JÉRÉMIE DUFAULT

Cybersécurité, admninistation informatique, réseautique et IA

jeremie@jdufault.net
418-928-1428

Conseiller en sécurité de l'information | Gouvernance des risques & Innovation IA

Professionnel de la cybersécurité avec plus de 15 ans d'expérience en TI, spécialisé en gouvernance de la gestion des vulnérabilités et en évaluation des risques pour des dizaines d'organisations clientes. J'accompagne les équipes de direction dans la priorisation des risques et la mise en place de stratégies de remédiation, tout en explorant concrètement l'apport de l'intelligence artificielle à la sécurité (outil de pentest assisté par LLM, classification automatisée des menaces MITRE ATT&CK). Mentor bénévole depuis 2009, j'aime transmettre mes connaissances autant qu'apprendre des autres. N'a pas peur de sortir des sentiers battus

EXPÉRIENCES

Conseiller en sécurité de l'information - Gestion des vulnérabilités

KPMG - Depuis novembre 2021

- Accompagnement de dizaines d'organisations clientes dans la structuration de leur programme de gestion des vulnérabilités : identification, priorisation par risque, plans de remédiation
- Rédaction de rapports stratégiques destinés à la haute direction pour soutenir la prise de décision
- Conception et développement d'un outil de pentest assisté par IA (LLM) : orchestration du flux de travail, évaluation de modèles, génération automatisée de rapports
- Phase initiale (2021-2023) en analyse SOC : triage et investigation d'alertes de sécurité (SOAR/SIEM), corrélation d'événements, escalade vers les équipes de remédiation

Technicien informatique

Institut national de santé publique du Québec (INSPQ) - Août 2020 à novembre 2021

- Migration automatisée Windows 7 vers Windows 10
- Automatisation de déploiement d'outils et correctifs
- Support technique niveau 3
- Résolution de problèmes interdépartementaux complexes

Spécialiste Technique sénior

6Tem TI - Novembre 2016 à août 2020

- Gestion des incidents complexes
- Administration serveurs et équipements réseau
- Implémentation solutions de sauvegarde
- Coordination migrations Microsoft 365

Spécialiste Technique sénior

Soges-Tech - Décembre 2011 à mars 2016

- Migrations serveurs Exchange et SharePoint
- Mise en place serveur MDT/WDS
- Supervision système de sauvegarde
- Dépannage infrastructures complexes

FORMATIONS

Baccalauréat en Cybersécurité

POLYTECHNIQUE DE MONTRÉAL

- Cyber-Enquête
- Cyber-Fraude
- Architecture et Gestion de la Cybersécurité

AEC Administration des réseaux et sécurité informatique

CÉGEP LIMOILOU

Divers

CERTIFICATS

- Digital Forensic Essential
- CCNA cours 1/2/3
- Microsoft OEM Presinstallation
- MCITP : Windows 7, configuration

COMPÉTENCES

CYBERSÉCURITÉ

- Gestion des vulnérabilités
- Analyse SOC
- Informatique judiciaire (forensic)
- OSINT (investigation par sources ouvertes)
- Gestion des incidents
- Gouvernance de la sécurité de l'information
- Évaluation et priorisation des risques

INFRASTRUCTURE RÉSEAU

- Fortinet
- Cisco
- Palo-Alto
- OPNSense
- HP

SYSTÈMES ET SERVEURS

- Conteneurs (Docker, LXC)

Spécialise technique / Technicien informatique

Ms Solutions - Novembre 2010 à décembre 2011

- Support technique pour entreprises et GMF
- Gestion des autorisations numériques
- Maintenance serveurs Windows
- Déploiement WDS/MDT
- Assistance système de sauvegarde Ahsay

PROJETS NOTABLES

Mise en œuvre et entraînement de modèles de langage spécialisés
Fine-tuning de BERT pour la classification automatisée d'attaque MITRE des CVE et Spécialisation de LLMs pour le langage Mermaid.js par Apprentissage Supervisé

Projets Applicatif via programmation assisté par intelligence artificielle
Projet personnel Mermaidstudio.net et portail Threat Intelligence complet

Mise en place et gestion de solution de déploiement
Mises en place de serveurs de déploiement MDT/WDS pour migration de Windows XP vers Windows 7 et Windows 7 vers Windows 10

Migration Microsoft365
Plusieurs migrations de produits Microsoft vers des versions plus récentes ou vers le cloud : Active Directory, Exchange, Sharepoint

Virtualisation de serveur physique (VMware, Hyper-V)
Plusieurs migration et mise en production de serveur virtuel vers des solutions de virtualisations comme VMware et Hyper-V

CENTRES D'INTÉRÊT

Cybersécurité

- Veille de sécurité informatique
- OSINT et renseignement numérique
- Techniques d'investigation numérique
- Tendances émergentes en cybercriminalité

Technologie

- Laboratoire informatique personnel
- Découverte de nouvelles technologies de sécurité
- IoT et sécurité des objets connectés
- Exploration des technologies open source
- Domotique et automatisation résidentielle
- Virtualisation avancée et orchestration de conteneurs
- Intelligence artificielle : Deep Learning, LLM
- Linux (Debian, Arch)
- Windows Server (AD, FS, DNS, DHCP)
- Virtualisation (VMware, Hyper-V, Xen)

ENVIRONNEMENT MICROSOFT

- Microsoft 365
- Entra ID
- MS Defender 365

AUTOMATISATION ET DÉPLOIEMENT

- MDT/WDS/SCCM/Intune
- PowerShell
- Migrations système
- Gestion de configuration

COMPÉTENCES TRANSVERSALES

- Gestion des incidents critiques
- Support technique avancé
- Documentation structurée
- Gestion de projets techniques

LANGUES

Français ★★★★★

Anglais ★★★☆☆