VERITI

HEALTHCARE ORGANIZATION ROLLSOUT VERITI TO SECURE AND PROTECT GLOBAL INTERESTS

Veriti eliminates the complexity and operational friction in managing multiple cybersecurity solutions by providing a consolidated, governing platform that continually and proactively monitors security gaps and misconfigurations across the organization's infrastructure and remediates them while ensuring business uptime.

HEALTHCARE INDUSTRY'S CYBERSECURITY CHALLENGES

The healthcare industry is a prime target for cyber attacks due to the valuable data it holds, including personal information like social security numbers, medical records, and insurance cards. As a result, healthcare providers must prioritize data security and confidentiality to protect their patients' sensitive information from nefarious individuals. However, the healthcare industry faces significant cybersecurity challenges, including:

EXTENSIVE AND OFTEN UNPROTECTED ATTACK SURFACE

Healthcare organizations face a high risk of cyber-attacks due to their extensive and often unprotected attack surface, which includes connected medical devices and the use of personal devices lacking endpoint security (BYOD). This adds to the common attack vectors that all businesses face.

THIRD-PARTY VENDORS

Numerous third-party vendors have access to sensitive patient data and critical assets in hospital settings, which increases the risk of a breach.

THE RISE OF TELEHEALTH

The COVID-19 pandemic has led to a surge in telehealth services, which cyber attackers can exploit due to the rapid and often insufficiently secured IT infrastructure rollout.

PATCHING MEDICAL IOT DEVICES

IOMT are vital for modern healthcare but are often difficult to patch or update due to unique operating systems. Some older devices are not designed for modern networks, and patching can be costly and time-consuming.

REGULATORY REQUIREMENTS

Healthcare organizations must comply with stringent regulatory requirements when patching medical devices. Any changes to their software or firmware could affect device certification and performance, requiring providers to carefully balance the need for security updates with the associated risks.

CUSTOMER

INDUSTRY

healthcare

LOCATION

Regional hospital, EMEA

DEVICES AND HOSTS

Endpoints - 3200
IoT – 760 devices
OT – 355 devices
Medical Devices – 211

CHALLENGES AND PAIN POINTS

Medical device failures impact patient care and safety.

Limited ability to keep up with cybersecurity vulnerabilities and patches.

Outdated operating systems pose a security challenge.

Inadequate compliance and pen testing efforts leave the hospital vulnerable to cyberattacks or regulatory fines

Vulnerabilities with a high CVSS score have been discovered in the hospital's environment, putting the organization at risk.

THE SHORTAGE OF SECURITY EXPERTS

Healthcare organizations face challenges in implementing effective security measures due to a shortage of security experts in the industry. This shortage can make it challenging to prioritize security during digital transformation and integrate effective security practices into healthcare models. Providers must address this challenge to ensure effective cybersecurity measures are in place to protect patient data and critical infrastructure.

FALSE POSITIVES

False positives in healthcare cybersecurity can have severe consequences, potentially endangering patients' lives and disrupting medical operations. They occur when security tools flag a benign event or behavior as a threat due to sensitivity, misconfiguration, or lack of consideration for medical devices and operations. Healthcare providers must be aware of this risk and ensure their security systems are appropriately configured and tested to prevent unnecessary downtime and protect patient safety.

VERITI FINDINGS

The customer chose Veriti to conduct a risk assessment and security configuration optimization after researching multiple cybersecurity vendors. Veriti was selected for its reputation for providing non-disruptive optimization processes and its experienced team of cybersecurity professionals.

During the comprehensive proof of concept (POC), Veriti's Unified Security Posture Management platform identified 180 Windows machines (including hosts, servers, and medical devices), running old operating systems, vulnerable to the old yet still relevant CVE-2019-0708 (AKA BlueKeep). This vulnerability is classified as "wormable," meaning malware exploiting this vulnerability on a system can propagate to other vulnerable systems (similar to the WannaCry malware attacks of 2017).

