FIELD MANUAL

CloudWave

Medical Device Cybersecurity Field Manual

A realistic guide to the design, development, and deployment of holistic medical device cybersecurity programs for healthcare organizations.

CONTENTS:

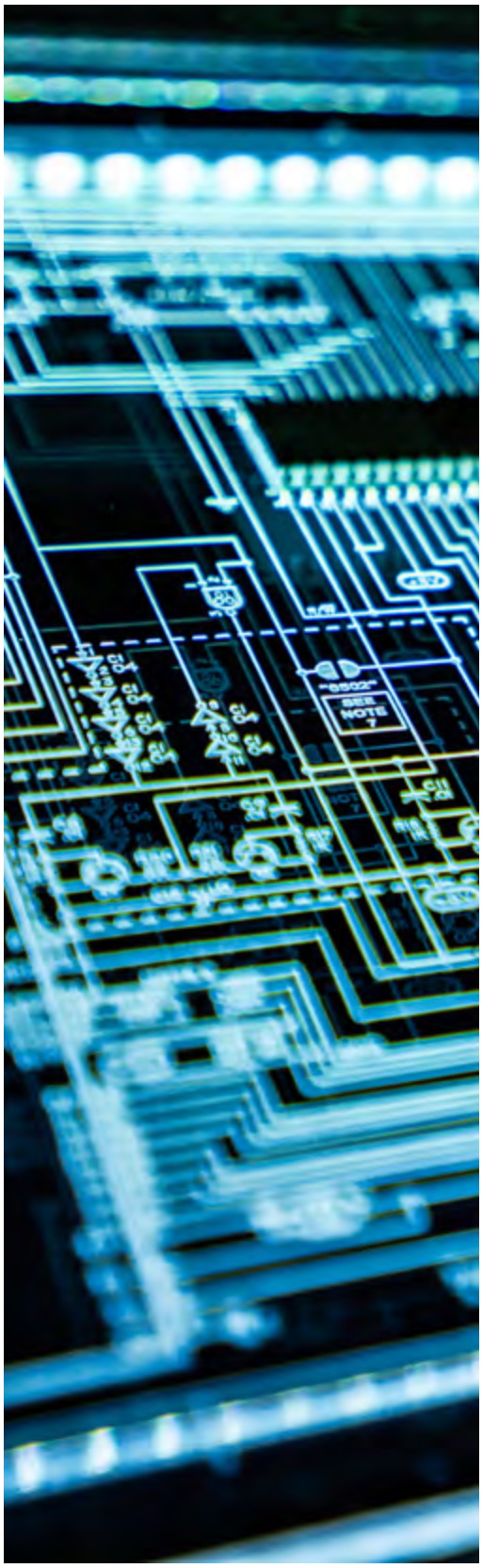
INTRODUCTION

Medical Device Cybersecurity Field Manual.

This manual aims to help you develop a holistic medical device cybersecurity program. The manual does not assume you have anything in place or any medical device or IT cybersecurity background.

CloudWave partners with the FDA and the DHS to evaluate and respond to healthcare sector threats involving medical devices. We have performed ongoing research into medical device cybersecurity and provided tabletop simulations to over 450 healthcare organizations, with medical device cybersecurity being a cornerstone of those simulations. We have also worked closely with medical device manufacturers to design, develop and deploy more secure medical devices.

Everything that we have learned about medical device cybersecurity to date is included in this manual. As you read through the manual, you will find a variety of guidance and tools. The manual is developed to act as a blueprint. Although you can skip to any section and derive what you need, the manual will take you from ground zero to successfully deploying a fully integrated and holistic medical device cybersecurity program.



MEDICAL DEVICE CYBERSECURITY NOT IT CYBERSECURITY

One mistake often seen is applying IT cybersecurity policies and procedures to medical device cybersecurity. Although some approaches to safeguarding IT systems can be recycled and used on medical devices, it is essential to remember that medical device cybersecurity is a separate and distinct practice in cybersecurity.

