CIRA strengthens defence in depth strategy, improves threat detection and response by 75%.

Case study at a glance

Company

Canadian Internet Registration Authority (CIRA)

Industry

Not-for-profit

Website

cira.ca

Business Need

Continual view across CIRA's growing IT network to ensure reliable services for individuals and businesses.

Solutions

Field Effect's Covalence® managed detection and response platform.

Field Effect's Incident Response (IR) Readiness package

Results

Improved quality of its defence in depth security approach by 40%.

Reduced time required for threat hunting and investigation by 15%.

Realized 100% improvement in its IR plan with the addition of Field Effect expert cyber security counsel and IR services.

cira

The
Company

With a mission to build a better internet for Canadians, the Canadian Internet Registration Authority (CIRA) may be best known for managing .CA domains, but there is much more happening at this fast-growing not-for-profit organization.

Scott McMullen, Manager of Network Security, joined CIRA six years ago. Working with a team of four, Scott is part of CIRA's IT operations, managing system administration and IT security. Prior to this, he worked at a technology company that was acquired by Honeywell. As Scott explains, it was CIRA's size, culture, and focus on people that attracted him.

"At CIRA, I'm no longer just a number at a big enterprise. We're very nimble, focused on our customers, and can make changes happen quickly without a lot of corporate red tape. I can see the results of my work much faster," he says.

CIRA not only manages one of the fastest-growing country code top-level domains (ccTLD)—more than 2.9 million .CA domains registered—the not-for-profit has a membership of 15,605 and offers registry services to help others manage ccTLDs, as well as technologies and programs for improving cyber security and privacy. CIRA also provides grants for community internet projects, among other initiatives.

The Challenge

With CIRA's growth and focus on innovation, it's no surprise the IT team is progressive. For Scott, the major need was strengthening its holistic security approach with a stronger level of monitoring and reporting.

"Like most growing organizations, we really needed more visibility across our network to stay well ahead of evolving threats," he shares. "We have a sizeable amount of traffic on our network and we must ensure our services remain secure and available."

Scott also wanted additional, proactive security services like incident response (IR).

> "
>
> Like most growing organizations, we really needed more visibility across our network to stay well ahead of evolving threats.

"At my last job, when the unexpected happened, we had to quickly look for someone to help us with the investigation, forensics, response, and remediation," he explains. "This taught me the value of being very proactive and making sure, whether you need it at that moment or not, IR is always part of your security plan."
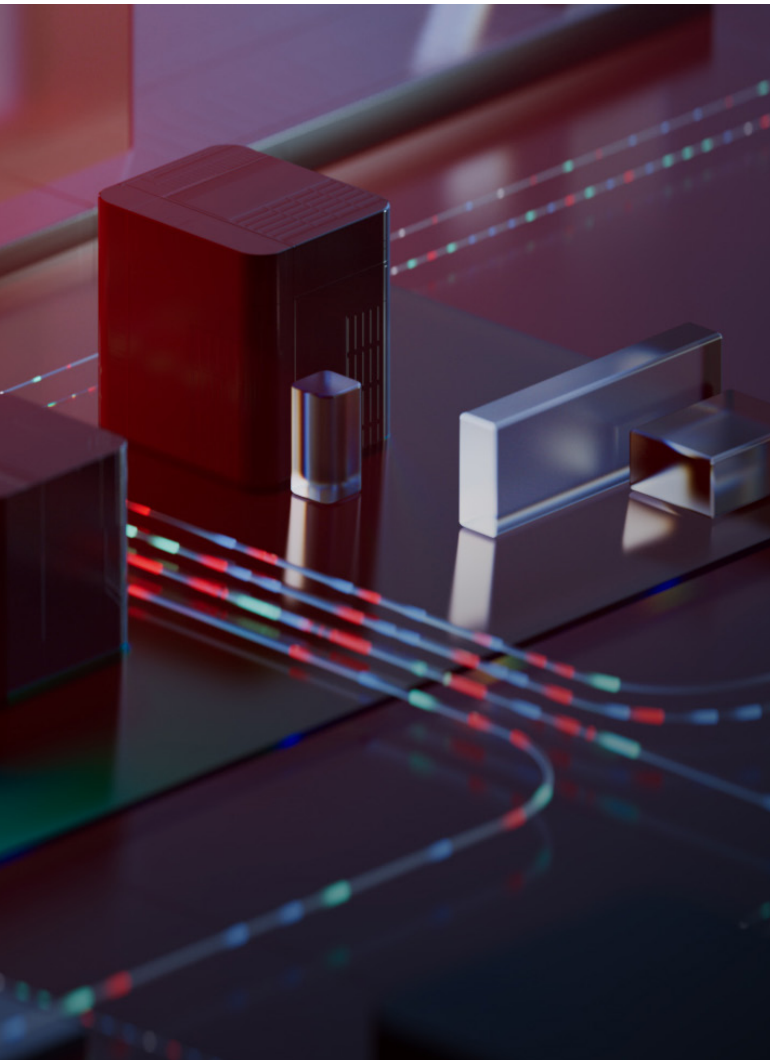
The Solution

