Case Study

Surfacing Hidden Security Gaps with IBM QRadar and MBS Techservices Inc.

A network monitoring solution for a logistics provider

As the attack surface grows and attack timelines shrink, it's becoming nearly impossible for cyber security teams to surface and investigate security issues in a timely manner. Speed and efficiency are crucial to their success, especially for small and resource-constrained security teams.

The traditional approach to event investigation and response — reactive, manual log analysis — is a slow, labour-intensive process that's not responsive enough to meet today's business needs and security challenges.

A Security and Compliance Manager for a large logistics company that provides parking management solutions for hospitals, universities, parking lot operators, and municipalities, says log analysis was a significant gap in his company's security capabilities.

The company hadn't experienced a significant incident, but the manager says the gap was concerning. "We felt like we were way behind where we should be, especially considering our size and rate of growth," he says. The company has been growing since its inception and currently has about 300 employees and 25 IT professionals. The Security Manager is the company's sole full-time cyber security professional.

Best-effort Log Analysis Doesn't Cut It Anymore

While the company's critical systems are being observed 24/7 by a third-party provider, its corporate systems and customer-facing website were being observed in-house using best-effort log analysis. He says, "We could log into a server and review a log, but there's no opportunity to correlate anything."

What he wanted was a centralized logging and retention solution with the ability to do correlation. The company's logs were scattered among its two data centres in Indianapolis and Vancouver, B.C., and were rolling over logs as space ran out.

While investigating automated log analysis solutions, the company was approached by MBS Techservices Inc (MBS).

MBS is a cybersecurity consulting company that focuses on layered defences through an integrated system of solutions such as SIEM, Network Monitoring, SOAR, Cloud Identity, and other solutions that support on-premises, cloud, and hybrid environments.

Based on the parking logistics company's need for centralized logging, MBS suggested the IBM Security QRadar Suite for automated log aggregation and analysis.

IBM QRadar is a threat detection and response suite that aggregates logs, automatically contextualizes and prioritizes alerts, and visually displays alert data for rapid consumption. IBM QRadar helps organizations speed up investigations by significantly reducing the number of steps and screens required to understand and respond to threats.

The suite brings together core technologies needed to support today's security professionals. It is built on an open platform with more than 900 pre-built integrations for flexibility and choice across IBM and third-party products. The suite includes capabilities for Threat Intelligence, Log Management, EDR, SIEM, and SOAR.

Surprising Results Out of the Box

To give IBM QRadar a test drive, MBS brought in experts from IBM for a proof of concept (POC), which yielded surprising results. The IBM experts helped the logistics company connect a small group of servers and network gear to IBM QRadar. The Security Manager says, "On the first day of the POC, we got a vast amount of valuable information. I called my boss and said, 'We have to buy this.'"

The company liked IBM QRadar's ability to correlate and automate. He says, "With all the automation, you don't need a lot of people looking at screens all day. It does the work for you."

With IBM Watson tied in, the logistics company got even better results. The Security Manager says, "Watson gives you a very detailed

report that links everything together — how something happening in one place is affecting something else."

"It's impossible to do this manually," he continues. "Everything is logged now, so Watson is a big part of this solution." IBM Watson's reporting includes interactive graphics that visualize the relationships involved in an event.

IBM QRadar is offered as a cloud-based solution that works well with the company's data centres. The Security Manager says, "We subscribe to QROC, which is QRadar on Cloud, and have data gateways installed on our local networks that relay everything up to QRadar." The company uses the QROC portal to do all the analyses and research.

Combining IBM QRadar and Watson has given MBS's clients potent and valuable tools and insights into their systems.

Uncovering Hidden Vulnerabilities

As a result of its partnership with MBS and IBM, the parking logistics company has all its corporate and website logs in one place, including logs from network gear, web servers, database servers, and Microsoft Active Directory.

The Security Manager says, "Until we had everything in that one pane of glass, it was tough to figure out where these attacks were coming from. Now, the source IPs and countries are right there in QRadar."

IBM QRadar is helping the large logistics company surface hidden security issues. For instance, the Security Manager found an "offence" — QRadar's lingo for a security event — relating to invalid

administrative credentials associated with a former administrator, and a process that had been running in the background for two years. That event prompted an exercise to dig in and evaluate similar areas.

The company also found many employees using decommissioned laptops for work — old devices that don't comply with its current security standards. He says, "QRadar has helped us uncover a lot of things like that."

IBM QRadar has also helped the logistics company improve its cybersecurity processes, not just for logging and event correlation, but from a broader IT security perspective.

