ARMIS uplight

CASE STUDY

Uplight increases productivity with Armis Centrix™

The Challenge

- Building more security into Uplight platforms and applications
- Keeping Uplight customer data secure

The Solution

- Holistic, application-tier insight into security findings, asset linkings, and asset owner
- Streamlined risk assessment with findings consolidation, asset context, and severity scoring
- Shift to programmatic and formalized security strategy across the business

The Results

- 90% less time spent identifying owners and assigning tickets with custom ticking rules
- Halved the time for resolution of critical findings, with ongoing improvements in reduction of response times anticipated
- Increased the number of closed findings by 7x over three months, reducing overall threat debt

Industry Energy Software

Location Boulder, CO

Number of employees 400

Armis Centrix™ for VIPR Pro – Prioritization and Remediation

Background

Founded in 2019, Uplight delivers a technology platform to more than 80 utilities, serving 110 million customers. The platform encompasses a data unification platform, an integration layer, as well as a set of APIs to easily deploy a number of Uplight applications for customer usage analytics, utilization reporting and customer self service.

The Challenge

While the company had a set of existing security practices, when Uplight's current VP of Information Security joined the company in mid-2022, he set out to implement a more programmatic and formalized strategy for securing the Uplight platform, applications and development processes.

The team identified a set of challenges across tools, processes, and cross-functional dynamics that stood in the way of both a consolidated strategy and consistent visibility into the state of risk management.

While the issues were discrete to technology and process domains, they were interconnected. Findings assessment was inefficient because the security team couldn't translate output from fragmented tools into a set of prioritized tasks based on business context.

Likewise, without adequate application and asset context input in the course of the assessment phase, security teams were also required to perform additional research in order to identify the relevant risk owner - especially when looking to understand ownership across applications.

These inefficiencies and manual steps in both the assessment and assignment phases also complicated the transition to consistent and reliable reporting on overall risk status, trends in vulnerabilities, as well as historical and relative performance in remediation activity.

1/2

Time to resolution of critical findings

7x

Increased number of closed findings over 3 months, reducing overall threat debt

90%

Cut time spent on identifying owners & assigning tickets with custom ticketing rules

The Solution

As an integral component of an overall plan, the security team defined a program to identify security risk, enable collaborative remediation and monitor the performance of how development, engineering and product management teams deal with vulnerability remediation tasks based on categorization.

With the Armis Centrix™ for VIPR Pro – Prioritization and Remediation platform deployed using integrations into existing cloud security, application security, code and host vulnerability detection tools, as well as infrastructure, identity stores, and code repositories, the security team was in a better position to generate a comprehensive overview of how detection findings related to the Uplight technology landscape.

By 'reverse engineering' the relationship between application components through the platform's asset linking capability, the security team was able to visualize how assets (and sets of assets) are architecturally related as components of a specific application.

Based on this view, the Uplight security team could systematically generate a consolidated point of reference of which distributed teams are responsible for deploying and maintaining the assets, and how findings related to both platform integrity and product security risks.

In addition, the team could better understand the directionality of findings and employ root cause analysis to clearly pinpoint high-impact fixes earlier in the SDLC that resolved multiple upstream findings.

Using automated ticketing integration and remediation task tracking, the security team could take the next step in operationalization.

Crucially, this centralized view also underpinned the development of reporting metrics for operational performance across teams for executive stakeholders, as well as engineering managers, product managers and the GRC function.

With a single source of data to rely on, the security team could clearly communicate how the company was tracking to security objectives, as well as overall and relative risk status by function or application.

The Results

The Uplight security team realized tremendous benefits such as:

- Freed up the security team by radically reducing time spent on assessing security findings and assigning remediation fixes
- Improved focus on highest risk findings by incorporating asset profiles, application context and threat intelligence (including CISA KEV)
- Reversed alert backlog through consolidation, automated ticketing and improved remediation response
- Enhanced collaboration with engineering and product teams on vulnerability risk and consolidated visibility into remediation activity across functions
- Alignment across stakeholders on acceptable risk tolerance, consistent reporting and performance metrics

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.