FLETCHLABS
SOFTWARE & SECURITY

Fractional SecOps

Senior security operations expertise, without the full-time headcount.

SERVICE PACKAGE
August 2026

fletchlabs.ca • info@fletchlabs.ca • Cambridge, Ontario, Canada

Executive summary

Most organizations need senior security-operations capability long before they can justify, or find, a full-time senior hire. Fractional SecOps is Fletch Labs' catch-all branch for that need: a broad menu of security-operations offerings delivered flexibly, either as scoped engagements with defined outcomes or as an ongoing retainer that flexes month to month. You get a fractional security team member, not a one-off project.

Why fractional

Industry research from ISC2 documents a persistent global shortage of experienced security practitioners[1], which puts senior operators out of reach for many small and mid-sized teams. Meanwhile, the cost of getting security wrong keeps climbing: the global average cost of a data breach reached a record USD $4.99 million in 2026.[2] Fractional capacity resolves that asymmetry: senior expertise applied exactly where your risk is, at a fraction of a full-time cost.

What the branch covers

Scope is set around your priorities and can shift as they do. Typical work spans:

- **Security tooling**: deployment, tuning, and management of SIEM, EDR, and vulnerability scanners.
- **Alert triage & incident response**: hands-on support when something looks wrong, from first alert to post-incident review.
- **Policy, process & playbooks**: development sized to your organization, not paperwork for its own sake.
- **Vulnerability management**: program oversight, including vulnerability assessments and penetration-testing support.
- **Cloud & infrastructure hardening**: practical security improvements across your hosting and network footprint.
- **Vendor & architecture input**: tool evaluation and security-architecture guidance. Vendor-neutral, we do not resell products.
- **Executive & compliance reporting**: posture and program-maturity reporting, backed by compliance and audit support (SOC 2, ISO 27001, similar) with continuous control monitoring and drift remediation.
- **Ad hoc project work**: the security tasks that come up between everything else.

Scoped or retainer, your choice

Scoped engagements suit well-defined needs: stand up and tune a SIEM, build an incident-response playbook, prepare for an audit. We agree on outcomes and deliver them.

Retainer arrangements suit ongoing needs: a set monthly capacity that covers triage support, tooling upkeep, reporting, and whatever project work rises to the top that month. Hours flex as your priorities change, with no renegotiation required for every shift in focus.

A named representative, every time

Whichever arrangement you choose, you are matched with a **named Fletch Labs representative** who remains your point of contact across engagements. That continuity matters in security operations more than almost anywhere else: your representative accumulates familiarity with your environment, tooling, history, and people, so each new task starts from context rather than a cold briefing. No rotating bench of strangers, and no anonymous ticket queue.

White-label arrangements for MSPs

Managed service providers, IT consultancies, and agencies frequently field security requests that sit just outside their in-house depth. We support those partners with **white-label delivery**: the same fractional capability described above, performed as an extension of your practice rather than as a competing vendor.

- **Delivery under your brand**: reports, playbooks, and documentation issued in your templates, with your logo and your voice.
- **Your client relationship stays yours**: we work through you, and we do not approach or solicit your clients.
- **Flexible visibility**: fully behind the scenes, or introduced as a named specialist on your team when a client wants to meet the practitioner.
- **Capacity on demand**: absorb overflow, cover leave and turnover, or add senior depth to a bid you would otherwise pass on.
- **Confidentiality in writing**: partner NDAs and non-solicitation terms are standard, not an upsell.

The practical effect is that you can say yes to security work without hiring for it, and keep the client, the contract, and the margin.

Engagement & pricing

Pricing is generally based on the scale of the environment (hosts or users in scope) or the task work that needs to be done. We can identify your needs together in a discovery call, and provide a tailored quote for your requirements.

Start a conversation

Tell us where security operations hurts today, whether tooling, triage, compliance, or all three, and we will propose a scoped engagement or retainer to match. If you are an MSP or consultancy, ask about white-label delivery under your brand.

Reach us at info@fletchlabs.ca or through fletchlabs.ca/contact.

Sources

1. ISC2, Cybersecurity Workforce research — https://www.isc2.org/research

2. IBM & Ponemon Institute, Cost of a Data Breach Report 2026 — https://www.ibm.com/reports/data-breach