Four of the vulnerable devices were directly connected to the internet, which increases the risk of a successful exploit.
Patching these systems is impossible without impacting medical devices' ability to function and comply with update/upgrade procedures. This had put the hospital at risk of a potential attack that could compromise sensitive patient data and disrupt critical healthcare services.

The overall number is the amount of medical devices they have with active vulnerabilities:

CVSS 9.3	CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148, CVE-2017-11882, CVE-2019-0541,CVE-2021-4104, CVE-2021-44228, CVE-2021-44832, CVE-2021-45046, CVE-2021-45105
CVSS 10	CVE-2019-0708

RESULTS

50%

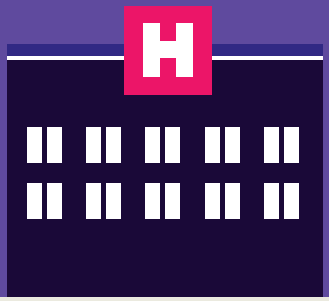
IMPROVEMENT IN PENETRATION TESTING ACHIEVED BY VERITI'S CONTINUOUS SECURITY CONFIGURATION OPTIMIZATION

8%

FEWER LOGS SENT TO SIEM DUE TO VERITI'S EXCLUSION CREATION, REDUCING OPERATIONAL FRICTION.

30%

REDUCTION IN FALSE POSITIVES RESULTING IN IMPROVED TIME TO RESPOND AND OPERATIONALIZATION OF THE SECURITY POSTURE



SOLUTION

The hospital chose Veriti's Unified Security Posture Management platform as a comprehensive solution to manage its security stack. The implementation of Veriti has provided a centralized platform to monitor and respond to security events across the entire organization.

"It all starts with being able to virtually patch our security solutions without having to wait for the next maintenance window to try and patch unmatchable medical devices." Said the CISO of the hospital.

The hospital leverages Veriti's unique virtual patching solution to enhance its cybersecurity posture. Veriti's real-time mitigation capabilities enable the hospital to address vulnerabilities and exploits as they arise, prioritizing them based on the risk they pose to the organization. By integrating different layers of security in the hospital's environment, Veriti enables the hospital to focus on hardening its overall security posture instead of just patching medical devices. With Veriti, the hospital can virtually patch relevant security solutions without updating outdated operating systems, ensuring a secure environment while minimizing disruptions to patient care.

VERITI FOR HEALTHCARE

COMPREHENSIVE SECURITY ANALYSIS

Veriti provides real-time visibility into an organization's risk posture and each security solution's function and use, enabling security teams to identify and prioritize security risks and make data-driven decisions to optimize their security investments.

NON-DISRUPTIVE REMEDIATION

Veriti enables organizations to take remediation actions without fearing that they will disrupt business operations. Using machine learning and advanced analytics, Veriti finds the root cause behind potential and actual business disruptions and provides one-click remediation actions to mitigate them, ensuring that there is no negative impact on business operations.

VIRTUAL PATCHING

Veriti enables virtual patching of vulnerabilities, which helps organizations protect their critical systems from exploitation by attackers without having to wait for the official patch release.

VERITI

"WITH VERITI, WE HAVE BEEN ABLE TO STREAMLINE OUR SECURITY OPERATIONS AND IMPROVE OUR ABILITY TO DETECT, RESPOND TO, AND REMEDIATE SECURITY INCIDENTS."

CISO OF THE HOSPITAL.

ABOUT VERITI

Integrated with the entire security stack, Veriti provides a consolidated governing security platform that continually and proactively monitors exposure to threats and provides actionable remediation paths for security gaps and high-risk vulnerabilities across the organization's infrastructure and attack surface

Veriti's mission is to eliminate unnecessary complexity and operational friction and reduce the time spent in manual oversight and managing multiple cybersecurity solutions. The solution platform enables security teams to proactively improve security posture and focus on tasks that require discretion while automating repetitive, tedious tasks.

VERITI.AI