Hygiene Manufacturer Enhances Detection Capabilities with Binary Defense's Expertise and MDR Plus Solution

Customer Profile

As a Global Hygiene Manufacturer with a workforce of over 3,000 employees spread across six continents, this organization has established a significant presence in North America, Europe, and Asia. With a commitment to quality and innovation, the manufacturer produces a diverse range of goods that cater to the needs of over a million customers worldwide.

Challenges

Serving numerous clients across continents presents unique security challenges, as adversaries exploit vulnerabilities for financial gain. The Hygiene Manufacturer's small security team was particularly concerned about protecting PHI and PII, especially with hospitals among its clients. Operating in an environment that integrates data from the Cloud, Identity, and two EDRs into their SIEM, they faced unidentified security gaps. To address this, they needed to swiftly implement a SIEM system and enlist a trusted advisor to enhance detection strategies. They sought external expertise to identify critical log information and outsourced knowledge for SIEM implementation and roadmap development.

Solution

Managed Detection & Response

MDR Agent - BDVision

Results

- Four targeted health checks identified critical security gaps and immediate improvement areas.
- 85% of the environment tuned within three weeks, driving rapid operational efficiency.
- 24/7 SOC monitoring and response provide clarity and peace of mind with proactive threat management.

Challenges

As a Hygiene Manufacturer with over 3,000 employees across six continents, including North America, Europe, and Asia, this Manufacturer produces goods that serve over a million customers. Serving a large number of clients across multiple continents presents unique security challenges, as adversaries aim to exploit vulnerabilities and target employees for financial gain. The Hygiene Manufacturer's security team, small and stretched thin due to competing IT and security priorities, was particularly concerned about protecting PHI (Protected Health Information) and PII (Personally Identifiable Information), especially with the health systems among its many clients. The security team, operating in an environment that integrates data from the Cloud, Identity, and two EDRs into their SIEM, faced unidentified security gaps that could potentially lead to a breach. To address this, the company needed to swiftly implement a SIEM system and enlist a trusted advisor to enhance its detection strategy. They sought external expertise to identify critical log information and outsourced the necessary knowledge for SIEM implementation and roadmap development.

Additionally, they required guidance on selecting a suitable SIEM to integrate with their on-premises infrastructure, considering bandwidth and traffic concerns with a limited cloud presence. The organization faced the challenges of constant threat evolution, training needs, staffing shortages, and skills gaps in this high-demand field, all while adapting to evolving security and compliance demands. The company wanted co-management visibility into the SIEM with search, report, and dashboard capabilities. The security team prioritized the capability to create and develop custom rules within the SIEM, highlighting flexibility and collaboration as the key requirements for the MDR solution they sought.

Solution

Binary Defense was selected for its capacity to fulfill the necessary flexibility and customization requirements, along with its robust partnership with the manufacturer's current security consultant, TrustedSec. The company recognized the advantage of combining TrustedSec's tabletop exercises with Binary Defense's capability to convert critical findings into enhanced detections, strengthening its defense strategy.

As a trusted leader in security operations, Binary Defense offers a personalized Open XDR approach to **Managed Detection and Response.**

This solution provides co-management of the client's preferred SIEM, alleviating the challenges of managing it alone while delivering expert guidance to refine their detection strategy. Binary Defense's personalized MDR solution enables expert detection engineers to collaborate closely with clients' security teams. Together, they develop customized detections, industry-specific use cases, tailored playbooks and health checks to ensure complete optimization of their SIEM.

Beyond leveraging the client's existing security tool investments, **MDR Plus** clients enjoy enhanced detection and response capabilities through **Binary Defense's MDR Agent, BDVision**. BDVision gives clients real-time detection and containment with sophisticated behavior-based threat detection and managed deception capabilities, ensuring rapid identification and neutralization of threats. Customers benefit from industry-leading observability, contextual feedback, early-stage attack detection, and advanced malware disruption.

Alongside enhanced detection and response capabilities, clients benefit from access to a team of experts who guide them in transitioning security tools as their security program scales and matures. Binary Defense's Detection Engineers are experts in Microsoft technologies for clients like the Hygiene Manufacturer, who heavily rely on Microsoft tools. They possess a deep passion and extensive skills in intelligence gathering, log analysis, and the development of both signature and behavioral detection rules. With a combined 20 years of experience in Microsoft environments and 5 years specializing in Microsoft Sentinel, their expertise is backed by industry-recognized certifications such as AZ-500, SC-200, AZ-900, MS-500, and MCSA/MCSE. Clients benefit from their proficiency in behavior analysis and pattern recognition, ensuring they stay ahead of adversaries and protect their environments with dedicated precision.

Results

85%

of the Manufacturer's environment was **tuned within the first three weeks of onboarding**

The Hygiene Manufacturer's partnership with Binary Defense yielded significant results. Binary Defense provided strategic recommendations in collaboration with a third party that implemented Sentinel for the Manufacturer. Guided by Binary Defense's Detection Engineers, Binary Defense completed a series of sessions within a month to ensure Sentinel's optimal performance and proper log ingestion. During onboarding, tailored playbooks and procedures were crafted to enhance response capabilities, providing comprehensive automated and manual response instructions for Binary Defense SOC analysts. Further detection engineering efforts resulted in deploying over 240 detections, including 231 custom Binary Defense detections, and conducting four health checks to identify gaps in logs, events, and detection coverage. Existing detections were transformed to include additional telemetry and details for improved investigation.Binary Defense Detection Engineers deployed the Standard Binary Defense Proprietary Ruleset, reduced false positives, tuned the environment by 85% within the first three weeks of onboarding, evaluated log ingestion, and identified parsing improvements while integrating the Binary Defense Threat Intel Feed.

The security team achieved greater clarity and peace of mind from Binary Defense's around-the-clock SOC monitoring, detection, investigation, and response efforts. With Binary Defense analysts handling triaging, monitoring, and continuous tuning of detections, more time was freed for mission-critical projects and valuable staff development.

By partnering with Binary Defense, the Hygiene Manufacturer significantly strengthened its security posture, improving detection capabilities and operational efficiency. This partnership allowed the security team to focus on mission-critical projects and development, while Binary Defense ensured continuous monitoring and response to potential threats.

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