CASE STUDY

Binary Defense Operationalizes Threat Intel to Protect Digital Commerce Enterprise from Supply Chain Attack

Customer Profile

Operating across the retail and restaurant sectors, this organization serves a global customer base while employing thousands of people worldwide. Renowned for its expansive self-service financial access network, the Digital Commerce Enterprise continually pursues innovative solutions to streamline operations, drive sales growth, and deliver maximum convenience to its customers.

Challenges

As a leading commerce enterprise in the restaurant and retail sectors, this organization faced mounting security challenges while striving to balance compliance, customer trust, and operational efficiency. Their security team struggled with extended threat dwell times, noisy SIEM alerts that buried true positives, and critical visibility gaps caused by unoptimized tools. With competing priorities and an overwhelmed staff, they turned to Binary Defense for a tailored solution to reduce noise, optimize existing investments, hunt through their environment to uncover hidden threats, and strengthen their detection strategy against cybercriminals.

Solution

Managed Detection & Response (MDR)
Co-Manage Platform
Hypothesis-based Threat Hunting

Results

- By operationalizing threat intelligence across detection engineering, threat hunting, and SOC analysts, Binary Defense built a multi-layered defense that kept the Digital Commerce Enterprise safeguarded from threat actors.
- SIEM experts successfully migrated the Enterprise from a legacy platform to a modern SIEM optimized for peak performance.
- SOC analyst saved the internal team 16,000+ hours in triaging and investigating noisy alerts
- Detection engineers implemented a tailored, threat-informed detection strategy focused on the high-profile threats most relevant to the organization and its sector, prioritizing detections designed to prevent the highest-impact incidents.

Challenges

As a leading Digital Commerce Enterprise in the restaurant and retail sectors, this organization recognized the critical need for a tailored defense strategy to safeguard customer data and preserve trust. While committed to improving efficiency, driving sales growth, and delivering innovative solutions that enhance operations and customer convenience, the enterprise also understood that achieving these goals required strengthening its security posture.
Like many in their industry, they faced mounting security challenges that required immediate attention. Prior to partnering with Binary Defense, the security team struggled with:

- Lingering Threats: Extended dwell times left the organization vulnerable, raising the likelihood of a successful attack slipping through the cracks.
- Noisy SIEM, Missed Signals: Untapped capabilities within existing security investments left the SIEM flooded with noisy alerts—overwhelming analysts and obscuring high-fidelity detections.
- Critical Visibility Gaps: With gaps in visibility due to critical logs not feeding into the SIEM, this significantly limited the team's ability to detect and respond to threats swiftly.
- Advanced Skill & Capacity Limitations: The Digital Commerce enterprise lacked internal skills and capabilities to conduct proactive threat hunts, eradicating hidden threats within their environment.
- Need for Expert Guidance: Their internal security teams needed outside expertise in SIEM migration and guidance on selecting the best-fit solution to scale with their organizational needs.

With competing priorities and a noisy security environment, the team needed a partner that could deliver a tailored solution to optimize tools, reduce noise, hunt for threats, and build a stronger detection strategy capable of detection and disrupting bad actors targeting their organization.

The Solution

To address these challenges, the Digital Commerce Enterprise partnered with Binary Defense to implement a tailored approach that deployed their Managed Detection & Response (MDR), Co-Managed Platform, and Hypothesis-Based Threat Hunting solutions.

24x7x365 MDR Coverage

Binary Defense MDR delivered around-the-clock monitoring and support, helping resource-limited teams stay protected without the need for a single headcount. Alerts were triaged, investigated, and only the high-priority cases are escalated—dramatically reducing noise and analyst workload while ensuring nothing critical is missed.

Co-Managed Platform

With Co-Managed Platform, Binary Defense experts wrapped around the client's existing security tools investments. The team performed comprehensive health checks, including an in-depth review of configuration documents, actionable recommendations, and a full log, event, and detection gap analysis to ensure the SIEM was operating at peak effectiveness.

