



University Boosts Threat Visibility and Security Posture by Deploying Stellar Cyber Open XDR Platform

A university identified the need to increase visibility across its faculty, staff, and student activity to better mitigate threats. After considering multiple approaches to satisfy their requirements, the Stellar Cyber Open XDR platform delivered the visibility they needed to better protect their environment without the complexity and cost of other products.



“ The Stellar Cyber Open XDR Platform is a product that very easily and quickly became our central security management point because of its ease of use and ability to deliver results without burying us with data.”

– University Information Security Architect

Before:



Lack of Visibility

Near impossible to see where and how threats might be impacting the environment.



Manual

Threat identification relied on expert personnel completing a manual review of collected logs.



Blindspots

The lack of enterprise-scale security solutions meant the security team continuously reacted to potential threats rather than proactively identifying them.

With Stellar Cyber:



Visibility

Stellar Cyber now provides the visibility the security team needs to mitigate critical threats fast.



Efficiency Gains

Instead of relying on manual processes security team now works directly from the Stellar Cyber incident queue speeding response times.



Intuitive

Stellar Cyber's ease of use means lesser experienced personnel can now participate in keeping the university secure.

“ The ‘Openness’ of Stellar Cyber has greatly benefited us. I have yet to find a product where Stellar Cyber didn't already have a connector available out of the box or one on the roadmap. If I do find one, I know I can call them and probably get what I need quickly.”

“ Before Stellar Cyber we were good at collecting log data, however collecting the data by itself didn’t give us the visibility we needed to understand our cybersecurity risk.”

The security team at this university came from the world of enterprise organizations where security budgets and resources enabled them to deploy sophisticated security stacks to combat threats. Unfortunately, this university, like most higher education institutions, did not have the good fortune of a significant budget and resources dedicated to security. That said, it was still their responsibility to keep the faculty, staff, and students protected from cyberattacks.

With a few security products deployed across their environment and existing practice of regular log collection, the team determined that a Security Information and Event Management product could improve the situation dramatically so long as it met their specific needs.

Specifically, they were looking for a product:

- That was easy to use
- Could be connected to their existing security products
- Provided great dashboards that required minimal customization
- Provided the visibility that was missing

Upon beginning the Stellar Cyber Proof of Concept (POC), the team almost immediately saw the potential gain this product could deliver without the management overhead other products would require.

First, Stellar Cyber automatically normalized and enriched data from every sensor and security tool used by the university upon ingestion into the platform. Then the AI and machine learning engines automatically evaluate and group related alerts and identify new threats based on abnormal user and asset behaviors, producing a prioritized list of incidents, with appropriate context, on the platform’s intuitive dashboard.

After the successful proof of concept, the security team became so comfortable with the product that they decided to move their POC system into production, delivering results from minute one. With Stellar Cyber, the university is able to deliver consistent security outcomes across its entire IT environment. The ease of use and intuitive nature of the platform also enables virtually anyone in the IT organization to participate in keeping the university focused on what they do best – educating the business leaders of tomorrow.



Stellar Cyber Open XDR platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments. With Stellar Cyber, organizations reduce risk with early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity, delivering an 8X improvement in MTTD and a 20X improvement in MTTR. The company is based in Silicon Valley. For more information, visit <https://stellarcyber.ai>.