DATASHEET

Co-Managed Platform

Maximize the Value of Your Security Tool Investments and Unlock Visibility with Binary Defense's Expertise

Deploying, maintaining, and monitoring SIEMs can be tedious and challenging without the resources and expertise to optimize fully. At Binary Defense, we collaborate with your organization to provide a tailored, Co-Managed SIEM solution that maximizes the usability and value of your data, effectively reducing blind spots and enhancing your security operations and posture. Our personalized Co-managed SIEM solution not only lowers costs and simplifies security operations but also fortifies your security stance with a custom detection strategy, continuous tuning, and 24x7x365 monitoring to safeguard against evolving threats.

120+ SIEMS

have been successfully deployed by the Binary Defense team of experts

Key Features:

Tailored Deployment

- Our experts collaborate with your team to pinpoint essential logs and eliminate unnecessary noise, thereby reducing SIEM costs.
- Tailored automation and playbooks are developed to streamline response to alerts.
- Areas of improvement are identified, and recommendations are provided to close security gaps, enhancing your long-term security posture.

Ongoing Tuning

- Ongoing policy and alarm tuning to reduce false positives
- Security posture and risk management reviews
- Security alarm enrichment with recommended triage and remediation steps

Personalized Detections

- A core set of Binary Defense Detections gathered from years of intelligence is deployed to the SIEM
- Expert detection engineering team works with you to create, deploy, and tune a personalized detection strategy that meets your needs and is constantly reviewed based on our Threat Intelligence and emerging threats.

Continuous Monitoring

- Peace of mind with 24x7x365 monitoring, alert triage and threat investigation
- Average 12-minute response times
- 30-minute SLAs for critical alerts/ detections
- BD experts helps with updates/ upgrades, health checks, troubleshooting, and engaging with third-party vendors

Co-Managed Platform Capabilities

Monitoring

Our analysts serve as an extension of your team, offering 24/7/365 expert monitoring with an attacker's mindset. This allows your team to focus on critical tasks when time is of the essence. We ensure an average response time of 12 minutes and 30-minute SLAs for critical alerts, so your team can act swiftly when it matters most.

Detections & Tuning

To achieve full optimization, continuous tuning and application of your detection strategy are essential. Guided by our expert detection engineers, this process minimizes false positives, enabling your team to concentrate exclusively on critical threats.

Implementation

Our expert detection engineers collaborates with your security team to implement your SIEM from the ground up within your environment. This process includes identifying and integrating critical log sources into your SIEM, developing a personalized detection strategy, performing the initial tuning, and ensuring that your SIEM alerts seamlessly flow into the BD environment.

Management

The Binary Defense team alleviates the burden of managing your SIEM alone. Our analysts provide comprehensive SIEM management, handling updates, upgrades, health checks, troubleshooting, and thirdparty vendor coordination. By leveraging our years of expertise, your team can efficiently address complex issues and maintain optimal performance.

	Managed Detection & Response				
	Onboarding	Monitoring	Detection & Tuning	Implementation	Management
Microsoft Sentinel	✓	✓	✓	✓	✓
Devo	✓	✓	✓	✓	✓
Sumo Logic	✓	✓	✓	✓	✓
Splunk	✓	✓	✓		✓
XSIAM	✓	✓	✓	✓	✓
Google Chronicle	✓	✓	✓		

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