Felix Boulet

Sainte-Marcelline-de-Kildare, Québec, Canada
LinkedIn : linkedin.com/in/felix-boulet

Profil

Chercheur en sécurité offensive, spécialisé dans l'identité, l'isolation multilocataire et les failles de conception architecturale. Plus de 8 ans d'expérience en cybersécurité, dont plus de 6 en sécurité offensive : recherche de vulnérabilités et tests d'intrusion. Classé 8e mondial au MSRC (2026), 1er au classement mondial Identité et auteur de plus de 30 CVE (Microsoft, Docker, KDE, VMware Aria). Collaboration directe avec les ingénieurs de Microsoft lors des deux dernières éditions du Zero Day Quest et coprésentation à BlueHat Asia avec un chercheur senior de l'éditeur. Je mets aujourd'hui cette compréhension des failles systémiques au service de la résilience des architectures infonuagiques et des systèmes d'IA.

Réalisations marquantes

- **Classements mondiaux Microsoft (MSRC) :** 8e chercheur mondial au classement « Most Valuable Researchers » en 2026 (29e en 2025, 26e en 2024); 1er au classement technique mondial Identité (2026), 2e en Dynamics 365 et Power Platform, et 6e au concours Zero Day Quest; présences régulières au top 10 trimestriel. Classement officiel 2026
- **Conférencier, BlueHat Asia 2026 (Singapour) :** *Taking Control: Four Simple Paths To Own an Entra ID Account*, recherche sur les chemins de compromission d'identité coprésentée avec un chercheur senior de Microsoft (septembre 2026). Annonce officielle
- **CVE-2025-9074 (Score CVSS 9.3) :** Découverte d'une évasion complète de conteneur dans Docker Desktop (Windows et macOS), couverte par la presse spécialisée (The Hacker News, CSO Online, SecurityAffairs) et analysée par Low Level et John Hammond.
- **Plus de 30 CVE et failles de conception cloud :** Découvertes confirmées dans VMware Aria (CVE-2024-22280), Microsoft (Azure, Office, SharePoint, Edge), Docker, l'écosystème Linux KDE (Kubuntu), et SonicWall. Nombreuses failles de conception cloud corrigées directement côté serveur sans attribution de CVE public.
- **Reconnaissance technique par Microsoft :** Profil officiel de chercheur publié par le MSRC (« From arcades to Azure: Felix's security research journey », février 2026) et invité au podcast officiel BlueHat de Microsoft (« Hacking at the Weeds with Felix Boulet », mai 2025).

Expérience professionnelle

Chercheur indépendant en vulnérabilités - 2020 - présent (temps partiel avant 2024)

- **Recherche sur les architectures d'identité et de confiance :** Analyse approfondie de la logique d'autorisation, des flux OAuth 2.0, OIDC et SAML, et de l'isolation multilocataire sur les plateformes infonuagiques à large échelle.
- **Chaînes d'attaque et failles de logique :** Découverte et documentation de vulnérabilités critiques de conception permettant notamment le vol de jetons, le contournement de l'AMF (*MFA*) et de l'accès conditionnel, menant à la prise de contrôle totale de locataires (*tenants*).
- **Divulgation responsable et remédiation avec les éditeurs :** Collaboration directe avec les équipes d'ingénierie et de sécurité produit (notamment Microsoft MSRC, Docker et KDE) pour la reproduction des PoC et la validation des correctifs d'architecture, ayant mené à plus de 25 CVE attribués dans le cadre de ces recherches indépendantes.
- **Autres divulgations :** Vulnérabilités divulguées de façon responsable et corrigées par Apple, Google et Microsoft sans attribution de CVE.
- **Développement d'outillage offensif spécialisé :** Programmation d'extensions Burp Suite sur mesure, de scripts d'automatisation et de harnais de validation (Python, Java) pour sonder les mécanismes de contrôle d'accès complexes.

Analyste principal en tests d'intrusion - Ministère de la Cybersécurité et du Numérique (MCN) - 2023 - 2024

- **Contribution méthodologique :** Contribution à la méthodologie de test d'intrusion de l'équipe, alignée sur le cadre WSTG, et à un gabarit de rapport normalisé axé sur la probabilité d'exploitation et l'impact opérationnel réel.
- **Contrôle qualité technique :** Animation de revues techniques par les pairs sur les livrables de l'équipe, à trois étapes : cadrage initial, validation à mi-mandat et revue des scénarios d'exploitation finaux.
- **Évaluation de systèmes gouvernementaux :** Réalisation de tests d'intrusion sur des systèmes du secteur public; présentation des vulnérabilités critiques avec des plans de correction concrets à des publics techniques et à la direction.
- **Formation et montée en compétences :** Animation d'ateliers techniques internes sur la reconnaissance passive et active, la délimitation des périmètres d'attaque et l'analyse de surface d'exposition.

