

AMIR HOSSEINPOUR

OT and ICS Security Consultant

amir-ot.pages.dev

PROFESSIONAL SUMMARY

Offensive security consultant bringing an attacker's perspective to operational technology (OT), industrial control systems (ICS) and IoT security for critical infrastructure. At White Tuque I ran six months of red team engagements for a Canadian independent power producer and turned the results into a resilience-checking playbook mapped to their compliance requirements, built the red team pipeline for a major Canadian insurer, and contributed to deception-based detection for a mining company. I assess OT/IT convergence environments in oil and gas, mining, utilities and manufacturing, hands-on with SCADA and PLC protocols (Modbus TCP, DNP3, S7, EtherNet/IP, Profinet), building automation (BACnet, KNX) and IIoT (OPC UA, MQTT), with findings mapped to the Purdue model and MITRE ATT&CK for ICS. At ASEC I worked with smart building construction companies and ran physical red team engagements. My embedded device research found a six-bug chain that could give root on any of the ~10 million robots in the Ecovacs Deebot fleet, with six CVEs filed. 15+ conference talks, including SecTor 2025 on red teaming the smart building; co-organizer of DEFCON Toronto (DC416).

CORE SKILLS

- **OT and ICS security:** ICS assessments, OT/IT convergence, industrial control system and critical infrastructure security across oil and gas, mining, utilities, manufacturing and smart buildings
- **Industrial protocols:** SCADA (Modbus TCP, DNP3), PLC (S7, EtherNet/IP, Profinet), building automation (BACnet, KNX), IIoT (OPC UA, MQTT)
- **Architecture and standards:** Purdue model, industrial segmentation, MITRE ATT&CK for ICS, threat modeling that weighs safety, availability and process integrity
- **Assessment methodology:** non-disruptive, non-destructive OT assessment; penetration testing; red team, purple team and physical red teaming; C2 operations with Cobalt Strike and Havoc
- **OT detection and deception:** honeypot-style decoys that turn any attacker contact into a high-confidence alert, giving early warning of reconnaissance and lateral movement without touching production
- **Embedded and IoT research:** UART access, firmware extraction and analysis, protocol analysis, vulnerability discovery, attack technique development, coordinated disclosure
- **Consulting delivery:** technical and executive deliverables, business and operational risk reporting, pre-sales scoping, proposals, SOWs and rules of engagement, mentoring

PROFESSIONAL EXPERIENCE

White Tuque – Offensive Security Specialist

Toronto, ON | October 2024 – Present

- Ran six months of red team engagements for a Canadian independent power producer, then combined the results into a months-long series of working sessions with their IT team. The outcome was a resilience-checking playbook mapped to the compliance requirements they must meet.
- Built the red team and penetration-testing pipeline for a major Canadian insurer, with recurring adversary simulations and tabletop exercises in place of a single annual test.
- Contributed to deception-based detection for a mining company: honeypot-style decoys that turn any attacker contact into a high-confidence alert, catching reconnaissance and lateral movement early without touching production, an approach suited to OT networks where controllers can't run endpoint agents.
- Assess OT/IT convergence and industrial control system environments for oil and gas, mining, utilities and manufacturing clients, testing SCADA and PLC protocols (Modbus TCP, DNP3, S7, EtherNet/IP, Profinet) and mapping findings to the Purdue model and MITRE ATT&CK for ICS.
- Deliver penetration testing, red team and purple team assessments for 20+ enterprise clients across Canada and the US, and operate Cobalt Strike and Havoc C2 on red team engagements.
- Translate findings into business risk and operational risk in reports engineering teams, security architects and leadership act on; support pre-sales with scoping, proposals, SOWs and rules of engagement; mentor interns.

ASEC – Penetration Tester

Toronto, ON | May 2024 – October 2024

- Worked with smart building construction companies on building automation and IoT security, including BACnet and KNX systems.
- Ran physical red team engagements for fintech clients that required them.
- Delivered application, API and network penetration testing for financial-services clients in Canada, the US, Australia and Europe, specializing in API and GraphQL security under Nick Aleks, author of *Black Hat GraphQL* and former Head of Security at Robinhood.

HackerOne – Security Researcher

Remote | February 2022 – Present

- 120+ validated vulnerabilities across Fortune 500 programs, including severe findings on PayPal, Airbnb, Sony, Booking.com and AT&T; vulnerability discovery in authorization, race conditions and multi-step business logic.

DEFCON Toronto (DC416) – Co-organizer

Toronto, ON | 2025 – Present

- Find researchers and presenters and program the monthly talks and workshops for Toronto's security community.
- Ran the AI Fight Club at Palo Alto Networks, a hands-on workshop for 200+ practitioners on attacking and defending LLM and agent systems.

RESEARCH AND PUBLISHED FINDINGS

- **Ecovacs Deebot fleet compromise (embedded device research):** soldered onto the UART, dumped the firmware, recovered cloud credentials and mapped the MQTT topic tree. The broker trusted whatever device identity a client claimed, and robots ran incoming commands as root with no signature check, so the six-bug chain could give root on any of the ~10 million robots in the fleet from any account. Six CVEs filed with MITRE; coordinated disclosure under the vendor's Safe Harbor; presented at BSides Toronto 2026; write-up on defcontoronto.ca.
- **Smart building red teaming:** SecTor 2025 talk "When Hackers Meet Burglars: Red Teaming the Smart Building," on attacking buildings where automation, access control and physical security meet.

SPEAKING AND COMMUNITY

- 15+ conference talks, including SecTor 2025, BSides Toronto 2026, TASK Toronto 2025 and 2026, DEFCON Vancouver (Microsoft-hosted) and InfoSec Hamilton.
- Organizing committee, TASK (Toronto Area Security Klatch), Toronto's longest-running security community: help plan its meetups and events.

TOOLS

- **Eidolon:** open-source (MIT) offensive security workspace with an AI agent in the loop: per-engagement isolation, scope tokens, hash-chained audit log and command gating. Also published `graphql_sdl_generator` and a Burp Suite extension that flags endpoints reachable without authentication.

TECHNICAL SKILLS

- **OT and ICS:** Modbus TCP, DNP3, S7, EtherNet/IP, Profinet, BACnet, KNX, OPC UA, MQTT; Purdue model; MITRE ATT&CK for ICS
- **Hardware and IoT:** UART, firmware extraction and analysis, device-to-cloud protocol analysis
- **C2 and offensive tools:** Cobalt Strike, Havoc, Burp Suite Pro, nmap, Metasploit, BloodHound, mitmproxy, Frida, objection
- **Programming:** Python, Go, Bash, JavaScript, TypeScript
- **Languages:** English, Farsi, Mandarin

EDUCATION

Bachelor of Computer Engineering, University of Sistan and Baluchestan