Manufacturing Enterprise Matures Security Posture Through Key Partnership with Binary Defense

Customer Profile

This Manufacturing Enterprise delivers advanced manufacturing solutions across diverse global industries. With over sixty thousand employees, the Manufacturing Enterprise serves a broad customer base of over 400,000 clients and collaborates with numerous vendor partners.

Challenges

The Manufacturing Enterprise had poor collaboration and struggled with detection strategy issues with their MDR provider – lack of tuning recommendations and quality alerts (limited context, copy/paste info). The resource-constrained team was also seeking assistance to migrate their SIEM and optimize their security data. The Manufacturing Enterprise sought a true partner who could scale services and operate as an extension of their team.

Solution

Managed Detection & Response

Co-Managed SIEM

Results

- Detection engineers pinpointed 25+ essential data connectors for log ingestion
- Over 300 custom use cases were developed
- Binary Defense successfully decreased the number of alerts from over 19,000 to 3,000, alleviating alert fatigue
- 29 custom playbooks were developed for rapid response

Challenges

This Manufacturing Enterprise delivers advanced manufacturing solutions across diverse global industries. With over sixty thousand employees, the Manufacturing Enterprise serves a broad customer base of over 450,000 clients and collaborates with numerous vendor partners.

As a global enterprise, the Manufacturer faces increasing challenges in maintaining visibility across its operations. Their environment integrates telemetry into Microsoft Sentinel utilizing Cribl from cloud, identity, EDR, and extended detection logs. With various mergers and acquisitions on the horizon, the security team needed assurance that their security program was mature and robust. They sought assistance in quickly establishing monitoring services for acquisitions. The internal security team struggled with detection strategy issues, receiving neither tuning recommendations nor quality alerts (limited context, copy/paste info) from their previous provider, resulting in poor SOC collaboration and a lack of genuine partnership. The security team, lacking resources, sought to outsource the management and migration of their current SIEM to a new one, struggling with expertise and integration issues. As a smaller, siloed team spread across SecOps, they needed a partner who could scale services over time and operate as an extension of their team.

The Manufacturing Enterprise assessed numerous vendors through a year-long RFP process and selected Binary Defense as a finalist. Ultimately, Binary Defense was awarded the RFP due to its response times (SLAs), clear and transparent communication through weekly meetings and QBR, ability to support specific log source formats, and its US-based resources that are local to the Manufacturing Enterprise.

Solution

Acknowledging the challenges faced by Manufacturing Enterprises, Binary Defense provided a comprehensive **MDR** and **Co-Managed SIEM** solution tailored to the client's distinct needs, environment, and existing security investments. The solution was customized to align with the client's specific risks and business requirements by understanding their environment and acting as an extension of their team to build out personalized use cases, rules, and playbooks. Binary Defense Detection engineers facilitated the transition from legacy SIEM to Sentinel and played a key role in planning and architecting Cribl to support the security team's implementation efforts.

To identify any existing security gaps, the Binary Defense team conducted an in-depth health check review of the client's security infrastructure, offering actionable recommendations to close security gaps. During onboarding, Binary Defense ensured that its threat intelligence feeds were integrated into its analytical threat hunts and that the Binary Defense 's SOAR platform effectively ingested alert data from their environments. This gave SOC analysts a comprehensive and unified perspective for monitoring their environments.

Binary Defense's proprietary standard ruleset was implemented within Sentinel, utilizing both signature and behavior-based detections. This deployment leveraged insights from our Threat Intelligence, Threat Hunting, Threat Research, and Incident Response teams, ensuring it was meticulously fine-tuned to reduce noise and enhance detection accuracy. Additionally, the detection engineers collaborated with the Manufacturing Enterprise security team to create watchlists for VIPs, critical servers, and privileged users to assist in the tuning process. Custom playbooks and workflows were developed to handle alerts from the client's EDR, streamlining the incident response process. The team also leveraged Binary Defense's threat intelligence feed integrated into the client's system, deploying rules to alert on Indicators of Compromise (IOCs).

Results

300+ custom use cases were developed

The implementation of Binary Defense's MDR solution led to substantial enhancements and measurable outcomes for the Manufacturing Enterprise. Binary Defense served as trusted advisors and liaisons with Microsoft, providing essential technical support during the Manufacturing Enterprise's transition from legacy SIEM to Sentinel.
In collaboration with the internal security team, detection engineers pinpointed 25+ essential data connectors for log ingestion. They integrated threat feeds curated by Binary Defense threat feed. Additionally, they implemented logging to detect when endpoints ceased logging and built out multiple dashboards for the internal security team. To ensure comprehensive monitoring and threat detection, Binary Defense developed and configured 29 playbooks for rapid response. They supported custom parsing and data connector development while deploying and fine-tuning the Binary Defense standard detections, Sentinel OOTB ruleset, and over 300 custom use cases provided by the Manufacturing Enterprise's security team. This tailored detection strategy provided thorough monitoring and identification of potential threats. By creating personalized playbooks and workflows, we enhanced the efficiency of alert management, significantly reducing the time and effort needed for investigations.

For seamless integration with the client's team, Binary Defense delivered continuous support, monitoring, and expertise, enabling the internal security team to concentrate on strategic initiatives. After just six months of refinement, Binary Defense successfully decreased the number of alerts from over 19,000 to 3,000, alleviating alert fatigue. To enhance long-term security maturity, they configured and supported the development of automation rules for further enrichment and planned the deployment of Cribl for future optimization of log ingestion.

To further aid the organization, Binary Defense performed maturity assessments and detailed their security posture, identified gaps in security, provided actionable recommendations to improve overall security, and worked closely with key partners to incorporate any key findings from tabletop exercises. The partnership successfully addressed security gaps and enhanced the Manufacturing Enterprise security team by rapidly deploying monitoring services during acquisitions, eliminating the need for additional security personnel.

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