IT cybersecurity focuses on protecting systems and data. Even HIPAA focuses on the protection of data. At first, this may sound as if it would be a practical approach for safeguarding medical devices. After all, IT systems and medical devices both have computer chips. They often use the same communication methods as the network, and it is vital to safeguard the data on those devices. Since medical devices often contain and rely upon Protected Health Information (PHI) and Personally Identifiable Information (PII), they are regulated under HIPAA and their FDA requirements.

However, the critical difference is that medical devices have one thing that classical IT systems do not; humans may rely on that computer to keep them alive. This may seem as if I am stating the obvious, but as obvious as that may seem, it is one of the most significant factors for designing, developing, and deploying a medical device cybersecurity program.

If you apply frameworks like NIST CSF, NIST 800-53, or HIPAA to medical device cybersecurity, you may achieve one thing: a false sense of security and readiness. Most IT cybersecurity practices need to catch up to what is required to support a medical device cybersecurity program.

This does not mean some IT cybersecurity approaches would not work in medical device cybersecurity. Instead, it would be best to consider the differences purposefully and clearly understand where things may fall short. Let us take the example of cybersecurity incident response.

When considering the incident response from the IT perspective, it focuses on protecting systems and data confidentiality, integrity, and availability. Protecting medical devices requires utilizing tools, tactics, policies, and procedures. This strategy does not condemn those approaches; it is critical to the organization's success. But even though some of the IT cybersecurity incident response procedures may be a good start for medical device cybersecurity, they fall short when responding to medical device cybersecurity incidents.

One of the foundational items needed to launch or evolve your medical device cybersecurity program successfully is to get all stakeholders to agree that medical device cybersecurity should be approached differently than IT cybersecurity. The impact on human life could be critical if an attacker is successful.

Another way to think of this is to reverse engineer the problem. Rather than start with "how do you protect" medical devices, you should start with how to protect the patient.

Things-to-Know and Consider

Medical Device Cybersecurity Focus
As you evolve your medical device cybersecurity, don't simply inherit IT security best practices or approaches.

IT Security Focus
IT Security has traditionally focused on protecting systems and data, not patients. This is an important distinction for consideration.

Staffing and Resources
Do you have the right people and expertise to help you design a medical device cybersecurity program?

START WITH THE PATIENT

Software Solves Everything! Or Does It?

If you listen to vendors' or even cybersecurity professionals' recommendations, you will often hear how the right software is the cornerstone of an effective medical device cybersecurity program. Nothing could be further from the truth.

CloudWave is a software company that provides some of the most robust cybersecurity software available; it is beyond capable of supporting a medical device cybersecurity program. The keyword there is supporting.

The cornerstone of any medical device cybersecurity program should be the patient, not the software. Software is an essential component, but it is not the only one.

By starting with the patient, you uncover questions, challenges, and needs that will help you formulate a more in-depth strategy and approach. Many organizations that start with the software usually respond to a vendor presentation and become software focused. Unfortunately, once the software deployment is complete, they realize there are many things the software does not address and find that the overall costs will be much more significant than first expected. Yet, when presenting the medical device cybersecurity strategy to leadership, no one highlighted that the overall investment to run a successful medical device cybersecurity program would be much higher. The software was just a small component.

RECOMMENDATION: Step back and consider all the components needed to support patient care before you start speaking to software vendors. This approach may not be comfortable for you or your IT cybersecurity team because we are more comfortable talking tech and safeguarding the device and data (see the previous section). Yet, we may see things differently if we step back and consider the protection of the patient first.

THE ATTACKERS PERSPECTIVE

Attackers will always have a vote. Some may even say that the attacker gets to choose all the options. They get to choose the attack type, the attack's time and date, the attack's ultimate objective, and how long and how many attacks to perform. Many of our approaches to cybersecurity are often based on the defender's perspective. We tend to minimize the attacker's skillset, tenacity, and audacity.

