CASE STUDY

Binary Defense's MDR & Co-Managed SIEM Solution Transforms Security Posture for an Industry-Leading Managed Healthcare Organization

Customer Profile

As a nationally recognized Managed Healthcare Organization serving several million members, this entity is dedicated to elevating the quality of care it delivers. Operating across multiple states, it is revolutionizing healthcare through innovative programs for its members. With thousands of employees and a responsibility to comply with evolving healthcare regulations, this organization prioritizes the security required to safeguard patient and provider data from malicious threats.

Challenges

As security remained a top priority, the internal security team faced challenges in maintaining efficient operations due to declining service quality from their MDR provider. This decline was compounded by the provider's unresponsive and opaque service approach. While contracted with the MDR provider, the security team couldn't monitor custom detections within the provider's platform and had to route them through Splunk logs, causing delays—a lack of direct communication hampered collaboration and prompt responses to alerts. Unfulfilled promises led to frustration and inefficiencies, with critical alerts often misclassified as false positives. Seeking a more responsive solution, the Managed Healthcare Organization turned to Binary Defense for tailored MDR and Co-Managed SIEM solutions.

Solution

Managed Detection & Response (MDR)
Co-Managed SIEM

Splunk

Results

- Implemented security enhancements based on Health Check Review recommendations
- 24x7x365 coverage of their environment
- Tailored detection strategy combined with Binary Defense standard ruleset
- Conducted a comprehensive analysis to identify key log sources and address detection and log source gaps

Challenges

As a nationally recognized Managed Healthcare Organization serving several million members, this entity is dedicated to elevating the quality of care it delivers to it's customers. Operating across multiple states, it is revolutionizing healthcare through innovative programs for its members. With thousands of employees and a responsibility to comply with evolving healthcare regulations, this organization prioritizes the security required to safeguard patient and provider data from malicious threats. As security remained a top priority, internal teams encountered numerous challenges in maintaining efficient security operations due to the declining service quality of their MDR provider. The decline in service by the MDR providers was further compounded by their unresponsive and black-box approach to service delivery. While under contract with the MDR provider, the Managed Healthcare Organization's security team couldn't monitor custom detections within their MDR provider's propriety platform and required the custom detections to be routed through Splunk logs, causing significant processing delays. A lack of direct communication channels impeded effective collaboration and prompt responses to security alerts, unfulfilled promises from the MDR provider led to frustration and inefficiencies and critical alerts were frequently misclassified as false positives, hampering the team's ability to respond effectively. Seeking a more responsive and flexible solution that will aid in long-term maturity posture improvement, the Managed Healthcare Organization turned to Binary Defense for its expertise in tailored MDR and Co-Managed SIEM solutions.

Solution

Binary Defense implemented a comprehensive Managed Detection and Response (MDR) and Co-Managed SIEM solution that utilizes the client's existing security tool investments. By adopting a flexible approach that leverages their existing SIEM, Splunk, Binary Defense detection engineers seamlessly integrated with the client's security team and tools. They develop a tailored detection strategy customized for the client's unique environment and industry. Alongside the tailored detection strategy, another crucial component was a health check conducted on the client's environment to identify security gaps and provide recommendations to strengthen their security posture. Binary Defense's expert detection engineers crafted customized use cases and detections within Splunk while providing continuous monitoring and triage of security alerts. This strategy ensured the SIEM's complete optimization, effectively protecting the Managed Healthcare Organization from threats. Additionally, robust communication channels were established to promote seamless collaboration between Binary Defense's SOC analysts and the Managed Healthcare Organization's internal team. With all their security challenges addressed, Binary Defense's SOC was able to provide 24/7/365 monitoring and response to emerging threats.

Results

Implementing Binary Defense's MDR and Co-Managed SIEM solution significantly enhanced the security operations of the Managed Healthcare Organization. The onboarding process began with a thorough health check conducted by the Binary Defense team to identify and address security gaps. The detection engineer team ensured all necessary applications were updated to the latest versions.

Binary Defense experts modified and enhanced existing data models and alerts for improved accuracy and efficiency. The team identified gaps in detection and log sources, offering valuable insights for improvement by recommending new logs to ensure comprehensive monitoring. After deploying Binary Defense's standard ruleset, detection engineers enhanced their capabilities by developing additional personalized security detections based on the client's risk factors. Continuous tuning and configuration management by Binary Defense experts ensured Splunk's optimal performance. Furthermore, Binary Defense accurately classified alerts, reduced false positives, and enhanced response efficiency to save the security team valuable time and resources.

In Conclusion

The Managed Healthcare Organization's partnership with Binary Defense transformed its security operations, addressing previous challenges and providing a more efficient, responsive, and customized approach to managed detection and response. The Managed Healthcare Organization continues to rely on Binary Defense's expertise to stay ahead of emerging threats and maintain a secure environment. Binary Defense's tailored MDR and Co-Managed SIEM solution has proven a valuable investment for a Managed Healthcare Organization, providing peace of mind and confidence in their security measures. With expert support and seamless collaboration, they can focus on their core business operations without worrying about security incidents or delays in response. Binary Defense continues to work closely with the Managed Healthcare Organization, ensuring their systems remain secure and up-to-date with evolving threats and technologies.

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

BINARY DEFENSE