Pathway to an Automated Security Operations Centre

The company is now in the tuning stage to eliminate false positives and unnecessary, repetitive information. The Security Manager says, "Sometimes, it can feel like too much information, so we're working with MBS on tuning it so that we only get the most interesting stuff."

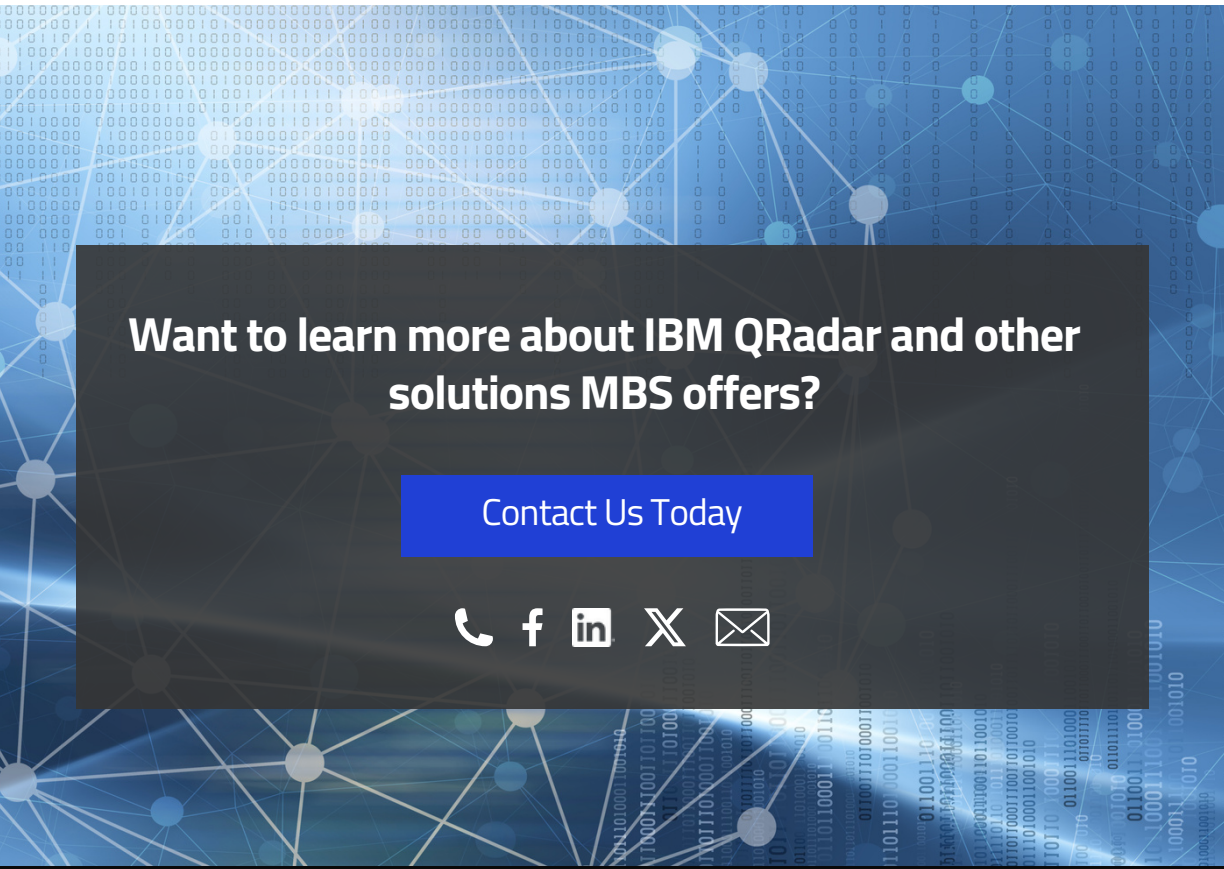
In addition, the tuning project will help the logistics company get to the next level, which is an automated security operations centre. The Security Manager says, "Long term, we want to do a lot more automation and bring our more sensitive networks into QRadar once we have it fully tuned and configured," enabling the company to cut costs.

MBS is helping the logistics company get more value from the product as it grows and matures with it.

MBS is very easy to work with," says the Security Manager. "My rep is really on the ball. Whenever I have a question, he's quick with an answer."

MBS Techsystems has also helped the Security Manager get involved in local networking events for cyber security professionals. He says, “It’s been super valuable to me and to the organization to get different perspectives.”

He also says IBM QRadar is a crucial line of defence against a crippling breach. “It’s an important part of our cyber security toolbox because it helps ensure that our systems are safe, so the whole company benefits from it.”



Want to learn more about IBM QRadar and other solutions MBS offers?

Contact Us Today