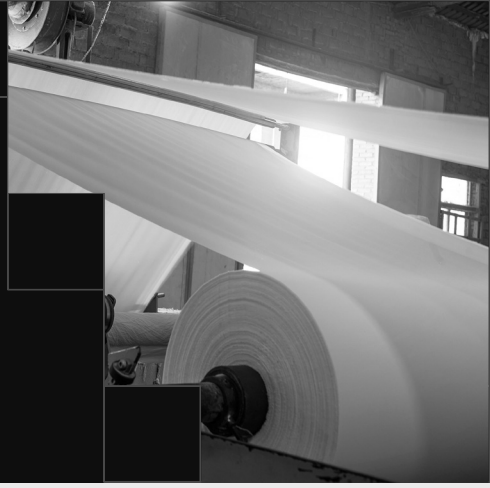
CASE STUDY

Global Paper Manufacturer Optimizes Security Operations with a Personalized MDR & Co-Managed SIEM Solution from Binary Defense



Customer Profile

Situated at the heart of innovation, this Global Paper Manufacturer excels in creating social expression products that celebrate special moments and milestones. With decades of experience and a commitment to quality, they have established a prominent position in their industry. Offering a diverse product range, customers can find what they need both in-store and online, with the convenient option of curbside pickup.

Challenges

The company faced major internal challenges with its previous MDR provider, prompting a security operations overhaul. The provider's platform was overwhelmed with alerts, causing "alert fatigue" and inefficiencies. The team had to create custom rules to manage alerts, limited by the provider's inability to integrate with custom playbooks or detections. This forced the team to conduct investigations themselves, which were complicated by their lack of expertise in Microsoft Sentinel. The security team at Global Paper Manufacturer recognized the need for a genuine partnership with an MDR provider and found Binary Defense to be the perfect solution.

Solution

Managed Detection & Response (MDR)
Co-Managed SIEM
Microsoft Sentinel

Results

- 24x7x365 coverage of their environment
- Reduced the time and effort required for investigations by implementing workflows and processes
- Developed custom playbooks to decrease response times and ensure efficient handling of alerts
- Decreased alert noise by fine-tuning Sentinel ruleset and creating custom watchlists

Challenges

Situated at the heart of innovation, this Global Paper Manufacturer holds a prominent position in their industry, offering a diverse product across both physical and ecommerce retailers globally. By serving a large customer base through different market channels the Global Paper Manufacturer encountered significant internal challenges with its MDR provider, prompting a thorough overhaul of its security operations. The MDR provider's platform was overwhelmed with excessive alerts, causing "alert fatigue" and inefficiencies within the security team. As a result, the internal team had to develop and implement custom rules to manage these alerts, which was made challenging by the provider's inability to integrate with custom playbooks or custom use cases. This forced the security team to perform their own investigations after escalations, a task made more difficult by a lack of their own expertise in Microsoft Sentinel. Additionally, the security team grappled with noisy alerts requiring manual intervention to reduce unnecessary log ingestion, an inefficient portal system for pulling logs and triggering alerts, a lack of customized detection procedures suited to their security needs, and insufficient expertise and manpower for engineering and tuning of Sentinel. Recognizing the need for external expertise, the internal team identified Binary Defense as the perfect candidate to address their challenges.

Solution

Acknowledging the challenges faced by the manufacturer, Binary Defense provided a comprehensive Managed Detection and Response (MDR) and CoManaged SIEM solution precisely tailored to the client's distinct needs and environment. The comprehensive solution was customized to align with the client's specific risks and business requirements by understanding their environment and acting as an extension of their team to build out personalized use cases, rules, and playbooks. To identify any existing security gaps the Binary Defense team conducted an in-depth health check review of the client's existing security infrastructure, offering actionable recommendations. During onboarding, Binary Defense's detection engineers identified several high-value Windows Event IDs that were not being logged into the SIEM and addressed other gaps. Research, and Incident Response teams, ensuring it was meticulously

fine-tuned to reduce noise and enhance detection accuracy. Additionally, the detection engineers collaborated with the Manufacturing Enterprise security team to create watchlists for VIPs, critical servers, and privileged users to assist in the tuning process. Custom playbooks and workflows were developed to handle alerts from the client's EDR, streamlining the incident response process. The team also leveraged Binary Defense's threat intelligence feed integrated into the client's system, deploying rules to alert on Indicators of Compromise (IOCs). They deployed Binary Defense's proprietary standard ruleset within Sentinel, ensuring it was fine-tuned to minimize noise and enhance detection accuracy. Additionally, the detection engineers collaborated with the Global Paper Manufacturer's team to create watchlists for VIPs, critical servers, and privileged users to assist in the tuning process. Custom playbooks and workflows were developed to handle alerts from the client's EDR, streamlining the incident response process. The team also leveraged Binary Defense's threat intelligence feed integrated into the client's system, deploying rules to alert on Indicators of Compromise (IOCs).

Results

Implementing Binary Defense's MDR solution yielded significant improvements and measurable results for the client. Identifying and logging 11+ high-value event IDs ensured comprehensive monitoring and detection of potential threats. The fine-tuning of the SIEM ruleset and creating custom watchlists reduced unnecessary alerts, allowing the security team to focus on genuine threats. Developing personalized playbooks and workflows enabled efficient handling of alerts, reducing the time and effort required for investigations. By acting as an extension of the client's team, Binary Defense provided continuous support, monitoring and expertise, allowing the internal security team to focus on strategic initiatives Additionally, integrating threat intelligence and deploying custom rules ensured proactive threat detection and response, enhancing the client's overall security posture.

11+ high-value event ID's were identified ensuring comprehensive monitoring and detection of potential threats

In Conclusion

Binary Defense's MDR solution successfully transformed the client's security operations, addressing critical pain points and significantly improving their security posture. The partnership between Binary Defense and the client exemplifies the impact of a tailored, collaborative approach to Managed Detection and Response combined with a Co-Managed SIEM solution. Looking ahead, the client plans to continue leveraging Binary Defense's expertise to stay ahead of evolving threats and further enhance their security capabilities. This ongoing relationship is poised to drive continued success and security resilience for the Global Manufacturer.