Cylera and Cisco Increase Healthcare IoT and Medical Device Security

Automated, Integrated, Device Data Sharing

NEW YORK, UNITED STATES, December 15, 2022 /EINPresswire.com/ -- Cylera, a pioneer in healthcare IoT and medical device cybersecurity and intelligence, announces its deep integration with Cisco's Network Access Control (NAC) product, the Cisco Identity Services Engine (ISE).

Industry NAC solutions ensure that only authorized users and devices are granted access to network resources. However, especially in healthcare and clinical settings, NAC solutions alone are not able to identify the wide range of IoT and medical device (IoMT) types, device manufacturers, unique and specialized protocols, software, firmware, etc., nor able to establish the appropriate security policies for user and device access control for these devices. This leaves a gap in cybersecurity and policy which can be devastating to patient care and healthcare services. The Cylera and Cisco integration addresses this issue.

> "Through our deployment experience, we know that many healthcare organizations are more or less operating blind when it comes to IoT and IoMT devices on their networks."
> *Ryan Gonzales, Cylera VP of Solutions and Services*

Cylera MedCommand™ shares its pioneering and patented device discovery, asset profiles, vulnerabilities, risk details, and threat intelligence for all IoT and IoMT devices in the network – something that IT tools can't typically provide.

"Through our deployment experience, we know that many healthcare organizations are more or less operating blind when it comes to IoT and IoMT devices on their networks," said Ryan Gonzales, Cylera's VP of Solutions & Security Services. "The IT teams do not have next-generation tools in their hands to help them know IoT and medical device protocols, workflows, and what's at risk if something should go awry. Also, Cylera has built and maintains its Cisco integrations in the standard MedCommand platform at no cost to our customers, and no consulting hours are required. Setup takes just a few seconds to configure and begin flowing device profiles and

policies from Cylera to Cisco's ISE."

Through Cylera's integration with Cisco, joint customers can now:
- Experience a whole new level of insight on their connected IoT and IoMT devices, performed agentlessly and passively, with zero device impact during vulnerability and risk analysis, and absolutely no disruption to patient care, privacy, or safety.

- Share data on new IoT and IoMT devices found by Cylera, to keep the ISE dashboard informed of assets with needed, granular details and updates over time on the devices in the network.

- Know the location of medical devices and IoT in the enterprise, what specifically the devices are, all the needed hardware, software, and firmware level information, and many other asset attributes.

- Save IT security teams endless hours in manual creation and maintenance of inventory/register of connected IoT and medical devices which can be shared automatically with Cisco ISE.

- Based on accurate knowledge of IoT and IoMT devices and their communication patterns and clinical context, Cisco TrustSec or dACL/SGACL policies can be created automatically and shared to Cisco ISE. This helps ISE administrators save time and eliminate human error. (A dACL is a "downloadable Access Control List" and a SGACL is a "Security Group Access Control List.")

- Solve micro-segmentation limitations by automatically creating and adjusting the Security Group Tags (SGTs) for IoT and IoMT devices that attach to the network. This means that enforcement of segmentation rules can be enacted by Cisco TrustSec technology which is embedded into the network fabric on all modern Cisco switches.

- Leverage and extend the value of customer's existing IT infrastructure investments - saving cost, time, and resources.

"In the past few years, both during Covid and now post-Covid, we've seen attacks and intrusions targeted at healthcare networks like never before," said Timur Ozekcin, Cylera's CEO and co-founder. "Both IT security and clinical engineering groups need know their connected IoT and IoMT devices, and that they have protection in place to assure the right access is being granted for the right users to the right resources. It's become a business essential."

Cylera is an IoT security partner with Cisco as well as a Cisco Technical Alliance Partner Ecosystem member. With its integration to Cisco Prime's wired and wireless IT management, Cylera can combine location information with Cylera's knowledge of the device details, to help modernize how quickly staff can find the assets they need for patient care, or when an issue comes up with devices. Integration with Cisco's DNA Center assures that asset device software updates, patching, license status and other underlying data are synchronized across Health Information Technology (HIT) and Health Technology Management (HTM) systems.

The Cylera MedCommand platform delivers a full suite of capabilities: IoT, IoMT, IT and even some Operational Technology (OT) asset identification and management, network analysis, vulnerability and risk assessment, network segmentation, threat detection and intelligence, and fleet utilization and optimization. All of these capabilities are undergirded by Cylera's next-generation, patented technology, and commitment to make healthcare delivery a safer, simpler, more secure environment. See www.cylera.com for more information, and download the Cylera – Cisco ISE Integration Brief.

About Cylera

Cylera is pioneering agentless healthcare IoT and medical device (IoMT) cybersecurity and intelligence, with a mission to safeguard what matters most: patient care, safety, privacy, and business continuity. Cylera is a privately held company, headquartered in New York City with offices in Cheltenham, U.K. and Madrid, Spain. www.cylera.com

Verity Blake/David Ferguson/Emily Goold
HeadOn PR
01242 335 246/07920792183
email us here
Visit us on social media:
Twitter
LinkedIn