CASE STUDY

Major University System Learns the Value of Threat Sharing and Security Collaboration

OVERVIEW

One of the largest university systems in the US was grappling with the challenges of maintaining efficient collaboration among its institutions to mitigate cyber threats. They sought an automated solution to foster bidirectional threat intelligence sharing and seamless collaboration, tailored to their unique requirements.

CHALLENGES

1. **Labor-Intensive Incident Reporting Process**
   - Delayed incident reporting through manual web-based incident submission forms.

2. **Manual Workflows**
   - Sharing, processing, and operationalization of threat intelligence between entities was manual and inconsistent.

3. **Legacy Tool Dependence**
   - Reliance on email notifications, spreadsheet logs, and information storage silos weighed down process efficiency.

4. **Delayed Alerts**
   - Absence of real-time notifications about cyber attacks and threats, including malware, vulnerabilities, and threat actors.
Solution: Collaborate (CSAP)

Cyware’s Collaborate (CSAP) platform was deployed. Collaborate is a bidirectional threat advisory sharing platform purpose-built to expedite and enhance security collaboration. This solution enabled the university to centralize all threat intelligence sharing and collaboration operations through a single platform, eliminating reliance on multiple tools. Each affiliated institution received access to a member portal, enabling efficient reception of threat intelligence, access to vital information, and streamlined incident reporting.

Cyware’s platform fosters efficient collaboration, permitting discussions on specific threats and creating exclusive working groups and collaboration forums for key personnel, such as CISOs, CIOs, and Security Analysts, based on their roles. Additionally, the platform facilitates tracking mitigation actions and conducting real-time threat assessments to evaluate the impact of cyberattacks, ransomware, and zero-day vulnerabilities on its members.
Cyware’s Collaborate (CSAP) Platform revolutionized the university’s cybersecurity posture, streamlining incident reporting, intelligence sharing, and enhancing overall communication. The key use cases solved were:

1. **Automated Advisory and Threat Intelligence Sharing**
   Replaced email distribution lists, thereby enabling the university to disseminate threat advisories, threat actor analyses, real-time incident notifications, and administrative business updates efficiently.

2. **Multi-Source Threat Intelligence Aggregation**
   Facilitated the automated collection and aggregation of threat intel from multiple sources. It also enabled the addition of university-specific custom threat intelligence sources via RSS Feeds.

3. **Streamlined Incident Reporting**
   Provided an intuitive interface for direct incident reporting, reducing administrative burden and bolstering incident response capabilities.

4. **Centralized Document Repository**
   Eliminated the dependency on SharePoint by offering a centralized document repository. Access to the document repository could be tailored based on the recipient group.

5. **Tailored Intelligence Distribution and Access**
   Allowed for tailored intelligence sharing with affiliates based on role and type of affiliate institution, enhancing communication efficiency.

6. **Bidirectional Information Requests**
   Through its Request for Information (RFI) capability, Collaborate (CSAP) expedited bidirectional information requests, enhancing communication, response times, and overall cybersecurity posture for the university and its affiliated institutions.
BENEFITS AND OUTCOMES

The deployment of Collaborate (CSAP) significantly strengthened the university’s security posture. Key benefits include:

- **Enhanced Threat Awareness**
  The platform provides enhanced situational awareness across the community through early warning threat advisory sharing, improving collective defense against threats.

- **Technological Consolidation**
  Collaborate (CSAP) eliminated reliance on multiple technologies, simplifying operations and reducing complexity.

- **Streamlined Operations**
  The platform streamlines operations ranging from email notifications to document storage, incident reporting, and information requests, thereby augmenting productivity.

- **Improved Collaboration**
  Collaborate (CSAP) fosters an enriched collaboration and knowledge-sharing ecosystem via its centralized document repository and communication features.

- **Bolstered Incident Response**
  The platform’s robust incident reporting mechanism has expedited response times while enhancing incident management.

For more information you can reach us at:

**Cyware**
111 Town Square Place Suite 1203 #4,
Jersey City, NJ 07310
sales@cyware.com  |  www.cyware.com