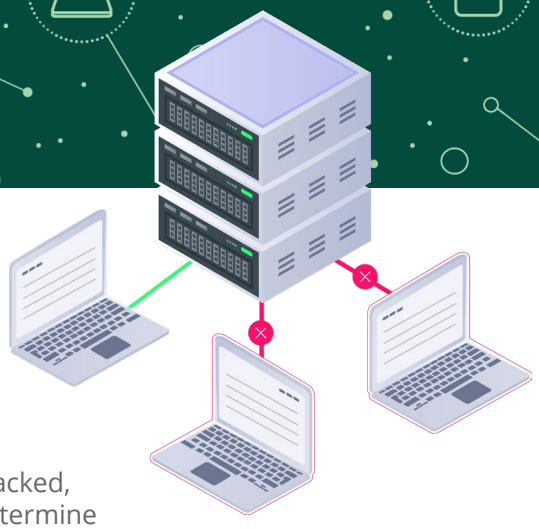
asimily



Asimily Policy Manager and Threat Detection

Protecting users means your team can both put up strong defenses to keep attackers out and find anomalous behavior internally. When OT/ IoT are attacked, their inherent limitations as purpose-built devices can make it difficult to determine how serious an issue is. Both for security and legal purposes, this is a necessity across all industries. To make this constant vigilance less burdensome, the right platform can help teams deliver compliant, skilled security work in the face of threats and incidents.

Ineffective OT/ IoT Policies Risk Missing Active Intrusions - Here's Why

The diversity of OT/ IoT devices makes it difficult to determine if their behavior is part of an active breach; each can have wildly varying acceptable behavior on a network. Further, devices have limited capacity for self defense. For example, most don't allow agent installation. Finally, the quantity of OT/ IoT alone can present a challenge.

01

Quantity and Diversity of Device Traffic Can Mask Attackers

OT and IoT represent diverse device types and therefore traffic types and patterns. For example, the use of ports 104 for DICOM (medical imaging devices) and 554 for IP cameras are completely ordinary. But reversed, they would be anomalous.

Without policies that consider domain-specific knowledge and device-by-device patterns, signs of compromise can be lost in the volume of data.

02

Policy Rules are too Hard to Calibrate Correctly

Not every organization can rely on policies from third party software that work perfectly for them. For example, a business that operates with companies in the Asia Pacific (AP) region may have different levels of tolerance for communication inside and outside of AP.

Two policy types are needed. One set that finds clear threats for any organization. And another that fits the organization's specific needs.

03

Attackers' methods change rapidly, requiring regular attention

Every rule for an OT/ IoT device must be precise to be effective and avoid blocking legitimate traffic. That requires attention and flexibility for policy-setting.

Policy engines that rely on specialized technologies like YAML may be less effective. This high burden on training and expertise to use policies for threat detection can hamper readiness against attackers' next novel technique.

Comprehensive Policy Protection for all Organizations

Unmonitored devices are threats. Rules for acceptable IoT and OT behavior should be flexible, powerful and suited for each organization's needs. Asimily's platform delivers all of the above.

IoT risk score trend

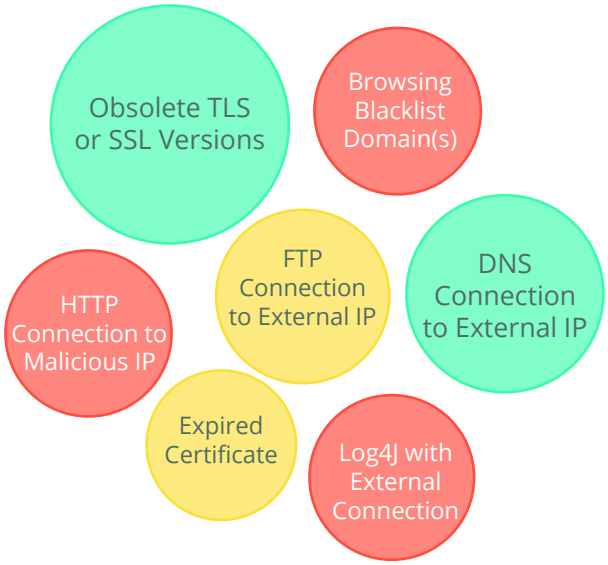
Stop Unwanted Configuration Changes and Behavior

