CASE STUDY

nwn carousel

Samaritan Medical's Real Life Customer Adoption of Managed Detection and Response

NWN Carousel and Samaritan Health Partner to Implement New Strategies to Deter Cyber-Attacks

Samaritan Medical Center

Executive Summary

Company: Samaritan Medical Center

Industry: Healthcare

Location: Watertown, NY

Challenge: Recognizing Cyber attacks before it is too late.

Solution:

- Detection and recovery from cyberattack gaining back access to sensitive files.
- Integration of security software and vulnerability management.
- Implementation of Managed Detection and Response.

Overview

Samaritan Medical Center is a hospital located in upstate New York. In 2020, Samaritan experienced a cyber-attack from a malicious email that locked them out of all computer domains. The 290-bed hospital tragically lost access to all Emergency Medical Records (EMR), restricting them from accessing any of their patients' records for six weeks.

Samaritan had many security measures implemented when the attack took place. These precautions included firewall, DNS security, and SIEM backup. The malicious email was still able to break through all these security measures.

After the attack, Samaritan partnered with NWN Carousel to perform Managed Detection and Response (MDR) to regain access to their files. NWN Carousel took a holistic approach to provide Samaritan with measures needed to manage the cybersecurity attack and prevent future instances. Starting with 24/7 monitoring, Samaritan was able to begin their security deployment. NWN Carousel launched a cyber investigation to find the threats and discover where the malware was able to breach their security.

Security analysts were assigned to work through the areas where Samaritan lacked expertise. Analysts worked to implement endpoint prevention and detection providing vulnerability management. They integrated ticketed reporting, customized reporting, and consolidation of tech vendors building on internal threat detection systems through escalation and merging of systems within the environment.

Implementing ongoing threat hunting allowed for Samaritan to build a security system that worked to identify malicious behavior early. Updated systems including MSSP alerts and multifactor authentication of emails created the ability to stop malicious behavior at the end point level. NWN Carousel guided Samaritan to identify attacks at the source to eliminate the malware before extreme damages occur. The final step to implementing MDR is to build a backup plan if all else fails. This was done through training the staff to identify, report, and respond as well as regular check-ins to stay up to date with security training. NWN Carousel worked with Samaritan to implement an MDR program and build a stronger security system against malicious attacks.

"You need to test your IT response as far as various types of cyber security incidents and how your IT team responds to that. But what's so much more important is you need to expand that out to the whole organization. You need to make sure everyone in your organization understands what it looks like."

Kyle Aumell
Technical Services & Cybersecurity Management, Samaritan Medical Center

Challenge

Samaritan Medical experienced the challenge of dealing with a cyber-attack from a malicious email. "Phishing" attacks occur when a subject opens a malicious email granting malware access to sensitive information. When staff members are not properly trained to detect these attacks, it makes detecting malware more difficult. Samaritan experienced a cyber-attack that granted access to their larger domain of confidential information. Cyberattacks can be extremely difficult to detect and are even harder to recover from. It is essential for all companies to be prepared for these attacks and have the proper security guidance to identify and respond to malware.

Positive Business Outcome

NWN Carousel partnered with Samaritan to pave the way for Managed Detection and Response. NWN Carousel helped Samaritan work through a cyberattack and build a stronger security system that allowed them to avoid future attacks. The Samaritan attack opened a new conversation to cybersecurity that started with educating everyone.

Samaritan gained new security measures that had not been implemented in the past. 24/7 monitoring and awareness led to an increase in security across the board. After their attack it was clear that there were minor security issues that needed to be patched. This included multifactor authentication of emails that could have put an end to the attack before it started. Through the process of awareness and integration, NWN Carousel helped Samaritan Medical to regain access to their systems while also building a stronger MDR plan.

NWN Carousel partnered with Samaritan Medical Center to achieve the following results:

- Detection and recovery from cyberattack resulting in gained access to sensitive files
- Integration of security software and vulnerability management
- Implementation of Managed Detection and Response