Felix Boulet

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

Profile

Security researcher specializing in complex systems evaluation, identity architecture, and design-level flaws. Over 8 years of cybersecurity experience, including 6+ years in offensive security: vulnerability research, penetration testing, and methodological mentoring for operational teams. Ranked #8 globally by MSRC (2026), #1 worldwide in Identity security, and credited with 30+ CVEs (Microsoft, Docker, KDE, VMware Aria). Experienced with large-scale architectures, having built a proven track record of cross-team and inter-organizational collaboration during consulting engagements and at the MCN. Extended this collaborative approach by working directly with Microsoft engineers during the last two Zero Day Quest editions, and co-presenting at BlueHat Asia alongside a Senior Security Researcher from Microsoft. Currently applying this deep understanding of systemic flaws to enhance the resilience of cloud architectures and AI agent systems.

Key Achievements

- **Microsoft Security Response Center (MSRC) Global Rankings:** Ranked #8 worldwide among "Most Valuable Researchers" (MVR) in 2026 (29th in 2025, 26th in 2024); #1 globally in Identity security (2026), 2nd in Dynamics 365 & Power Platform, and 6th in the Zero Day Quest competition; recurring top-10 quarterly finisher. Official 2026 Ranking
- **Speaker, BlueHat Asia 2026 (Singapore):** *Taking Control: Four Simple Paths To Own an Entra ID Account*, research on identity attack paths co-presented with a Senior Security Researcher from Microsoft (September 2026). Official Announcement
- **CVE-2025-9074 (CVSS Score 9.3):** Discovered a full container escape in Docker Desktop (Windows & macOS), covered by specialized media (The Hacker News, CSO Online, SecurityAffairs) and analyzed by Low Level and John Hammond.
- **30+ CVEs & Cloud Architectural Flaws:** Confirmed vulnerabilities in VMware Aria (CVE-2024-22280), Microsoft (Azure, Office, SharePoint, Edge), Docker, the KDE Linux ecosystem (Kubuntu), and SonicWall. Multiple critical cloud design flaws remediated directly server-side without public CVE assignment per vendor policy.
- **Technical Recognition by Microsoft:** Official researcher profile published by the MSRC ("From arcades to Azure: Felix's security research journey", February 2026) and featured guest on Microsoft's official BlueHat podcast (*Security Unlocked*, Episode 62, May 2025).

Professional Experience

Independent Vulnerability Researcher - 2020 - Present (Part-Time before 2024)

- **Identity & Trust Architecture Research:** In-depth analysis of authorization logic, OAuth 2.0, OIDC, and SAML protocols, and multi-tenant isolation across hyper-scale cloud platforms.
- **Attack Chains & Logic Flaws:** Discovered and documented critical design-level flaws enabling token exfiltration, MFA and conditional access bypasses, leading to full tenant takeover.
- **Coordinated Vulnerability Disclosure & Vendor Remediation:** Direct collaboration with vendor engineering and product security teams (notably Microsoft MSRC, Docker, and KDE) to reproduce PoCs and validate architectural patches, leading to 25+ CVEs credited from this independent research.
- **Additional Disclosures:** Vulnerabilities responsibly disclosed and fixed by Apple, Google, and Microsoft without CVE assignment.
- **Custom Offensive Tooling Development:** Engineered custom Burp Suite extensions, automated exploitation scripts, and testing harnesses (Python, Java) to probe intricate access control mechanisms.

Lead Pentester - Ministry of Cybersecurity and Digital Affairs (MCN) - 2023 - 2024

- **Methodology Contribution:** Contributed to the team's penetration testing methodology, aligned with the WSTG framework, and to standardized report templates focused on exploitability and real-world operational impact.
- **Technical Quality Assurance:** Led technical peer reviews of team deliverables at three stages: initial scoping, mid-engagement validation, and final exploitation scenario reviews.
- **Government Systems Assessment:** Conducted penetration tests on public-sector systems and presented critical findings with actionable remediation plans to technical and executive audiences.
- **Training & Skills Enablement:** Led technical workshops on passive and active reconnaissance, attack surface mapping, and perimeter enumeration.

Senior Offensive Security Consultant - KPMG (EGYDE Conseils) - 2020 - 2023

- **Red Team & Purple Team Engagements:** Executed adversarial attack simulations across complex hybrid enterprise environments (Linux, Windows, Active Directory, Entra ID, web, and mobile apps).
- **Evasion Tooling Development:** Built in-house tools for code obfuscation, defensive perimeter evasion, and control effectiveness testing against modern EDR and SIEM solutions.
- **Secure Software Development (DevSecOps):** Advised software engineering teams on embedding automated security checks into CI/CD pipelines and prioritizing pragmatic vulnerability fixes.
- **Executive Communication & Knowledge Transfer:** Briefed executive stakeholders on technical attack vectors and cryptographic implications; mentored junior consultants and collaborated with SOC teams.

Cybersecurity Analyst (SOC & Threat Hunting) - Devolutions - 2018 - 2020

- **Operational Monitoring & Threat Hunting:** Triaged, correlated, and investigated security alerts across enterprise stacks (SIEM, EDR, Defender for Office 365), and engineered tailored behavioral detection rules.
- **Defensive Tooling & Audits:** Led technical and financial comparative evaluations for new SIEM deployments; conducted risk assessments and corporate security audits.

Education

- **Master of Science in Computer Science, Cybersecurity Concentration** - Université de Sherbrooke - 2026
  - Specialization in security architecture, applied cryptography, software security, digital forensics, and AI technologies management.
- **Cybersecurity Summer School** - Université de Sherbrooke - 2023
  - Law 25 regulatory compliance, digital identity frameworks, Post-Quantum Cryptography (PQC), and AI in cybersecurity.
- **Specialized Certification in Autonomous Agents (Hugging Face)** - 2026
  - Agentic architectures, reasoning loops, tool calling, and secure Large Language Model (LLM) integration.
- **Certificate in Computer Network Cybersecurity** - Polytechnique Montréal - 2020
  - Cloud security, Industrial Control Systems (ICS/SCADA), penetration testing, and incident response.

Certifications

- **OSCE3 (OffSec Certified Expert 3)** - OffSec - 2023
  - **OSWE (Web Expert):** White-box source code auditing in Python, Node.js, PHP, Java, and .NET; static and dynamic application logic analysis and custom automated exploit scripting.
  - **OSEP (Evasion & Breaching):** Custom loader and payload engineering in C# (.NET), VBA macros, PowerShell, and low-level Win32 API interaction to bypass defensive controls.
  - **OSED (Exploit Development):** Reverse engineering with IDA disassembler and debuggers, custom x86 assembly shellcoding (space and context constraints), and memory mitigation bypasses.
- **OSCP (OffSec Certified Professional)** - OffSec - 2020
  - Network reconnaissance, Linux/Windows privilege escalation, lateral movement/pivoting, and manual exploitation without automated tooling.
- **LFD121: Developing Secure Software** - The Linux Foundation - 2022
  - Secure software design principles, threat modeling, and DevSecOps CI/CD pipeline integration.
- **GCIH (GIAC Certified Incident Handler)** - GIAC - 2018
  - System artifact analysis, basic malware reverse engineering, and network/host incident triage.

Reference Links

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