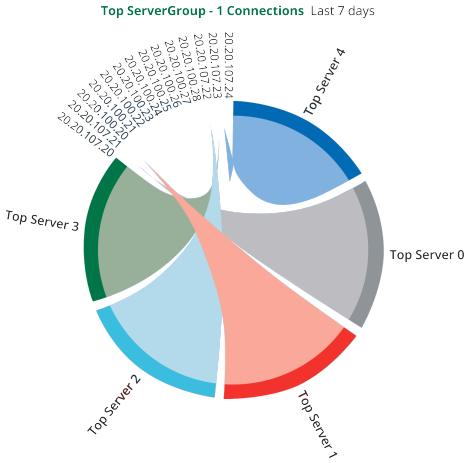
Case Study: Higher Education

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

"Seceon OTM provided us an immediate value proposition by correlating numerous threat events (normally requiring a great deal of time and effort from our security staff) and delivering alerts in real time, notifying us of a threat much earlier than the security services we were using. OTM is very easy to install, configure and operate." **– Kevin Stillman, CISO, SUNY**



Seceon OTM makes it easy to visualize traffic flows.

Executive Summary

Seceon OTM provided real time threat detection and remediation within minutes of the threat occurrence, compared to a dedicated, managed security service, which responded after four hours.

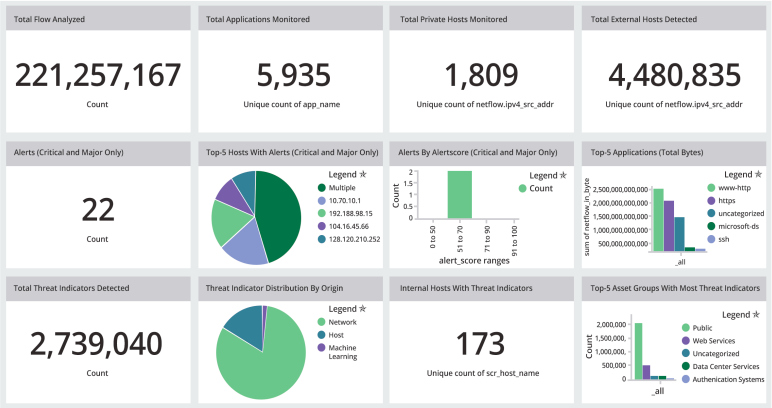
Challenges faced by SUNY and other Higher Education Colleges

Like so many colleges and universities today, SUNY's IT staff maintains multiple technology responsibilities, including security, and is constrained by limited budget, staff and specific talent/knowledge. With such confines, 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 OTM Helped

After evaluating several other security platforms, including one homegrown SIEM and others requiring significant up-front and operational investment, SUNY turned to Seceon and its Open Threat Management Platform (OTM) for automated, real-time threat detection and remediation. SUNY acknowledged great value in a solution that ***automatically correlates all events*** from next generation firewall, network flows and server logs together, ***using dynamic threat models that leverage machine learning to surface and prioritize threats***. With simple-to-implement provisioning and integration, Seceon OTM gave SUNY a single, comprehensive view across the entire enterprise, regardless of architecture, and the ***ability to quickly and easily set or***

correct policies to prevent, detect or eliminate threats. With its user-friendly dashboards and alerts, Seceon OTM was up and running within a few short hours, detecting legitimate threats and providing detailed action steps for staff to eliminate the threat or initiate automated remediation. Seceon OTM gave SUNY's limited staff an automated, virtual security operations team with real-time visibility into all assets, students, faculty and staff.



Key Features of Seceon OTM that helped SUNY Staff

1. ***Vulnerability Alerts***: Assessment for forensic and preventive use. Superior ability to detect threats in real-time.
2. ***Correlation Engine***: Correlate several events together to create a real contextual understanding of vulnerabilities and real threats in the system.
3. ***Visualization***: Comprehensive, bird's eye view of North-South and East-West traffic. Although this was not primary use, it helped in understanding several IT issues.
4. ***Automation***: Streamlined, efficient policy creation, threat detection and response; requires no complicated rules to write or figure out where to apply policy to contain the threat with the least impact to the services.

"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

The OTM detects almost all forms of threats such as ***DDoS, brute force attacks, malware, ransomware, advanced persistent threats, lost or compromised credentials, insider threats***, in minutes as they become active and stops them from doing further harm.

Seceon OTM 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 such as ***next generation SIEMs/UTMs*** neither detect all the threats that the OTM does, nor work as fast to stop threats on their own. These ***competitive products cost over five times more*** and don't provide the operational or breach cost savings that the OTM can provide.

The average lost record costs about $50 in 2016 according to the industry's leading expert – Verizon Enterprise Solutions. However, student medical records cost $350 per lost record. The typical breach where thousands of records are lost can cost $50,000 and upwards to $350,000 per breach. 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.

The OTM 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: ***The OTM pays for itself in less than two months, often immediately. It costs 20 percent of the nearest like competitor and works a hundred times faster, within minutes, to detect a breach and to protect your intellectual property and brand.***

To learn more, please contact: ***sales@seceon.com***