asimily

Organizational Risk Score for IoT

IoT, IoMT, and OT are different from typical IT. They have unique attack surfaces, defenses, and weaknesses. It's the natural result of being built for a narrow purpose, not multiple purposes like IT workstations and servers.

That's why their risk must be measured in ways appropriate for devices. Simple organizational risk scores for IT go up when an open vulnerability is found and declines when one is remediated. A more nuanced approach for devices - which can't always be patched - gives a more accurate view to help truly reduce risk with intention and accuracy.

Why traditional Organizational Risk Scores fail for IoT / IoMT

Organizational Risk Scores (ORS) are difficult for organizations with significant IoT / IoMT / OT investments. Here's why:

01

Organizations need a way to see if a Vulnerability is Risky for *Them*

Not every vulnerability present is a risk for an organization. Compensating controls or other breaks in the attack chain can make the same vulnerability risky for some organizations and not risky for others.

Without better insight into actual, present risk, organizations struggle to reduce real risk effectively. They typically waste effort, or delay risk reduction, sometimes for years.

02

They need a highly accurate, up-to-date inventory

Most organizations want a better handle on what's on their networks. The ease at which Smart TVs, cameras and even industrial equipment can be added to a network leads to unexpected devices regularly appearing.

Not every organization is ready to maintain a good inventory. Some are hard-pressed to keep a detailed, accurate record of their devices.

03

Without a relevant benchmark, organizations can't judge progress

Every industry and sector is different, with wildly differing business models and profitability. That leads to acceptably different ranges for spending on cybersecurity, including devices.

An organizational risk score without comparisons is hard to interpret. At the least a time series helps, but even more helpful is a comparison to similar organizations.

Get a Risk Score That Works for IoT

A reliable, well-understood Organizational Risk Score for devices can help motivate teams, unlock resources, and show progress and efficacy of your efforts.

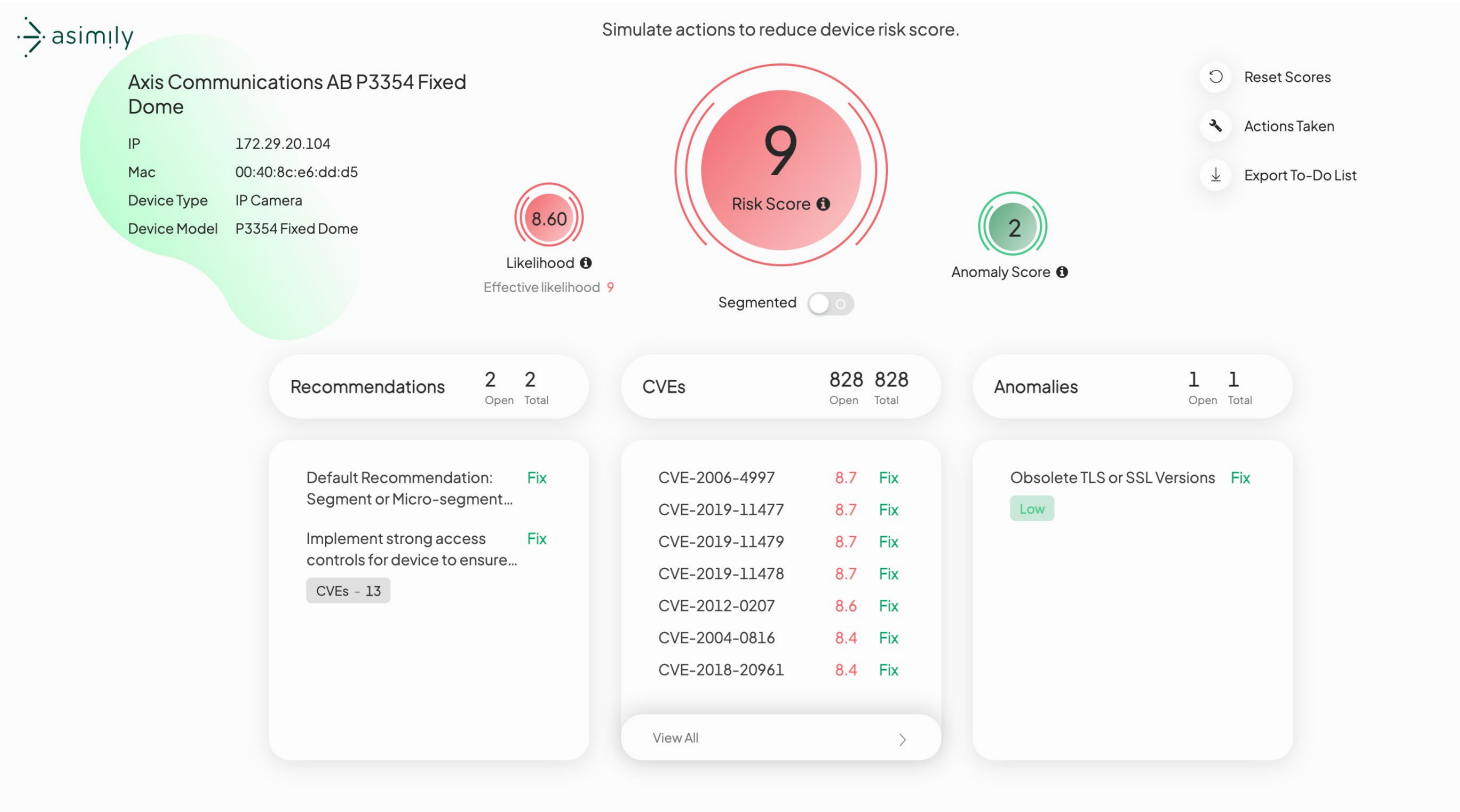
IoT risk score trend

Copyright © 2024, Asimily, Inc. All rights reserved

Why traditional Organizational Risk Scores fail for IoT / IoMT

Organizational Risk Scores aren't just for board slides. They have numerous uses that can help enhance defensive readiness and security operational efficiency.

For example, if any newly discovered risk simultaneously becomes a trend for you and your industry peers, it could be a zero-day attack. Knowing that quickly can completely change your organization's response to vulnerabilities or anomalies. You'll have confirmation of a known, exploitable and new vulnerability to take appropriate measures quickly.



With Asimily, inventory and visibility of IoT devices becomes the starting point for real risk reduction.

- Organizational Risk Score is usually correlated with known, normal activity, such as installation of new IoT/ OT/ IoMT devices or their retirement. When ORS does not change as expected, further investigation is usually needed.
- It is difficult to show benefits to non-security teams (such as boards or auditors) between breaches or attacks. Showing all the hard work that happens to prevent a next incident is important for security teams to demonstrate their value to organizations and stakeholders.
- A reliable, well-understood Organizational Risk Score for devices can help motivate teams, unlock resources, compare your security posture to others worldwide, and show progress and efficacy of your efforts.
- The history of an ORS is an excellent teaching tool for new security team members, and preserves institutional memory around changes in past risk - good and bad.

Copyright © 2024, Asimily, Inc. All rights reserved

Asimily Can Help

Securing the Internet of Things is more complex than securing traditional IT equipment. Uneven security practices at 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 IoT devices for a more secure future.

Asimily's 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

Copyright © 2024, Asimily, Inc. All rights reserved