Achieving Medical Device Security Without Jeopardizing Patient Health

PROBLEM:

Medical IoT devices, legacy hospital systems, and critical applications all need 100% uptime and protection from attacks in today's healthcare environment. Yet, most are vulnerable to cyber-attacks, including insulin pumps, X-ray machines, and medical applications running on VMs. Security tools and best practices used today are struggling to protect these environments, putting hospitals and their patients at risk. Typical deployments like EDRs and agents are a problem because they can't be supported and other approaches which block, or shut down, systems to remediate aren't conducive to a patient's wellbeing. In addition, these medical systems don't generate useful information for threat detection tools to do their job, which further compounds the problem.

NEW APPROACH:

ARIA SDS finds and removes threats at the network conversation level to stop attacks, while leaving infected devices online. Since ARIA is deployed within the network, and not on the device, it can provide threat visibility and attack protection all the way down to intra-VM traffic that may be at risk.

SOLUTION:

Our approach combines the best elements of a packet broker, packet recorder, data breach service, microsegmentation platform, and the industry's first intelligent threat containment system. The ARIA SDS platform provides missing internal network visibility derived from packet data sent directly to security tools and processes. It also adds the unique ability to verify and stop attacks at the conversation level. All on a software-defined delivery platform with fully open APIs to work in any environment. ARIA was purpose built to help automate the incident response process and stop the attacks that matter by making what you have today work better.

BENEFITS:

The following benefits of ARIA SDS drastically speeds up and improves the entire incident response process to detect, investigate, contain, and protect against modern cyber-attacks.

- Surgically contain threats without taking infected devices offline to remediate.
- Provide IoMT and legacy medical devices missing threat detection.
- Deliver security for exposed VM, container, and IoMT environments without agents or EDRs.
- Automatically stop data breaches and any exfiltration of PII/ePHI data to meet compliance.
- Easily add network-based microsegmentation to protect critical assets.

We are a perfect fit for the ultimate goal of securing today's medical-grade networks. All while safeguarding patient lives, improving security performance, maintaining compliance, and reducing overall cost.

Learn more about our approach to Protecting Commercial IoT and Enhanced Network Security

Contact Us Today: sales@ariacybersecurity.com or (978) 954-5038