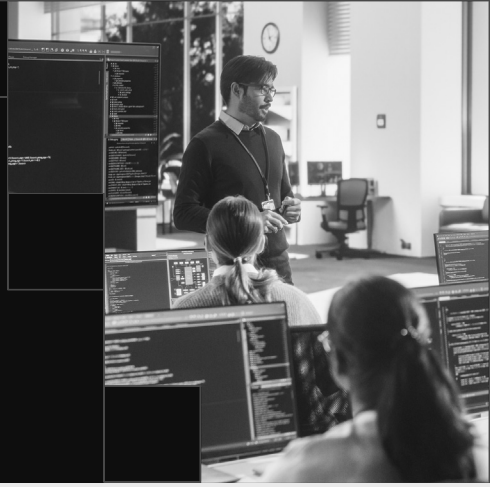
CASE STUDY

Hospital Realizes Significant Time Savings After Partnering with Binary Defense Phishing Response Service



Customer Profile

A hospital recognized by Newsweek as one of America's Best Hospitals in 2023 comprises multiple hospitals, regional health centers, and primary and specialty care facilities within a single state. Catering to over a million patients annually, this institution is committed to enhancing the well-being oftheir patients.

Challenges

Phishing attacks remain a formidable threat, especially in healthcare. Deceptive emails targeting patient data security and healthcare operations demand a stronger defense system. Hospitals, facing resource limitations and regulatory demands, rely heavily on email, making them susceptible to phishing. A successful phishing attack can lead to financial losses, breaches, and reputation damage. The small team at the Hospital faced challenges in handling a large influx of potentially harmful emails, prompting a need to reassess their focus or seek a reliable partner for responding to potential phishing attempts.

Solution

Binary Defense Phishing Response Service

Results

- 95+ hours saved every month
- Reallocated resources to critical security projects, alleviating a substantial burden on the team
- Improved security posture through a customized phishing response strategy Received tactical and strategic recommendations from a trusted advisor
- 1,963 combined SIEM alerts and User-submissions
- 40 escalations resulted in 1 requiring action from the Hospital

Challenges

Phishing attacks continue to be a profitable and successful attack vector when targeting PHI or delivering ransomware to hospitals and health systems, with potentially millions of records left compromised. Hospitals are already struggling with resource constraints, shrinking budgets, and maintaining compliance with ever-changing regulatory requirements. Relying on email as a primary form of communication is crucial to ensure the delivery of care to patients and maintaining operations. With over a million patients yearly, this dependency on email correspondence made the Hospital increasingly vulnerable to phishing attacks. If an employee fell prey to a phishing email, it could result in financial losses, data breaches, potential HIPAA violations, and damage to the hospital's reputation. The hospital's team was drowning in the sheer number of emails requiring investigations, and the daunting aftermath of a single successful email attack weighed heavily on the small security team. Hired initially to focus on high-priority security projects, these employees were redirected due to the overwhelming volume of potentially harmful emails that demanded attention, dedicating more than 60% of their time to investigating and responding to suspicious emails between Splunk alerts and user submissions. To reduce the risk of successful phishing attacks and protect patients' PHI and PII, the security team needed to either offload these tasking investigations or find the resources to effectively respond to usersubmitted emails and emails flagged by their SIEM.

Solution

The Hospital partnered with Binary Defense as a trusted advisor to develop a tailored strategy for addressing their specific phishing response requirements. This collaboration allows the security team to reclaim valuable time, enabling them to refocus on critical initiatives and reduce the mean time to response (MTTR) for malicious emails reaching their employees. The security team no longer has to conduct tedious, manual investigations but leverages the Binary Defense phishing analysts to conduct full-scope email investigations of user-submitted emails and phishing alerts generated by their SIEM. During the investigation, the Binary Defense phishing analyst conducts proactive analysis leveraging intelligence correlation and hunting to identify indications of additional

successful phishing attacks present in the hospital's environment. Following an investigation, the phishing analyst provides tactical and strategic recommendations to fortify the email attack surface of the Hospital and enhance its defensive capabilities. By finetuning detections and offering remediation recommendations, Binary Defense's skilled phishing analyst significantly minimizes risks for the Hospital, ensuring their team's peace of mind.

Results

Over the course of 5 months, Binary Defense's phishing analyst investigated 1,963 suspicious emails caught by the SIEM and user submissions. Out of 1,963 cases, the phishing analyst escalated 40, with only one requiring action from the Hospital's security team. As a result, the security team has saved over 95 hours per month since teaming up with Binary Defense. Beyond the quantifiable measures of escalated and investigated emails, the partnership with Binary Defense has brought forth a qualitative shift in the hospital's phishing response approach. Binary Defense's phishing analysts were able to customize the service to the Hospital processes and procedures. This led to the hospital's security team fully embracing the suggested remediation recommendations, instituting new procedures, and strengthening its detection capabilities. To enhance its security measures, the Hospital leveraged both Binary Defense's Phishing Response Service and Managed Detection & Response Services, adding extra layers of defense. This approach ensures the hospital remains proactive in protecting patient data and maintaining trust in its services.

Only 1 of 1,963

high-value event ID's were identified ensuring comprehensive monitoring and detection of potential threats

Binary Defense is a trusted leader in Managed Detection and Response (MDR), helping organizations across industries stay ahead of modern cyber threats. Our team of SOC analysts, threat hunters, detection engineers, and researchers works around the clock to deliver outcomes that matter: earlier threat detection, faster response, and stronger long-term security.

We take an attacker's mindset to defense, combining deep expertise with proactive tradecraft to protect what matters most.

Learn more at binarydefense.com, explore our blog for the latest insights, or follow us on LinkedIn.

600 Alpha Parkway, Stow OH 44224
sales@binarydefense.com

FORRESTER
WAVE STRONG PERFORMER 2025
Managed Detection And Response Services

BINARY DEFENSE