Connected Device Security and Vulnerability Management for Universities

INVENTORY AND VISIBILITY   **VULNERABILITY MITIGATION**   **THREAT DETECTION AND INCIDENT RESPONSE**   **RISK MODELING**

Asimily is a cybersecurity platform for IoT devices that provides vulnerability mitigation, visibility, threat detection/ incident response and risk modeling. By going one layer deeper into understanding data on devices, their vulnerabilities, and customer environments, real risks can be prioritized for efficient mitigation. Vulnerabilities with the highest likelihood of being exploited, on the highest impact devices, get priority overall. This greater efficiency and powerful risk simulation for devices gives teams time to advance their device strategy with stronger security and operational health. Combined with threat detection, comprehensive inventory, and risk modeling and Asimily is a single platform for all device security needs.

Vulnerability Mitigation

Identify vulnerabilities and prioritize remediation with Asimily's patented technology to enable continuous security posture management and compliance.

- Unique Likelihood and Impact analyses let teams focus on the biggest risk, not just a long list (of vulnerabilities)
- Prioritize vulnerabilities to the top 2% of the riskiest devices
- 10x time reduction when using targeted remediation
- Asimily analyzes each vulnerability to disrupt its attack methodology, yielding quicker, simpler fixes (from over 180 and counting techniques)


Likelihood

Impact		Low	Medium	High
	High	35	77	**43**
	Medium	2,743	986	205
	Low	51	9	0

Devices

Device Risk Score Example: the riskiest 1% of Devices, equivalent to 43 of the organization's devices fall in the high likelihood + high impact category. These devices are classified as "high-risk".

Complete Inventory and Visibility

The riskiest asset is the one you didn't know you had. If you're not aware it exists— or even which devices and programs connect to which networks—you're also not tracking patch management or monitoring its status. It's very common for connected devices to get lost or misplaced.

- Automatically gather a complete inventory using analysis of network traffic correlated with other data sources

- Automated *true* risk-scored inventory of connected IoT devices

- Accurate device profiling to capture key information like operating systems (OS), IP addresses, MAC addresses, port numbers, applications, hostnames, and version numbers

- Network Communication Mapping

- Get insights into usage, utilization, availability and reliability
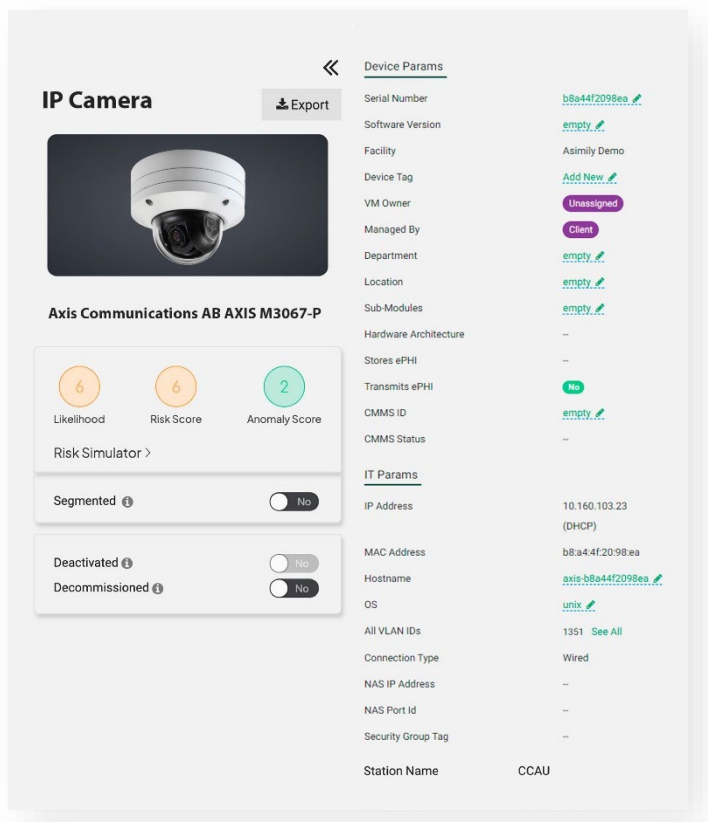
Risk Modeling

Analyze security risks before procurement. Asimily collects data from multiple systems and combines the information into a usable security risk assessment for connected IoT devices.

- Best practices hardening recommendations based on all known installs of specific devices

- Determine the benefit of security work before committing to it, raising team efficiency

Threat Detection & Incident Response

Regularly monitor and detect any suspicious activity that could indicate the beginning of an attack. This evaluation is crucial to fight back sooner, as it will categorize attacks based on your existing policies.

- Detect anomalies and mitigate them

- Continuously checks for policy violations based on any behavior

- Block novel attacks with a powerful, flexible non-templated rule creator to stay ahead of attackers' new tactics, techniques, and procedures (TTP)

- Accelerate Forensic Analysis & Investigations with centralized packet capture

Connect With Us

info@asimily.com
440 N Wolfe Road
Sunnyvale, CA 94085
(833) 274-6459
(833) ASI-MILY