Large-Scale US School System Selects Devo for Next-Gen SIEM, Increasing Ingestion levels by 30%

CUSTOMER SUCCESS STORY

This large-scale US school system was previously using Splunk ES but grew unhappy with the solution. Their team, composed of threat-hunters, was paying for a SIEM that did not give them the tools they needed. They were paying for a very expensive solution that was not providing the necessary value.

They were in need of a solution that could scale to meet their growing ingestion levels while also working to help save them budget. The team was looking for something that could give them access to more of the features they needed on a daily basis, such as advanced threat hunting and data science capabilities.

The team began to assess alternative SIEM solutions that they could migrate to quickly in order to replace Splunk ES before their contract was up.

WANTED

The school system's security team is primarily composed of threat hunters. With the licensing model they purchased with Splunk ES, they were paying for deeper features that did not meet their needs. They wanted something more flexible that gave them access to stronger logging capabilities and core analytics to compliment the work they were doing.

With the incumbent, their ingestion levels were rapidly increasing. They wanted a solution that was able to handle not only their current ingestion, but their future forecasted levels of ingestion. Preferably, they knew they would be on the hunt for a cloud-based solution to do this more easily.

The team was already using a variety of technologies that they wanted to be able to move over and integrate with their new solution of choice. They were working heavily with Crowdstrike and Cribl. They also were using XSOAR and wanted to integrate this automation into their new SIEM the same way they were able to with Splunk ES. As they work to carry out daily threat hunting investigations, they were also on the hunt for a Platform that could display their data in a visually appealing way with flexible dashboards.

INDUSTRY: Education
HEADQUARTERS: North America

CHALLENGE

This US school system was paying for Splunk ES but not getting the necessary value for a team of threat hunters. They were paying for a complex tool that did not include the core analytics and threat hunting capabilities that were needed to carry out essential daily tasks.

SOLUTION

The Devo Platform can easily scale to handle current and future ingestion levels for the team. The Devo Platform also gives them access to user friendly and advanced threat hunting and data science capabilities. Devo gave them a solution to get their daily work done while also saving budget to allocate to other tasks that would have otherwise not been pursuable.

REQUIREMENTS

- The ability to seamlessly integrate with Crowdstrike and XSOAR
- Advanced scalability that could grow with their company growth
- Access to user-friendly threat hunting and data science capabilities
- Event correlation
- The ability to run high performance queries from all current data sources

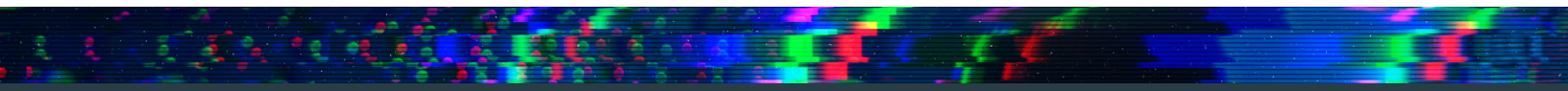
WHY DEVO

A variety of critical capabilities made Devo stand out as an attractive SIEM solution to the customer, including:

- Devo gives users the ability to access endless integrations. By selecting Devo, the team was able to seamlessly integrate their pre-existing SOAR, XSOAR.
- Devo's cloud native model can easily scale to meet their growing ingestion levels. Within just a short amount of time, **the team has already been able to increase ingestion by 30%**.
- Devo offers an appealing and inclusive pricing model. When assessing alternatives in the market, Devo's **TCO came in 35% lower than other competitors**, saving them the budget to allocate to other projects they had previously been unable to fund.
- Devo provides advanced threat hunting and data science capabilities to secure their organization.
- Access to 400 days of always hot data out of the box at no additional cost.
- The ability to run high performance queries from all data sources, including Crowdstrike.
- Access to advanced activeboard and visualizations. The team is able to go into Devo Exchange and access pre-made activeboards for them to deploy in their own environment, saving them both time and resources.

NEXT STEPS

The team is very interested in leveraging Devo Security Operations more in their day to day work. Devo Security Operations has the ability to integrate seamlessly with their existing security ecosystem to enrich investigations with valuable context. The team plans to become more familiar with Security Operations to improve their security posture as much as possible.



Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.