Consultant senior en sécurité offensive - KPMG (EGYDE Conseils) - 2020 - 2023

- **Mandats Red Team et Purple Team :** Exécution de scénarios de compromission adversariale sur des environnements d'entreprise hybrides, incluant Linux, Windows, Active Directory, Entra ID, applications web et mobiles.
- **Développement d'outils d'évasion :** Conception d'outils internes pour l'obfuscation de code, le contournement des défenses périmétriques et l'évaluation de l'efficacité des solutions EDR et SIEM.
- **Sécurisation du cycle de développement (DevSecOps) :** Accompagnement d'équipes logicielles dans l'intégration de contrôles de sécurité automatisés au sein de pipelines CI/CD et priorisation pragmatique des correctifs.
- **Vulgarisation et transfert technique :** Présentation des vecteurs d'attaque et des enjeux de chiffrement aux équipes de gestion; formation continue des consultants juniors et collaboration avec les équipes SOC.

Analyste en cybersécurité (SOC et Détection) - Devolutions - 2018 - 2020

- **Surveillance opérationnelle et Threat Hunting :** Triage, corrélation et investigation d'alertes de sécurité sur des piles technologiques d'entreprise (SIEM, EDR, Defender for Office 365) et conception de règles de détection comportementales personnalisées.
- **Évolution de l'outillage de défense :** Réalisation de l'analyse comparative technique et financière pour l'implantation d'un nouveau SIEM; participation aux analyses de risques et audits de sécurité.

Formation

- **Maîtrise en informatique, cheminement en cybersécurité** - Université de Sherbrooke - 2026
  - Spécialisation en architecture de sécurité, cryptographie appliquée, sécurité logicielle, criminalistique et gestion des technologies d'intelligence artificielle.
- **École d'été en cybersécurité** - Université de Sherbrooke - 2023
  - Enjeux de conformité à la Loi 25 québécoise, encadrement de l'identité numérique, cryptographie post-quantique (PQC) et applications de l'IA en cybersécurité.
- **Formation spécialisée en agents autonomes (Hugging Face)** - 2026
  - Architectures agentiques, boucles de raisonnement, appels d'outils (*tool calling*) et intégration sécurisée de modèles de langage (LLM).
- **Certificat en cybersécurité des réseaux informatiques** - Polytechnique Montréal - 2020
  - Sécurité des environnements infonuagiques (Cloud), systèmes de contrôle industriels (SCADA et ICS), tests d'intrusion et réponse aux incidents.

Certifications

- **OSCE3 (OffSec Certified Expert 3)** - OffSec - 2023
  - **OSWE (Web Expert) :** Audit de code source (*white-box*) en Python, Node.js, PHP, Java et .NET; analyse statique et dynamique de logique applicative et programmation de scripts d'exploitation automatisés complets.
  - **OSEP (Evasion & Breaching) :** Programmation de chargeurs (*loaders*) et d'outils sur mesure en C# (.NET), macros VBA, scripts PowerShell et interactions avec les API Win32 pour contourner les contrôles de sécurité.
  - **OSED (Exploit Development) :** Rétro-ingénierie avec les désassembleurs et débogueurs IDA, écriture et optimisation de *shellcode* en assembleur x86 (gestion des contraintes d'espace et de restrictions contextuelles), et utilisation de techniques avancées de contournement de protections mémoire.
- **OSCP (OffSec Certified Professional)** - OffSec - 2020
  - Reconnaissance réseau, élévation de privilèges Linux et Windows, pivotement d'infrastructure et exploitation de systèmes sans outils automatisés.
- **LFD121 : Developing Secure Software** - The Linux Foundation - 2022
  - Principes de conception de code sécurisé, modélisation des menaces et intégration au pipeline CI/CD (DevSecOps).
- **GCIH (GIAC Certified Incident Handler)** - GIAC - 2018
  - Analyse d'artefacts système, rétro-ingénierie de base de charges malveillantes et triage d'attaques réseau et système.

Liens de référence

- **Classement officiel MSRC 2026 :** https://www.microsoft.com/en-us/msrc/blog/2026/07/congratulations-to-the-msrc-2026-most-valuable-security-researchers1
- **Annonce BlueHat Asia 2026 :** https://www.linkedin.com/feed/update/urn:li:activity:7483829645021274113/
- **Profil de chercheur MSRC :** https://www.microsoft.com/en-us/msrc/blog/2026/02/from-arcades-to-azure-felix-security-research-journey
- **Podcast Security Unlocked, épisode 62 :** https://shows.acast.com/security-unlocked-3/episodes/hacking-at-the-weeds-with-felix-boulet