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

Devo enables large university to centralize all logs and leverage a single source of truth to proactively remediate threats.

This public research university has three campuses, with its

each campus worked with its own IT department, leading to a need for more visibility. The university provides protection to over 31,000 students. Students could sometimes, without even realizing it, click malicious links or engage in other accidental behaviors. The team was working to manually chase these instances and build out alerting for their main use cases, leading to high levels of manual burnout.

The security team needed to consolidate three security

unit. As a result, the university was in a position of increased security risk. The team's CISO explained,

"As we began collapsing our systems, we realized that

and logging instances and that standardizing on a single platform, centralizing these instances made sense technically as well as logically"

INDUSTRY

ENVIRONMENT

- Three geographically dispersed campuses
- Protecting over 31,000 students

SECURITY CHALLENGES

- Resources were strained due to the operation of
- Lacked advanced correlation rules to defend against threat actors
- security management

SOLUTION

Additionally, because the university leveraged multiple dashboard content and alert rules. As a result, each team was duplicating efforts and creating a disjointed security infrastructure. Without complete visibility into their environment, the university was working in a reactionary manner and building alerts to patch up holes rather than

The team needed an advanced platform that would consolidate data ingestion and operations into one view.

The university only needed to search for a new solution for a short time. The team was very drawn to the Devo Security enable the team to achieve its two main goals: consolidate all logs into one solution and increase visibility. With Devo, The university can centralize all of its logs and provide teams across their campuses with one single source of truth to proactively remediate threats.

Devo also enables the team to scale as the university each campus, they could save money on physical hardware the cloud. The lead Analyst at the university explained:

"Devo really hits that sweet spot for us, especially with it being cloud-focused. The primary advantage is being able to get that dynamic ramp-up of computation when we do have more logs or searches going on. That's been a really big advantage for us. We don't see the performance hit that we would if we were to just stick with our on-prem hardware."

hours each week. They have been able to use this newly become much easier with the enhanced visibility they have team's lead analyst explained:

"Within Devo, a lot of the content is built out for us. From alerting to activeboards, we are able to speed up our daily

rather than manually creating it ourselves."

The Devo Platform has allowed the team to consolidate all data in one place while giving them access to advanced content and capabilities to solve threats actively.

The team has drastically improved visibility across their campuses by implementing Devo. The team's lead analyst explained:

"We've had various incident response situations that have been a lot easier to view as it crossed between our previously solid network boundaries because of Devo's perspective as our more centralized view rather than

The Devo Security Data Platform has reduced time spent team to focus more actively on current threats. In selecting Devo to replace their tech stack, they were also able to phase out a managed detection platform that was costing them almost $100K annually. They have freed up this cost and allocated their budget to other areas of their organization.

their environment.

> *"Knowing that Devo is collecting all of our logs helps me sleep better at night, and I know my team is equipped to respond to any threats appropriately"*
>
> ***- CISO, Major Public University.***

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