The Situation

Securing campus networks is a unique challenge for universities. The abundance of personal laptops and mobile devices entering the network makes it more difficult to lock down computing resources or enforce standardized configurations. At universities today, the tech-savvy population demands unfettered access to Internet resources and social networking sites, providing unlimited infection vectors for botnet operators and cyber criminals.

Universities have the added challenge of operating a borderless network with student and faculty bringing a wide variety of devices with various operating systems and applications in and out of the network.

While students two years ago mainly brought laptops and smartphones with them to college, in the age of the Internet of Things (IoT), students are now using tablets (61%), smartwatches (27%) and gaming consoles (25%) on campus, dramatically increasing the number of devices connecting to the campus network. In addition to students bringing more devices with them to school, 60 percent of faculty, students and IT professionals use four or more devices on campus which drives up activity on the network.

Most colleges and universities now provide services at multiple locations—branch campuses, learning centers, study-abroad locations, and remote research sites—in addition to the main campus. Operating in different countries adds to cybersecurity complexity, and international threat actors reside in some countries hosting remote campuses for U.S. schools.

The Challenge

Institutions of higher learning, have to be open, but at the same time keep security tight. They must support collaboration, making systems publicly available and enable knowledge sharing. At the same time, protect valuable data, the individual and the universities reputation.

Situational awareness for the university IT security team starts with the millions of logs generated in the network infrastructure by users, network devices, servers, applications and a multitude of other sources. The logs are the key source of security information that enables the university IT security team to detect potential cyberthreats and breaches and take appropriate action.

The Solution

Sun Mgt's SIEM/SOAR-as-a-Service offering using LogPoint SIEM and Palo Alto XSOAR for log aggregation and automation, with automated playbooks responding to security events.

LogPoint SIEM (Security Incident and Event Management) - leverages advanced analytics, accelerated by machine learning, to improve your cybersecurity posture and efficiently automate relevant responses to both internal and external threats.

LogPoint's license model is based on the number of nodes in the network sending log data, rather than data volume or transactions. This makes the cost of the SIEM solution 100% predictable, eliminating budget concerns and, most importantly, eliminating the need to make decisions about leaving out log sources that may compromise security. There's no extra cost related to the growth of the company's data volume or how many events per second you receive.

How LogPoint solves the challenges customers face today:

- Provides a single pane of glass – consolidation of various tools
    - Dashboards, searches, reporting incidents, configuration, UEBA
- Pre-built:
    - Dashboards – 400+
    - Reports – 170+
    - Use Cases – 5000+
    - Alerts – 1000+
    - Log Source Support – 900+
- Supported log sources – 900+ (parsers and normalizers pre-built)
- Tie into TIP's (Threat Intelligent Platforms), pre-built alerts from MITRE ATT&CK, sophisticated analytics capabilities
- Flexible Deployments
    - IaaS
    - On-prem, Hardware, VM, Cloud, thru MSSPs
    - Taxonomy: classify and normalize from many inputs to one common output
    - Normalization after ingestion of logs – results in faster searches
    - Policy-based routing (based on key-value pairs)
    - Archiving (repositories, RGAC, Retention, Encryption)

Palo Alto Cortex XSOAR - is a comprehensive security orchestration, automation and response (SOAR) platform that unifies case management, automation, real-time collaboration and threat intel management to serve security teams across the incident lifecycle.

How XSOAR Works

- XSOAR ingests aggregated alerts and indicators of compromise (IOCs) from detection sources—such as Security Information and Event Management (SIEM) solutions, network security tools, threat intelligence feeds, and mailboxes—before executing automatable, process-driven playbooks to enrich and respond to these incidents.
- These playbooks coordinate across technologies, security teams, and external users for centralized data visibility and action.

How XSOAR Helps

- Improve Investigation Quality – Use a collaborative workspace, machine learning and cross-correlations
- Automate Repeatable Steps – Automate actions to standardize and scale incident response
- Unify Security Functions – Gather intelligence from multiple products on a single console

XSOAR Value

- Standardize and scale processes - XSOAR playbooks help you codify and enforce a process that's common across your security team. These playbooks can be fully automated, fully manual, or any combination of the two, with each scenario having its own advantages for increased efficiencies.
- Lower response times with automation - XSOAR can automate thousands of actions across your security products, handing back time to you for investigation and decision-making. These automations can be for alert ingestion, data gathering, response actions, and updating info back in the point products.
- Coordinate actions across security products - You now have a process-centric view of how to respond to a particular incident that's not tied to any one security product. All security products have their purpose, but playbooks provide you an abstracted view of the 'process' and make it easier to replace one product with another whenever you need to.