Although the internal security team recognized the need to reevaluate its SIEM, they relied on Binary Defense for strategic guidance. By developing a deep understanding of the client's security maturity and long-term goals, Binary Defense collaborated directly with internal stakeholders to design and execute a migration plan—delivering a smooth, strategic transition that enhanced the client's overall security posture.

Threat-Informed Detection Engineering

Binary Defense's detection engineers, experts across multiple SIEM platforms, worked directly with the client's team to develop a threat-informed detection strategy. Rather than chasing every signal, this strategy prioritized detections most relevant to the client's business and sector, targeting high-profile threats with the greatest potential impact.
In addition to developing a threat-informed detection strategy, Binary Defense detection engineers evaluated the Enterprise's MITRE posture and identified gaps, deployed the BD baseline library to fill the identified gaps, addressed gaps in log/event flow, and integrated the BD Threat Intelligence feed.

Hypothesis-Based Threat Hunting

To uncover stealthy threats that evade traditional automated tools, Binary Defense deployed its hypothesis-based threat hunting service. Threat hunters conducted targeted hunts using custom queries, advanced malware analysis, and investigative techniques. These hunts aimed todetect lateral movement, zero-days, and other evasive behaviors. By combining intelligence, intuition, and deep technical expertise, they identified anomalies and hidden risks while integrating findings directly into the client's security architecture.

When potential threats were validated, Binary Defense hunters provided full context—including root cause analysis and malware insights—so the client could focus response efforts where seconds matter most.

In Action

When news of the npm supply chain attack surfaced, Binary Defense immediately mobilized a multi-layered response to protect the Commerce Enterprise's environment.

Detection Engineering

Detection engineers quickly built and deployed new detections targeting malicious behaviors tied to the campaign. At the same time, targeted hunts were executed to uncover signs of Trufflehog activity, suspicious endpoint behaviors, and related indicators of compromise.

Threat Intelligence

The Binary Defense Threat Intelligence team published an advisory outlining the evolving attack and released a two-part episode on its ThreatTalk series to break down the latest developments and help clients and the broader community understand the risks.

Threat Hunting

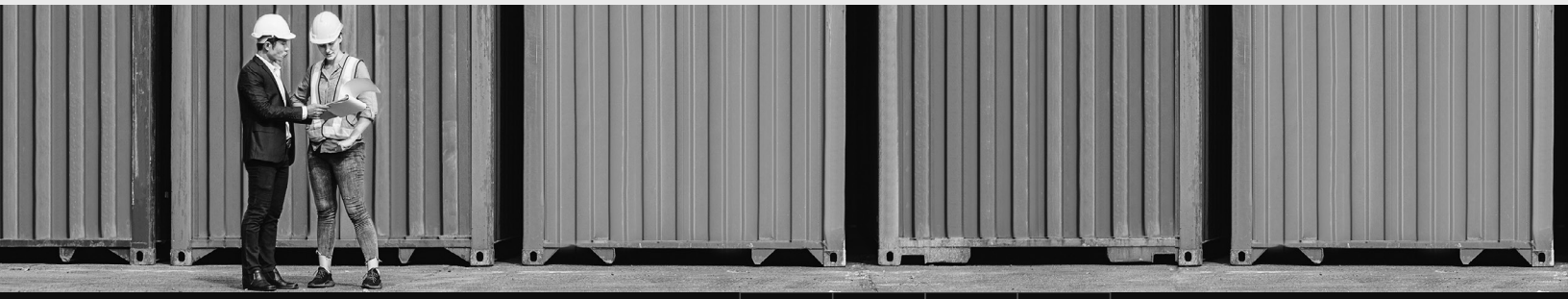
Binary Defense Threat Hunters conducted both static and dynamic analysis of compromised npm packages, focusing on the following TTPs:

- NPM package installation processes
- File write events indicative of compromised npm packages
- Script write events containing a string known to be associated with the obfuscated backdoor
- Script content including distinct function names used by Shai-Hulud
- Connections to GitHub URLs indicative of Shai-Hulud infections
- Process execution events indicative of Trufflehog

Security Operations Center (SOC)

Binary Defense SOC analysts delivered 24x7x365 monitoring, escalating suspicious activity through custom playbooks tailored to the client's alert escalation protocols.

