Cynerio

Healthcare IoT Cybersecurity Platform

Secure. Faster.

Active Attack Detection – No-Cost Healthcare IoT Attack Snapshot

Solution Overview

Hospital cyberattacks and ransomware continue to exponentially rise, and IoMT and IoT devices are now equally liable as phishing to be the origin of a healthcare breach. Unfortunately, traditional IT security approaches don't provide visibility into or remediation for healthcare IoT attacks, since those devices are often unpatchable and can't be agented.

To fill this gap, Cynerio is working with hospitals and healthcare facilities to identify ongoing healthcare IoT attacks and infections that traditional legacy security solutions routinely miss. Cynerio Active Attack Detection is a one-week, no-cost evaluation of your healthcare IoT footprint to help keep your hospital secure against the attacks that increasingly target IoT devices.

Benefits

- ✓ Identify active attacks on your hospital's healthcare IoT in one week at no cost and with no strings attached
- ✓ Expedited and optimized Cynerio deployment, network traffic analysis, and reporting to provide an instant snapshot of healthcare IoT attacks and risks
- ✓ Live healthcare IoT ransomware and malware attacks detected in over 80 percent of Cynerio engagements
- ✓ Full Cynerio support from installation to final reporting
- ✓ Low total cost of ownership – get detailed healthcare IoT threat intelligence in a few hours
- ✓ Smoothly transition to ongoing healthcare IoT attack identification and mitigation

About Cynerio

Cynerio is the one-stop-shop Healthcare IoT security platform. With solutions that cater to healthcare's every IoT need – from Enterprise IoT to OT and IoMT – we promote cross- organizational alignment and provide hospitals the control, foresight, and adaptability they require to stay cyber-secure in a constantly evolving threatscape. We empower healthcare organizations to stay compliant and proactively manage every connection on their own terms with real-time IoT attack detection & response and rapid risk reduction tools, so that they can focus on a hospital's top priority: delivering quality patient care. For more information visit www.cynerio.com.

Forrester Wave Leader 2020

Gartner Cool Vendor 2020

Sample Attack Analysis Overview

External entities, some originating from Russian and Estonian IPs, are attempting to attack an Airstrip OB patient monitoring server via exposed web services at x.x.x.x. The connections are routed into the internal network via a Citrix network component (10.254.x.x) and are utilizing Log4Shell (CVE-2021-44228) and other known exploits.

Attack Mitigation and Remediation Actions

External Actions

Block External Address
This action will block access to the listed IPs/URLs from ALL network entities.
Add the following network IP/URLs to the firewall group - 'Blocked Addresses'
45.83.x.1
45.83.x.2
217.60.x.x
netsystemsresearch.com
195.54.x.x
121.140.x.x

Internal Actions

Micro-segmentation
Quarantine

Attack Assets

3 MRI

Susceptible Assets

30

Was the attack successful? y/n

YES

Threat Intelligence

Name	Details
Log4j Vulnerability	The vulnerability affects Log4j and its successor Log4j2, which are developed by the Apache Foundation and widely used as part of open-source tools by both enterprise applications and cloud services for logging purposes. Systems and servers that use Log4j between versions 2.0-beta9 and 2.14.1 may all be potentially affected by CVE-2021-44228, which includes many software programs, services and applications written in Java. The vulnerability allows for repeated and reliable unauthenticated remote code execution and can be used to exfiltrate PHI, cause service disruption, or enable a ransomware attack.
Microsoft .Net Framework 4.0 end-of-life	Microsoft .Net Framework 4.0 is at end-of-life and no longer receiving security updates despite being vulnerable to several critical risks, including unauthenticated remote code execution.
CVE-2017-9841	The CVE-2017-9841 vulnerability lets a malicious user remotely run PHP code on affected websites by exploiting a breach in PHPUnit. This can allow the user to, for example: •Access sensitive content on the target's website (files, database credentials, database content…) •Change files' content •Send spam •Install malware
Microsoft Exchange Server Remote Code Execution Vulnerability CVE-2021-26855	The Microsoft Exchange server attack chain begins with the exploration of this flaw, also known as a server-side-request-forgery (SSRF) vulnerability. When exploited, HTTPS connections are established to authenticate user access.