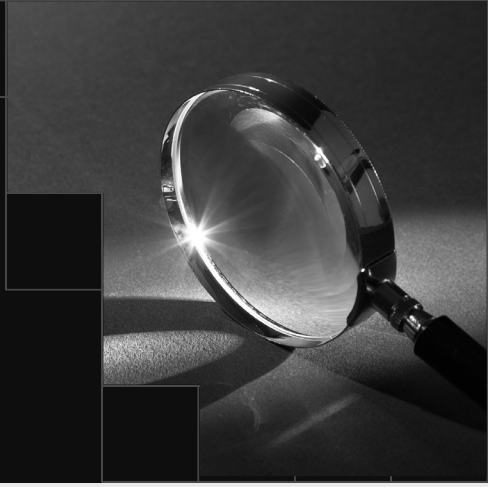
CASE STUDY

Technology Company Reduces Blind Spots and Leverages Existing Security Tool Investments with Binary Defense's MDR Solution



Customer Profile

The Technology Company provides software and services that help corporations gain a competitive advantage from their IP. With over 1,000 employees, the Technology Company's software is used by over a million corporations all over the world.

Challenges

The Technology Company had no previous MDR provider, no internal SOC, and a small team juggling multiple responsibilities. They sought a MDR provider capable of scaling alongside their organization while enhancing their current security posture. The internal team at the Technology Company faced limitations in both bandwidth and expertise, preventing them from thoroughly investigating and addressing security incidents as they arose. They needed a provider with deep security expertise and the ability to collaborate effectively with their team and tools in a tailored manner.

Solution

Managed Detection & Response (MDR)
Co-Managed SIEM
Managed – EDR

Results

- Over four months, Binary Defense triaged over 40,000 alerts, escalating only 75 to the internal team
- Implemented 60+ alert filtering rules to reduce alert fatigue and lower ingestion costs
- Improved detection strategy with the development of over 40 custom detections

Challenges

This Technology Company provides software and services that help corporations gain a competitive advantage from their intellectual property. With over 1,000 employees, the Technology Company's software is used by over a million corporations all over the world.

As the organization expanded and its client base grew the small security team began evaluating the need for a Security Operations Center (SOC), considering both an in-house SOC or outsourcing through a Managed Detection and Response (MDR) provider. The small security team managed various responsibilities, lacking a dedicated individual for detection and response efforts. The internal team at the Technology Company faced limitations in both bandwidth and expertise, preventing them from thoroughly investigating and addressing security incidents as they arose. They needed a provider with deep security expertise and the ability to collaborate effectively with their team and tools in a tailored manner.

The Technology Company was worried about blind spots and limited detection capabilities in their security tools and environment, which could allow attackers to go undetected and breach their defenses. They sought a provider that could create custom escalation procedures and response playbooks to support their global operations. They aimed to enhance their SIEM by filtering events, crafting precise detections, and refining the system to reduce log ingestion costs. At the time, they had not established any proactive alerts within their SIEM and relied solely on the default detections included when they initially purchased their legacy SIEM years ago. The team had not invested time in developing new detections and lacked a tailored detection strategy. Consequently, the Technology Company recognized the need to advance its security program. This prompted the team to search for an MDR provider that could scale with their organization while strengthening their security posture.

Solution

Binary Defense developed a customized Managed Detection and Response and Co-Managed SIEM solution tailored to the specific needs of the Technology Company, easing the burden of managing their SIEM alone. The Technology Company benefited from 24/7 SOC monitoring, alert triaging, and continuous detection tuning, providing comprehensive threat surveillance and response support every day, including weekends and holidays.

With Binary Defense SOC handling alert triage and investigations, the security team gained actionable alerts from investigations enriched with threat intelligence from the Binary Defense Threat Intel Platform.

Collaboration between the Binary Defense analysts and the internal security team ensured that all relevant data, access, and context were meticulously documented. The internal security team has complete visibility and data ownership due to the Binary Defense analysts working within their SIEM. The internal security team had the ability to actively engage with investigations and Binary Defense analysts through the BD Platform. In addition to analysts acting as an extension of the Technology Company's team, Binary Defense's MDR solution enhanced detection and response coverage through detection engineering tuning efforts, ensuring a robust detection strategy.

Binary Defense's detection strategy was precisely tailored to the Technology Company's industry, environment, and specific needs. By fortifying defenses and identifying threats early in the attack lifecycle, detection engineers performed a comprehensive visibility gap analysis to assess the Technology Company's protection profile and unique use cases, refining detection methods as necessary. The internal security team gained significant advantages, including customized detections, targeted business use cases, personalized playbooks, and the identification of critical log sources. These enhancements not only reduce alert fatigue but also help lower log ingestion costs. Post-onboarding, continuous adjustments to policies and alarms ensure minimal false positives while maintaining the system's effectiveness against evolving, sophisticated threats.

Results

The Technology Company significantly benefited from Binary Defense due its analysts, Detection Engineers, Customer Success Manager, Technical Account Manager and Executive Sponsor all acting as trusted advisors. They offered strategic recommendations to address security gaps and maximized the use of existing security tool investments. The Binary Defense team developed a customized solution aligned with the internal security team's specific needs and requirements while seamlessly adapting to their unique workflows. The Binary Defense worked as an extension of the internal security team to develop customized playbooks and structured call trees for around-the-clock monitoring.

60+

alert filtering rules were implemented to reduce alert fatigue and lower ingestion costs

By efficiently triaging alerts, Binary Defense saved the Technology Company's limited security team time and resources. Over four months, Binary Defense triaged over 40,000 alerts, escalating only 75 to the internal team. At the same time, Binary Defense detection engineers collaborated with the internal team to reduce alert fatigue and lower ingestion costs by implementing 60+ alert filtering rules. Additional Detection Engineer efforts included conducting multiple health checks, deploying the Standard BD Proprietary Ruleset, implementing the BD SOAR Platform, incorporating threat intelligence feeds, identifying critical log sources, and creating over 40 custom detections

This tailored approach enabled the Binary Defense team to adapt and scale seamlessly with the Technology Company, ensuring continuous analyst coverage every hour of daily. The Technology Company's security team gained peace of mind knowing uptime and data fidelity were protected through their strategic partnership with Binary Defense.

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

BINARY DEFENSE