The University of Oklahoma

CASE STUDY

University of Oklahoma Selects Devo Platform to Centralize SIEM, Logging Instances While Defending Campuses Against Threat Actors

Standardized, cloud-native platform results in faster, more effective event investigation.

SUMMARY

The University of Oklahoma is a public research university located minutes from Oklahoma City. With its recent convergence of three security groups and a desire to centralize logging and SIEM instances, the university turned to Devo to deploy a single cloud-hosted platform that would consolidate instances while giving its security team the information it needs to investigate and respond to incidents quickly, effectively and appropriately.

THE CHALLENGE

According to Aaron Baillio, chief information security officer for the university, the convergence of its three security groups inspired further discussion around system consolidation.

"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."

As he and his search team developed criteria for a new singular SIEM platform there were several requirements at the top of their "must-have" list.

The University of Oklahoma

INDUSTRY

- Education

ENVIRONMENT

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

SECURITY CHALLENGES

- Resources were strained due to 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

- Devo Platform

KEY BENEFITS

- All SIEM and log instances now on a single platform
- Data collection is now comprehensive and centralized
- Team can respond more quickly and effectively to security events

> *"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."*
>
> ***– Aaron Baillio***
> ***CISO, The University of Oklahoma***

"The first was that it had to be cloud-hosted, as the university has three geographically separated campuses which collected logs locally, including cloud log instances from other sources. We also wanted advanced correlation rules, complete with predefined or customized use cases, to defend the university against threat actors."

THE SOLUTION

Based on these criteria, Baillio didn't have to search very long.

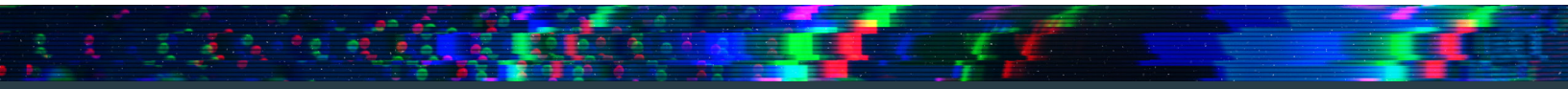
"That's what really stood out about the Devo platform, that it could do everything we wanted," he said. "So, when it came to choosing a new SIEM for our organization it was kind of a no-brainer."

THE RESULT

With the Devo Platform deployed and all of the university's logs and data collected on a single platform, Baillio is confident that when his team is investigating an incident it has everything it needs — particularly the correct information — so they can respond quickly and effectively.

And the relationship with Devo is built to last.

"Devo met all of our criteria when we were doing our search and continues to innovate and provide a roadmap that really excites us," he said.



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**.