Regarding medical device cybersecurity, we can represent the attacker's perspective by starting with the patient. To do that, we need to ask, "What could an attacker do to this patient if they were to compromise this medical device in some way, shape, or form?" In doing this, we define the types of incidents we need to plan for, respond to, manage, and recover from as part of a medical device cybersecurity program.

There are a few different ways to define how attacks impact patients, including considering the number of staffed resources and timeline. You could review each medical device category and determine the type of attack, for example, smart pump versus MRI. Another approach would be to consider attacks against diagnostic systems versus life support systems. Approaching the broader categorization problem is faster and allows for broader conversation with your peers and colleagues. It also can help you refine compliance, detection, and response needs.

RECOMMENDATION: Build a matrix identifying what you want to consider for each device category. You may decide that diagnostic devices' security assessment level is less detailed than for life support devices. Your response to diagnostic devices may be different than for life support devices. The key is to purposefully think about how these categories of devices shape your medical device cybersecurity program. It can also help you in terms of planning. For instance, if you have limited funds or

resources, you may propose developing a multi-phase approach by safeguarding and segregating life support devices as an organization. A separate phase would later focus on diagnostic devices. Part of the matrix should also include evaluating the risks of device manufacturers.

All these considerations start with the patient and consider the attacker's perspective. We must continually step back and ascertain the impact on patient safety and the attacker's potential for harm. If we can maintain these approaches as the guiding principles, we can also lay the foundation for a defensible program. A defensible program is one in which we could support a robust legal defense. You are defining a strong future defense by laying the foundation that your program focuses on patient safety and not only protecting systems and data.

NOTE: Please remember that you should consult legal counsel as you develop your medical device cybersecurity program.

Summary of Medical Device Security Program Considerations:

- There is much more to medical device cybersecurity than just deploying software
- Consider the legal ramifications of your program's design
- Evaluate Medical Device inventory and classify devices
- Consider other strategies, such as network segmentation
- Assess the medical device and manufacturer risks

This manual will help you plan to address all those decisions and challenges. The first step is to think about **Incident Response** before defining the rest of your medical device security program.

Things-to-Know and Consider

Attackers Get a Vote

The attacker decides the how, when, why and much more – if your cybersecurity strategy does not consider this, you will achieve a false sense of security.

Start with the Patient

By always starting with the patient and asking, "What could an attacker do to this patient when connected to a device" you can think of defenses and strategies that are specific and patient-centered.

Remember Defensibility

Consider liability as you design your medical device cybersecurity program. Always consult your legal counsel.

INCIDENT RESPONSE CONSIDERATIONS

Cybersecurity incident response is often a misunderstood concept. In the over 450 tabletop simulations conducted, few organizations have performed well in a fast-moving realistic attack, partly due to cybersecurity response not keeping up with the attacker's modern tactics and very few well-known practices or guidance regarding responding to a medical device cybersecurity attack.

Getting medical device cybersecurity incident response right is critical. Before we jump into it, let's walk through a mini-tabletop simulation. This simulation could apply to any hospital; it works best if you play along. After the simulation, I will walk through what was expected and provide suggestions for designing your medical device cybersecurity program.

Simulation Instructions - How You Can Participate:
As this simulation unfolds, think about how you would handle this event based on the time of day, day of the week, level of training, and procedures deployed. Think about how well your IT cybersecurity policies and procedures would work. Document what your current response plan would do or identify areas where it may be deficient.

Simulation Details:
This simulation is a light version of our program. However, it is based on an actual incident the team responded to in 2019.

03:00 Sunday

An alert is raised by your cybersecurity software involving a patient monitoring system. The alert is related to a possible SSH Brute Force attack against Port 23 of a server on your network.

03:04 Sunday

An alert is raised that a client IP address is performing port and address scans of network assets.

03:05 Sunday

An alert is raised that a client IP address is attempting to utilize SMB to query network assets.

03:07 Sunday

Nurses in the ICU observe that their desktop computers used for patient monitoring have locked up and do not seem to work.

03:08 Sunday

Nurses in the ICU report that several medical devices seem to be acting "weird" and are concerned about their stability.

