CLAROTY

Healthcare

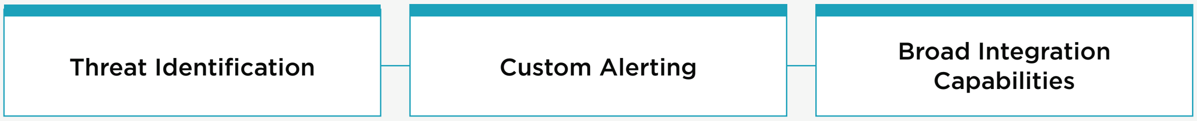
MODULE OVERVIEW

Claroty xDome 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 Cyber-Physical Systems (CPS). With clinical workflows increasingly dependent on connected devices, HDOs are at a greater risk of disruptive and costly cyber events such as 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 Claroty xDome'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.



Claroty xDome ATD Module

How It Works

Claroty xDome leverages passive DPI (deep packet inspection) technology and the industry's broadest portfolio of CPS 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 Claroty xDome 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. Claroty xDome for Healthcare detects both known and emerging threats across hospital environments with:

Known IoC Alerting: Claroty xDome 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 for 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. Claroty xDome 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 CPS devices such as a BAS communicating with a guest network or an IoMT device using an 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 Capabilities & Workflows

Integrate with SOC workflows such as security appliances and orchestration tools to unify alerts and security processes into a centralized workflow. Leverage existing infrastructure and expand its capabilities while lowering manual efforts to track down and remediate threats.

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.

Advanced Offering Only*

About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. 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. To learn more, visit claroty.com.

CLAROTY