VISIBILITY & INSIGHTS AND ANOMALY & THREAT DETECTION

Accurate Device Detail for the Extended Internet of Things

The explosive growth of the Extended Internet of Things (XIoT) has created unprecedented challenges for healthcare delivery organizations (HDOs). Understanding the full scope of these constantly moving devices is incredibly difficult for most healthcare delivery organizations (HDOs). The problem is that HDOs don't have all the information they need about the devices in their environment. Manual data collection processes and general-purpose discovery tools are not enough to provide the HDO with the level of detail needed to properly manage their XIoT devices.

KEY BENEFITS:

- Passive network data collection provides dynamic device information
- Highly accurate device classification
- Eliminate time-consuming manual data collection

MEDIGATE'S VISIBILITY & INSIGHTS AND ANOMALY & THREAT DETECTION

Medigate Visibility & Insights and Anomaly & Threat Detection (VIA) discovers and profiles every connected device. By parsing the unique XIoT device language, VIA provides accurate device identification and analyzes risks to keep HDOs safe and operational. All XIoT devices are profiled with over 100 data points, including serial number, operating system, and software version. This accurate data is made available to a whole host of network, security, and management tools to improve the overall function of the healthcare operation.

HOW IT WORKS

VIA connects passively to the network core and examines all network traffic to identify connected XIoT devices. Using unique deep packet inspection (DPI) techniques and over 170+ unique device language parsers, the platform can accurately identify every device on the network. This informaiton is delivered to a unique Software as a Service (SaaS) interface, with detailed reeporting and analysis available.

WITH VISIBILITY, INSIGHTS, AND ANOMALY DETECTION, HDOS GET:

- **Detailed device profiles:** Accurate detail from over 100 unique device attributes such as device IDs, version information, physical location, serially attached devices, vulnerability assessments, network connectivity, and more.
- **Network communications maps:** Inform decision making with an XIoT device connection matrix, communication world map, protocol visibility, and VLAN visibility.
- **Accurate alerts:** Highlight key information about risky device activity, such as unencrypted PHI, or plain-text credetials, HDOs can prioritize immediate action.
- **Vulnerability assessments:** Passively assess and correlate XIoT devices to correlate known vulnerabilities and prioritize their patch management workflows.

CONCLUSION

Many HDOs struggle to achieve accurate visibility for XIoT devices, which can threaten their operations. Medigate has learned the unique languages of clinical devices and does not guess what they're saying through AI or Machine Learning. This approach delivers advanced insights from device data, such as XIoT device anomaly detection, vulnerability correlation, and alert notification. With Medigate, unlocking the data available in all connected devices empowers HDOs to connect with confidence.

ABOUT CLAROTY

Claroty empowers industrial, healthcare, and commercial organizations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.