Devo Improves Analyst Experience at Major Public University by Reducing Routine Engagements by 6X

CASE STUDY

BACKGROUND

This major public university is made up of three primary campuses. Before Devo, each campus IT team leveraged its own SIEM solution and operated in silos. As the University sought to improve its day-to-day operations, the IT team looked for a solution that could enable greater cohesion, encourage collaboration, and increase visibility across the university's system. Additionally by centralizing tools, the team would be able to see cost savings.

BEFORE IMPLEMENTING DEVO

Prior to using Devo, the team of 13 analysts was using Elastic products. One of their most significant paint points with Elastic was the time spent building manual alerts. Without access to a library of out-of-the-box content to deploy in each environment, the analysts spent most of their days manually building out content to address critical use cases. This resulted in hours per week being spent simply building out the software needed to perform their jobs. Instead of spending time actively remediating threats, the team was forced to work reactively, and they remarked that much of the process was about "patching up holes" rather than strategically monitoring the environment. Analysts at the university were spending more time tuning multiple SIEMs than actively investigating, leading to potential security risks.

Additionally, with Elastic, the IT team was limited in its access to historical data. Due to the cost of managing on-prem hardware, the team did not have enough budget to afford the hot historical data needed to conduct day-to-day functions. This hindered the team's ability to act quickly when conducting investigations.

INDUSTRY

- Education

ENVIRONMENT

- More than 45,000 endpoints
- Three geographically dispersed campuses
- Providing protection for over 31,000 students

SECURITY CHALLENGES

- Resources were strained due to the operation of multiple SIEMs and log instances
- Lacked advanced correlation rules to defend against threat actors
- Needed a single cloud-based SIEM for improved security management

SOLUTION

- The Devo Security Data Platform

KEY BENEFITS

- All SIEM and log instances are now on a single platform
- Data collection is now comprehensive and centralized
- The team can respond more quickly and effectively to security events
- Access to out-of-the-box alerting content at no additional cost

> *"With our previous solution, if we needed to look over a period of time, maybe a week or two weeks of logs, and filter on that, we would put in our filter, put in our logs, click search, and walk away because we knew that we were not going to get an answer anytime soon."*
>
> ***- Lead Analyst, Major Public University.***

AFTER IMPLEMENTING DEVO

With Devo, the university has centralized its Elastic tech stack into one universal SIEM for all campuses. By leveraging the Devo Security Data Platform, the team has been able to reduce burnout and make their SOC more efficient.

One way that Devo has improved the analyst experience at the university is through a robust library of out-of-the-box content. **Devo Exchange,** Devo's built-in content marketplace, extends the capabilities of the team. Analysts are now able to download pre-built Security Operations alerts and Activeboards. Devo Exchange has provided the team with a catalog of ready-to-use content created by the Devo team that can be deployed at any time. The team has saved hours of time and effort that they were previously using to manually create these kinds of resources in-house.

Additionally, by moving SIEM operations to one cloud-native solution, the university can easily manage its logs across campuses in one centralized tool. The lead analyst noted that this is one of the largest advantages for him personally. The incumbent on-prem solution was displaying a lag in computation. Moving over to the cloud has not only made processes smoother by giving them access to a dynamic ramp-up of computation but also by allowing the team to save time. What **used to be a 30-minute engagement has now been reduced to as little as 5 minutes,** as they no longer have to waste time switching between the vast array of tools across their tech stack.

The Devo Security Data Platform also includes 400 days of hot data out-of-the-box. Having access to more historical data out-of-the-box has saved the team a copious amount of time. In the past, they had been wasting hours, maybe even days, trying to threat hunt across their historical data. With access to 400 days of hot data at no additional charge, analysts at the university now have the storage they need in order to run searches more quickly. The team can redirect time saved to actively focus on threats rather than sit and wait for the data to load. The team's lead analyst explained,

"With Devo, the way that it is able to stage loading and information, we can get an idea of where we should be looking if we can narrow down the time range. And then just getting a holistic view of the entire scope of the original problem we are looking into. It has really sped a lot of that up so that we're not playing the waiting game."

THE UNIVERSITY'S PRIMARY ANALYST USE CASES WITH DEVO:

- Failed login attempts

  Before using Devo, the team was manually sifting through failed login attempts to get to the bottom of things. The team's lead analyst explained:

  "From an operations perspective, something that can create a lot of noise in an organization of our size is whenever someone has a network mount that is currently configured. They then try to change their password, and then that network mount is still trying to log in with their old password. So we started getting a whole lot of failed login attempts for a specific account on a certain divide or range of devices depending on their situation."

  The lead analyst was able to solve this problem directly with Devo by downloading prepacked alerting from Devo's Security Operations application. Now, an alert is triggered when several failed login attempts occur within a specific time range, reducing their team's previous workload and allowing them to more actively remediate potential threats.

- The Impossible Traveler

  The university has a variety of abroad programs and many foreign login attempts. As a result, the team often monitors its environment for potential impossible traveler scenarios. Before Devo, the team did not have a systematic way of monitoring for impossible travel. The university's lead analyst told the team,

  "We were very cautious whenever an account was logging in where we don't have any study abroad programs. Whenever we don't have a current relationship with a university over there, but we start seeing logins from our user accounts from that country, it used to ring a lot more alarm bells."

With Devo, the team has been able to download prepacked alerting that is triggered when these suspicious logins occur. Access to this out-of-the-box content has allowed their analysts to work more efficiently to squash the threats before they have the chance to become problematic.

THE RESULT

The university's team analyst expressed that, beyond solving for their primary use cases, leveraging Devo has reduced burnout through ease of use and improved visibility.

Using Devo has improved the analyst experience at OU by reducing investigation time in order to boost efficiency and combat burnout. The team now has full visibility across their entire organization, enabling greater efficiency and cross-campus collaboration. They save time by using an all-encompassing tool rather than switching between tabs to find the right tool in their tech stack to problem solve. James and his team can spend more time proactively fighting threats before the attack.

> “*It can be like drinking from a fire hose, especially when you are trying to figure out what tool to log in to get what information. Devo is something that not only solves that pain point, but we get all of our log information into that single place, and it also helps us break out of the campus-centric model. It doesn't really matter what campus' logs you are trying to focus on. You can find them pretty much in the exact same format as any other campus so that you do not have to fill in blanks and try to figure out what can seem like 5 different languages at once.*”
>
> ***- Lead Analyst, Major Public University***

Devo
3 Center Plaza
Suite 302
Boston, MA 02108

Devo unleashes the power of the SOC. The Devo Security Data Platform, powered by our HyperStream technology, is purpose-built to provide the speed and scale, real-time analytics, and actionable intelligence global enterprises need to defend expanding attack surfaces. An ally in keeping your organization secure, Devo combines the power of people and AI to augment security teams, leading to better insights and faster outcomes.