Binary Defense's MDR Solution Safeguards Global Manufacturer Amidst Numerous Mergers and Acquisitions

Customer Profile

Founded over a century ago, this Global Manufacturer has evolved into a leading family-owned manufacturing and distributing enterprise with a presence across 20+ locations worldwide. Their commitment to producing high-quality goods while fostering an excellent workplace and supporting the communities they operate in sets them apart in the industry.

Challenges

Their rapid expansion and acquisitions have increased exposure to sophisticated threats, requiring a strong and adaptive security strategy. The Manufacturer faced significant challenges due to the lack of a dedicated SOC and an immature security program. Their team was stretched thin, handling both IT and security tasks. The infrastructure was fragmented, with data from the cloud, on-premises servers, and multiple EDRs integrated into their SIEM. Without a centralized SOC, there were vulnerabilities due to inadequate alert investigations that could lead to a breach. The security team felt blind to threats as they lacked the capacity to properly investigate all alerts.

Solution

Managed Detection & Response

MDR Agent - BDVision

Results

- Implemented 57 targeted filtering rules to significantly reduce log ingestion costs, optimizing resource use for greater cost efficiency.
- Over 40 custom detections built by Binary Defense Detection Engineers bolstering client defensive capabilities.
- Expanded protection for the manufacturer’s IoT environment by integrating Managed Network Detection and Response through our Extrahop partnership, effectively mitigating potential risks.

Challenges

Founded over a century ago, this Global Manufacturer has evolved into a leading family-owned manufacturing and distributing enterprise with a presence across 20+ locations worldwide. Their commitment to producing high-quality goods while fostering an excellent workplace and supporting the communities they operate in sets them apart in the industry. Their rapid expansion and acquisition activities have increased exposure to sophisticated threat actors, necessitating a robust and adaptive security strategy.

The Manufacturer faced significant security challenges due to the absence of a dedicated SOC and an immature security program. Their team was stretched thin, juggling both IT and security tasks. The Manufacturer's infrastructure was fragmented, comprising data from the cloud on-premises servers and multiple EDRs integrated into their SIEM. The absence of a centralized in-house SOC created significant security vulnerabilities, chiefly due to inadequate alert investigations that might have resulted in a breach. The security team felt blind to threats because they didn't have the bandwidth to properly investigate all alerts coming from their security tools. Rapid growth and recent acquisitions further strained the team, hindering their ability to deploy agents on critical servers and endpoints swiftly. Their team didn't have the expertise to develop robust detections within their SIEM. The internal team urgently required a comprehensive strategy to establish adequate security measures and a proactive threat detection program to reassure newly acquired entities and bolster their security posture.

Solution

Binary Defense was selected as the ideal MDR provider due to its ability to capitalize on its partnership with the Manufacturer's existing security consultant, TrustedSec. As TrustedSec is Binary Defense's sister company, this collaboration enabled the Manufacturer to integrate TrustedSec's services with Binary Defense's expertise seamlessly. This synergy translated key insights into advanced detections, fortifying their defense strategy.

Binary Defense crafted a customized solution to meet the Manufacturer where they were in their security journey. The Binary Defense team optimized the Manufacturer’s existing security tool investments while advising on new tools to address security gaps. Guiding SIEM migrations,

Binary Defense has the ability to aid in the transition from an on-premises SIEM to a cloud-based SIEM. Many customers like the Manufacturer benefit from **MDR Plus**, which includes advanced detection and response capabilities of **Binary Defense's MDR agent, BDVision.** Binary Defense was able to layer BDVision over existing EDR systems to enhance real-time detection and containment capabilities. This solution offers behavior-based threat detection, malware disruption, and managed deception features, complementing the Manufacturer's security tools to achieve superior security outcomes.

To give the Manufacturer peace of mind while reducing alert fatigue, Binary Defense SOC analysts provide 24/7 monitoring, escalating only high-fidelity alerts to the client's security team. The Manufacturer benefited from analytical threat hunts fueled by threat intel feeds through the BD Threat Intelligence Platform and BD's Standard Proprietary Ruleset for detecting evasive threats. High-fidelity alerts are escalated through continuous refinement of detections and implementing a customized detection strategy. These efforts are a direct result of Binary Defense's expert detection engineer's aiding in developing watchlists for VIPs, critical servers, and users/groups.

Using pre-built and customized playbooks, SOC analysts execute automated and manual response actions approved by clients. To ensure the investigation and response efficiency of SOC analysts, Binary Defense leverages the Binary Defense SOAR platform to ingest metadata (alert data) from customer environments, offering analysts a single pane of glass for a comprehensive review, with correlation logic integrated into customers' SIEMs. When deeper investigation is needed, clients can request Analysis on Demand (AoD). Senior analysts use tools like Binalyze to deploy agents on client endpoints, collecting forensic artifacts relevant to investigations. This automation streamlines the digital forensics process, saving time and resources while ensuring precise and thorough analysis of digital evidence.

Results

The partnership with Binary Defense yielded impressive results for the Global Manufacturer. Collaborating with the team, Binary Defense fortified defenses around their OT environments and facilitated their transition from on-premises to the cloud, accommodating their growth effectively. Binary Defense ensured BDVision deployment during each acquisition, covering every endpoint and critical server. BDVision was run alongside MS Defender to provide enhanced deception capabilities defending against sophisticated threat actors.

57 filtering rules were implemented by the Binary Defense Detection Engineers to reduce log ingestion costs

Binary Defense senior analysts provided crucial support for potential cybersecurity breaches , conducting thorough investigations. They bridge the gap between MDR and IR by examining suspicious events that could significantly impact the Manufacturer's business operations. This gave the Global Manufacturing company's security team access to advanced capabilities, skills, and experience. During onboarding, detection engineers developed detections that were added to the OTX IOC feeds, with daily antivirus updates and authored alarm rules. Additional efforts included the Binary Defense team identifying critical log sources, deploying the Standard BD Proprietary Ruleset, providing ongoing tuning to significantly reduce alarm volume per client request significantly, and creating custom 40 detections, enabling 28. Throughout numerous health checks, Binary Defense assessed sensor connections, reviewed license subscriptions, ensured webUI responsiveness, analyzed event flow, checked filter rule errors and warning messages, associated new agents with assets, and optimized connectivity in specific apps. With a focus on reducing log ingestion costs, Detection Engineers implemented 57 filtering rules to achieve this.

The Binary Defense team enhanced the Manufacturing Company's security maturity. It mitigated risk by expanding the scope of its IOT Environment, leveraging partnerships for Managed Network Detection and Response. The constant collaboration between all involved parties addressed immediate security challenges and laid a foundation for long-term security resilience and maturity. By integrating Binary Defense's MDR Plus solution, the Manufacturer enhanced its security posture, safeguarded its operations, and supported its growth ambitions with a more secure and efficient framework.