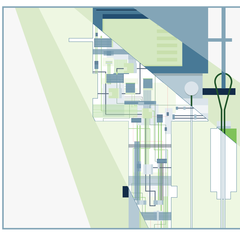
Cynerio

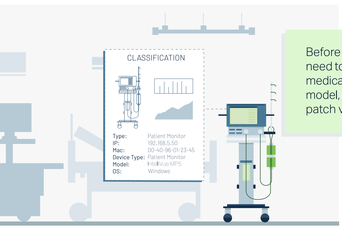
WHAT YOU CAN DO TO MITIGATE THE CYBER-RISKS OF YOUR CONNECTED MEDICAL DEVICES



The interconnection of unsecure medical devices over hospital IT networks has led to a new breed of cyber-risks that impact patient safety and privacy and disrupt patient care.

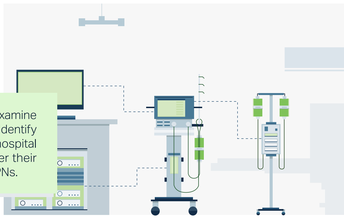
The state of medical device cyber-security is years behind modern IT systems, and as awareness increases, healthcare security teams need to build new defenses tailored specifically for medical devices and their network environment.

Here are 9 essential activities for building and optimizing a dedicated security layer that mitigates the cyber-risks of your connected medical devices.



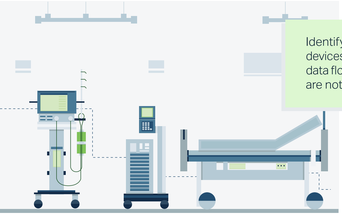
1 DISCOVERY & CLASSIFICATION

Before assessing and mitigating the risks, you need to discover and classify all the connected medical devices in terms of their type, make and model, their operating system and latest security patch version.



2 NETWORK MAPPING

After identifying the devices, the next step is to examine their communications and network configuration. Identify other systems they communicate with over the hospital network and via the Internet, and check whether their communications are isolated within VLANs or VPNs.

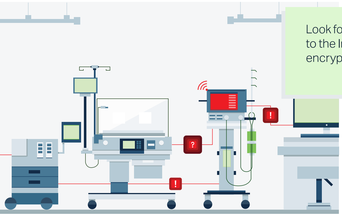


3 CLINICAL CONTEXT

Identify which devices transfer and store PHI and which devices are directly connected to patients. Determine which data flows are associated with clinical workflows and which are not.

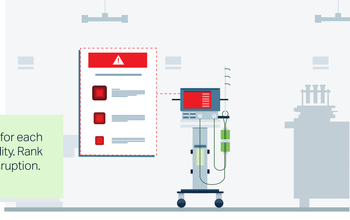
4 RISK IDENTIFICATION

Check for vulnerabilities on the devices such as hard-coded passwords, weak authentication, unpatched outdated operating systems and medical software. Identify potential threats that could exploit each vulnerability.



5 RISK PROBABILITY

Look for potential attack vectors including connection to the Internet or to less secure workstations, lack of encryption and unsecure protocols.

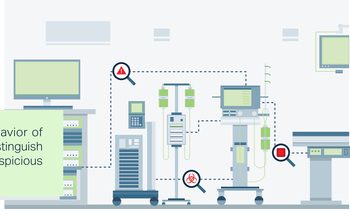


6 RISK SEVERITY

Determine the potential impact of a cyber-attack for each device based on its vulnerabilities and risk probability. Rank the risk for patient safety, privacy and service disruption.

7 PROACTIVE PREVENTION

Request the latest patches for devices with outdated operating systems and set access control policies that restrict non-essential communications.



8 DETECTION

Continuously monitor and analyze the behavior of medical device communications in order to distinguish between legitimate medical workflows and suspicious data exchanges.

9 METRICS & ANALYTICS

Log all medical device risk assessment and mitigation activities. Create scorecards for the medical device risk level and set KPIs for medical device cyber-risk mitigation.

Cynerio is a leading provider of medical device security solutions. Built on healthcare-driven behavior analysis, Cynerio's technology provides clear visibility into the clinical network environment, assesses cyber-risks on the device, network and application layers, protects against cyber-threats and detects real-time cyber-attacks, minimizing service downtime and ensuring patient safety.