CASE STUDY

Healthcare Technology Company Optimizes SIEM With Binary Defense's MDR & Co-Managed SIEM Solution

Customer Profile

A technology company committed to equipping healthcare professionals with cutting-edge digital tools to gain insights into their patients' vital organs. This Technology Company serves over 500,000 healthcare professionals worldwide.

Challenges

The Technology Company's data storage and security systems are crucial elements of their products, as they handle the collection, storage, and analysis of sensitive patient information. Consequently, the company must maintain the highest security standards to safeguard their customers' and patients' data. With limited resources, the company required external expertise to effectively implement, fine-tune, and monitor their SIEM.

Solution

Managed Detection & Response Co-Managed SIEM

Results

- Seamless transition of outdated SIEM to an advanced SIEM
- Successfully triaged over 31,000 alerts within just three months
- Minimized alert fatigue with just 116 escalations out of 31,000 alerts
- Achieved a unified view, extracting valuable insights from dashboards and reports

Challenges

Third-party technology companies serving the healthcare industry must adhere to the same stringent regulations governing patient data as hospitals. By offering life-saving digital tools to healthcare professionals, these companies store sensitive patient information, making hospitals dependent on their reliability for uninterrupted patient care. Faced with limited manpower, the Technology Company recognized the need to enhance its security controls to stay compliant with regulations. Consequently, they decided to upgrade to a more advanced SIEM. Their existing SIEM inundated their small team with countless alerts and false positives, overwhelming their capabilities. They sought to resolve these issues and configure a new SIEM correctly to avoid repeating past mistakes. Achieving a fully optimized SIEM required the solution provider to assist in identifying and ingesting all critical logs, creating custom detections and use cases tailored to their environment and business, and continuously fine-tuning to eliminate unnecessary noise. Just like many other organizations, particularly in healthcare, this is challenging due to limited budgets and talent shortages. These obstacles highlighted the necessity of external expertise, revealing that relying solely on internal resources would not suffice for a smooth transition

Solution

Binary Defense's Managed Detection & Response (MDR) service combined with Co-Managed SIEM emerged as the optimal solution to facilitate the Technology Company's transition from its existing SIEM to a more advanced SIEM Having implemented, tuned, monitored, and managed countless SIEMs, Binary Defense's expert detection engineers ensure seamless implementation, 24x7x365 monitoring, and a personalized detection strategy for optimal SIEM performance. Collaborating with the client's security team, Binary Defense's detection engineers pinpoint critical logs while eliminating unnecessary noise, leading to cost savings and reduced alert fatigue. The Binary Defense detection engineers excel in behavior analysis and pattern recognition to help organizations stay ahead of adversaries. Furthermore, Binary Defense collaborates closely with security teams to identify new custom detection use cases and continuously tune the system to reduce false positives. This level of collaboration enables the Technology Company's internal team to focus on critical security tasks, ultimately strengthening its overall security posture.

Results

Binary Defense played a crucial role in the transition of the Technology Company's previous SIEM to a more advanced SIEM. To enhance efficiency in the Technology Company's security operations, automation was implemented to reduce noise by incorporating threat intelligence. This allowed for the adjustment or rejection of potential alerts, streamlining the process significantly. As a result of these automated processes that decided whether to close or escalate alerts, over 31,000 alerts were effectively triaged within three months. The security team found the 116 escalated alerts from the Binary Defense SOC analysts to be actionable and valuable for compliance reporting. In addition to reducing alert fatigue, Binary Defense's implementation team developed customized dashboards, reports, and metrics that were essential for the Technology Company's security operations. These dashboards were comprised of data ingestion, source volume, ingestion trends, alerts by source, top 10 detections and alerts, and the most prevalent MITRE tactics and techniques in investigations. With these newly gained insights, the Technology Company now had a single-pane-of-glass of its environment. The partnership between the Technology Company and Binary Defense led to several significant improvements, such as enhanced visibility into security events and incidents, more efficient handling of security alerts and escalations, improved compliance reporting, and reduced workload for the Technology Company's small security team.

31,000+

alerts were triaged, with only 116 being escalated to the Technology Company's security team.

In Conclusion

With Binary Defense's MDR and Co-Managed SIEM solution, this Technology Company now enjoys a fully optimized SIEM. Binary Defense's personalized approach allows the security team to count on continuous enhancement and vigilant monitoring of their environment and security tools. Leveraging Binary Defense's proven expertise in managing an advanced SIEM, the Technology Company stays a step ahead of adversaries and safeguards critical patient data. The Technology Company can now concentrate on its primary mission of delivering top-tier healthcare technology services. Meanwhile, it assures customers that they are meeting regulatory compliance, providing them with peace of mind. With Binary Defense's assistance, this Technology Company is well-equipped to handle any potential threats and continue to provide reliable products to hospitals and their patients.

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

BINARY DEFENSE