Binary Defense Helps Automotive Manufacturer Strengthen Global Security with Advanced SIEM

Customer Profile

Operating in the competitive world of global automotive manufacturing, this well-established enterprise has operations spanning five continents. Dedicated to expanding its reach within the automotive channel, this Global Automotive Manufacturer transformed from a single store into an international distributor of automotive parts serving thousands of customers.

Challenges

This Global Automotive Manufacturer faced significant security challenges due to a small, inexperienced internal team and complex systems. The Manufacturer encountered security issues threatening efficiency and customer trust. With new regulations and sophisticated threats, they needed a solution to protect their data and systems. Complexity stemmed from acquiring multiple companies with varying system integrations and security tools, complicating standardization. To meet regulatory demands and assure customers, the team needed a more resilient environment. The outdated SIEM overwhelmed the team with difficult alerts and rules. Realizing the need for a more advanced SIEM, they sought an MDR partner to facilitate a seamless transition.

Solution

Managed Detection & Response (MDR)

Co-Managed SIEM

Results

- Detection Engineers collaborated to configure it's AWS environment, ensuring compliance with SIEM logging requirements
- Achieve insight into two domains in just 2 months
- Binary Defense's SOC effectively eliminated the need for an additional headcount for the Automotive Manufacturer
- Critical logs were fully transitioned and operationalized within 8 weeks

Challenges

This Global Automotive Manufacturer faced significant security challenges due to a small, inexperienced internal team and complex, fragmented systems. Operating in the competitive world of global manufacturing, this well-established company has operations spanning five continents.

The Global Automotive Manufacturer encountered several security hurdles threatening operational efficiency and customer trust. With new regulatory requirements and an increasingly sophisticated threat landscape, they needed a robust solution to safeguard their data and systems.

This lack of standardization made finding common ground and implementing uniform security measures across the board challenging. Faced with new regulatory requirements, the security team frequently spent time filling out questionnaires to assure customers of their security posture. They needed to build a more resilient environment to meet these expectations and maintain customer trust.

The Manufacturer's internal security team was small and relatively inexperienced. With only a handful of team members to support five global locations, they struggled to manage a rapidly growing number of security tools and integrations.

The environment's complexity stemmed from the acquisition of multiple different companies, each with varying levels of system integration and differing security tools. Their legacy SIEM in place was not equipped for the current state of their environment and overwhelmed the small team with alerts and rules that were difficult to manage. The internal security team realized the pressing need to transition to a more advanced SIEM solution but was daunted by the time and resources required for such a move. They realized the importance of enhancing its security posture and looked for an MDR partner to facilitate a seamless SIEM transition to achieve this objective.

Solution

The Global Automotive Manufacturer partnered with Binary Defense to address these challenges by implementing a comprehensive **Managed Detection and Response (MDR)** and **Co-Managed SIEM solution**. Using a consultative approach, Binary Defense ensured the solution was tailored to meet the client's specific needs and challenges. Intending to replace their legacy SIEM, Binary Defense identified a more advanced SIEM that had a data-first approach, providing unmatched visibility across the client's environment, as the ideal SIEM to transition to.

This advanced SIEM's zero-lag performance provided the Global Automotive Manufacturer with real-time results and analytics, significantly reducing MTTR. This enabled precise identification of threat actors with full context, delivering the complete attack narrative through ready-to-use content, automation, and AI-driven threat detection and investigation combined with Binary Defense's expert SOC analyst. By applying an attacker's mindset, Binary Defense developed a personalized strategy that combined cutting-edge technology with expert human oversight. This included ongoing tuning, proactive monitoring, and customized detections to protect the Global Automotive Manufacturer's business. Binary Defense's deep expertise in SIEM implementation proved critical in transitioning from the legacy SIEM to the more advanced SIEM platform. The Binary Defense detection engineers handled all deployment aspects, from initial configuration to critical logs to tool integration.

The MDR and Co-managed SIEM solution provided continuous monitoring and management, alleviating the burden on the manufacturer's internal team. This gave the security team 24x7x365 threat detection and response, ensuring rapid identification and mitigation of security threats. Binary Defense also focused on empowering the Global Automotive Manufacturing internal team to optimize and improve their SIEM through knowledge transfer. This enabled the team to build operational alerts, increasing their visibility into internal IT activities and misconfiguration.

Results

The partnership with Binary Defense yielded impressive results for the manufacturer within just two months. Binary Defense achieved log integration and visibility for the Global Automotive Manufacturers and their sister company. This quick turnaround was crucial in enhancing their overall security posture. With an efficient deployment process, critical sources were operational within eight weeks. The ongoing support and continuous tuning efforts ensured that the SIEM system remained optimized and effective. The Global Automotive Manufacturer engineering team gained the knowledge and skills to create internal alerts within their new SIEM. This capability allowed them to monitor internal IT activities and misconfigurations without overburdening the Security Operations Center (SOC).

92 of 1,885

alerts were escalated to the Global Automotive Manufacturers security team after being triaged by Binary Defense analyst

As optimization continued for just over three months, Binary Defense's security analysts triaged 1,885 alerts and escalated only 92 to the manufacturer's security team. This significant reduction in alert volume allowed the internal team to focus on strategic initiatives and reduced the risk of alert fatigue. By partnering with Binary Defense, the manufacturer saved the cost of hiring an additional headcount. The advanced use of the SIEMs capabilities enabled the internal team to concentrate on their core security needs, while Binary Defense handled continuous monitoring and threat response.

In Conclusion

The manufacturer's decision to partner with Binary Defense proved to be a game-changer for their security operations. The combination of an advanced SIEM, MDR, and a Co-managed SIEM solution addressed their immediate challenges and laid the foundation for a more resilient and efficient security posture. The manufacturer is well-positioned to meet future security demands with enhanced visibility, reduced alert management burden, and improved internal capabilities.

The ongoing collaboration with Binary Defense will continue to evolve and adapt to the Global Automotive Manufacturer's needs. The following deployment phase will expand visibility to other business units, further strengthening their security framework.

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