The University of Oklahoma selects Devo to centralize its SIEM and reduce the time spent on routine investigations by 50%.

CASE STUDY

DEVO

Devo enables the University of Oklahoma to centralize all logs and leverage a single source of truth to proactively remediate threats.

SUMMARY

The University of Oklahoma is a public research university with three campuses across the state, with its flagship University in Norman, OK. Before Devo, each campus worked in siloed IT departments with different tools and processes. This inhibited OU from gaining proper visibility into its environment. OU turned to Devo to centralize its logs into a single solution and streamline IT team workflows. With Devo, OU's SOC now has a holistic view across the enterprise, enabling the team to improve visibility and save hours of analyst time.

THE CHALLENGE

The University of Oklahoma has three primary campuses. Prior to Devo, each campus was working with its own IT department, leading to a need for more visibility. OU provides protection to over 31,000 students. Students could sometimes, without even realizing it, click malicious links or 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 OU security team needed to consolidate three security groups – as well as five SIEM and logging instances – into a single unit. As a result, OU was in a position of increased security risk. The CISO of OU explained,

"As we began collapsing our systems, we realized that we also had at least three, four or even five different SIEM and logging instances and that standardizing on a single platform, centralizing these instances made sense technically as well as logically."

Each IT department across OU's campuses was using different on-premise software. Not only was this inefficient and cost prohibitive, but it also created blindspots and threatened the university's security posture.

The University of Oklahoma

INDUSTRY

- Education

ENVIRONMENT

- More than 45,000 endpoints
- Three geographically dispersed campuses
- Protecting 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 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

50%
reduction in time spent on routine investigations

$100K
savings in reducing tech stack

<5
minutes to onboard new data

<30
days to migration

Additionally, because OU was leveraging multiple SIEMs, each team spent critical hours manually building 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, OU was working in a reactionary manner and building alerts to patch up holes rather than problem-solve for prevention.

The OU team needed an advanced platform that would allow them to automate routine processes and give them access to out-of-the-box content to secure their organization and free up analyst time. The team needed a cloud-native SIEM to consolidate data ingestion and operations into one view.

THE SOLUTION

The University of Oklahoma only needed to search for a new solution for a short time. The team was very drawn to the Devo Platform because, as a cloud-native solution, it would enable the team to achieve its two main goals: consolidate all logs into one solution and increase visibility. With Devo, The University of Oklahoma can centralize all of its logs and provides teams across their campuses with one single source of truth to proactively remediate threats.

Devo also enables OU to scale as the university continues to grow. By giving up their locally hosted SIEM on each campus, they could save money on physical hardware while improving ramp-up time and overall performance in the cloud. James Cassidy, an Intermediate Security Analyst at OU, 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."

Devo also gives the team access to out-of-the-box content and the ability to download pre-built activeboards through Devo Exchange. Access to this content saves the team **3 hours each week**. They have been able to use this newly freed-up time to actively remediate threats, which has become much easier with the enhanced visibility they have obtained from materials downloaded from Exchange. James Cassidy 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 processes by just grabbing content from the Exchange rather than manually creating it ourselves."

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

THE RESULT

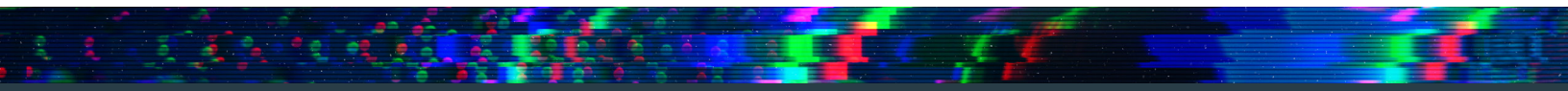
The OU team has drastically improved visibility across their campuses by implementing Devo. James Cassidy explained,

"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 focusing on campus-specific logs."

The Devo Platform has reduced time spent on regular investigations by approximately 50%, allowing its 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.

Based on their success with the Devo Platform, the team is considering fully implementing Devo Behavior Analytics in 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, University of Oklahoma***



Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native security analytics platform that combines the power of people and intelligent automation to confidently defend expanding attack surfaces. An ally in keeping your organization secure, Devo augments security teams with AI — enabling you to continuously scale SOC efficiency, increase the speed of threat detection and response, and gain greater clarity to empower bold action, minimize risk, and maximize outcomes. Learn more at **www.devo.com**.