CLAROTY MEDIGATE by Claroty

HEALTHCARE

CASE STUDY

ORTENAU KLINIKUM ADDRESSES NETWORK DETECTION BLIND SPOTS WITH SIGNATURE-BASED DETECTION AND ALERTING

Introduction

Digital transformation in healthcare environments has caused the number of connected devices to grow rapidly in recent years. As health systems expand care delivery models across new facilities such as remote care, mobile medical devices, telemedicine, and home healthcare, new connectivity introduces new cyber risks to unmanaged devices. Unmanaged devices consist of connected devices that tend to live outside of traditional IT, such as medical devices, IoT (Internet-of-Things) devices, and OT (operational technology).

In 2021, Ortenau Klinikum recognized a gap in its ability to gain visibility across its network. They lacked a central way to identify all connected devices, understand network traffic, and how they were communicating with each other. Network visibility and enhanced management of medical devices were particularly lacking in their operations. Addressing these gaps led them to adopt the Medigate Platform from Claroty.

Since the adoption of The Medigate Platform in 2021, the security team has played a central role in its utilization, contributing significantly to the enhancement of security measures at Ortenau Klinikum. Once the Medigate Platform was implemented across their security infrastructure, Ortenau Klinikum noticed immediate value-add. One of the primary users of the Medigate Platform at

ORTENAU KLINIKUM

About the Company

Ortenau Klinikum is a large, regional-based health system with about 6000 employees spanned across seven locations in the Ortenau region of Germany. They offer a comprehensive range of medical and nursing services to patients, with a focus on high-quality care. Ortenau Klinikum's information security is overseen by its information security officers within the IT department. The security team adeptly handles diverse security workflows, encompassing IT systems, medical devices, and other assets typically considered unmanaged.

Ortenau Klinikum stated: “We now know what is in our network at any given minute. Especially with our medical devices, it has turned what was once a blurry picture into a high-quality one.”

The Medigate Platform’s visibility became immediately actionable through its reporting dashboards. Leveraging Medigate’s robust and customizable dashboards, the IT team can access a real-time view of assets on the network, risks & vulnerabilities, and efficiently assess network hygiene at scale. Additionally, Ortenau Klinikum implemented a dashboard for their Clinical Engineering team, enabling them to track the visibility and utilization of their medical devices.

Despite the immediate impact of the asset visibility provided by The Medigate Platform, Ortenau Klinikum faced a challenge in quickly identifying known threats that may already exist within their network and potential impacts on devices.

Solution

Ortenau Klinikum began using The Medigate Platform’s ATD (Advanced Anomaly & Threat Detection) capabilities to solve network detection challenges. With ATD, Ortenau Klinikum could gain instant visibility into both known and unknown threats looming across their hospital networks.

With The Medigate Platform’s signature-based detection and alerting, known threat signatures could be tracked directly in the platform in real-time. A simple user interface displays the content of each signature and any changes that happen over time. There is also the ability to enable and disable signatures as relevant in order to properly tune the system. These capabilities, combined with the clinical context that The Medigate Platform’s ATD module provides, enable the ability to better understand, detect, and respond to known threats as they enter the network with insights into the relevant assets and indicators.

And, since the Medigate Platform is built on AWS, Ortenau Klinikum has immediate access to new features and threat definitions along with leveraging AWS Services providing the inherent scalability of AWS, encrypted connections between on-premise networks and AWS, along the the ease of integration into the AWS landscape.

The team at Ortenau Klinikum also uses the MITRE ATT&CK Enterprise Framework across various security operations workflows. Having each alert appearing in the Medigate Platform mapped to the proper technique proved helpful in efficiently giving guidance on how to best approach each threat.

Conclusion

Overall, Ortenau Klinikum believes that signature-based detection and alerting have significantly enhanced the efficiency of their security operations, especially for medical devices. While the ultimate success of a cybersecurity program would ideally be no alerts, gaining visibility into known threats and impacted assets across the hospital network enables an effective strategy for risk reduction. This clinically-aware approach to network detection mitigates risks and potential impacts on patient care.

Moving ahead, Ortenau Klinikum plans to leverage the ATD module to enable their healthcare delivery organization to expand their healthcare cybersecurity journey through:

- Maintaining continuous monitoring of their clinical environment to detect early indicators of compromise for both known and emerging cyber threats
- Harnessing the ideal combination of clinically-aware behavioral and signature-based detection methods to enhance prioritization of the most critical risks in healthcare delivery
- Revealing immediate visibility into potential risks throughout the entire attack chain, optimizing response efforts across existing security tools & workflows

About Claroty

Claroty empowers industrial, healthcare, commercial, and public sector 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, network protection, 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.