Benoit Gagnon-Perrault

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

SOMMAIRE

Analyste cybersécurité bilingue avec une expérience pratique en environnement SOC et une solide formation technique. Détenteur de certifications GIAC et CompTIA. Expérience avec Microsoft Sentinel, Defender XDR, Arcsight et Splunk. Compétent en analyse de logs, détection des menaces et investigation de sécurité. Reconnu pour ma curiosité technique ainsi que ma facilité d'apprentissage, j'apporte une compréhension approfondie des enjeux de cybersécurité.

COMPÉTENCES

SIEM et surveillance de la sécurité : Microsoft Sentinel, Elastic (ELK), Microsoft Defender EDR, ArcSight
Détection et réponse aux incidents : Triage des alertes, Analyse des incidents, Analyse des IOC, Escalade, Documentation
Requêtes et scripts : PowerShell, Python, Kusto Query Language (KQL)
Sécurité des réseaux : Réseautique, Protocoles réseau, Sécurité offensive, Gestion des vulnérabilités, IAM
OS, bases de données et Cloud : Windows, Linux, SQL, Microsoft Azure, Amazon Web Services (AWS), WAF
Cadres de référence: NIST, CIS Controls, MITRE ATT&CK

EXPÉRIENCE EN CYBERSÉCURITÉ

Conseiller en Cyber Sécurité Niveau 1, SOC 24/7, *Hydro-Québec, Montréal* **2020 - 2021**

- Prise en charge, triage et qualification des incidents de sécurité via Microsoft Sentinel (SIEM) et ArcSight, en assurant une surveillance continue et en priorisant les événements selon leur criticité et en respectant les SLA établis.
- Analyser les demandes et incidents liés aux comptes, aux authentifications et aux accès, puis effectuer les premières vérifications et escalades au besoin.
- Corrélé les données de télémétrie de Microsoft Defender for Endpoint provenant des terminaux, des identités et des environnements infonuagiques afin d'enrichir les alertes et de soutenir la classification préliminaire des incidents.
- Rédigé des requêtes en Kusto Query Language (KQL) afin de développer des cas d'utilisation de détection, d'identifier les logiciels non autorisés et de soutenir les enquêtes de sécurité.
- Contribué à la réponse à un incident majeur d'hameçonnage visant une division de recherche en identifiant les IOC, en participant aux mesures de confinement et en appuyant les activités de remédiation.

ÉDUCATION & CERTIFICATIONS

Applied Cybersecurity Certificate | SANS Technology Institute | 2026
Bachelier en Génie Civil | École de technologie supérieure (ÉTS) | Montréal, QC | 2012
Cyber Attack Academy | Schank Academy | 2019 (Programme d'un an)
Certifications GIAC: GIAC Continuous Monitoring Certification (**GMON**); Certified Incident Handler (**GCIH**); Security Essentials Certification (**GSEC**); Foundational Cybersecurity Technologies (**GFACT**)
CompTIA: Security+

PROJETS DE CYBERSÉCURITÉ

Laboratoire SOC automatisé et enrichissement par IA [VMware, Splunk, n8n, Slack]

- Mise en place d'un SOC virtualisé avec Splunk pour la surveillance des événements de sécurité d'un poste Windows 10.
- Réalisation d'attaques contrôlées à partir de Kali Linux afin de valider les capacités de détection.
- Intégration de n8n, Splunk et l'API Claude afin d'automatiser l'enrichissement et l'analyse des alertes de sécurité.

Investigation de Postes Windows [Powershell, Windows, Security Onion]

- Investigé des incidents sur des postes Windows à l'aide de Powershell en analysant les journaux et IOC.

EXPÉRIENCE PROFESSIONNELLE ADDITIONNELLE

Estimateur/ Chargé de Projets, *GJ Ménard, Bromont* **2021 - 2024**

- Géré jusqu'à 20 projets d'excavation tout en assurant le respect des échéanciers, des budgets, des spécifications techniques et des exigences des clients.
- Préparé et analysé plus de 500 estimations de coûts avec un taux de succès de 33%.

LANGAGES

Français : Courant (Langue Maternelle) | **Anglais** : Courant (Niveau Professionnel) | **Espagnol** (fonctionnel