This scenario could continue to evolve, but we will use these events to illustrate a few points for our needs in this manual. We intend to introduce concepts to consider as we continue designing and developing your medical device cybersecurity program.

Before diving into recommendations and practices, take a few minutes to think about all we have discussed. Everything we have reviewed comes down to how well you can detect, analyze, and respond to an attack. But while software supports it, this is done by more than just software.

The incident concerns patient impact, which needs to be the core focus. This incident represents an active attacker in your environment who appears to target medical devices at 3 PM on a Sunday.

The 3 AM Test:
You can use this snippet of a simulation to add another test to your design – "what if this happened at 3 AM on a Sunday?" We call that the 3 AM test, and we find that most cybersecurity strategies are designed to work at 10 AM on Monday when there are plenty of on-the-ground resources, a full complement of leaders, and easy access to clinical engineering and third parties. But, at 3 AM on Sunday, you are short-staffed or not staffed, and suddenly things begin to fall apart. Considering the 3 AM Test, you can ensure that practices, policies, and procedures will survive regardless of the time of day or day of the week.

Continuous Monitoring

We just explained the 3 AM test, and as you probably agree, it is an important consideration. You can deploy excellent world-class software, but what good is it if an alert occurs at 3 AM on a Sunday and no one sees it until 9:30 AM the following day? How you will monitor your system 24x7 is a critical item to consider. Medical devices are more than just 9-to-5 assets, and patients do not only need care during the day. Yet many IT Security teams are not 24x7, and even those with after-hours support may rely on a helpdesk or text messages to deal with critical events. It is one thing to deal with a crucial alert at 3 AM for a server and yet another for a medical device attack.

Even if you have a 24x7 operation monitoring your alerts, you must also consider their training. Do they have the appropriate knowledge to provide overwatch to a medical device attack? Most IT incident response focuses on determining what is occurring to the device or network, whereas medical device incident response needs to determine the patient impact; ideally, you can do both simultaneously.

Anomaly Awareness

In the outlined scenario, the nursing staff observes strange behavior (alert's context). In some situations, you may only have on-the-ground observations of anomalies, which means that you must address clinical end-users training and the clinical engineering team to evaluate device behavior in the context of cybersecurity. Providing specialized security awareness training must be performed as the threat landscape evolves and incorporates comprehensive nursing education and management. The helpdesk should also analyze reports of anomalies in the context of cybersecurity to support early detection of zero-day events or other events that do not raise system alerts.

Clinical Cybersecurity Rapid Response

A concept that CloudWave's team pioneered in 2018 is known as Clinical Cybersecurity Rapid Response. In the scenario above, the attack targeted systems in the ICU, but this could easily have been the Cath-Lab, Surgical Suites, PACI, or similar highly critical hospital areas. In all these areas, life support systems support patient care. The need to evaluate the threat is something the IT Security team can only do with help. Assessing the threat, carrying out the on-the-ground response, and determining the impact on patient care must be carried out in parallel, as time is of the essence.

To accomplish this process, your clinical Rapid Response team must be trained to support cybersecurity issues. Remember, the Rapid Response team is limited in resources, and a cybersecurity attack can simultaneously impact many patients. Ultimately you need to design training and scenarios for these teams that remain current over time.

The Monitoring Dilemma

One scenario not illustrated above is an attack that breaches a third-party medical device network. These networks are deployed and maintained by the vendor. In all cases, you may be unable to deploy monitoring tools (hardware or software) to these networks. Doing so may violate warranties and, in some cases, possibly put patient safety at risk. It is also possible that any cybersecurity device deployed to these networks would need to be cleared by the FDA.

This requirement creates a monitoring dilemma. Your software solution (remember, do not start with the software) may not identify attacks for those devices on these third-party networks. You should ascertain the warranty and patient safety implications of monitoring these devices.

NOTE: CloudWave has a solution for monitoring medical devices that have been ok'd by the FDA and do not require FDA clearance. Inquire if you are interested in learning more.

