Health System Reduces Adversary Dwell Times with Binary Defense's 24/7 MDR Service

Customer Profile

A Healthcare System dedicated to making a daily impact, offering comprehensive services in 31 medical specialties across numerous communities within a single state. This extensive network is committed to enhancing patient care and accessibility. With a team of thousands of highly skilled physicians and compassionate caregivers, the system encompasses multiple hospitals and more than 40 medical clinics and specialty centers.

Challenges

The Healthcare System was dissatisfied with their MSSP due to a lack of maturity and partnership. They required external expertise to elevate their security program and sought assistance in migrating to Sentinel. They were concerned about ingestion costs and needed support with on-prem monitoring. They required an external SOC to enhance their detection and response capabilities. It was crucial for them to find a true partner rather than just a service provider.

Solution

Managed Detection & Response

Co-Managed SIEM

Results

- Achieved 50% reduction in alert volume
- Continuous tuning efforts resulted in the completion of 19+ tuning
- Successfully transitioned from legacy SIEM to Microsoft Sentinel
- Optimized endpoint logging to ensure ingestion rates remained within budget constraints

Challenges

This Healthcare System, committed to delivering impactful care through over 30 medical specialties, serves communities across the state with a network of hospitals, clinics, and specialty centers. With thousands of skilled physicians and caregivers, their focus on quality healthcare is unwavering. However, as their operations grew, so did the complexity of their cybersecurity needs.

The Health System faced a critical challenge: they needed external expertise to elevate their security program. Migrating from their legacy SIEM to Sentinel was a top priority, but the tight timeline and complexity of the task demanded specialized support.

The team had grown dissatisfied with their previous Managed Security Service Provider, citing a lack of maturity and true partnership. They sought a co-managed solution where a trusted partner could provide Tier 2 support, optimize their SIEM to focus on critical logs and data, and reduce ingestion costs. Additionally, the Health System needed assistance with infrastructure auditing, enabling on-premises monitoring, and improving endpoint security.

Beyond technical requirements, the Health System faced organizational challenges. Their internal teams worked in silos, often at different speeds and with varying priorities. Centralization and strategic alignment were vital. They needed a partner who could integrate their security risk assessments, unify disparate functions, and create a cohesive, forward-thinking security program.

After evaluating eight vendors, the Health System narrowed their options to two finalists. Ultimately, they selected Binary Defense as their trusted partner. The decision was rooted in confidence: Binary Defense demonstrated the expertise, flexible capabilities, and partnership approach necessary to support their transition to Sentinel and build a robust, strategically aligned security architecture.

Solution

Binary Defense provided a tailored **MDR** and **Co-Managed SIEM solution**, offering the Health System a customized and expert approach to its security challenges. By utilizing and integrating with the Health System's existing security tools, Binary Defense developed a SIEM deployment plan, ensuring

a seamless transition to Microsoft Sentinel within a strict three-month timeframe. Binary Defense service includes 24/7 detection and response, supported by expert security analysts.

Beyond the vigilant monitoring of the Health System's environment, Binary Defense analysts manage a prioritized queue of alerts from the Health System's SIEM. These events are assigned to an analyst who utilizes all available data, platforms, and technologies to assess the significance, risk, and impact related to the threat. During an investigation, the analyst collaborates with the client's team to ensure all relevant data, access, and context are obtained. Binary Defense updates the case management system with activities and findings so that the Health System can engage with the investigations via the Binary Defense Platform.

To identify and address gaps in the Health System environment, Binary Defense's detection engineers conduct health checks, deploy Binary Defense Standard Rulesets, and develop customized detections and playbooks for swift detection and response. Combining the expertise of SOC analysts and detection engineers, Binary Defense offers a personalized solution that provides strategic recommendations and a customized detection strategy. This approach eases the burden of the Health System's security team independently managing the SIEM. With detection engineers bringing a combined 20 years of experience with Microsoft, Binary Defense delivered personalized detection strategies, ongoing tuning, and monitoring without increasing headcount. To enhance response times and reduce threat dwell times, Binary Defense implemented advanced customization through detection tactics, automation via Binary Defense's SOAR Platform, and personalized playbooks designed for specific incident handling procedures. These solutions were tailored to meet customers' needs, seamlessly integrating with their workflows and processes to effectively address threats to their data, organizations, and customers.

Results

The partnership between the Health System and Binary Defense delivered transformative results, significantly enhancing the organization's security capabilities and operational efficiency.

50%
reduction in alert volume was achieved by Binary Defense

Within just three months, Binary Defense guided the Health System through a seamless transition to Microsoft Sentinel. This strategic migration resulted in a 50% reduction in alert volume, cutting through noise and enabling the security team to focus on critical threats. By optimizing endpoint logging and fine-tuning data ingestion, Binary Defense helped the Health System maintain budget-friendly operations without compromising visibility. A comprehensive detection library, including 500+ carefully crafted rules and data enrichment playbooks, provided confidence in the Health System's coverage and detection strategy.

Following onboarding, the collaboration evolved into continuous improvement initiatives. Binary Defense detection engineers streamlined data flows, identified redundant logs, and conducted 19+ tuning sessions to ensure peak system performance. These efforts enabled the Health System to effectively manage ingestion costs while reallocating resources toward higher-priority tasks.

Binary Defense's SOC played a pivotal role in incident response, leveraging both automated and manual actions based on customized playbooks. For example, during a phishing attempt targeting a Health System employee, Binary Defense analysts quickly identified and mitigated the threat by purging malicious emails, blocking senders and domains, and recommending immediate steps such as resetting credentials, revoking sessions, and scanning the affected device. This swift action prevented potential financial and reputational damage while strengthening the Health System's defenses against similar attacks in the future.

Through expert guidance, proactive tuning, and seamless execution of response actions, Binary Defense empowered the Health System to achieve a robust, cost-effective, and strategically aligned security program, ensuring continued protection for its critical operations and sensitive data.

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