From detection engineering to threat hunting to SOC monitoring, Binary Defense operationalized intelligence on the npm supply chain attack, swiftly acting to ensure the Digital Commerce Enterprise remained unaffected and protected throughout the npm supply chain attack.



The Results

The Digital Commerce Enterprise significantly enhanced its ability to detect and disrupt threats through the deployment of Binary Defense's solutions. The Binary Defense team successfully transitioned the organization from a legacy SIEM to a modern platform, establishing proactive system health monitoring, troubleshooting defects and stability issues, and providing ongoing detection tuning, and SIEM consulting. As part of the migration, the team aggregated and replicated three vulnerability baselines and converted 23+ detection watchlists from their EPP into new, actionable detections within their SIEM. All this work directly contributed to Binary Defense analysts triaging and investigating more than 98,000 alerts, escalating 155 events, of which 15 were confirmed True Positive incidents within a 90-day period. This effort saved the internal security team an estimated 16,316 hours, enabling them to redirect focus to strategic priorities. While the SIEM migration delivered immediate time savings and improved visibility, the longer-term value came from Binary Defense's Threat Hunting team, which further reduced noise and strengthened detection across the environment.

Over a six-month period, the Binary Defense Threat Hunting team achieved a >75% reduction in tuning and maintenance requirements, dramatically decreasing false positives while improving triage and incident response. By tailoring detections to behaviors anomalous to the client's unique environment, the threat hunters maximized ROI on existing security platforms.

Collaboration between threat hunters, detection engineers, and SOC analysts drove measurable outcomes:

- Developed and deployed 600+ behavioral detections in the client's EPP, based on more than 700 targeted hunts.
- Deployed several behavioral detections for windows persistence, that were validated by findings of PUA and RMM installation.
- Migrated 150+ critical baselines and detections from EPP into SIEM.
- Created 123+ new behavioral detections in EDR, consolidated into 39+ SIEM detections.
- Conducted 72+ network-based hunts in NDR, resulting in 50+ active threat detections deployed in EDR.
- Built specialized behavioral detections for RDP and SSH traffic, as well as advanced detections for HTTP smuggling and CVE-driven attacks.
- This continuous cycle of hunting, tuning, and intelligence sharing steadily improved the client's security posture—delivering faster detection, stronger defenses, and a measurable reduction in operational overhead.

The Results

By partnering with Binary Defense, the Digital Commerce Enterprise transformed its security operations from reactive and overwhelmed to proactive, resilient, and intelligence driven. What began as a need to optimize noisy tools and address skills gaps evolved into a strategic partnership that fortified defenses, accelerated detection, and delivered measurable business value.

Through MDR, Co-Managed Platform, and Hypothesis-based Threat Hunting, Binary Defense not only reduced false positives and improved detection accuracy but also saved over a thousand analyst hours—giving the internal team the freedom to focus on higher-priority initiatives. The rapid response to the npm supply chain attack underscored the strength of this collaboration, proving that operationalizing threat intelligence and building detections tailored to the client's environment provide a true competitive edge against today's adversaries.

For the Digital Commerce Enterprise, security is no longer a barrier to growth—it is a foundation for innovation, efficiency, and customer trust. With Binary Defense as a trusted partner, the organization is equipped to detect, disrupt, and outpace attackers, both now and in the future.

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

FORRESTER®
WAVE STRONG PERFORMER 2025
Managed Detection And Response Services

BINARY DEFENSE