Fingerprinting & Location

In the scenario, we provided details about the types of devices involved and their location. But what if we did not provide those details? If your teams cannot identify the type of device (at the very least, the manufacturer) and the device's location, how do you dispatch your rapid response team to determine the patient's state and impact? It is essential to decide on the location and type of device to support incident response and threat intelligence and vulnerability assessment activities. Major software vendors in this space support these features to varying degrees.

Critical Success Target Window

The concept of the Critical Success Target Window is that you must successfully contain an attack within a very short amount of time (often minutes, not hours). This method is not something that a traditional IT Security approach typically will address. But when you start with patients, time is of the essence. You need to move quickly but with professionalism and context. As you design your program, consider what you could do in the first minutes of an attack, and then keep improving by optimizing your response.

Protocols vs. Playbooks

Playbooks are an interesting approach to cybersecurity incident response. They are pieces of documentation that make for a great reference resource. Interestingly, the first victim when we conduct tabletop simulations is the playbook. Teams bring their playbooks, but all references to the playbook are soon put aside after about five minutes.

We have found that when an incident evolves quickly, and you have minutes, not hours to respond at 3 AM on Sunday, the last thing you will do is open a playbook. We suggest adopting a protocol-based incident response for medical device cybersecurity.

The protocol-based incident response aims to simplify the response and ultimately drive muscle memory. This approach is familiar to clinicians and was adopted from the Maryland Shock Trauma Center in 2014. As you consider how you will train your teams to respond in a coordinated fashion to medical device cybersecurity incidents, you should consider developing protocols instead of playbooks.

COMPLY – DETECT – RESPOND

The first part of this manual focused on providing a practical set of knowledge and considerations that you can use to help lay the foundation for the design, development, and deployment of a medical device cybersecurity program. As you now know, we recommend that you start by thinking of the patient first, keep the attacker's perspective in mind, and consider how you prepare well for a real-world attack.

In this next section, the approach changes to be more prescriptive, providing a series of questions to consider and recommendations that you can use in formulating your medical device cybersecurity program. The questions only partially represent all considerations but provide a strong foundation. More importantly, I hope these items familiarize you with a medical device cybersecurity program's various components.

The recommendations are the current best approach. Over time these recommendations may become dated, so evaluate the information and determine if it still makes sense for you and your objectives.

Objective: Go beyond just software deployment. You are responsible for designing, developing, and deploying a world-class medical device cybersecurity program that would meet or exceed the FDA Medical Device Cybersecurity Regional Incident Preparedness & Response recommendations playbook first published in 2018 by the FDA and MITRE.

If you agree with this objective, the items presented here will help you achieve that goal. Even if that is different from your objective, you will find that you will develop a much more mature and robust medical device cybersecurity program by considering each item in the following sections. We will consider what it takes to comply with best practices and regulations, detect threats and attacks and respond to incidents.

Addressing these areas will ensure you can meet or exceed the FDA recommendations. Conversely, if you fail to balance and manage these areas, you could have a medical device cybersecurity program that is less mature and effective.

Comply

Our goal here is to identify those practices that allow us to comply with industry best practices (specifically medical device cybersecurity) and regulations (HIPAA).

Detect

We want to ensure that we can identify threats, vulnerabilities, and attacks but also want to be sure that we can take action regardless of the time of day or day of the week.

Respond

We want to ensure that we can evaluate and respond to attacks while doing all we can to ensure patient safety as best as possible.

Step back before getting into the considerations for the comply, detect, and respond buckets. Having some "pocket questions" is wise to help get colleagues on the same page. The purpose is to create higher-level dialogue and demonstrate that a medical device cybersecurity program must be well thought out.

