HEIMDALL
SBOM & VULNERABILITY MANAGEMENT

With Heimdall, medical device manufacturers can quickly answer the question 'which of my products are impacted by a critical new vulnerability?'

A RIGHT SIZED SOLUTION FOR YOUR MEDICAL DEVICE

Heimdall is a vulnerability management tool that enables automatic management of a Software Bill of Materials (SBOM), identifies known & exploitable vulnerabilities, and enables prioritized remediation risk reduction in an easy, economical, and reliable way.

SHIFTS IMPACTING MEDICAL DEVICE MANUFACTURERS (MDMs)

MDMs used to be able to ship a device, hope there were no cybersecurity issues, and address problems as they were found. Today, by utilizing MedCrypt's healthcare-specific tools and APIs, leading MDM's can more easily, efficiently, and proactively build security features into their devices and gain visibility into new and legacy devices to meet regulatory and customer security requirements.

WHAT DO YOU DO TODAY?

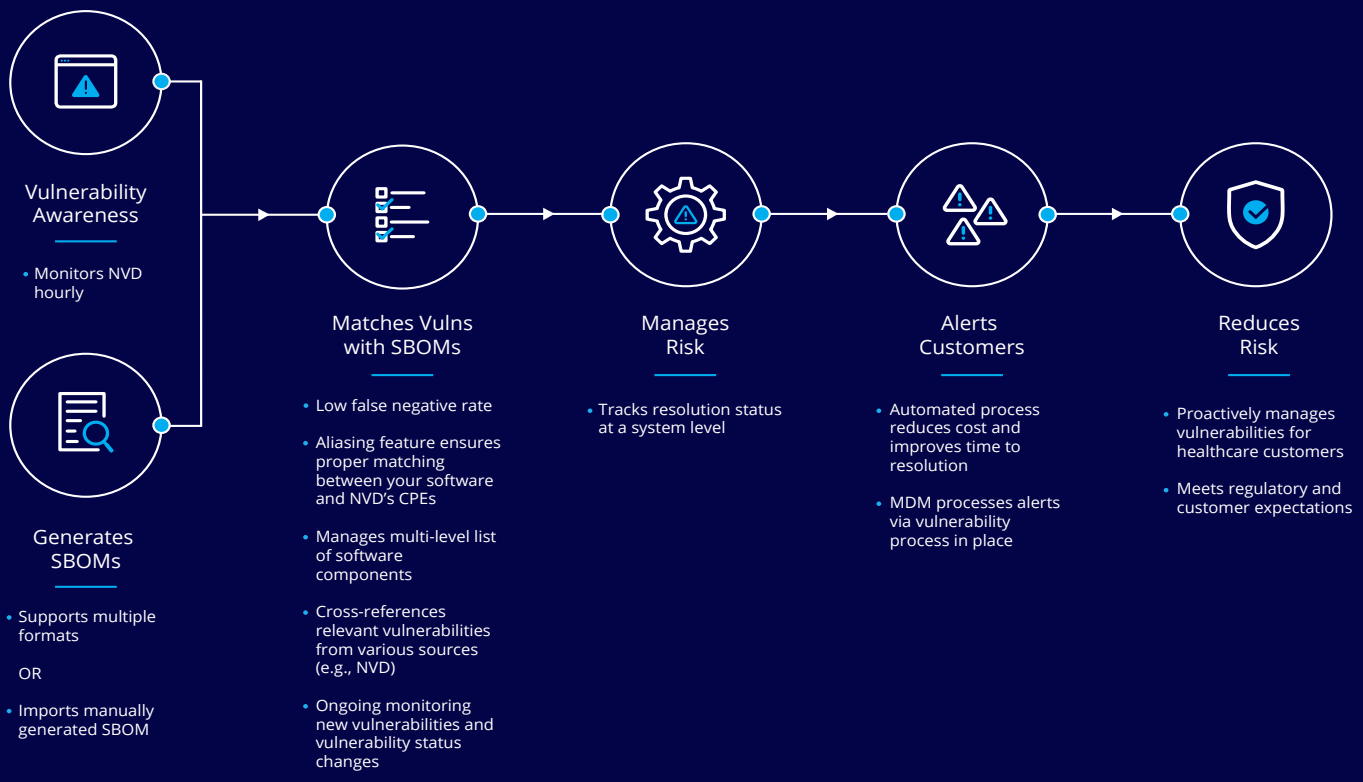
If another WannaCry-like attack began to actively exploit a Windows vulnerability, is your current SBOM strategy up to the task?

- Could you rapidly identify which of your products and their respective versions are impacted?
- Could you swiftly determine the severity of the vulnerability?
- Will you be able to proactively help your customers know which devices are at risk?

WHAT COULD YOU DO WITH HEIMDALL?

With MedCrypt's Heimdall SBOM solution, manufacturers can implement an end-to-end vulnerability management process, thus advancing their ability to improve and maintain device security posture and ultimately meeting regulatory guidances and customer requirements.

HOW HEIMDALL WORKS



WHAT HEIMDALL BRINGS TO YOUR SBOM-BASED VULNERABILITY MANAGEMENT

Building a vulnerability management system and processes that consider the device SBOM is an essential prerequisite for security best practices. Such an approach provides a number of critical benefits:

- Address regulatory requirements for premarket security risk management and postmarket surveillance and maintenance - for new and legacy devices
- Generate SBOMs in consistent manner across product lines
- Produce and maintain secure products by safeguarding device operations and patient's lives
- Produce and maintain secure products by safeguarding device operations and patient's lives
- Full visibility of all components of the device software (including their dependencies)
- Seamless integration into existing vulnerability management process
- Support hospital requests for SBOM and vulnerability data to support their risk management and reduce incident response times
- Forensically link vulnerabilities to device event behavior (when implemented with the entire MedCrypt suite)

ABOUT MEDCRYPT

MedCrypt provides proactive security for healthcare technology. MedCrypt's platform brings core cybersecurity features to medical devices with just a few lines of code, ensuring devices are secure by design. MedCrypt announced a $5.3 million Series A funding round in May of 2019, bringing the total funds raised to $12.3 million with participation from a strategic medical device manufacturer, Eniac Ventures, Section 32, Y Combinator, and more. The company is based in San Diego, California. For more, please visit www.medcrypt.com.

San Diego, California, USA
(877) MDC-RYPT (877-632-7978)
info@medcrypt.com | www.medcrypt.com

medcrypt