ARMIS

LEHIGH UNIVERSITY

CASE STUDY

Moving to proactive security stance management

The Challenge

- Maintain a proactive approach to security posture
- Minimize risk exposure window by reducing time between notification and remediation
- Incorporate asset risk context to drive prioritization of security findings

The Solution

- Scope assessment on a specific set of assets, identify asset owners and provide fix information through existing workflows to facilitate more effective remediation
- Supplement findings categorization with asset profiles and prioritization rules based on business and environmental context labeling

The Results

- Reduced time spent on assessment by 80% with findings consolidation and de-duplication across tools
- Facilitated 40% decrease in tool costs, with consolidation and retirement of overlapping tools.
- Reduced time spent on fix workflows by as much as 80% through ownership assignment and ticketing integrations

Industry Higher Education

Location Bethlehem, PA

Number of students 8,000

Armis Centrix™ for VIPR Pro – Prioritization and Remediation

Background

Lehigh University (LU) is a private research university in Bethlehem, Pennsylvania. The university was established in 1865, and serves around 8,000 students.

The Challenge

The security team recognized that its vulnerability and exposure assessment process was not effective in prioritizing risk, which negatively impacted interaction with the teams responsible for implementing the fixes. The team identified several related issues that stood in the way of taking a more proactive approach to the university's technology risk posture: primarily manual assessment of vulnerability contributed to protracted mean time to remediation from notification the team couldn't consistently correlate security findings with the asset it was detected to perform risk assessments - in particular, critical findings on Internet accessible systems.Because of inconsistent prioritization outcomes, it was challenging to maintain a collaborative approach to interacting with the teams responsible for implementing the fixes - extending the risk exposure window.

In the absence of correlation and contextualization of asset profiles and vulnerability findings, the team would sometimes request a fix to a system that was not Internet exposed - undermining the willingness to collaborate on implementing fixes.

In addition, the team was looking to reduce spend on multiple detection tools without compromising findings coverage.

"Armis Centrix™ allows us to analyze vulnerabilities, raise service tickets to the appropriate individuals and teams, and gain a complete picture of vulnerabilities across our environment. Armis Centrix™ helps to reduce the operational load on our security team, while at the same time improving the efficiency of the vulnerability management process - from prioritization to remediation."

Eric Zematis
CISO, Lehigh University

80% Reduced time spent on assessments

75% Reduced workload for system administrators

40% In cost savings from tool consolidation

The Solution

The Lehigh security team integrated Armis Centrix™ for VIPR Pro – Prioritization and Remediation with its existing scanning tools and ticketing system. Once the findings ingestion and normalization pipeline was up running and performing de-duplication of scanner findings, the security team applied labels to enrich asset profiles, defined prioritization rules based on business and environmental context, and incorporated threat intelligence input on the likelihood of exploit.

The combination of the platform's findings aggregation, consolidated and enrichment via asset descriptions and weightings, allowed the team to implement scoping of actionable findings, based on asset risk profile and vulnerability finding criticality.

The outcome drove a material reduction in the number of alerts, and allowed the team to focus their assessment activities on findings identified as high risk based on Lehigh's specific context and exploitability scoring.

With a clear understanding of which findings were a priority for remediation, the security team utilized the Armis solution's fix assignment and integration with Jira to automate raising tickets to the appropriate person or team responsible for the implementation of the fix.

The team also took advantage of remediation campaigns, the product's feature for bulk ticketing for findings with a common fix and path to resolution to further facilitate automated collaboration and drive operational efficiencies.

In addition to operational efficiencies, the team also gained consolidated visibility for tracking and monitoring - helping to better manage the risks identified by the security team. With bidirectional integration into the ticketing systems used by fixers, the security team could track the progress of individual tasks, and can now centrally monitor all remediation activity.

In terms of tool consolidation, the Armis solution's asset-centric approach allowed the team to compare findings across overlapping tools for the same set of assets and determine the overlap and delta. Based on the coverage by CrowdStrike Falcon, the team could retire the overlapping scanning tool with confidence.

The Results

By transforming the process of finding and fixing risk, the Lehigh team saw:

- Improved operational efficiency for proactively managing security stance
- Enhanced ability to identify the priorities specific to their environment and risk scoring and weighting
- Minimized manual efforts to facilitate and monitor remediation activity
- Reduced costs through retirement of overlapping tools, and higher utilization of licensed CrowdStrike modules

ARMIS

1.888.452.4011
www.armis.com

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.