Consideration	Discussion
How does my medical device cybersecurity program integrate with my other IT security systems?	If you think back to the scenario we presented earlier, it is apparent that medical device cybersecurity is a team sport. It is not just clinical engineering or an IT Security effort. Determine how your strategy will work with your existing IT Security systems.
How do you create a common operating system?	Although an attacker may attack a medical device, it is more probable that the attack will start somewhere on your network or other devices. Having a common operating picture is crucial.
What unique expertise will you need?	It is essential to realize that even if you have a mature IT Security team, they may require additional training. You must also augment the skills of your clinicians, rapid response team, and clinical engineering teams.
What specific policies and practices are required?	IT Security policies and procedures focus on protecting assets (systems and data), and medical device cybersecurity is about protecting human life. Make sure this difference is understood.
What happens if there is an incident?	Responding to a medical device cybersecurity incident differs from responding to a traditional IT Security incident. The use of specialized protocols and other techniques needs to be evaluated and implemented.
Is this building a complete solution or just a single piece of the overall solution?	This question is critical, especially considering everything reviewed in this manual.

Comply Considerations

These action items and considerations are designed to help you develop your ability to comply with best practices and regulations.

Action Item	Consideration
Deploy Medical Device Specific Cybersecurity Policy and Practices	IT Security policies may apply to medical device cybersecurity, yet often they do not address the specific requirements of this specialty area (training, qualifications, response levels, etc.).
Establish a Manufacturer Risk/Security Assessment Framework	Develop a manufacturer assessment framework to evaluate medical device risk and security.
Institute an "End of Life" Management Program	Medical devices often rely on end-of-life operating systems or software. A plan for transitioning these systems out of the environment should be developed to demonstrate ongoing risk management.
Determine a Medical Device Cybersecurity Team Model	Identify who will participate in the primary and tertiary medical device cybersecurity teams.
Develop a Medical Device Threat Intel Program	Identify the specific threat sources for medical device cybersecurity. Explain why you chose these threat sources and how they are monitored.
Governance and Management	Determine your governance model and how you will administer and manage your medical device cybersecurity program.

Detect Considerations

These considerations are designed to help you consider how you will detect and analyze threats, vulnerabilities, and potential attacks.

Action Item	Consideration
Deploy Deep Packet Inspection Network Monitoring	Deep packet inspection is essential for monitoring network-based attacks and critical for medical device monitoring and fingerprinting.
Employ Deception Technologies	Determine how to protect devices from unknown attacks or activity on segregated networks. Integrated deception technologies are an essential consideration.
Utilize Host Intrusion Detection for Monitoring Stations	Consider host-level monitoring for a medical device supporting infrastructure such as patient monitoring stations.
Assure Asset Fingerprinting and Management Systems are Deployed	Automated fingerprinting and classification of devices are essential for threat analysis and incident response.
Create a Vulnerability Assessment Program	A program to perform vulnerability assessments is critical. Do not rely on "network-based assessments," but ensure you have a program that performs targeted vulnerability assessments of representative populations.
Establish COP and 24x7 Monitoring	Ensure that your medical device program integrates with the broader enterprise cybersecurity program. This process should yield a single common operating picture (COP) and 24x7 monitoring of the environment.

Respond Considerations

These considerations are focused on those items required to respond to a medical device cybersecurity incident effectively.

Action Item	Consideration
Deploy Medical Device Specific Cybersecurity Policies and Practices	Develop or utilize a team specifically trained to respond to medical device attacks – 24x7. This ensures that patient care can be provided while making patient safety decisions.
Establish a Manufacturer Risk/Security Assessment Framework	Develop and deploy Rapid Response Protocols to address medical device cybersecurity IR.
Institute an "End of Life" Management Program	Train your team in Rapid Response.
Determine a Medical Device Cybersecurity Team Model	Perform tabletop simulations to develop muscle memory and identify tipping points. Ensure all lessons learned are addressed. The tabletop should stress every area of your program, from policies to attack detection to fingerprinting to rapid response and patient safety.
Integrate Medical Device Cybersecurity IR with IT Security IR	Integrate your rapid response capability with your IT Security and other IR components, including disaster recovery and OEM.

