Hospital Augments Staff with Binary Defense Senior Analyst

Customer Profile

A hospital recognized by Newsweek as one of America's Best Hospitals 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 of their patients.

Challenges

The Hospital was frustrated with their MSSP provider due to a lack of communication and support, coupled with a capacity-constrained internal team. Facing a strict timeline for onboarding a new MDR provider, they sought a partner who would leverage existing security tools and data sources and facilitate future SIEM transitions. The Hospital also wanted to enhance threat detection with threat intel and receive access to senior analysts to support true positive investigations.

Solution

Managed Detection & Response

Co-Managed SIEM

Results

- 3,537 alerts were triaged by Binary Defense SOC resulting in 111 were escalated to the Hospitals security team
- In a single quarter 5 of the top alerts and 4 of the top 10 escalation categories were from Binary Defense's detection packages
- Access to Tier 3 analysts offering comprehensive analysis and validation for potential cyber security compromises

Challenges

With two hospital campuses, multiple regional health centers, and 50+ primary and specialty care locations throughout a single state. With more than a million patient visits a year, the Hospital has led the way to healthier futures for children through quality patient care, education, advocacy, community service, and medical discovery.

The Hospital faced strict timelines for implementing and onboarding a new MDR provider to ensure continuous coverage. There was a lack of communication with their current MSSP, coupled with limited resources, knowledge, and capacity, constrained the small security team. The security team knew they needed an MDR provider that could leverage existing security tools in their environment to avoid unnecessary technology replacements. The Hospital's environment includes data from the cloud, identity, and EDR systems, which are all ingested into Splunk. The Hospital sought external expertise to enhance threat detection capabilities with threat intelligence and required the MDR provider to facilitate future SIEM transitions. They were keen to avoid proprietary solutions and insisted that all activities be conducted within their SIEM, ensuring data ownership and the retention of custom detections, playbooks, and business-specific use cases. The Hospital evaluated seven vendors and selected Binary Defense as a finalist. Ultimately, Binary Defense was awarded the contract and identified as the ideal MDR partner.

Solution

Binary Defense, leveraging its understanding of the Hospital's current technology investments and providing guidance for transitioning to a more advanced SIEM, significantly enhanced the Hospital's threat detection capabilities and fortified its security posture. By working as an extension of the Hospital's security team, Binary Defense provides the initial triaging of alerts, tailored management, continuous tuning, and expert detection engineers to fully optimize the client's SIEM operations while lowering the total cost of ownership. With the flexibility to create custom detections and playbooks to address specific business use cases, Binary Defense instilled confidence in the Hospital to support their organizational growth. Binary Defense's SOC analysts deliver around-the-clock monitoring, ensuring alerts are enhanced with actionable intel from the Binary Defense Threat Intel Platform and equipping the Hospital with

rich context and remediation recommendations to thwart adversaries and safeguard their environment. All analyst findings and activities are documented in the associated ticket and available for client collaboration. Tickets include a summary of incident triage, how the event was detected with mappings to the Cyber Kill Chain and MITRE ATT&CK, expected business impact, and recommended next steps. Beyond triaging, monitoring, and ongoing tuning, Binary Defense strengthens these efforts through the expertise of its Analysis-on-Demand team. This team grants the Hospital access to Tier 3 analysts who offer comprehensive analysis and swift responses to alerts necessitating detailed investigation. With deep expertise in forensics and malware reverse engineering, senior analysts collect forensic artifacts crucial for the investigation. Resulting in the Hospital gaining rich context and actionable remediation recommendations, enabling effective threat management.

Results

When the Hospital partnered with Binary Defense, they aimed to enhance their cybersecurity posture, optimize the use of existing security tools, and streamline processes for detecting and responding to threats. The results of this collaboration exceeded expectations, transforming their security operations and delivering tangible value.

300+ alerts were triaged by Binary Defense SOC resulting in 111 were escalated to the Hospitals security team

The journey began with a seamless onboarding process. Within just two months, Binary Defense worked closely with the Hospital's internal security team to conduct a Splunk health check, fine-tune custom detections, and address data logging gaps. They also implemented monitoring alerts to track system performance and ensure high-value events were captured effectively. This meticulous groundwork laid a solid foundation for better detection and response capabilities.

As the Hospital continued to expand, transitioning from Splunk to Microsoft Sentinel became a strategic priority. Binary Defense's detection engineers acted as trusted advisors, collaborating with the Hospital's engineering team and serving as intermediaries with Microsoft support. The transition not only reduced the volume of alerts but also improved efficiency—within one quarter, Binary Defense's SOC triaged 3,537 alerts, escalating only 111 critical incidents to the Hospital. By reducing data ingestion costs and optimizing resource allocation, the Hospital achieved significant operational savings while maintaining robust security coverage.

During a quarterly business review, Binary Defense's impact became even more evident. Their proprietary detection rules significantly enhanced the Hospital's visibility into potential threats. Five of the top alerts and four of the top ten escalations originated from these advanced detection packages, enabling the Hospital to quickly identify and respond to anomalous activities across its infrastructure.

In one instance, Binary Defense's Analysis on Demand (AoD) team played a pivotal role in investigating a potential Business Email Compromise (BEC) incident. The Hospital received an email from a legitimate vendor asking for updated banking information for invoice payments. While the sender appeared genuine, Binary Defense's T3 analysts uncovered evidence that the vendor's account had been compromised and used by threat actors to submit fraudulent invoices. The AoD team provided detailed recommendations, including blocking the compromised domain, initiating fund recovery efforts, and conducting company-wide training to prevent future BEC attempts. Their swift response not only mitigated the immediate threat but also strengthened the Hospital's defenses against similar attacks.

Through this partnership, Binary Defense delivered more than just technical expertise—they became a trusted extension of the Hospital's security team. With improved visibility, streamlined processes, and expert support, the Hospital was able to focus on its core mission, confident in its ability to stay ahead of evolving threats.

About Binary Defense

Binary Defense is on a mission to Make the World a Safer Place by combining Threat Intelligence, Technology, and Analyst Tradecraft with industry-leading processes to provide results-driven cybersecurity services that address the most pressing security challenges facing organizations today.

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