accruent

Medical Device Security Analyzer

JOIN THE HEALTHCARE TECHNOLOGY MANAGEMENT REVOLUTION: TRACK, IDENTIFY, RESPOND AND MITIGATE MEDICAL DEVICE RISK

There are steps you need to take to protect your medical devices from a cyberattack: identify your risks, develop your plan and automate your processes. These steps are made easier with the Accruent **Medical Device Security Analyzer**.

Analyze and report against all medical devices, network data and software

Reconcile MDS2 data and other security attributes against inventory

Automate workflows unique to your organization when potential security risks or gaps are found

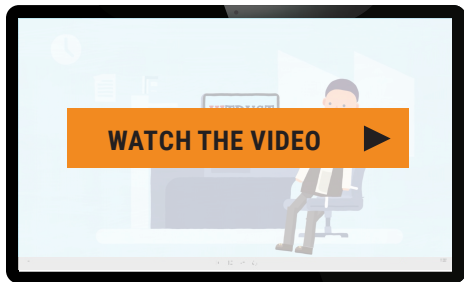Integration with hospital's network monitoring tools

TRACK, IDENTIFY, RESPOND AND MITIGATE DEVICE RISK ACROSS YOUR ENTIRE INVENTORY

The landscape of intelligent devices and equipment in health care organizations is changing rapidly because devices are increasingly intelligent and interconnected.
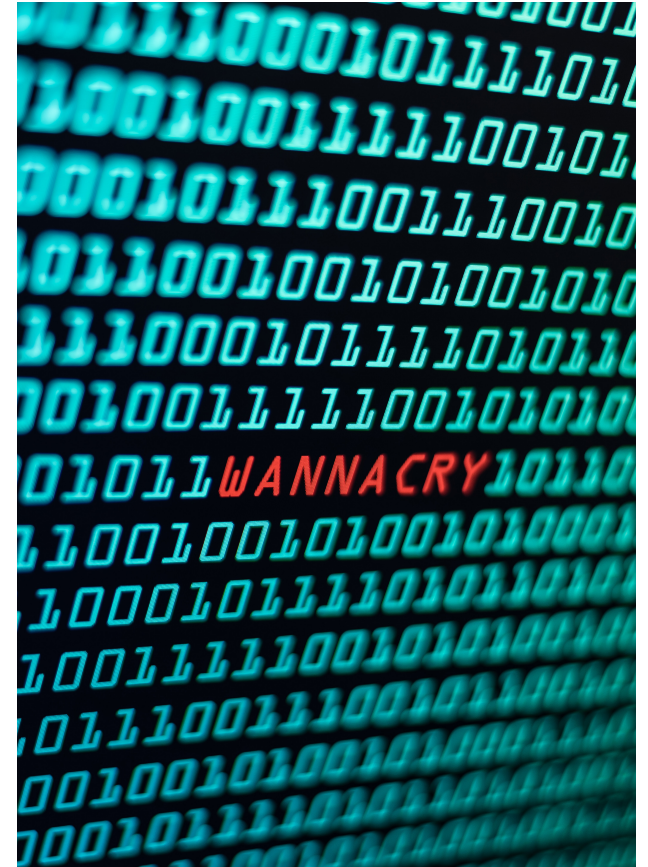
MDISS (Medical Device Innovation, Safety & Security Consortium) considers cybersecurity risks a major public health concern, especially since it is estimated that patients in the U.S. healthcare system will be exposed to over 500 billion interactions with connected medical devices in the next 10 years.[2] The cost of cybersecurity is also a concern. Annual global spend on cybersecurity is approaching $100 billion and global losses to businesses are nearing $1 trillion.[3]

More than 67% of medical device manufacturers and 56% of healthcare delivery organizations (HDOs) believe an attack on their devices is likely to happen within the next 12 months.[4]

Many health systems are having a difficult time implementing a cyber security program to identify where cyber security risks and gaps exist. The need for healthcare executives to reassess their cybersecurity policies and strategies has never been more critical.

