CASE STUDY

University of Zurich[UZH]

The University of Zurich's Central IT Department Unifies Security with Stellar Cyber

Stellar Cyber uses AI and Advanced Correlations to Reveal Hidden Threats and Boost Analyst Productivity

The University of Zurich is the largest university in Switzerland, with more than 25,000 students. Located in the city of Zurich, it was founded in 1833 and currently offers programs in Philosophy, Human Medicine, Economic Sciences, Law, Mathematics and Natural Sciences, Engineering, Computer Sciences, Robotics, Theology and Veterinary Medicine – the widest range of subjects and courses of any university in the country. The University has a rich academic tradition – as of May 2020, 13 Nobel laureates have been affiliated with University of Zurich as alumni, faculty or researchers.

STELLAR CYBER®

With a mandate to deliver centralized IT services for its large student and faculty population with a limited budget and security staff, the University wanted a new security platform that would economically consolidate needed security applications while still integrating with existing tools.

BEFORE

Wasted Time
it can take analysts days or weeks to find threats

False-Positives
distracting from real security issues

Restricted Resources
to cover all needs within the university family

Limited Staff
to cover all security

License Fees
paid for various security features

WITH STELLAR CYBER

Lightning Fast
allows analysts to find threats in minutes rather than days

50% Less
false-positives than other products tested

Secures 150+
colleges and institutes within the university family

24/7
automated security coverage

Saves Money
on license fees using 20+ native security applications

> When the University of Zurich's central IT department needed a solid platform for cybersecurity, Stellar Cyber was the solution that correlated data from multiple sources, improved threat hunting capabilities, and increased analyst productivity by separating real threats from false positives."

Integrating with Existing Tools

The security team at the University of Zurich's Central IT Department was hoping to find a modern solution for its security needs, rather than just building out another SIEM. While UZH researched and tested other solutions, Stellar Cyber's Open XDR was the best choice because it integrated nearly two dozen security applications under a single, intuitive dashboard.

Deployment of Stellar Cyber was straightforward – it was a plug-and-play installation that began to produce results quickly right out of the box. Stellar Cyber's built-in multitenancy would also allow the security team to efficiently support over 150 institutes and colleges within the University family.

"We were impressed by the built-in multitenancy," said the IT Security Officer at the University of Zurich's Central IT Department. "We support many different colleges and university departments, each with its own issues, and we need to track them individually. Every other product we saw required a very expensive upgrade to support multi-tenant operations, if it was even offered as an option."

Improving Threat Visibility

Stellar Cyber's built-in detections immediately delivered better visibility for the security team. "With a few basic settings, we quickly made many meaningful detections and discovered a lot of security events we might have missed before," said the IT Security Officer. "In fact, during the first month of use, we had a security case that we were able to point out within hours instead of several days. Another thing we noticed was that the rate of false positives was

> "Traffic volume was causing a lot of false positive alerts, and it was really impacting our ability to catch and respond to the real threats...Stellar Cyber reduced our analysis expenses and enabled us to kill threats far more quickly."

