CASE STUDY

Global Sports Group Maintains High Data Fidelity & Strengthened Consumer Trust with Binary Defense's MDR Solution

Customer Profile

The Global Sports Group is a global premier membership organization for professional athletes. With a workforce of over 700 and a solid brand reputation, the Global Sports Group must ensure high data fidelity with limited downtime

Challenges

The Global Sports Group struggled with a limited team tasked with operating an in-house SOC and optimizing security tool investments. There was a lack of continuous monitoring, and the team lacked the actionable intelligence, expertise, and context to address potential threats when alerts were recieved. They recognized the need for external expertise to optimize their tools, integrate threat intel, and provide guidance to enhance their security posture.

Solution

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

Results

- Binary Defense created 177 custom detections for the Global Sports Group
- Detection Engineers developed 30 clientspecific use cases
- In a single quarter, Binary Defense analysts reviewed approximately 2,232 alerts, but only escalated 14 to the Global Sports Group's security team

Challenges

The Global Sports Group is a global premier membership organization for professional athletes. With a workforce of over 700 and a solid brand reputation, the Global Sports Group must ensure high data fidelity with limited downtime.

The Global Sports Group struggled with a limited team tasked with operating an in-house SOC and optimizing its security tool investments. The Global Sports Group's environment included telemetry from the cloud, identity, and EDR feeding into their SIEM. The resource-constrained team led to a lack of continuous monitoring with no holiday coverage for their security solutions. When alerts were received, the team lacked the actionable intelligence and expertise to address potential threats, wasting time and resources on false positives. The absence of context and expertise when interpreting their SIEM's alerts further drained their resources. With a global workforce and a significant media presence, the security team was deeply concerned about the potential damage to their brand and reputation if an attacker successfully breached their environment. They faced knowledge gaps and recognized the need for external expertise to optimize security tools, integrate threat intelligence, and provide guidance to enhance their security posture. Protecting their brand and reputation was crucial, as a breach could result in substantial revenue loss due to diminished trust from advertising partners.

Binary Defense was chosen as the Global Sports Group's MDR provider, thanks to its robust partnership with its sister company, TrustedSec. The Global Sports Group's recognized the advantage of integrating TrustedSec's Incident Response and Penetration Testing with Binary Defense's capability to transform significant findings into enhanced detections, thereby fortifying its defense strategy.

Solution

To address visibility challenges and ensure 24/7 monitoring, the Global Sports Group selected Binary Defense's tailored solution, featuring its MDR service and MDR Agent, BDVision. This solution provided the small security team with expert analysts triaging and monitoring alerts from the client's environment, incorporating telemetry from cloud, identity, EDR and extended detection logs into their SIEM.

Binary Defense implemented threat intelligence with advanced behavior-based detection techniques to identify and alert on real-time attacks, including evasive and emerging threats that traditional signature-based methods might overlook. BD Vision's containment feature allows immediate isolation of compromised endpoints and identities, preventing the spread of threats and enabling swift remediation. Using deception technology to divert and neutralize attackers, Global Sports Group significantly enhanced its overall security upon deployment on critical servers.

Alongside its advanced capabilities, Binary Defense collaborated with the security team and key tech alliances such as ExtraHop, Devo, and TrustedSec. Together, they provided expertise and guidance for implementing Devo's SIEM and ExtraHop's NDR solution while integrating TrustedSec's pen test results to create new custom detections. Binary Defense detection engineers developed a tailored detection strategy and playbooks, deployed Binary Defense's proprietary ruleset while providing ongoing tuning efforts to reduce false positives. Binary Defense SOC analysts go beyond the initial triaging and alert monitoring by enriching alerts with valuable context from Binary Defense's Threat platform. These actionable alerts address critical incident questions and guide effective responses, particularly when alerts are escalated to clients. Acting as an extension of the client's security team, analysts provide rapid response actions by utilizing customized playbooks. These playbooks detail both automated and manual response actions that Binary Defense analysts can execute on the client's behalf.

Results

Binary Defense worked as an extension of the Global Sports Group's security team to achieve its objectives, including enhancing their global security posture, consolidating technology for enhanced visibility and awareness, and reducing overall risk exposure

In a single quarter, Binary Defense analysts reviewed approximately 2,232 alerts, but only escalated 14 to the Global Sports Group's security team. This indicated that merely 0.63% of alerts required escalation. The Global Sports Group's QBR conducted by dedicated CSMs and TAMs presented reports highlighting a remarkable 72.8% monthly reduction in escalation counts. This low escalation rate over the past quarter underscores the success of tuning and detection engineering efforts within the client's environment, showcasing the ROI for the client. In addition to saving the Global Sports Group valuable time, expert SOC analysts collaborated with the security team to create a longterm security roadmap, including increased network visibility through a NDR solution, implementation of Devo, and deployment of deception technology to deceive attackers and stop threats proactively.

177 custom detections were created for the Global Sports Group

Binary Defense also 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 Sports Group's telemetry by implementing proprietary Binary Defense rulesets, creating 177 custom detections, addressing 30 client-specific use cases, implementing custom playbooks, reducing log ingestion costs by fine-tuning DNS from firewalls, and transferring crucial knowledge to the internal security team. This comprehensive approach resulted in improved coverage and enhanced protection with deception technology, creating simulated environments and exposures to deceive attackers on critical serves to stop threats proactively. Acting as a knowledgeable partner, Binary Defense fine-tuned the Global Sports Group's environment, enhancing its ability to detect and respond to threats quickly and more effectively across a vast detection surface.

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