



Global Lab Testing Company Transforms Security Posture With Binary Defense MDR Service



Customer Profile

A global leader in providing laboratory testing services to a diverse range of industries. As a leader in laboratory testing, this company employs thousands of individuals across hundreds of locations, serving a vast customer base with the mission of making the world a better place.

Challenges

This Laboratory Testing Company faced several significant challenges: numerous unsupported legacy systems posing considerable risks, a shortage of manpower and expertise, shrinking budgets, and the critical need to comply with regulatory requirements. These issues created a formidable task for the internal security team that had to be addressed. It became evident to the Global Testing Company that their current MSSP lacked the necessary skills and knowledge to aid their team in tackling these challenges, creating insufficiencies that led to gaps in their environment.

Binary Defense Solution

Managed Detection & Response (MDR)

Results

- ~ 8,000 triaged alerts and over 200 investigations were conducted on behalf of the security team
- Successfully implemented a global security posture, consolidating technology for enhanced visibility and awareness and reducing overall risk exposure
- Increased coverage and visibility by deploying an EDR tool on over 1,400 endpoints

Challenges

As a global leader in providing laboratory testing services, this company serves a wide range of industries, requiring a strong and mature security posture. Facing increasing pressure to protect their data from adversaries and tackle numerous security challenges led the Global Testing Company's security team to seek a new MDR provider. They encountered significant risks from a large number of unsupported legacy systems, a lack of manpower and expertise, shrinking budgets, and the need to meet regulatory requirements. It became clear that their current MSSP (Managed Security Services Provider) lacked the necessary skills and knowledge to help them address these challenges, which led to gaps in their security environment. The company also struggled with inconsistency across their organization and a lack of visibility into their environment, hampering their security efforts and leaving them vulnerable to potential threats. With a small security team and limited resources, they were overburdened with the extensive tasks required to keep the organization secure. These issues pushed the security team to seek a new MDR partner. Additionally, leadership pressure necessitated the appointment of a new security advisor due to the additional auditing and regulatory standards requirements, which hindered the closure of several major enterprise contracts. A trusted advisor was needed to help transition away from ineffective technology, improve visibility, and ensure that security measures complied with regulatory requirements.

Solution

Binary Defense was chosen as the ideal MDR partner due to its ability to grow and adapt in tandem with the Laboratory Testing Company's team and organization. The **Managed Detection and Response (MDR) service** supports resource-limited teams by efficiently triaging, analyzing, prioritizing, and performing comprehensive chain analysis on all security events, regardless of the alert volume. Expert analysts collaborate with security teams to alleviate alert fatigue by maximizing the effectiveness of their current security tool investments. They achieve this by identifying critical logs, developing a customized detection strategy, and providing ongoing tuning. Through optimizing security tools, analysts can convert

raw alerts into clear, actionable data enriched by contextual investigations, giving security teams vital information to streamline their threat response. Additionally, small security teams gain 24x7x365 coverage through a dedicated Security Operations Center (SOC), providing constant monitoring, threat detection, and actionable guidance to enhance security posture and address the root cause of recurring incidents. Through enhanced support from Binary Defense's SOC, security teams can concentrate on other vital tasks and initiatives without being overextended.

Results

Binary Defense worked as an extension of the client's security team to achieve its objectives, including implementing a global security posture, consolidating technology for enhanced visibility and awareness, and reducing overall risk exposure. Over 6 months, Binary Defense analysts triaged nearly 8,000 alerts and conducted thorough investigations into over 200 cases on behalf of the security team. The expert analysts from Binary Defense collaborated with the security team to create a long-term security

8,000+
alerts were triaged and over 200 investigations
were conducted on behalf of the security team

roadmap, deploying Microsoft Sentinel and improving the security team's environment and monitoring capabilities. They provided deep expertise and the flexibility to adapt to changing circumstances and provide effective solutions that evolve with the organization's needs. Binary Defense optimized the Global Testing Company's EDR (Endpoint Detection and Response) by implementing new security rules, training the internal team extensively, and transferring crucial knowledge. This comprehensive approach resulted in improved coverage and enhanced protection for 1,400 endpoints, significantly boosting the organization's cybersecurity posture. In addition to increased visibility across over a thousand endpoints, the Binary Defense team successfully transitioned the Global Testing Company from an ineffective SIEM to Sentinel. This process involved the Binary Defense team working alongside the internal security team to develop a personalized detection strategy tailored to the organization's unique needs. Acting as a knowledgeable partner, Binary Defense fine-tuned the Global Testing Company's environment, enhancing its ability to detect and respond to threats quickly and more effectively.

In Conclusion

Ensuring compliance demands dedicated effort and expertise, which many organizations often lack. Leadership teams must balance cost control with robust security measures, presenting a common challenge for companies like the Global Laboratory Testing Company. Managing budget constraints while implementing comprehensive security solutions is crucial. Partnering with an MDR provider like Binary Defense that delivers value and expertise is vital to transforming your security posture. The right partner can greatly enhance your organization's security capabilities by addressing pain points and leadership concerns and achieving strategic security goals, all while focusing on your team's desired outcomes.



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