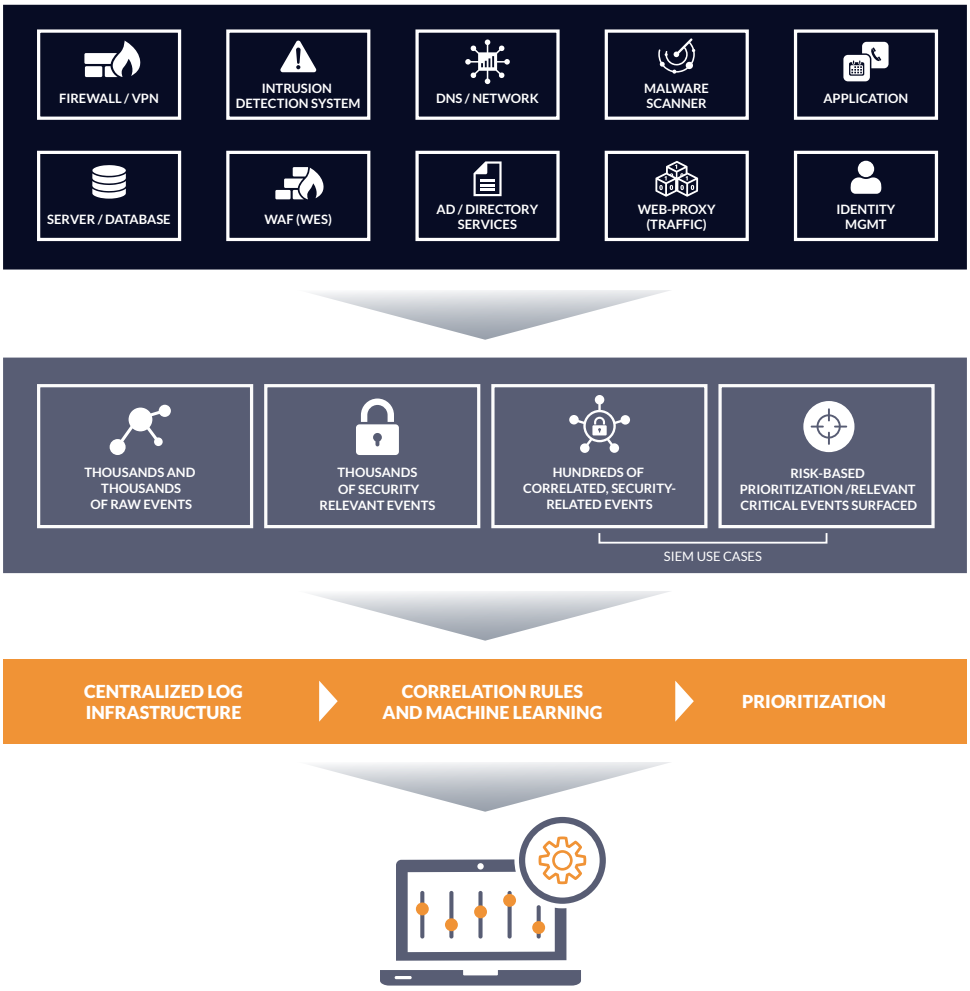
half what it was with other products we tested, and our ability to train the Machine Learning so it recognized previous attack vectors makes it even more effective."

"Traffic volume was causing a lot of false positive alerts, and it was really impacting our ability to catch and respond to the real threats," the IT Security Officer added. Stellar Cyber reduced our analysis expenses and enabled us to kill threats far more quickly."

Stellar Cyber collects data from all areas of the attack surface, correlating what might be seen as unrelated incidents and analyzing them to determine whether they represent a real threat or a false positive. Even with the university's high traffic, it spots threats other systems might not catch. "Previously, we were getting a lot of false positive alerts, and it was really impacting our ability to catch and respond to the real threats," said the IT Security Officer. "The automated prioritization of high-fidelity alerts in the Stellar Cyber platform made analysis far more productive and enables us to kill actual threats far more quickly."

As is common with many educational institutions, UZH's Central IT department is on a tight budget with a limited staff, although it is heavily tasked with securing all of its unique entities against a broad range of threats.

High Speed High Fidelity Detection & Automated Response



By correlating comprehensive data along the entire cyber kill chain and presenting it in an intuitive dashboard, Stellar Cyber largely eliminated the need for Stage 1 analyst tasks (manually correlating data from multiple tools). And, by making analyst efforts much more productive, it saves time and money. Analysts who would otherwise have to spend days or weeks tracking down a threat can spot them in minutes via the Stellar Cyber interface.

"In key situations, we have been able to connect the dots and quickly identify the attack situation in order to get an overview of the attacker's infrastructure (involved, external IP addresses) and already contacted or connected internal endpoints," said the UZH's IT Security Officer. "In addition, the easy-to use 'Automation' feature allowed us to quickly set up monitoring and response and automatically notify the affected IT manager about newly infected endpoints in their area of responsibility. That kind of automation gives us 24/7 coverage without manpower."

Another savings came from tool reduction: Stellar Cyber incorporates next gen SIEM with network, user, and including malware detection and IDS, enabling the University's central IT department to save on license fees by potentially sunsetting some of the stand-alone tools it currently uses.

When the University of Zurich's central IT department needed a solid platform for cybersecurity, Stellar Cyber was the solution that correlated data from multiple sources, improved threat hunting capabilities, and increased analyst productivity by separating real threats from false positives.