CASE STUDY

Manufacturing Technology Leader Optimizes Sentinel With Binary Defense's MDR & Co-Managed SIEM Solution

Customer Profile

A motion and control technology company delivering advanced manufacturing solutions across diverse global industries. This Technology Company serves a broad customer base and collaborates closely with numerous vendor partners.

Challenges

The Technology Company's security team was small and siloed across SecOps, lacking both the expertise and the resources to effectively monitor the high volume of activity occurring within their environment. Their inability to manage the growing workload and the potential threats slipping through the cracks significantly jeopardized the company's overall security posture. Recognizing these challenges, the security team understood the critical need for external expertise. They sought help from specialized security consultants to alleviate the burden of managing Microsoft Sentinel alone and to ensure a more robust and comprehensive security strategy.

Solution

Co-Managed SIEM
Managed Detection & Response (MDR)

Results

- Reduced alert fatigue, decreasing the number of alerts from over 19,000 to 3,000 with 6 months of ongoing tuning efforts
- Peace of mind from around-the-clock coverage
- Cost savings from SIEM optimization through continuous tuning
- Achieved resolution of complex Microsoft Sentinel issue that had plagued the organization for months
- Successfully transitioned from an inefficient SIEM to Microsoft Sentinel in under two months

Challenges

Motion and control technology plays a crucial role in manufacturing processes across various industries. This organization faced heightened security challenges due to the critical nature of its global operations, extensive customer base, and vendor management responsibilities. The security team, which was small and siloed across IT, lacked the expertise and resources to monitor the high amount of activity in their environment. The security team did not have expertise to fully optimize Microsoft Sentinel, which directly resulted in alert fatigue. Recognizing the need for external expertise, they sought help to alleviate the burden of managing Microsoft Sentinel alone. Finding a partner capable of adapting their services to match the organization's rapid growth was crucial. The organization required an MDR partner willing to tailor services over time and act as an extension of its security team.

Solution

The Technology Company selected Binary Defense as a trusted partner to handle the implementation, ongoing tuning, and monitoring of Microsoft Sentinel. Binary Defense developed a customized MDR and Co-Managed SIEM solution to meet the specific needs of the Technology Company, alleviating the burden of managing Microsoft Sentinel alone. This gave the security team access to a 24x7x365 Security Operations Center (SOC) staffed by experienced cybersecurity professionals who could continuously monitor their environment for threats and provide aid in immediate response and remediation. In addition to expanded coverage, Binary Defense's Co-Managed SIEM solution features expert detection engineers who develop a personalized detection strategy tailored to the client's industry and environment. This approach enhances the client's ability to quickly identify and respond to threats. After the initial tuning of the SIEM,

there are regular ongoing adjustments of policies and alarms to minimize false positives and ensure that the system remains effective and adaptable to new and evolving threats. The Co-managed SIEM solution provides resource-strapped security teams with comprehensive visibility and continuous monitoring, safeguarding the client against the latest cybersecurity threats and ensuring a robust defense mechanism is always in place.

Results

Over a period of 1–2 months, Binary Defense detection engineers collaborated with the internal security team to create dashboards and logging systems, greatly improving visibility. This newfound insight was extremely valuable for the organization, which had previously lacked this level of expertise. Additionally, Binary Defense managed to lower the overall cost of log ingestion and maintenance and reduce alert fatigue through continuous tuning efforts. After six months of refinement, Binary Defense successfully Results decreased the number of alerts from over 19,000 to 3,000, alleviating alert fatigue. To further aid the organization, Binary Defense performed team maturity assessments and provided detailed security posture assessments, identifying gaps and suggesting actionable recommendations to improve overall security. The partnership between Binary Defense and the Technology Company seamlessly integrated Co-Managed SIEM services, effectively expanding the organization's team without the need for additional FTEs (full-time employees).

19,000+

alerts were tuned to just 3,000, alleviating alert fatigue on the security team

In Conclusion

For organizations in the motion and control technology sector, a robust security posture and program is nonnegotiable. The partnership with Binary Defense has enabled this Global Technology Company to strengthen its security posture through a tailored Co-managed SIEM solution, expert support, and ongoing collaboration. By selecting Binary Defense, they have not only strengthened their security operations but also forged a long-term partnership dedicated to safeguarding both their data and their customers' data from adversaries.

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

FORRESTER
WAVE STRONG PERFORMER 2025
Managed Detection And Response Services

BINARY DEFENSE