Every connected device has limits on its acceptable behavior. For example, participating in DDoS is always bad and performing a necessary function is always good. Judging behavior between those extremes requires effort. Attackers' TTPs change often and acceptable OT/ IoT behavior yesterday might be an indicator of compromise today. Every organization has its unique needs and risk tolerance that also affect the rules for OT/ IoT behavior.

Asimily's Approach to Policies for Threat Detection

Asimily balances power and flexibility for time-strapped security organizations. It includes expert-created rules delivered by Asimily for rapid response to new threats and custom rule creation for your organizations. Avoiding complex programming languages, Asimily's policy wizard allows for rules to be created simply, without requiring dedicated team members or special expertise. When (or before) a new attack on OT / IoT hits the headlines, Asimily's security analysis team offers new rules to its customer base. Customers can always create their organization-specific rules.

Anomalies by Quantity and Risk Level



With Asimily, Policy Management becomes simple, powerful and flexible for your unique needs

- Setting policies via simple templates avoids the need to learn complex technologies like YAML, so they are easier to create, maintain, update and understand
- Three major policy types combine to give power and flexibility - Anomaly, Suppression, and Action
  - Anomaly policies detect and trigger alerts for specific behaviors
  - Suppression policies prevent alert fatigue and storms by halting notifications that would otherwise be triggered
  - Action policies aid with editing device fields, including device labeling, for a more accurate inventory and more accurate management
- Policy reports demonstrate a strong security readiness and are useful for audits, cyber insurers and regulators
- Policies can be based on more than 30 precise fields, including powerful ones like network neighbor configurations, external destination reputation and more
- Custom tags unique to your organization can be used for Policy Creation
- Policies can trigger alerts, perform certain actions, or both

Asimily Can Help

Securing the Internet of Things is more complex than securing traditional IT equipment. Uneven security practices at OT/ IoT device manufacturers paired with minimal visibility by IT and security teams make connected equipment a major security risk. The distributed and broadly installed nature of these devices means that a risk-based approach is required. This can be done, and Asimily helps companies implement and manage a risk-focused, comprehensive, and efficient method of protecting OT/ IoT devices for a more secure future.

Asimily's OT/ IoT Risk Management Platform

- Creates a complete IoT inventory, collecting 100+ attributes for each device;
- Identifies and prioritizes the riskiest vulnerabilities;
- Recommends simple, validated mitigation actions;
- Conducts a full flow analysis for each device, recording all communication patterns across the network;
- Calculates risk for every connected device based on device attributes, dataflows, vulnerabilities, anomalies, configuration, and overall criticality of the device on operations;
- Generates ACLs for targeted segmentation for use by a NAC;
- Flags anomalous device behavior based on profiling data from millions of IoT devices;
- Makes it easy to set policies to monitor accepted risks and identify suspicious activity proactively;
- Automates packet capture for forensic analysis of any IoT device to support root cause analysis;
- Documents when the device is being used so users can understand utilization and operational efficiency;
- Allows device configuration snapshots to be taken, to thwart ransomware and simply recovery;
- Risk simulator helps determine the benefit of work before it is performed, increasing team efficiency.
- Centralized information makes IT/OT convergence easier, while finding "unmanaged" devices.

Asimily can help enterprise organizations drastically reduce cyber risk while minimizing resource and time costs.

To see how Asimily can help your organization, **arrange a demo today.**

About Asimily

Asimily is an industry-leading risk management platform that secures IoT devices for medical, diagnostic, life sciences, pharmaceutical, and enterprise companies.

Connect With Us

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