CASE STUDY

Private R1 University

How a leading research university maximized their cybersecurity investment for lasting protection with integrated security services from NuHarbor.

Overview

For one of the world's leading academic and research institutions, the sustainable security of global infrastructure, assets, and data is paramount. With increasingly sophisticated attacks on the rise, an effective cybersecurity program for a network spanning 135 countries must provide continuous enterprise-wide visibility and trustworthy threat intelligence.

Industry: Higher Education

Size: 17,000 Students
6,552 Faculty and Staff
200,000 Alumni

Even the most advanced technology is limited in its power to affect change and drive positive outcomes without qualified human expertise. The University needed an updated approach to existing IT practices that would prioritize security, streamline operations, expand threat awareness, and improve incident response.

Business Goals

- Sustain a worry-free work environment
- Maximize technology investment
- Protect mission-critical data and proprietary assets
- Establish a cybersecurity plan for lasting protection
- Harness big data to enhance University operations

The Challenge

- Limited resources to effectively leverage existing tools, and build and maintain a comprehensive cybersecurity program
- Lack of visibility across disparate University systems and data sources
- Siloed IT, compliance, and information security business units rife with political segmentation
- Needed to justify cybersecurity investment for non-technical stakeholders

75%
rise in cyberattacks against higher education institutions in 2021.
Source: CSO

55%
of security teams believe the majority of their time spent investigating issues is wasted.
Source: BetaNews

62%
of security teams are understaffed.
Source: IBM

The Solution

Establishing a Baseline

The University owned Splunk Enterprise Security – a top-rated SIEM platform used to monitor, detect, and investigate threats – but needed outside support before their environment could produce trustworthy, actionable insights. Splunk recommended NuHarbor, whose established reputation as an industry leader made it easy for the CISO to choose a four-week professional services engagement complete with:

- DATA SOURCE CLEANUP
- IDENTIFICATION AND ONBOARDING OF CRITICAL DATA SOURCES
- ENABLEMENT TRAINING

> "
> NuHarbor has been instrumental to our SOC operations. Without their flexibility, expertise, and quick reaction, our small SOC team could not operate. NuHarbor continually engages us at the operational and executive levels. They're always looking for new, creative solutions. Not only are they willing to think outside the box, they actually deliver."
>
> **University CISO**

Convincing Stakeholders With Outcomes

With that foundation of trust, NuHarbor was contracted to provide premium health monitoring of the security environment and on-demand engineering for 24x7 administrative and development support. After a significant security incident, it was clear the University's infrastructure remained exceedingly vulnerable – immediate remediation guidance was essential, and advanced threat intelligence was critical for long-term protection. The CISO looked to NuHarbor. Its proprietary Cyber Threat Analysis Center (CTAC) sprang into action, quickly identifying indicators of compromise to understand the vulnerability and deliver a plan for remediation. NuHarbor emerged as the go-to cybersecurity consultancy.

4 weeks

The time it took to achieve environment-wide visibility with NuHarbor

Planning for the Future

NuHarbor deployed a comprehensive security suite, combining the existing service with 24x7x365 human security review and threat hunting, curated threat intelligence, and managed Security Orchestration Automation and Response (SOAR) functionality for better monitoring and early response to threats. The University adopted technology procurement recommendations for endpoint protection and vulnerability management to enhance the security scalability established with Splunk Cloud.

The Outcomes

In partnership with NuHarbor, the University navigated internal roadblocks and external vulnerabilities to produce positive business outcomes:

- Maximized investment in Splunk after just four weeks
- Expanded situational awareness and rapid detection and response capabilities
- Alleviated the strain on an overburdened security group
- Maintained data ownership, visibility, and control
- Achieved enterprise-wide visibility cross a global network

NuHarbor makes cybersecurity stronger and easier for the University to focus on what matters most: supporting its academic and research mission, and serving its students, faculty, staff, and alumni.

To learn more about NuHarbor, please visit nuharborsecurity.com.