The recent WannaCry Ransomware attack got attention by affecting more than 300,000 systems across 150 countries.[1]

WATCH THE VIDEO ▶

Watch the video to learn how Accruent MDSA tracks, identifies, and mitigates medical device risk at **accruent.com**

ACCRUENT MDSA CYBERSECURITY RISK MANAGEMENT AND MITIGATION

Medical Device Security Analyzer (MDSA) applies a two-pronged approach to the management and mitigation of cybersecurity risk.
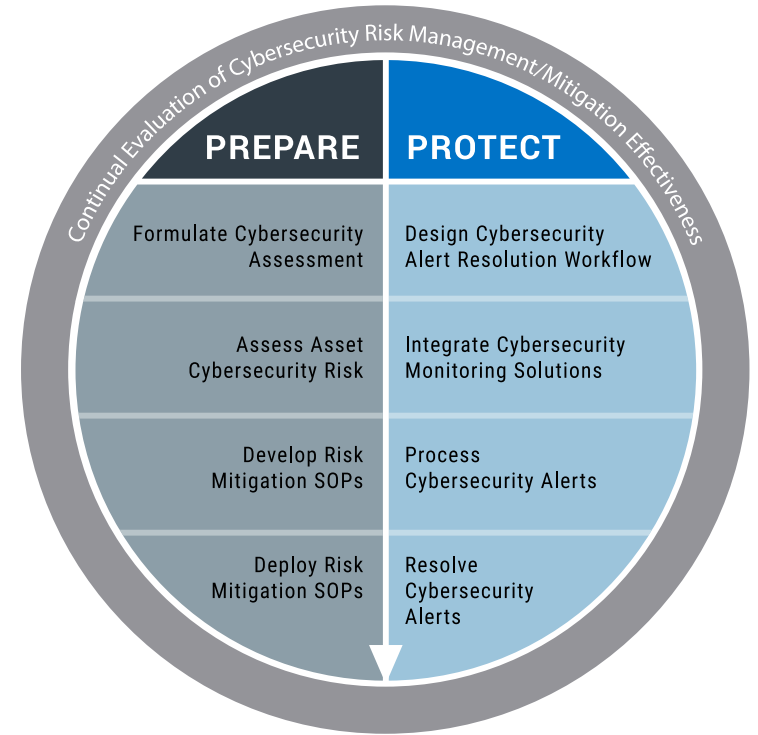
PREPARE

Accruent's MDSA/IoT solution capabilities are designed to enable organizations to gather as much information as possible that contributes to the device or system's cybersecurity risk:

- Identify significant risks or gaps, and track the remediation or mitigation

- Create or update standard operating procedures (SOPs) for technicians onboarding, maintaining and retiring equipment

- Automate the calculation of cybersecurity risk per device taking into account attributes such as the type of information handled by the device, connectivity types, unique roles-based user accounts, capability to be updated, etc.

PROTECT

After you have prepared, Accruent's MDSA ensures the best protection by partnering with providers of discovery and monitoring tools so you can promptly respond to cybersecurity anomalies in a prioritized, measurable, and consistent manner. Together these tools:

- Monitor the network traffic and the information going to and from devices

- Send alerts to the appropriate staff if there is activity that falls outside the normal traffic pattern

- Give the ability to manage and understand utilization data in order to right-size equipment fleet

Continual Evaluation of Cybersecurity Risk Management/Mitigation Effectiveness

PREPARE | **PROTECT**

PREPARE	PROTECT
Formulate Cybersecurity Assessment	Design Cybersecurity Alert Resolution Workflow
Assess Asset Cybersecurity Risk	Integrate Cybersecurity Monitoring Solutions
Develop Risk Mitigation SOPs	Process Cybersecurity Alerts
Deploy Risk Mitigation SOPs	Resolve Cybersecurity Alerts

[1] M. Busdicker, P. Upendra (2017) The Role of Healthcare Technology Management in Facilitating Medical Device Cybersecurity. Biomedical Instrumentation & Technology. Sep 2017, (Cyber Vigilance: Keeping Healthcare Technology Safe and Secure in a Connected World) Vol. 51, No. s6 , pp. 19-25

[2] Medical Device Cybersecurity: A Guide for HTM Professionals, 2018, edited by Stephen L. Grimes, FACCE, FAIMBE, FHIMSS and Axel Wirth, CPHIMS, CISSP, HCISPP.

[3] Axel Wirth (2017) The Economics of Cybersecurity. Biomedical Instrumentation & Technology: Cyber Vigilance: Keeping Healthcare Technology Safe and Secure in a Connected World, Vol. 51, No. s6, pp. 52-59.

[4] Medical Device Security: An Industry Under Attack and Unprepared to Defend, Ponemon Institute© Research Report. May 2017. p 15

Contact sales@accruent.com to schedule a demo

accruent

800.774.7622 | ACCRUENT.COM