PROJECT SKELETON

This manual provides a starter set of tasks to consider as you move from envisioning your medical device cybersecurity program to planning and deploying. You will still want to develop a detailed project plan. One of the most important lessons we have learned from working with our clients is to spend considerable time working through policies and procedures, and establishing a cross-functional team that can support your efforts is crucial. Medical device cybersecurity is not an island, and having a cross-functional team (nurses, doctors, IT, clinical engineering, vendor representation, executive sponsorship, HR, legal, compliance, etc.) involved from the start will help to ease policy and procedure adoption, which ultimately should be the foundation of your program.

Although this skeleton plan is divided into three sections, you could refactor this to suit your needs. One key to success is thinking about medical device cybersecurity at your organization as a product, and this plan is for the development of your "1.0" release. Once the initial program is deployed, you can determine what is working well or needs to be optimized and begin working on your "2.0" release and beyond. Remember that a medical device cybersecurity program is an ongoing and never-ending evolution.

Policy & Governance

This section focuses on developing your policy and procedural foundation. Establishing your cross-functional team, key objectives, and cadence are critical to success.

Project Task

- Policy Draft Development
- Policy Draft Review
- Policy BETA Testing
- Vendor Assessment Framework Draft
- Vendor Assessment Framework Review
- Vendor Assessment Framework BETA
- Establish Governance Framework
- Finalize Medical Device Security Policy 1.0
- Finalize Medical Device Vendor Assessment Framework 1.0
- Conduct First Medical Device Cybersecurity Governance Meeting
- Patient Disclosures
- Executive and User Education
- Identify Current Medical Device Asset inventory

SECURITY ARCHITECTURE

Security architecture can mean different things in different settings. For this plan's purposes, we define security architecture as the standards and practices required to safeguard patients connected to medical devices. In short, this section should enable your policies and procedures to come to life and be employed day-to-day.

Project Task
Establish Medical Device Network Security Standards
Establish Medical Device Network Segregation Architecture
Develop Medical Device Evolve and Replace Strategy
Present Medical Device Network Plan and Architecture
Establish Medical Device Honeypot Program
Establish Medical Device Vulnerability Assessment Program
Perform Baseline Medical Device Vulnerability Assessment

