

State Agency Boosts Threat Visibility with Stellar Cyber Open XDR Platform

A state agency relies on a lean security team to ensure a successful cybersecurity attack does not adversely impact day-to-day operations. Understanding the need to increase their ability to identify and stop threats faster, the team sought a new product to become the hub of their security operations activities. After many discussions with Stellar Cyber subject matter experts, the state agency selected the Stellar Cyber Open XDR Platform.



“ With the Stellar Cyber Open XDR Platform, what we used to do manually now happens automatically.”

– IT Specialist, State agency

Before:



Lack of Visibility

It is nearly 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 security team's visibility to mitigate critical threats quickly.



Efficiency Gains

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



Intuitive

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

“ Stellar Cyber is working great. We are now getting the visibility into things we didn't know were happening, finding threats earlier in the kill chain.”

“ Before Stellar Cyber, our security operations were primarily manual, relying on the efforts of the security analysts to keep the department running. Now Stellar Cyber does the “heavy lifting” for us, enabling us to respond to threats faster.”

The state agency saw the need to uplevel its security framework and the team pursued different approaches to meet their needs. For example, they inquired about bringing in one of the leaders in the SIEM market but determined the complexity and cost made it impossible. So instead, Stellar Cyber met with key department members to discuss the Stellar Cyber Open XDR platform. After initial discussions, Stellar Cyber’s subject matter experts met with critical individuals multiple times, providing in-depth demonstrations of the product.

These case studies and live demonstrations of Stellar Cyber’s Open XDR platform proved the solution was:

- Easy to use
- Could be connected to their existing security products
- Provided the visibility that was missing

First, Stellar Cyber automatically normalized and enriched data from every sensor and security tool used

by the agency 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. Based on the discussions and live demonstrations, the agency selected Stellar Cyber as the new hub of its security operation activities. Coincidentally, the agency was moving to a new building, which gave the security team a chance to deploy a new platform and uplevel their entire security environment.

After deploying Stellar Cyber, the agency initiated pentesting to stress-test the security infrastructure. Stellar Cyber proved its value by detecting the pen tester’s activity before their exploits could reach their objective. Now, after more than a year on the Stellar Cyber platform, the agency is enjoying the peace of mind that comes from knowing they are well-equipped to detect and mitigate any threat that comes their way and looking forward to having Stellar Cyber do more for them in the future.



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>.