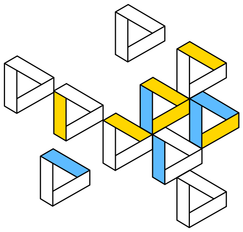
embed

CASE STUDY

Modernizing the Higher Ed SOC

How the University of Montana Reduces Noise and Trains the Next Generation of Analysts



> “ Embed brings a level of consistency and transparency we simply can’t achieve manually. It helps us move faster and make better decisions with the resources we have.”

JONATHAN NEFF
CISO, UNIVERSITY OF MONTANA

CUSTOMER
University of Montana

INDUSTRY
Higher Education

ENVIRONMENT
Public university, highly open email ecosystem

SECURITY TEAM
3 full-time security staff

FOCUS AREAS
Phishing defense, workforce development

CHALLENGE
High alert volume, limited staff capacity, need for trust and transparency in AI

SOLUTION
Embed’s agentic security platform, beginning with email investigations

OUTCOMES
Reduced noise, more consistent investigations, faster triage, and hands-on training for future security analysts

Before Embed: A Complex, Alert-Heavy Environment

As a public university, the University of Montana operates in an inherently open environment. Email communication is central to academic life and far less restrictive than in regulated industries, such as finance or healthcare.

“At a university, we get emails from everybody,” explained Jonathan Neff, UM’s Chief Information Security Officer. “We are regulated (FERPA, HIPAA, GLBA), but our filtering is less restrictive than many other regulated organizations because of the nature of public higher education.”

That openness creates significant security noise. At the same time, UM’s security team is lean. With just three full-time staff members responsible for protecting the university, the team must balance daily security operations with major compliance obligations, including those under the GLBA and HIPAA.

“It’s a lot of responsibility for a very small team,” Neff said.

The Turning Point

UM’s security leadership recognized they needed a way to force multiply their efforts without handing control over to opaque automation. That search led them to Embed.

For Neff, AI wasn’t about replacing analysts. It was about acceleration. “I see AI as an optimization tool that helps you get to the answer faster,” he said.

With Embed in place, user-reported phishing emails are analyzed immediately and consistently. “Embed processes the report first and tells us whether it’s valid,” Neff explained. “It does a much better and more consistent job than we could manually and better than Microsoft on its own.”

The team also correlates email analysis with endpoint behavior to better understand user actions and potential risk, helping them focus attention where it matters most.

WHY EMBED

Security Noise Cancellation®

Cuts through high alert volume

Agentic AI built by practitioners

Mirrors how real analysts investigate threats

Transparency and trust

Every conclusion is explainable

Human-centered automation

Accelerates analysts instead of replacing them

embed

Embed's agentic security platform delivers intelligent automation and transparent investigation capabilities across your entire attack surface. Whether you're triaging alerts, defending your cloud infrastructure, or securing endpoints, Embed empowers your team to move faster—with confidence.

Building Trust Through Transparency

In higher education, trust is critical, not just within the security team, but across the institution.

"The transparency of how Embed gets to its recommendations is hugely important," Neff said. "When we take action, I need to be able to explain why. It can't just be 'because IT said so.'"

This transparency allows UM to confidently use AI as decision support today, while laying the groundwork for more automation in the future.

Security Operations Meets Workforce Development

Beyond operational gains, Embed has become part of something bigger at UM: building the cybersecurity talent pipeline.

Interns use Embed to review phishing cases, understand investigative logic, and learn how expert analysts reason through threats. In turn, they gain hands-on exposure to modern, AI-enabled security operations.

"It was a two-way interaction," Neff shared. "Students got real experience, and they were also providing feedback back into the platform."

The next step for UM is to move Embed up the workforce development lifecycle, getting it into the CyberMontana student SOC hands before they move to the Information Security Office.

"Giving students real tools and real data is essential," Neff said. "By the time they graduate, they really do know what they're doing."

The Impact

With Embed handling the noise, UM's security team can focus on higher-value work while students gain practical experience that prepares them for real SOC environments.

For UM, the result is a smarter, more scalable approach to security operations: one that reduces alert fatigue today and helps train tomorrow's analysts at the same time.

The Future

Looking ahead, the University of Montana views Embed as more than a point solution for phishing. As the security program matures, Neff sees potential to apply Embed's transparent, agentic approach to additional risk and compliance workflows over time. For a resource-constrained SOC in a highly open environment, that combination, reducing noise today while laying the groundwork for smarter, more scalable security tomorrow, matters deeply. Just as importantly, Embed helps UM fulfill a broader mission: preparing the next generation of cybersecurity professionals with real-world experience in how modern security operations actually work.