

How a Canadian Financial Institution Transformed Their Detection Engineering Program with SpecterOps Training

Company Overview

A leading financial institution in Canada came to SpecterOps to help solve a problem; they prioritized robust cybersecurity defenses to protect their systems and customers but needed additional support. Their security team recognized the need to elevate their detection engineering capabilities to match the sophistication of modern adversaries.

How Does Our Approach Compare to Best Practices?

A few years ago, their detection engineering program needed a strategic injection of expertise. The team needed to answer some critical questions: What are industry experts doing? How can we improve our detection development process? They needed a rigorous, research-driven methodology to build a resilient detection program.

Discovering SpecterOps

The company found SpecterOps through word-of-mouth references within the security industry. SpecterOps had built a reputation for high-quality training and research, with blog posts that the team regularly referenced in their work. SpecterOps was a known leader in the field, not just to the security practitioners but also to management who recognized the value of their training programs.

The team's first exposure came through free public seminars about BloodHound Community Edition, the Attack Path Management tool, and other security topics, which demonstrated the depth and quality of SpecterOps' expertise.

The Solution: Investing in Training

In 2022, the financial institution enrolled several team members in SpecterOps' public online training offerings, specifically the detection engineering course and a purple teaming workshop. This initial investment proved transformational for the organization.

The training had a massive and immediate impact on the detection engineering program. The team gained insights into:

- **Research-driven methodology:** How to thoroughly research threats and techniques before building detections to reduce false positives
- **Deep technical understanding:** Looking beyond surface-level SIEM logs to understand what's happening at the OS and kernel level and to detect sophisticated attacks that evade traditional monitoring
- **Attacker perspective:** Learning to view systems through an adversary's eyes, enabling proactive detection
- **Rigorous documentation:** Implementing comprehensive documentation frameworks to make every detection repeatable, auditable, and tied to a defined threat hypothesis

Three years later, when the opportunity arose to attend SpecterBash 2025 (SpecterOps' annual community and training event), the company chose to send team members again.

“The 2022 training had a massive impact on our program... as a result, we're looking at a modern, well-documented library now, with different levels of fidelity for different threats.”



Security Team Member
Canadian Financial Institution

Implementing the ADES Framework

The financial institution adopted the Alerting and Detection Strategy framework taught in the course and integrated it into their detection development process. This framework became the foundation for how they approached new detection creation and existing detection evaluation.

Program Modernization

As the team upgraded to next-generation tooling and enhanced their EDR capabilities, they used this migration as an opportunity to apply their new methodology comprehensively. The team reviewed their entire detection library, which included numerous legacy detections that “wouldn’t pass the smell test today.” Using the rigorous methodology learned from SpecterOps, they rebuilt their detection library from the ground up.

The result is a modern, well-documented detection library with different levels of fidelity appropriate to various threat types and scenarios.

A Measuring Stick for Progress: 2025 Revisit

When the team returned to SpecterOps training in 2025, the experience served a different purpose. Rather than learning net new concepts, it became a measuring stick for their progress.

The team could:

- ✓ Compare where they were three years ago to where they are now
- ✓ Validate that their implementation aligned with current expert practices
- ✓ Confirm that while methodology had evolved somewhat, their foundation remained solid
- ✓ Feel confident in their detection engineering maturity

One team member noted: "I was happy with the course and happy with where we are and how we've applied what we've learned from that."

The SpecterOps Difference

Blue Team Focus

The company particularly appreciated SpecterOps’ blue team perspective. As one team member explained: “It’s easy to be a red team and break things. It’s a lot harder to sit with a company on the blue side and help them make it better for the future.” This constructive, defense-focused approach aligned perfectly with the team’s needs.

Solid Foundations Built from Focused, Relevant Training

The SpecterOps training content is highly focused on the detection engineering domain, making it directly relevant and immediately applicable to the security team and their day-to-day work.

The organization now has a detection engineering program built on a solid foundation of expert methodology, comprehensive documentation, and rigorous research practices that will serve them well as threats continue to evolve.

Learn more at specterops.io/get-a-demo

