

Max Mirkin

Cybersecurity Director · Security operations, threat hunting, fraud prevention and security engineering

Toronto, ON max@mirkin.ca linkedin.com/in/maxim-mirkin-b14682222 github.com/Unworthy8414
godelswork.shop

Summary

Security leader who runs the program and still builds the tools it depends on. Led Questrade's JSOC and security function through a CISO transition, growing the team from 6 to 25 and the budget by \$2M. Built fraud prescreening that prevents over \$8M a month in losses. Cut SOC escalations from 250+ a day to one with AI automation, freeing the same team to also cover vulnerability management, threat intelligence and hunting. Background in threat hunting, fraud, reverse engineering and offensive security at RBC and Questrade; took four inventions to RBC's patent board.

Experience

Questrade Financial Group

Toronto, ON · May 2025 – Present

Director, JSOC

Took over the JSOC and ran the security function through a CISO transition.

- **Scope:** SOC, incident response, threat hunting, client-facing digital threat hunting, vulnerability management, threat intelligence, security development and customer identity. Later absorbed SecDevOps.
- **Team and budget:** Grew the JSOC from 6 to 25 people and secured \$2M in added budget after repeated cuts. Interviewed and recommended the incoming CISO, and interviewed CTO candidates.
- **Audit and compliance:** Led the company through its SOC 2 audit and multiple Deloitte audits.
- **AI automation:** Automated SOC triage and incident response end to end with AI. Analysts now handle at most one escalated event a day, down from over 250.
- **Fraud prescreening:** Built fraud prescreen engines for the trading platform and Flexiti's credit card with two developers, infrastructure included. The engines prevent over \$8M a month in fraud losses.
- **Device fingerprinting:** Built browser and mobile fingerprinting in-house that outperformed LexisNexis and FingerprintJS on both cardinality and hash consistency. Bound client sessions to device fingerprints, closing off session hijacking as an attack path.
- **Fraud investigations:** Developed ML and heuristic correlation models that let investigators confirm genuine fraud victims and catch false claims. Worked 8+ false claim cases personally in the first six months.
- **Phishing:** Built a real-time TLS certificate stream in Rust with proprietary detection, plus a phishing site scanner and a malvertising detector. Customer compromises from phishing sites fell from 20+ a month to zero.
- **Endpoint security:** Solo-built ExtGuard/Ladon, an endpoint agent on 2,000+ Mac and Windows machines. It proxies package managers, vets MCP servers, checks AI prompts and monitors browser extensions.
- **Coverage gaps:** Brought in the company's first cloud detection and response (CDR), covering 10,000+ digital assets, and added DAST.
- **Developer-owned AppSec:** Introduced SAST with a developer-owned model. Teams secure their own stack from code to deployment, including IaC, and use security engineering as advisors, not gatekeepers.
- **Upskilling:** Made HackTheBox certification mandatory for the team. Trained SecDevOps in manual code review and the SOC in raw log analysis.

Director, Questrade Optimization & Security Team

Returned to Questrade to cut costs and fix reliability and performance across the group's technology.

- **Optimization:** Audited licensing, architecture, compute and database performance across the group, identifying \$25M in annual savings. Introduced ClickHouse for real-time trade analytics and rewrote most search and charting services from $O(n^2)$ to $O(\log n)$.

- **Flexiti:** Found NoSQL injection in 7 places, separated card data from web logs, and pushed to replace per-vendor deployments with one central portal.

Principal Cyber Threat Hunter – RBC

Toronto, ON · Nov 2023 – May 2025

- Co-led a six-person team that designed, built and ran RBC's in-house security tools.
- Built custom JavaScript anti-phishing tooling that baited attackers and correlated threat actors, saving over \$4M a year in fraud losses.
- Built a Python ML classifier using gradient boosting that detects malicious hosts from their fingerprint configurations.
- Automated threat-hunt validation through exploitation with a custom LLM RAG wrapper and hot-loaded extensions, saving over \$450K in analyst hours.
- Presented four inventions to RBC's patent board and senior executives; two were implemented. Also helped build tools that detect infringement of RBC's IP.
- Investigated 258 potential insider-risk cases, including git exfiltration, unauthorized apps, internal phishing and cloud data egress across Azure, AWS and GCP.
- Built a Telegram scraping network for threat intelligence on EMT fraud sales, mapping 8 threat-actor clusters.

Senior Threat Hunter – Questrade, Inc.

Toronto, ON · Apr 2021 – Sep 2023

- Led Questrade's threat hunting program, using MITRE ATT&CK, OWASP and NIST RMF and prioritizing hunts by new CVEs and world events.
- Led dozens of unstructured hunts that found 50+ vulnerabilities across on-premises and cloud systems (AWS, GCP, Google Workspace, Salesforce), which were then patched.
- Led a cyber fraud investigation that resulted in a criminal investigation of the fraudster.
- Wrote Go, Python and JavaScript automation for log analysis and playbook alignment, saving 100+ hours of operations time.
- Worked with the JSOC, TVM, Cyber Strategy & Risk and Enterprise Architecture teams, cutting response times by 50%. Set hunt KPIs and mentored the team.

Consultant and Project Assistant – Secureye

Toronto, ON · Jun 2019 – Feb 2020

- Managed IT security projects that upgraded physical security infrastructure at 12+ client sites.
- Ran counterintelligence assessments that found and exploited 8 system vulnerabilities, documenting each gap for remediation.
- Wrote scripts that automated vulnerability scanning across client networks, surfacing an average of 14 issues per assessment.

Part-time roles

Founder and CEO – VIMWIRE Ltd.

Toronto, ON · Nov 2022 – Present

- Built and solely maintain Godelswork.shop, a proprietary TypeScript replacement for Carnap that teaches propositional and first-order logic.
- Used at the University of Toronto by about 1,000 students a month, scaling to 10,000.

Chief Software Architect, Philosophy – University of Toronto

Toronto, ON · May 2018 – Present

- Lead a six-person team on Project Carnap, the department's sentential logic platform, setting priorities and delivering every milestone on time.

- Designed its security architecture around database protection, preventing SQL injection against student data. Zero security incidents since deployment.
- Set secure coding standards that cut security defects found in QA by 30%.

Skills

- **Leadership:** security strategy and roadmap, org design and hiring, budget ownership, build-vs-buy and vendor evaluation, executive briefings, SOC 2 and external audits, team upskilling.
- **Security operations:** SOC, incident response, structured and unstructured threat hunting, threat intelligence, vulnerability management, insider risk, cloud detection and response.
- **Fraud and identity:** fraud prescreening, device fingerprinting, anti-phishing and brand protection, customer identity (CIAM).
- **Engineering and offensive security:** reverse engineering, penetration testing, application security (SAST, DAST, code review), SecDevOps, AI and ML for detection (LLMs, RAG, gradient boosting).
- **Programming:** Python, Go, Rust, JavaScript, C, C++, C#, Haskell, SQL, KQL.
- **Platforms:** SIEM, SOAR, EDR and threat intelligence platforms, including Wiz, CrowdStrike, Splunk, QRadar, Chronicle, Datadog, ELK, Mimecast, Rapid7, Mandiant, Entra ID, Device42, Canary, ANY.RUN and AlertLogic.
- **Languages:** fluent in English, Russian and French.

Education and certifications

- **Bachelor of Arts**, University of Toronto. Double major: Philosophy, and Philosophy and History of Science. 3.96 GPA; Dean's List all four years.
- **Associate of ISC2:** passed the CISSP exam; full CISSP certification expected by December 2026.