

H I R I N G R O U N D

CHRIS BOUCEK

Senior Security Product Leader.

AI-native. Battle-tested. Available.

Twenty years in deep network and systems. Ten years in MDR. Seven years owning detection-and-response at fleet scale. Four 0-to-1 launches. \$30M+ ARR. CISSP. Built for what comes next.

build@cboucek.net · linkedin.com/in/chrisboucek · cboucek.net



Security operations is broken at exactly the moment AI is rewriting it.

\$4.5M

Average enterprise cost per security incident

75%

of SOC alerts are false positives

50M+

breached identities surfaced weekly

\$200B+

global cybersec spend 2026

The senior product talent that can ship AI-native security at customer-actionable scale is scarce. That's the gap.

A rare combination, built over a decade in the trench.



CHRIS BOUCEK

CISSP · PMC-IV · Field CTO



Deep-stack security operator

Twenty years in network + systems compounded into seven years owning the eSentire NDR product surface — a 3,000-sensor Zeek/Suricata fleet across 1,500 tenants in 70+ countries. Real-time DPI, JA4+ encrypted-traffic productized, full PCAP retrieval. Maintains a personal Zeek/Suricata/JA4+ lab on Proxmox for ongoing R&D and continuous education — staying close to what operators actually run in production.



AI-native PM craft

Build MCP servers, custom LLM agent pipelines, and eval frameworks as part of how I work. Brought the practice to the org as practice, not personal experiment. Lands at every agentic-AI security shop I talk to.



Customer + executive room presence

20+ customer calls/month sustained for years. \$4M+ personally closed as Solutions Engineer counterpart in 2024-2025. CISO / SOC / DevSecOps relationships at tier-1 US enterprises and allied national cyber-defense.



External presence

SuriCon Montreal 2025 · ILTACON DC 2025 · Black Hat Toronto 2022 · University of Guelph Master of Cybersecurity sessional faculty.

Twenty years compounding.



Foundation first. Layered. Compounded. The seat I'm pitching is the layer after seven years owning NDR at fleet scale.

Battle-tested at fleet scale.

3,000+

Zeek/Suricata sensor fleet owned

1,500+

tenant organizations served

70+

countries deployed

\$30M+

ARR platform under product ownership

4x

0-to-1 product launches · multi-\$M ARR each

\$4M+

closed 2024-2025 as SE counterpart

Built on twenty years of deep network and systems mastery. +55% fleet growth · +35% revenue growth during tenure · NPS 72 on flagship.

Three converging inflections that need senior product muscle.



Agentic AI rewrites SecOps

MCP servers, SOC analyst agents, and eval frameworks are moving from research to production faster than most teams can absorb. The compounding edge is senior product judgment from someone who has built with these tools and learned where they break. That's where I have been investing my own time.



Identity becomes the perimeter

Credential exposure, identity-aware NDR, and identity-threat detection (ITDR) are the fastest-growing categories in security. Operators who understand both the network plane AND the identity plane are the scarce hire.



Customer-actionability is the new differentiator

Threat intel volume has stopped winning deals. Threat-actor-to-customer-action linkage wins them. That's where 10 years on the MDR vendor side compounds.

Four 0-to-1 launches. Full-cycle. Multi-\$M ARR each.

01 Incident Response

Stood up a new team of expert IR responders. Built insurance-partner workflows, retainer-based pricing, and SLA-bound investigation handoffs. First-year revenue exceeded plan.

02 Multi-tenant NDR

3,000+ Zeek/Suricata sensor fleet. JA4+ encrypted-traffic productized into the production pipeline. Full PCAP retrieval at fleet scale.

03 Dark Web Monitoring

Productized dark-web sourcing of credential exposure, leaked secrets, and threat-actor activity. Customer-actionable enrichment built into MDR alerts.

04 SaaS Threat Intelligence

Threat intel productized from MDR/SOC-identified IOCs and proactive threat hunting — turning customer-environment signal into a sellable intelligence product. Different sourcing model than commercial feed resale.

Each launch owned end-to-end: problem framing · pricing · packaging · GTM · regional launch · first-year revenue.

The combination most senior security PMs don't have.

Most GTM-led security PMs

Customer-strong, technical-light

- ✓ Customer-room presence
- ✓ Pricing + packaging fluency
- ✗ Hands-on Zeek/JA4+/Suricata depth
- ✗ AI-native build craft
- ✗ Engineering-room credibility

Most tech-led security PMs

Technical-strong, GTM-light

- ✗ Customer-room presence
- ✗ Pricing + packaging fluency
- ✓ Hands-on Zeek/JA4+/Suricata depth
- ✓ AI-native build craft
- ✗ Engineering-room credibility

Chris Boucek

Both. Compounded over 20 years.

- ✓ Customer-room presence (20+ calls/mo)
- ✓ Pricing + packaging fluency (\$4M+ closed)
- ✓ Hands-on Zeek/JA4+/Suricata depth
- ✓ AI-native build craft (MCP, agents, evals)
- ✓ Engineering-room credibility (CISSP, F5, CCNP)

Education, certifications, and external presence.



Certifications

- CISSP — (ISC)² · Assessed by UK ENIC as RQF Level 7 (Master's equivalent)
- Pragmatic PMC-IV — Pragmatic Institute
- CCNP · VCA-DCV · VCA-Cloud · ITILv3 (EXIN) · F5 LTM Advanced
- Dale Carnegie Leadership Training for Managers



Education

- B.A. — University of Windsor / University of New York in Prague
- Sessional Instructor — University of Guelph, Master of Cybersecurity



Speaking & Thought Leadership

- SuriCon Montreal 2025 — Cloud detection and visibility
- ILTACON Washington DC 2025 — Legal-sector cyber direction
- Black Hat Toronto 2022 — Packet capture in hybrid infrastructure
- 451 Alliance (S&P Global) IDI — May 2026



Work Authorization & Mobility

- Canadian citizen · Remote-Canada eligible · Guelph, ON base
- TN visa under USMCA · NEXUS + Global Entry active
- EU work rights via Czech citizenship (pending, expected 2026)

What you get in the first 12 months.

0 - 30 days	30 - 90 days	90 - 180 days	6 - 12 months
Listen first Customer + team listening tour. Voice-of-customer audit. Identify the seam in the existing roadmap where this hire compounds fastest. Calibrated. Curious. No premature opinions.	Calibrate + ship one thing Roadmap reset against the North Star. First shippable milestone with hard acceptance criteria — small enough to ship, large enough to matter. Eval framework in place.	Scale the wedge Pricing + packaging review. Sales enablement built. First 5 design-partner conversations on a 0-to-1 wedge. Internal advocacy carrying field signal into product, packaging, and GTM.	Compound Either a 0-to-1 launch or a major product evolution shipped. Analyst-relations cadence (Gartner, Forrester, 451). External presence at category events. Team mentored. AI-native PM craft adopted at team scale.

Default operating principle: be the most curious person in the room, not the smartest. Build trust first, ship second, scale third.

Let's build
something that lasts.

Chris Boucek, CISSP

build@cboucek.net · [linkedin.com/in/chrisboucek](https://www.linkedin.com/in/chrisboucek) · cboucek.net

