong grasp of cloud environments, notably Azure and AWS. Backed by GIAC cybersecurity certifications and ongoing technical training. Recognized for rigor, analytical thinking, and the ability to resolve technical problems efficiently.

SKILLS

SIEM & Security Monitoring : Microsoft Sentinel , Microsoft Defender EDR, ArcSight, Splunk
Incident Detection & Response : Alert Triage, Incident Analysis, IOC Analysis, Escalation, Documentation
Queries & Scripting : PowerShell, Python, Kusto Query Language (KQL)
Network Security : Offensive Security, Vulnerability Management, IAM
OS & Cloud : Windows, Linux, Microsoft Azure, Amazon Web Services (AWS)
Frameworks: NIST, CIS Controls, MITRE ATT&CK

CYBERSECURITY EXPERIENCE

Tier 1 Cybersecurity Analyst, 24/7 SOC, *Hydro-Québec, Montréal* **2020 - 2021**

- Received and triaged security incidents via Microsoft Sentinel (SIEM) and ArcSight, prioritizing events by criticality and meeting established SLAs.
- Analyzed account, authentication, and access-related requests and incidents, performing initial checks and escalations as needed.
- Correlated telemetry data from Microsoft Defender for Endpoint across endpoints, identities, and cloud environments to enrich alerts and support preliminary incident classification.
- Wrote Kusto Query Language (KQL) queries to detect unauthorized software, gather initial event context, and support security investigations.
- Contributed to the response to a major phishing incident targeting a research division by identifying IOCs, assisting with containment, and supporting remediation efforts.

EDUCATION & CERTIFICATIONS

Applied Cybersecurity Certificate | SANS Technology Institute | 2026
Bachelor's Degree in Civil Engineering | École de technologie supérieure (ÉTS) | Montréal, QC | 2012
Cyber Attack Academy | Schank Academy | 2019 (One-year program)
GIAC Certifications: GIAC Continuous Monitoring Certification (**GMON**); Certified Incident Handler (**GCIH**); Security Essentials Certification (**GSEC**); Foundational Cybersecurity Technologies (**GFACT**)
CompTIA: Security+

CYBERSECURITY PROJECTS

Automated SOC & AI-Enriched Detection Lab

- Built a virtualized Splunk SOC to monitor and investigate security events from a Windows 10 endpoint.
- Conducted controlled attacks from Kali Linux, generating security telemetry for detection and analysis.
- Integrated n8n with Splunk and Claude API to automate alert enrichment and provide additional investigation context.

Windows Endpoint Investigation [Powershell, Windows, Security Onion]

- Investigated incidents on Windows endpoints using PowerShell, analyzing logs, processes, services, and IOCs to identify and contain malicious activity.

ADDITIONAL PROFESSIONAL EXPERIENCE

Estimator / Project Manager, *GJ Ménard, Bromont* **2021 - 2024**

- Managed up to 20 excavation projects, ensuring adherence to timelines, budgets, technical specifications, and client requirements.
- Prepared and analyzed over 500 cost estimates, identifying budget variances and improving bid accuracy by approximately 10% to 15%.

LANGUAGES

French: Fluent (Native Language) | **English**: Fluent (Professional Level) | **Spanish** (Functional)