When CIRA formed a partnership with Field Effect, a global cyber security company with managed detection and response (MDR) solutions and services, this provided the ideal opportunity for Scott and his team.

"Through our defence in depth strategy, we have defensive security layers in place—including threat monitoring—but we really needed to take our monitoring, detection, and response to the next level," says Scott. "After meeting with the Field Effect team to hear more about their capabilities, we were really impressed with the depth of cyber security knowledge and background in incident handling. We knew this was the best step for us to take."

The CIRA team chose the Covalence® managed detection and response solution, as well as Field Effect's IR Readiness package.

Scott likes Covalence's intuitive design and its sophisticated capabilities. "Covalence's advantage is it's truly a managed monitoring service that provides the intelligent, automated alerting that keeps us well ahead of issues."

"It gives me the confidence that I can be hands-off. I don't need to be in the platform every day as I know I'll receive a text or email with clear detail if there is something we need to investigate, as well as weekly reports," he adds.

Covalence's monitoring capabilities are a key piece in CIRA's daily work managing its Anycast domain name service (DNS) and registry services.

As Scott explains, "ensuring our services remain secure and available is key to our business. For example, we continually gather and analyze network traffic for signs or attempts of compromise. Attackers are also scanning our network for opportunities to circumvent our security controls—with Covalence's blacklisting capabilities turned on, we can see the blacklisted IP addresses attempting to connect to our services and this shows the number of malicious attempts blocked."

For Scott, Covalence's level of threat analysis is also impressive. "We get solid information about potential threats and risks, with detail that helps us immediately see how to prioritize resources and respond."

Covalence has its own high-resolution monitoring sensors and uses proprietary technologies and methodologies, including sophisticated analytics and predictive modelling, to continually identify emerging cyber threats and vulnerabilities. It also provides monitoring coverage across a company's IT infrastructure—endpoints, networks, and cloud services—with clear, understandable analysis accessible from one platform. This gives IT teams a consolidated view of monitoring results across every aspect of their IT environment.

Covalence takes this one step further with its AROs alerting and reporting. Through its Actions, Recommendations, and Observations (AROs) process, it provides threat alerts as focused, useful, and actionable data.

"From the alerts and reporting, I immediately see all of the detail, the priority level, and the recommended type of response," adds Scott. "I don't need to sort through security event logs or investigate a volume of non-priority alerts. At the same time, if there is something benign that may require action down the road, it will be included in the reports. Field Effect analysts are also checking each alert. This provides a second set of very experienced eyes across our network."

