Case Study: Higher Education

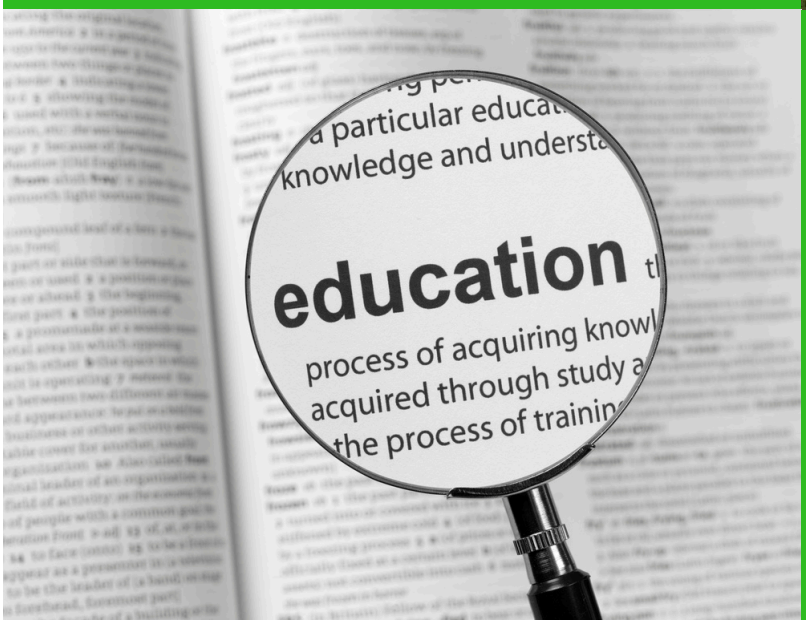
Seceon OTM platform – Cybersecurity for the Digital Era Powered by Artificial Intelligence, Machine Learning, Behavioral Analytics and a Big, Fast Data Engine

Executive Summary

Seceon OTM provided real-time threat detection and remediation within minutes of a threat occurrence, compared to a dedicated MDR provider, which responded after four hours.

"The S*eceon OTM platform gave us immediate value by correlating numerous threat events (normally requiring a great deal of time and effort from our security staff) and delivered detections and alerts in real-time, notifying us of a threat much earlier than the MDR security services we were using. Seceon's OTM platform is very easy to install, configure and operate*"

– Kevin Stillman, CISO, SUNY



Challenges faced by SUNY and other Higher Education Colleges

Like so many colleges and universities today, SUNY's IT staff has multiple responsibilities, including security, and is constrained by limited budgets, staff and lack of specific talent/knowledge. With these constraints, it was imperative for SUNY to clearly understand where key data was located, which data was the highest risk, and how to best protect it.

Recognizing their limitations, but still needing to find a solution to protect and defend high-value assets in a university environment, SUNY IT leaders sought an affordable, enterprise-class solution for classifying data and detecting and eliminating dangerous threats in a way that would be easy for its very small staff to monitor and manage.

How Seceon's OTM Platform Helped

After evaluating several other security platforms, including a popular SIEM vendor and multiple point solutions that require significant up-front and operational investments, SUNY turned to Seceon. Its Open Threat Management Platform (OTM) automates real-time threat detection and remediation. SUNY acknowledged the value in a solution that **correlates all events** from next-generation firewalls, network flows, identities, and server logs together, **leveraging Seceon's Dynamic Threat Models (DTM) that use machine learning to surface and prioritize threats.**

With simple-to-implement provisioning and integrations, Seceon's OTM platform gave SUNY a single, comprehensive view across the entire enterprise, regardless of architecture or location. They benefitted from **quick and easy set up of policies to prevent, detect, or eliminate threats.** With its user-friendly dashboards and alerts, Seceon's OTM platform was up and running within a few short hours, detecting legitimate threats and providing detailed actionable steps for staff to eliminate the threat or initiate automated remediation.

Seceon's OTM platform gave SUNY's limited staff an automated, virtual security operations team with real-time visibility into all attack surfaces across students, faculty, and staff.

Key Features of the Seceon OTM platform that Helped SUNY Staff

1. **Vulnerability Alerts:** Assessments for forensic and preventive use. Ability to to detect and prioritize threats in real-time.
2. **Correlation Engine:** Correlates several events together, from multiple sources and timeframes to create contextual and situational understanding of vulnerabilities and threats.
3. **Visualization**: Comprehensive, bird's-eye view of North-South and East-West traffic. Although this was not a primary use case, it provided greater understanding of several IT and networking issues.
4. **Automation:** Streamlined, efficient policy creation, threat detection and response; requiring no complicated rules to write or the need to figure out where to apply policies to contain threats with the least impact to services and users.

"During the Mirai, 'Internet of Things' DDoS attack, Seceon quickly enabled us to find and remediate systems that were carrying out the attack. An issue that might have taken days to clean up was fixed within minutes"

-George Insko, Security Architect, University of Kentucky

Results and Return on Investment

Seceon's OTM platform detects almost all forms of threats such as **malware, ransomware, DDoS, brute force attacks, advanced persistent threats, lost or compromised credentials, and insider threats**, in minutes as they become active and stops them from doing further harm and creating a large blast zone.

Seceon's OTM platform is like having an advanced team of security analysts working 24x7; only it works hundreds of times faster than any analyst. Typically, the closest competitive solutions include **next-generation SIEMs/UTMs** and neither of these solutions detect all the threats that the Seceon OTM does. They also do not work as fast to stop threats on their own. These complicated stacks of point solutions **cost over five times more** and don't provide the operational or license cost savings of the Seceon OTM platform.

Verizon's DBIR report states that the average cost per lost student medical record is $350. IBM reports the cost of a typical breach where thousands of records is now over $4.45M in 2023. Verizon and other industry experts estimate 40 percent of all universities and businesses are breached at least once per year, and this rate is growing.

Seceon's OTM platform dramatically increases the odds that no or a rare few records will be lost, potentially saving tens to hundreds of thousands of dollars per breach.

Bottom Line: Seceon's OTM platform pays for itself in less than two months. It costs 20% less than the nearest like competitor and works a hundred times faster, within minutes, to detect a breach and to protect the intellectual property and brand of your organization.

About Seceon

Seceon enables organizations to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates security programs with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platform. The platform delivers gapless coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI, and ML models built on behavioral analysis and correlation engines to create reliable, transparent detections and alerts. Over 9,000 organizations globally are running efficient security programs with automated cyber threat remediation and continuous compliance.

Learn more about Seceon and schedule a demo today.

Learn more about Seceon

Schedule a Demo www.seceon.com/contact-us/