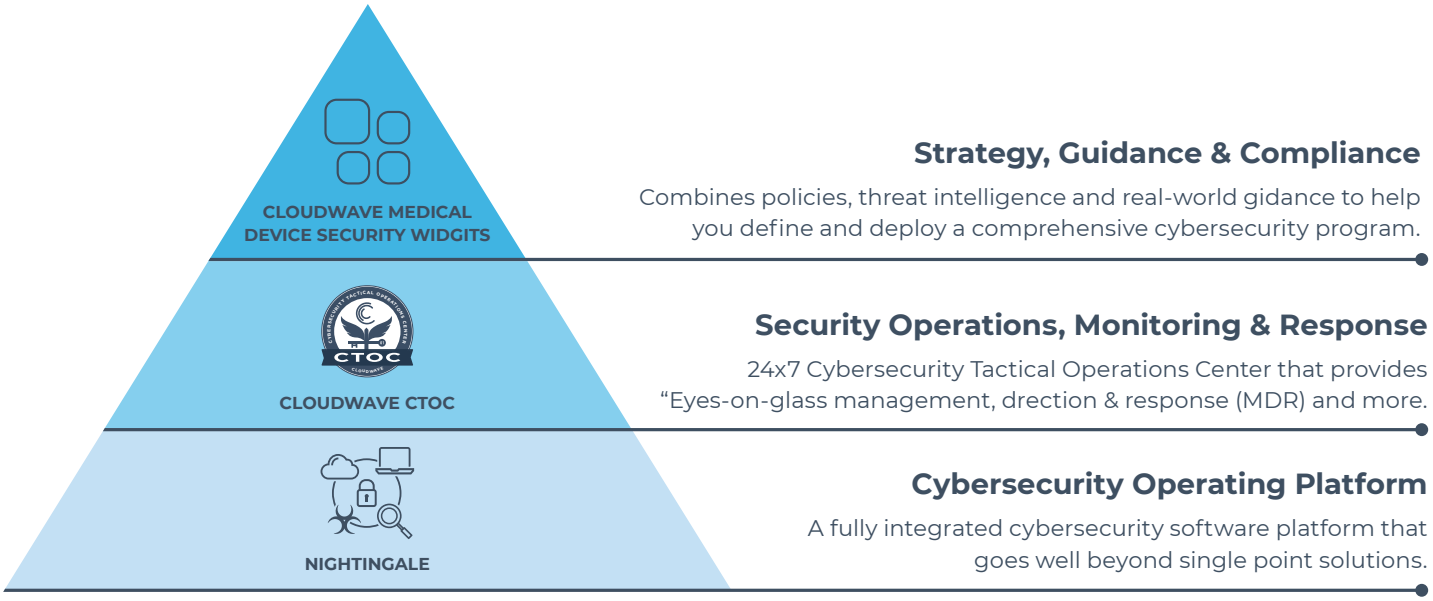
SECURITY OPERATIONS

This section focuses on how you will operate your medical device cybersecurity program 24x7. This includes responding to alerts, monitoring and integrating threat intelligence, indicators of compromise, manufacturer disclosures, and more. Further, you should be able to educate your end-users in anomaly detection and reporting and develop and train your rapid response program for medical device cybersecurity incident response.

Project Task
Establish Medical Device Monitoring Program
Establish Threat Intelligence Program
Develop & Deploy a Medical Device Cybersecurity Rapid Response Team
Develop & Deploy Medical Device Cybersecurity Awareness Training Program

CLOUDWAVE'S MEDICAL DEVICE SECURITY SOLUTION

This manual focuses on helping you design, develop, and deploy a holistic and effective medical device cybersecurity program. Hopefully, you have found the information presented meaningful, thought-provoking, and valuable. Suppose you decide that walking the path to achieving a holistic medical device cybersecurity program is not something you want to do alone. In that case, we invite you to evaluate CloudWave's Medical Device Security solution. CloudWave's Medical Device Security solution goes well beyond the typical medical device cybersecurity program.



CloudWave's Medical Device Security solution combines a robust cybersecurity software platform, 24x7 medical device cybersecurity operations monitoring and response, policy and procedural templates, tabletop simulations, end-user training for awareness, and medical device incident response in a unified solution.

A CONTINUING JOURNEY

This field manual aims to help you gain a foundational understanding of the components, practices, and perspectives required to design and develop a holistic medical device cybersecurity program. Even though the information presented here has been successfully used to deploy mature medical device cybersecurity programs at several hospitals, it is not the end of the journey. As threats continue to evolve and attackers become bolder and more daring, our ability to evolve will be challenged.

A well-designed foundation is critical to supporting the weight of the challenges that will arise and test this cybersecurity specialty. With time I foresee the need for cybersecurity clinicians, automated responses to medical device security, FDA-cleared security appliances, and more. An essential item that was not covered in this field manual is recovery and prolonged operations. Companies like CloudWave are working hard to anticipate and address these challenges. The foundation you put in place today will be the difference between your ability to evolve in the future or returning to the drawing board.

If CloudWave can be of assistance to you, please reach out. We are incredibly passionate about our mission and responsibility to the healthcare sector. If you want to kick around an idea, talk about the future, or investigate deploying our Medical Device Security or other solutions, we would love to speak with and get to know you...our partners, in the fight against those who would try to do patients harm.

LEARN MORE AT

gocloudwave.com

CloudWave's Cybersecurity division is an Information Sharing and Analysis Organization (ISAO) in coordination with government agencies like the Department of Homeland Security (DHS) and the Cybersecurity & Infrastructure Security Agency (CISA), and regularly evaluates and provides guidance about national cyber threats. CloudWave's team provides real-time threat intelligence about medical devices under their Memorandum of Understanding (MOU) with the U.S. Food and Drug Administration (FDA).