National Solutions Firm Sees 30% Increase in MITRE ATT&CK Coverage with Devo and Reliaquest

CASE STUDY

By making the switch to Devo's cloud-native SIEM & partnering with Reliaquest, the agency's security team has been able to hire an additional analyst and improve business operations.

SUMMARY

This competitive solutions firm is based in Boston, MA, with a team that specializes in technology and staffing services. The firm works with 70% of the Fortune 100 companies to match top talent to job opportunities across the nation. The firm became unhappy with its previous SIEM solution, McAfee. Their outdated solution was extremely expensive, largely because the team needed to hold 365 days of hot storage. Additionally, the firm's on-premises environment required manual updates, which cost them hours of time on a regular basis.

With their license up for renewal, the firm's team decided to evaluate a variety of modern SIEM solutions. In particular, they required a solution that would work well with their desired partner, Reliaquest, while providing improved visibility into their cloud resources. With Devo's SaaS solution, all product updates are automatically installed, saving the team hours of time per update cycle. The Reliaquest team is able to build out advanced custom alerts for the team within the Devo Platform so they can work more proactively on production and engineering issues.

INDUSTRY

- Staffing and Recruiting

ENVIRONMENT

- 60 years in the industry
- 30,000 consultants deployed nationwide
- 3,000 clients partner with the firm

SECURITY CHALLENGES

- Lack of visibility across multiple domains
- Unable to ingest all of their needed data without overwhelming their previous system
- Manual labor required for an on-prem solution
- Inability to create or rely on custom alerting to reach automation

SOLUTION

- The Devo Platform
- The Reliaquest team

KEY BENEFITS

- Full visibility within a single pane of glass
- The ability to not only handle previous ingestion levels but double it
- High-level threat hunting and alerting capabilities
- The ability to build out custom alerts

30% increase
in MITRE ATT&CK coverage

Access to
24/7 monitoring

Hire **1 new analyst**
due to cost savings

All log sources
migrated in **90 days**

Able to increase
ingestion levels by **2X**

Extracted value
in first **2 weeks**

THE CHALLENGE

The solutions firm was using McAfee as their SIEM solution. Their team was dealing with a very complex system, correlating between multiple logging tools and environments. With McAfee's solution, they lacked a cohesive view into each environment, which created serious blindspots, especially in their cloud-based tools.

When suspicious activity was detected in their environment, security analysts were not automatically notified. In fact, they often stumbled upon them by chance, putting them in a reactive state, which gave them limited ability to respond and remediate the incident in a timely manner. The firm needed to enable its team to quickly create and configure alerts so they could proactively defend the organization.

The solutions firm also has a regulatory requirement that calls for them to have access to 365 days of hot data at all times. Data retention was not offered as an out-of-the-box feature with McAfee. Therefore, McAfee became too cost prohibitive and cumbersome to run, which negatively affected their compliance with regulatory agencies.

As a cloud-first organization, the firm's team sought a cloud-based solution for their SIEM. They needed something that could improve cloud visibility and give them access to pre-built alerting.

THE SOLUTION

The firm's team ultimately chose the Devo Platform to increase visibility, enable out-of-the-box data retention, and provide them with next-gen logging integration. With Devo, the team now has full visibility into their cloud resources and non-standard log sources. As a result, they can build new rules through the Reliaquest team and perform analysis by correlating with MITRE ATT&CK framework tactics and techniques.

Devo provided the team with a single solution to store all their data from a multitude of sources while giving them the capability to configure alerts and data analysis to eliminate vulnerabilities and minimize blind spots. The solutions firm's team commonly works with Azure and Microsoft 365 stack. Unlike McAfee, Devo gave the team the ability to seamlessly ingest these logs into the Platform, which provided the cloud connectivity they required.

With Devo, Reliaquest was able to drastically improve the team's alerting capabilities. The Devo Platform allows for alerts to be pre-configured. Therefore, Reliaquest has the ability to build their own custom alerts. Now, the team receives alerts proactively before incidents arise, improving their security posture. A Security Engineer from the team noted:

> “*With the alerts being built for us by Reliaquest, we can rely on their team to tell us what is actually happening. They have the freedom to work within Devo to do the first-line triaging and alerting for us. We save a ton of time by having this front line of defense.*”

With the Devo and Reliaquest partnership, the solutions firm has a newfound fidelity. The team is now able to direct their time toward building alerting automation and improving the analyst experience.

The Devo Platform provides 400 days of hot data out-of-the-box, enabling the firm to achieve regulatory compliance. Devo's ease of use has also improved their incident response capabilities. They have access to a much more robust alert stack, allowing them to build cases for additional conditions.

The solutions firm was also drawn to Devo's easy migration process. When their previous contract expired, Devo was able to ramp the team up quickly with free training and hands-on support. Devo provided their team with free training, allowing them to hit the ground running as soon as their new solution was in place.

THE RESULT

The team was able to implement and master Devo quickly with the help of Reliaquest. In explaining the migration process, one of the client's Senior Engineers explained:

“It took us about three months just to get everything built and in place for our on-prem pieces to send the information to Devo, but once we were up and rolling, ***we moved all of our log sources and all of our alerting in just over 90 days***."

In the past, the solutions firm had struggled to ingest all of their necessary data. With the combined power of Devo and Reliaquest, they were able to quickly **double their ingestion levels**. Their team immediately recognized a return on their investment.

Busch further explained,

"We have absolutely seen an ROI. We've been **able to hire one more analyst with the money we saved on our licensing**."

As Reliauqest is able to build out custom alerts for them to use within Devo, the team reported that they had seen approximately a **30% increase in MITRE ATT&CK coverage**. Since the firm's team had no alerting in place, partnering with Reliaquest and Devo has drastically improved the productivity of their SOC.

The solutions firm has also been able to free staff time, spending a lot less time supporting different pieces of the SIEM, including trying to build out the alerts that Reliaquest took over.

Devo Exchange is a vibrant community-based marketplace full of valuable content that the team can browse, install and manage with push-button simplicity. Their team reported that using Devo Exchange has **saved them weeks worth of time**.

Devo Connect, the platform's online user community, gives the firm access to fast and easy answers from Devo experts in no time. Most importantly, Devo and Reliaquest have also been able to save the team time in every investigation they run.

"Devo **saves us hours in every investigation**. Previously, just getting the data to return with searches and things like that was cumbersome. A lot of the interfaces were very slow. We haven't had any issues like that with Devo. It has been very quick"

Working with both Devo and Reliaquest has enabled the solutions firm to shift their focus to things other than SIEM alerting and event management. Reliaquest picks up this task for their team so that they have more time to focus on production and engineering issues. The team has shifted toward a more proactive stance with the help of Devo and Reliaquest. They now work as one cohesive team rather than two siloed teams.

WHAT'S NEXT

Devo offers a variety of tools beyond the capabilities that the team was looking for. The solutions firm plans to work more with Devo's SecOps and SOAR capabilities to build out their toolset and expand functionality for Reliqquest to perform alert triage.

> *We **extracted value within the first two weeks** because we were able to ingest our cloud solutions, but at the 60 to 90-day point, **we 100% realized our investment, and we were completely satisfied**.*

Devo
255 Main Street
Suite 702
Cambridge, MA 02142