HEALTHCARE

MODULE OVERVIEW

ANOMALY & THREAT DETECTION

The Healthcare Threat Detection Challenge

The modern healthcare network has dramatically reshaped patient care delivery. Health systems' infrastructure, staff, and workflows are highly dependent on a wide range of connected devices that make up the Extended Internet of Things (XIoT). With clinical workflows increasingly dependent on connected devices, HDOs are at a greater risk of disruptive and costly cyber events as a result of breaches or malicious attacks.

A unified insights and alert system provides automated methods to monitor, prioritize, and respond to affected devices through device visibility and remediation workflow capabilities. The Medigate Platform's Anomaly & Threat Detection (ATD) module has been purpose-built to help tackle the uptick in both known and emerging threats facing the connected devices that are reshaping care delivery today.

Clinically Aware Threat Identification

Advanced Custom Alerting

Agentless Continuous Monitoring

Medigate Platform ATD Module

How It Works

The Medigate Platform leverages passive deep packet inspection technology and the industry's broadest portfolio of XIoT protocol coverage to provide a highly centralized and detailed view of devices in the healthcare environment. By continuously monitoring network traffic for anomalous behavior and indicators of compromise, the Medigate Platform helps you detect, prioritize, and respond to threats before they can impact patient care.

Threat Identification

Due to the unique nature of clinical workflows and an increasingly active threat landscape, Identifying when a cyber threat is present in hospital environments can be challenging. The Medigate Platform detects both known and emerging threats across hospital environments with:

- **Known IoC Alerting:** The Medigate Platform alerts when a device is operating outside of "known good" behaviors, communicating with malicious IPs, or showing potentially malicious actions such as multiple failed login attempts.
- **Signature-Based Alerting*:** The solution incorporates proprietary research from Claroty Team82 and public sources to build a library of known network signatures to detect previously disclosed threats and attack techniques.
- **MITRE ATT&CK Enterprise Framework** Group, prioritize, and visualize threats using known tactics and techniques to aid SOC personnel with alert investigation and remediation.

Customized Alerting

Between scale, architecture, user base, and needs–no two healthcare environments are identical. The Medigate Platform enables you to customize alerts to fit a threat detection strategy based on unique organizational detection priorities and goals. Custom alerts cover multiple aspects of device parameters, including:

- **Custom Communication Alerting*:** Understand and alert on device communication patterns across the network to identify abnormal behavior and traffic across XIoT devices such as a BMS communicating with a guest network or an IoMT device using unsecured protocol.
- **Device Status Change Alerting*:** Pinpoint significant device changes within healthcare environments. When a device reappears after being offline for a significant period, has a significant change in risk profiling, or undergoes a network status change, it may be worth further investigation.

Enhanced SOC & Security Workflows

Integrate with SOC workflows such as security appliances and orchestration tools to unify alerts and security processes into a centralized workflow. Implement agentless, continuous monitoring for security teams for use cases such as enhanced compliance and device hardening validations.

- **Integrate with existing security infrastructure:** Enrich existing workflows by integration with common SIEM and EDR like Splunk, IBM Qradar, CrowdStrike, and more, to extend capabilities across the entire healthcare network while removing the learning curve associated with complex medical device security.
- **Alert auto-actions:** Manage system alerts more efficiently by creating automated alert workflows to optimize triage and remediation across multiple device owners and groups, reducing redundancy and streamlining collaboration.

Anomaly & Threat Detection

Medigate Platform Essentials	Medigate Platform Advanced Modules
Robust, customizable threat detection engine based on behavioral baselining and anomaly detection	Clinically aware threat detection for agentless monitoring of known and unknown threats, device communications and changes supporting the MITRE ATT&CK enterprise framework

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.

*Advanced Offering Only**

CLAROTY MEDIGATE by Claroty