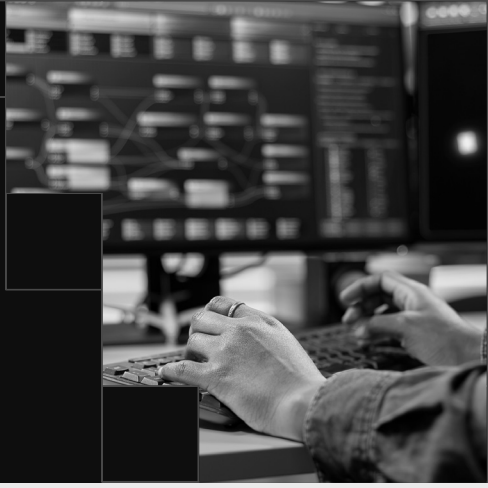
CASE STUDY

Health System Reduced Alert Volume & Logging Costs with Binary Defense MDR & Co-Managed SIEM Solutions



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 Health System security team lacked experienced professionals and planned to transition from a legacy SIEM to Microsoft Sentinel. Handling thousands of events per second, the rising ingestion costs were significant, requiring external expertise for evaluation. By seeking outside expertise, the Health System hoped their evaluation would focus migration on essential logs, reducing noise and costs. Besides high ingestion costs, they faced challenges with their underperforming legacy MDR provider. The security team sought a partner to improve posture, transition to Sentinel quickly, provide 24/7 support, and unify security operations.

Solution

Managed Detection & Response (MDR)
Co-Managed SIEM
Microsoft Sentinel

Results

- Matured security postured through continuous tuning of detections
- Gained external expertise to successfully transitioned from legacy SIEM to Microsoft Sentinel
- Achieved 50% reduction in alert volume
- Optimized endpoint logging to ensure ingestion rates remained within budget constraints

Challenges

As a renowned Health System committed to delivering top-quality healthcare services to its patients, it operates in an industry where data security and compliance are crucial. The Health System aimed to enhance its security posture to address evolving threats and meet regulatory requirements effectively. The internal security team lacked tenured security professionals and had set out to transition from a legacy SIEM to Microsoft Sentinel. The security team was handling several thousand events per second, and the rising ingestion costs were significant, necessitating an evaluation by external experts. the Health System aimed for the migration to focus solely on essential logs, thereby reducing unnecessary noise and costs. In addition to facing substantial log ingestion costs, the Health System encountered challenges from their legacy MDR provider failing to meet expectations and being unable to enhance their security posture over time. The security team sought a unified partnership to improve security oversight, transition to Sentinel within a tight timeframe, provide advanced support with around-theclock monitoring, and centralize their security visibility. With these security objectives in mind, the Health System recognized Binary Defense as the ideal partner to fulfill those requirements.

Solution

Binary Defense provided a tailored solution that combined Managed Detection and Response (MDR) with a Co-Managed SIEM service, 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 tailored a SIEM deployment plan, ensuring a seamless transition to Microsoft Sentinel within a strict three-month timeframe. The service included 24/7/365 detection and response, supported by expert security analysts. Beyond managing the initial triaging of alerts, Binary Defense brought a unique service offering within the MDR service called Analysis On Demand, providing the clients security team access to advanced analysts for in-depth investigations when additional analysis is required. Binary Defense collaborated with the Health System to identify and address gaps in their current

environment. By offering strategic recommendations and a tailored detection strategy, they alleviated the burden of managing the SIEM independently. With detection engineers bringing a combined 20 years of experience with Microsoft and 5 years with Sentinel, Binary Defense delivered personalized detection strategies, ongoing tuning, and monitoring without increasing headcount. Their expert analysts enhanced customization through detection tactics, automation, and playbooks, all designed to improve response times.

Results

The collaboration between the Health System and Binary Defense achieved remarkable outcomes. Within three months, the Health System successfully transitioned to Microsoft Sentinel, owing to Binary Defense's careful planning and execution. This transition resulted in a 50% reduction in alert volume, significantly cutting through the noise and allowing the security team to concentrate on critical alerts. Binary Defense assisted the Health System in optimizing endpoint logging to ensure ingestion rates remained within budget constraints. A thoroughly vetted detection library and approach were implemented, fostering confidence in the coverage and strategy. Once onboarding was complete, the partnership progressed Results towards SOAR integration, continuous tuning, and use case development. By minimizing the data sent for analysis, the Health System effectively managed ingestion costs and was able to reallocate resources. This was a direct result of the dedicated team of Binary Defense detection engineers identifying redundant logs, streamlining data flow, and offering ongoing support for continuous improvement to the Health Systems security posture.

50%

reduction in alert volume was achieved, significantly reducing noise and enabling the security team to focus on critical alerts.

In Conclusion

The partnership between the Health System and Binary Defense has not only addressed their immediate security challenges but also set them up for future success by establishing an agile security posture. Through this partnership, the Health System now benefits from a centralized, efficient, and highly effective security operations that is equipped to manage current threats and can proactively adapt to evolving risks. This has been achieved by implementing cutting-edge technologies and employing a team of skilled professionals dedicated to monitoring and responding to potential security breaches around the clock. By choosing Binary Defense as its security partner, the Health System can confidently focus on its core mission of delivering exceptional healthcare services to its patients, knowing that its enhanced security posture is capable of safeguarding sensitive data and maintaining compliance with industry regulations. This collaboration ensures that patient trust is upheld, and the healthcare staff can work in a secure environment, ultimately contributing to a healthier, more secure community.