Through the CIRA-Field Effect partnership, Field Effect has also integrated CIRA's D-Zone DNS Firewall into Covalence. Critical for protecting web traffic, a DNS firewall sits between a company's network and the internet and blocks users from accessing malicious content. Scott explains, "businesses can take advantage of Covalence's monitoring capabilities and experience an added layer of control over internet use with phishing and malware protection through our DNS firewall, all from the Covalence platform."
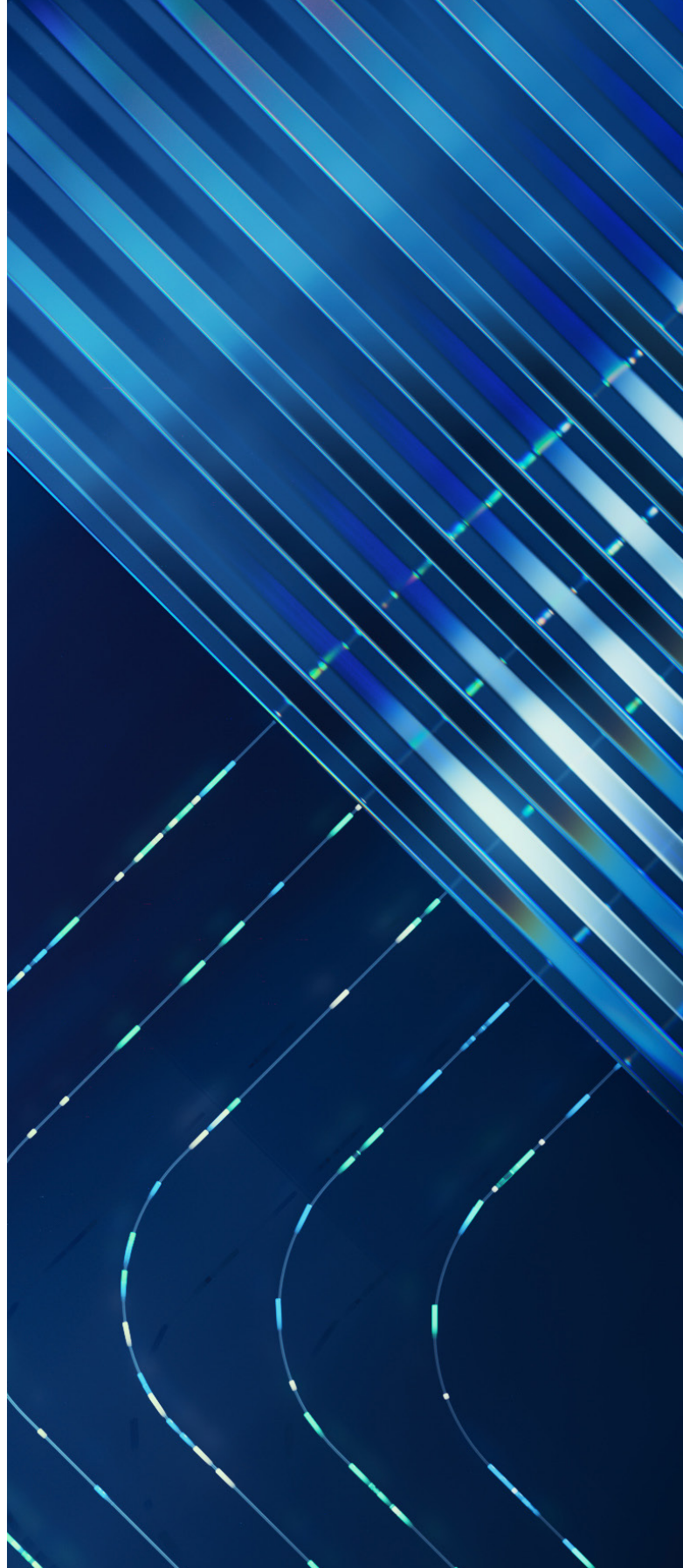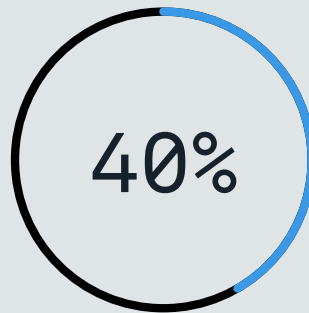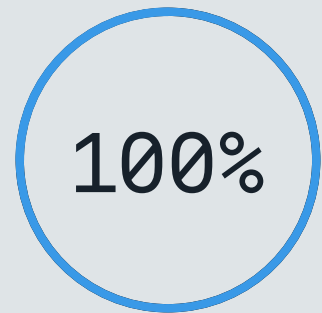
The Results

Using the Covalence managed detection and response solution, Scott estimates his team has experienced a 40% improvement in its holistic security approach.

75%
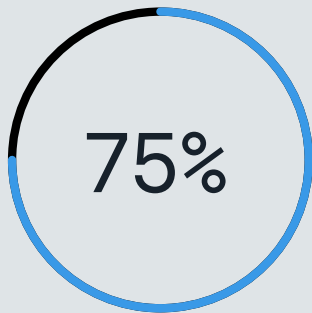
More powerful threat detection and response

40%

Strengthened defence in depth approach

100%

Improved incident response plan

"We know Covalence is continually at work 24/7 stopping new threats and providing the data that helps us understand the potential threat attempts to our network and actions to take."

