

SCM INSURANCE SERVICES



COMPANY PROFILE

3,000 employees
Albert Canada HQ
Insurance & Financial Services

DSIRED OUTCOME

Increase visibility into unknowns
Implement more automation
Reduce manual workflows
Increase high-fidelity detections
Streamlined alert management
More effective incident response
Alignment to client-centric requests
MITRE ATT&CK inspired detections

SECURITY DEPLOYMENT BEFORE CYBEREASON

Unnamed MSSP
Open-source tools for detection
AWS Cloud

PRODUCTS EVALUATED AGAINST CYBEREASON

Carbon Black
Crowdstrike

CYBEREASON DEPLOYMENT

Cybereason Enterprise
NGAV
Active Monitoring
Endpoint Controls
Training & Implementation

SCM Insurance Services has been supporting the insurance and risk management community for more than 30 years with over 200 locations and over 3,000 employees across North America. They provide claims adjusting, third-party administration (TPA), risk management, investigative and surveillance services, risk mitigation, medical insurance services, forensic services (accounting/engineering), and risk intelligence.

The Challenge

Prior to onboarding Cybereason solutions, SCM met their security needs primarily through an outside managed security service provider. The MSSP had been engaged for nearly three years for detection and alerting when the SCM security team uncovered gaps in threat visibility after routine penetration testing exercises that simulated cyber attacks.

This discovery led the SCM team to undertake a deep-dive examination of their security posture, programs and tools in place. This analysis exposed the need for an internally-managed endpoint detection and response (EDR) solution, with Cybereason being one of three solutions selected for the evaluation process by SCM.

The team's overall goal was to align their operations with critical business processes and enhance their ability to deliver on client requests while maintaining hardened controls and techniques against cybersecurity threats in the environment.

The Evaluation Process

With corporate environments changing rapidly, the proliferation of work-from-home users and off-VPN devices, the threat landscape has become increasingly dynamic. SIEM solutions and other similar tools offer visibility into certain types of threats, but lack the depth and breadth of an EDR

solution to create a clear and complete picture for security teams. In July of 2019, the SCM team started proof-of-concept testing for various EDR solutions. Of the EDR candidates, only Cybereason stood out as being capable of providing the necessary platform for automated threat hunting at scale.

The SCM security team required a solution capable of adapting to their environment and able to identify threats, alert on adversary tools and techniques against the MITRE ATT&CK framework, and quickly respond and mitigate those threats.

During the evaluation process, SCM noticed that other EDR vendors would create individual alerts on events, but were unable to determine the full scope of the incident and cross-correlate alerts across the enterprise. An EDR solution was needed that provided the ability to not only ingest individual alerts based on MITRE ATT&CK, but also provide the necessary context back to the security team for full analysis and a comprehensive response.

When Cybereason joined the evaluation process, the SCM security team quickly determined that the Cybereason Defense Platform was the most capable in identifying a malicious operation across the various stages the attack kill chain, whether it was at the initial compromise stage, in the command and control phase, or during the evasion attempts. This is best exemplified by Cybereason's unique Malop™ interface that provides a contextualized view of the full narrative of an attack. Cybereason emerged as the leading solution during the PoC when it was the only solution able to detect an obfuscated Mimikatz tool.

During the PoC process, Cybereason was put through the same rigors as other vendors, and very early in the deployment Cybereason was able to surface events on previously unseen malicious activity like coin miners and other malware that had long since been installed on the endpoints but had been missed by other security technologies and services.

The Solution

SCM ultimately decided to implement the [Cybereason Enterprise](#) option which combines NGAV prevention and endpoint controls with EDR detection for deep contextual correlations in real-time across all endpoint assets, as well as engaging in a thorough compromise assessment and implementing Cybereason's continuous threat hunting managed service.



“The reason why we chose Cybereason was because of our need for comprehensive detection that’s mapped to MITRE ATT&CK, [...] to produce an alert faster[...], and to increase the speed to mitigation”

NICK LAPOINTE

Information Security Administrator,
SCM Insurance Services



Learn more at [Cybereason.com](https://www.cybereason.com) →





The **Cybereason Defense Platform** allows the SCM team to identify threats quickly with a high degree of accuracy through enriched data from all endpoints, leverage fully contextualized intelligence for high fidelity detections that eliminate advanced threats at any point in the kill chain, and remediate automatically or with a single click to kill processes, remove persistence, prevent execution and isolate targeted machines.

The Outcomes

Like most modern security teams, SCM was primarily focused on the unknown threats that had previously evaded defenses and were embedded in their environment. The need for visibility, context, and streamlined response was critical to meet this need.

After implementation, Cybereason immediately improved the overall tracking of incidences and reporting KPI's communicated up the internal chain of command, bolstering this key component of an incident response program. Cybereason has increased detections for the SCM team while leveraging the MITRE ATT&CK knowledge base for faster detections, increased situational awareness, and a reduced mean-time to response (MttR).

With Cybereason's built-in active threat hunting capabilities, the solution is more akin to having an additional person in their SOC rather than just another tool in their toolbox.

"It's like having an actual employee in the environment that actively protects the host. So, while we can't watch everything all the time everyday, we have full confidence that Cybereason is watching all and is keeping threats in check - it's a great marriage. And it significantly reduced our time threat hunting and quickened analysis of weird behaviors in the environment for sure. With Cybereason, from day one you can start building investigations easily with little to no threat hunting knowledge."

- Nick LaPointe
Information Security Administrator, SCM Insurance Services

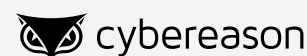
"We decided we needed to move to an EDR solution, so we tested three, and of those evaluated we decided to go with Cybereason."

NICK LAPOINTE

Information Security Administrator,
SCM Insurance Services



Learn more at [Cybereason.com](https://www.cybereason.com) →





“We’ve never had a vendor be as passionate about their product and reaching out and delivering on customer success as much as Cybereason has. And it gives you the warm fuzzies knowing that we picked the right solution and that Cybereason has our backs when the need is there”

NICK LAPOINTE

Information Security Administrator,
SCM Insurance Services

Snapshot - Cybereason Products & Services Deployed

Cybereason Enterprise

Threat prevention, detection, incident response & recovery

Automatically uncover advanced threats that evade perimeter defenses. Enrich those detections with contextualized intelligence, and cross-correlate with other relevant detections across the enterprise. Streamlined incident response and wide-ranging remediation options.

NGAV

Multi-layered prevention, proven endpoint protection

Instantly block 0-day, fileless attacks, new malware variants and other novel threats, ending lengthy investigations.

Active Monitoring

24/7 surveillance and investigations delivered via services

Cybereason security specialists examine detections, determine the scope and severity of any malicious operation (Malop™), and provide remediation recommendations to your security team while you maintain full control of your platform and your data.

Endpoint Controls

Securely manage endpoints

Cover security requirements and address compliance needs with controls tied to different types of devices, implement personal firewall policies, and enforce disk encryption.



Learn more at Cybereason.com →

