Prioritize and Remediate Medical Device Cyber Threats Using Asimily and Nuvolo

THE **CHALLENGE**

The hyper-proliferation of connected medical device in modern healthcare systems has created fertile grounds for cyberattackers. The legacy and static nature of many of those devices leaves them susceptible to malware, ransomware and exfiltration of sensitive patient data. These types of attacks leave the healthcare system vulnerable to adverse patient health outcomes, legal and financial liability and erosion of customer and market confidence in the brand.

At the core of the problem is a lack of a single trusted, existing medical device inventory. The next biggest challenge is the absence of a single, standardized process for secure and compliant ingress or onboarding of new medical devices into the fleet. These challenges are compounded by legacy network monitoring and vulnerability detection tools being incapable of understanding the nature of the medical devices seen on the network. Security operations team are blinded by a plethora of the white noise generated by false positives. Even worse, they don't detect medical devices at all until they have been compromised.

Today, when attacks and vulnerabilities are detected, they trigger a manual process where the security operations and HTM teams need to go through a cumbersome, manual process to identify which devices are at risk. In the case of a broad-reaching vulnerability, healthcare organizations are unable to effectively prioritize what they should tackle first and how to coordinate activity between security operations and HTM. There is also no way to correlate an identified attack to other at-risk devices on the network or in inventory.

The end result is a danger as the organization is highly susceptible to cyberattack resulting from a haphazard understanding of their connected device environment. The risk is extended with no effective way to monitor the known medical device signatures for anomalous behavior. From a process perspective, the organization compounds the problem by having no effective way for HTM and security operations to systemically collaborate for threat remediation.

SOLUTION **Features**

- Automated inventory identification of deployed medical devices

- Enrichment of device information with clinical and business context

- Clear onboarding processes for new devices to ensure ongoing inventory hygiene

- Modern machine learning and AI to understand device relationships and chatter patterns

- Dynamic, contextual risk scoring to prioritize cyber risks and focus action for desired impact

- Integration with public threat and vulnerability databases

- Real-time monitoring to detect attacks without impacting clinical operations Enrichmentof security incidents with contextual business and clinical data

- End-to-end security incident creation and orchestrated remediation workflow

- Correlation of attacks and vulnerabilities across device fleet to minimize threat surface

- System of action to coordinate activities across security operations and HTM

- Help with segmenting devices and blocking anomalies on the network

- Simple, mobileHTM interface to streamline threat response (even when offline)

- Instant visibility into the organization's compliance posture

- Detailed audit trail of all security incidents from detection to remediation

THE **SOLUTION**

Asimily and Nuvolo have created a strategic partnership and an OOTB integration between their industry leading technologies - Asimily Insight and Nuvolo Medical Device Cyber Security Platform. The integrated solutions addresses all of these challenges in a cohesive and systemic way.

The integrated platform delivers end-to-end medical device monitoring and lifecycle management, enabling healthcare systems to protect the organization, patients and their brand against cyberattacks. Some of the key capabilities include:

The integrated Asimily-Nuvolo platform identifies and inventories existing devices and enriches the discovered data with rich clinical and business context to paint a complete picture of the infrastructure. The platform augments this capability with a clean and secure onboarding process for new devices, which is front-ended by a powerful and user-friendly mobile app that makes it efficient for HTM staff.

As security events are detected, the integrated platform serves as system of action by initiating real-time corrective workflows and driving collaboration across HTM and security operations to isolate and remediate threats or vulnerabilities. The platform also performs advanced correlation to identify other at-risk devices in the inventory. This functionality is critical as it allows the organization to proactively initiate orchestrated workflow for prioritized remediation across the entire environment.

Every step in the process is tracked, audited and reportable to drive organizational learning, reduce time-to-remediation and demonstrate ongoing compliance with internal and regulatory requirements.

ABOUT **ASIMILIY**

Asimily is a team with backgrounds in healthcare, security, machine learning and analytics. We have built and launched solutions for connected devices at startups to Fortune 500 companies. We provide a solution to comprehensively monitor and manage devices through their entire life-cycle in the healthcare environment. This will allow different players in the ecosystem to focus on their core job of providing great healthcare. Privately held, Asimily is headquartered in Sunnyvale, CA.

For more information, visit:www.asimily.com

ABOUT **NUVOLO**

Nuvolo is revolutionizing medical device cyber security by innovating on ServiceNow, the world's leading enterprise cloud platform. The company's vision is to be the global leader in cyber security for enterprise operating technology, powered by a culture of innovation and a relentless commitment to customer service. Privately held and founded in 2013, Nuvolo is headquartered in Paramus, NJ with offices throughout the U.S. and internationally in London and Pune, India.

For more information, visit: www.nuvolo.com