He has reduced the time spent investigating security alerts and threat hunting by more than 15%. "Through Covalence and the Field Effect analysts, we have the value of cyber security expertise and support by our side."
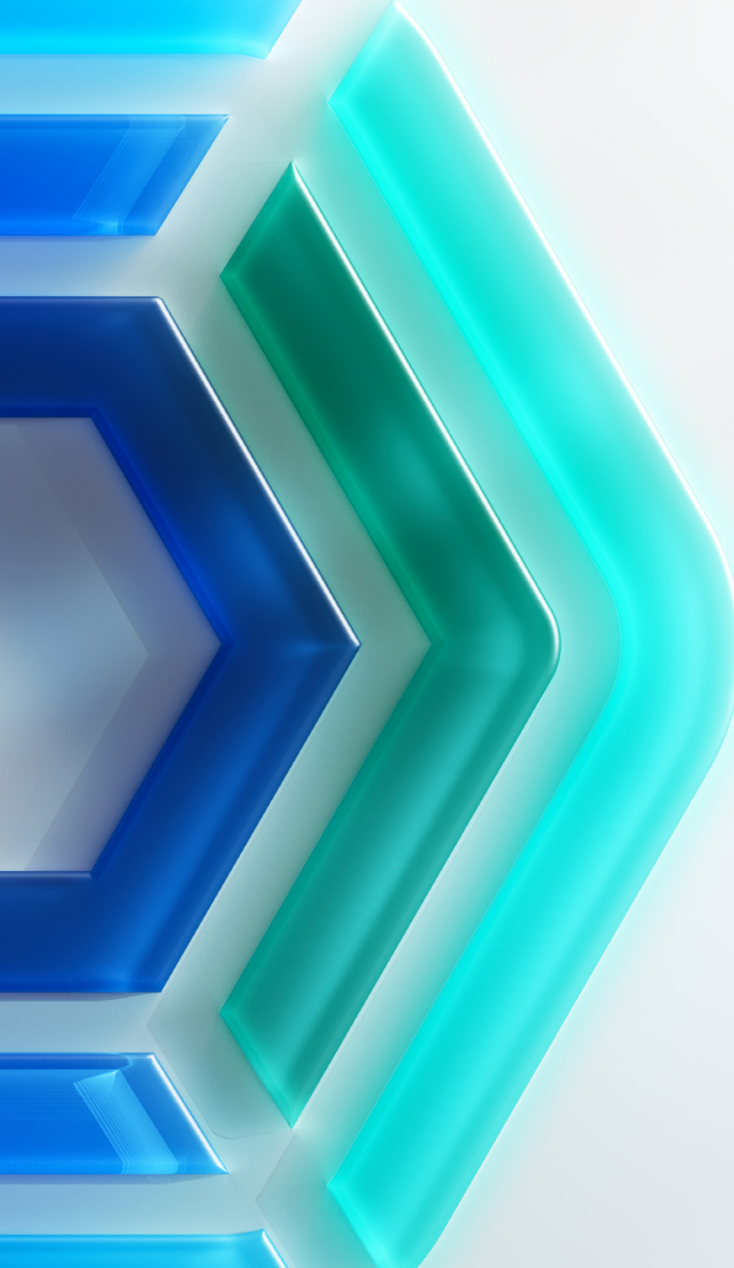
Through the addition of Field Effect's IR Readiness package, Scott has also improved his team's ability to plan for potential incidents. The package of services is designed to help businesses and organizations put the right planning in place to respond effectively, and minimize recovery costs and downtime.

While CIRA has not experienced an incident to date, Scott explains, "when it comes to responding to a security incident, an organization of our size doesn't always have the expert resources and in-house tools needed for advanced forensics and discovery. Field Effect makes it easy to add this to our toolkit and its experienced team gives us the confidence that we are well prepared for any situation."

"

Covalence's monitoring, detection, and response capabilities provide a critical security layer for our entire IT environment. It's a 'set and go' managed service that provides complete peace of mind, improves our security, and continually saves us time.

Scott McMullen

Manager of Network Security — CIRA

The most sophisticated managed detection and response solution on the planet, made simple.

Covalence is an easy-to-deploy, cost-effective cyber security solution that monitors and protects your entire threat surface—endpoints, networks, and cloud services—all from a single platform. No add-ons, no modules, and no gaps in your security. Covalence not only monitors every aspect of a business's threat surface, but it also reduces alert fatigue and false positives by aggregating data from multiple security events into simple, actionable remediation steps.

Covalence

About Field Effect

Field Effect, a global cyber security company, is revolutionizing the industry by bringing advanced cyber security solutions and services to businesses of all sizes.

After years of research and development by the brightest in the business, we have pioneered a holistic approach to cyber security. Our complete Managed Detection and Response (MDR) solution, flexible simulation-based training platform, and expert-led professional services form a unified defence that results in superior security, less complexity, and immediate value. We build solutions that are sophisticated, yet easy to use and manage, so every business owner can get the hands-free cyber security they expect and the sleep-filled nights they deserve.

Contact our team today.

Email:
letschat@fieldeffect.com

Phone:
Canada + United States
+1 (800) 299-8986

United Kingdom
+44 (0) 800 086 9176

Australia
+61 1800 431418

FIELD EFFECT