Platform Management

This service (“SIEM Management”) may also be referenced as: Platform Management, Tuning and Configuration, Monitoring

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the *Platform Management* offering (“Services”) as described below and in the quantities and volumes defined in, and subject to, your quote through which you purchased the Services.

2. Scope of Services

Binary Defense will deliver ongoing operational management of the Client’s platform, including proactive monitoring, tuning, and custom detection engineering. This service is designed to maintain platform health, optimize detection efficacy, and ensure visibility into the Client’s security environment through custom and vendor-curated use cases, all as further described below.

2.1. Service Definitions and Parameters

- **Platform**
  - Refers to the third-party platform solution deployed, cloud hosted or on-premise in the Client environment (e.g., Devo, Sumo Logic, Palo Alto Networks XSIAM, Google SecOps).
- **Platform Vendor**
  - Refers to the third-party platform service provider (e.g., Devo, Sumo Logic, Palo Alto Networks XSIAM) through which Client procures the Platform.
- **Custom Use Case**
  - A detection rule or logic tailored to a specific need, threat scenario, or asset unique to the Client, created based on capabilities and access provided.
- **Ruleset Tuning**
  - Modifying detection logic, thresholds, and correlations to reduce false positives/negatives and adapt to environmental changes.
- **Out-of-the-Box (OOTB) Rules**
  - Default detection content provided by the platform vendor.
- **Overage**
  - Usage that exceeds the contracted metrics such as ingest volume (GB/day), license count, or endpoint quantity. Billed at then-current rates. Binary Defense reserves the right to audit Client usage and invoice overages accordingly when applicable.

-

Platform Management:

- Proactive system health monitoring
- Basic troubleshooting of minor defects, errors, and stability/update issues
- Work with Client to implement workarounds to restore functionality when applicable
- Vendor escalations on behalf of Client as needed
- Custom use case and detection creation based on the capabilities of the platform and access provided to Binary Defense
- Ongoing tuning to Binary Defense custom rulesets and vendor-curated out-of-the-box rulesets • Dashboard & report configuration for log sources/events

2.1.1. Options

- **Supported Platforms**
  - Binary Defense currently supports Devo, MS Sentinel, Sumo Logic, Palo Alto Networks XSIAM, Google SecOps, USMA and Splunk.
  - With respect to Platform Vendor's products and services, Client agrees that the such services and products are provided by or through Platform Vendor pursuant to Platform Vendor's standard terms and conditions (the "Vendor Terms") and that Binary Defense is not responsible, and disclaims all liability, for Platform Vendor or Platform Vendor's products and services, including, without limitation, for any loss, damage, or liability relating to (or arising from) Platform Vendor or Platform Vendor's products and services.
- **Custom Use Case Engineering**
  - Included where platform access and data allow.
- **Additional SKU Required**
  - For onboarding support, platform migration, or enhanced consulting outside of standard platform management.
  - To be agreed to mutually by the parties as applicable

2.2. Planning, Governance, & Implementation

2.2.1. Planning Activities & Responsible Parties:

N/A

2.2.2. Governance Activities:

- Initial dashboard setup and ongoing adjustments to visualizations.
- Regular Reviews and Audits
  - Log Source Coverage: Assess whether all critical assets are being logged and monitored
  - Rule Tuning Audits: Regularly audit detection rules for false positives/negatives and optimize accordingly.
  - Access Reviews: Validate who has access to the SIEM platform and whether access aligns with roles.
- Change Management Oversight Change Approval: Ensure governance over changes to rules, connectors, log sources, and integrations.
  - Impact Analysis: Evaluate potential risk and business impact of platform changes.
  - Documentation: Maintain records of changes for audit and rollback purposes.

2.2.3. Implementation Activities:

- Platform access provisioning by Client to Binary Defense
- Review of current rule performance and assets
- Baseline tuning and custom content creation

2.3 Client Obligations & Assumptions

The below does not limit or diminish Client's obligations under the Agreement.

2.3.1. Obligations:

Client must provide:

- Licensing and sufficient access to the applicable platform
- Administrative access to the supported platform
- Approval to engage vendors on their behalf, when required
- SOAR connectivity credentials for in scope technology, or provide BD the needed access to generate required credentials, for integration with the BD SOAR platform.

2.3.2. Assumptions

- All services delivered remotely
- All communication in English

- Platform is fully deployed and accessible at the start of service
- Client maintains vendor license and service agreement
- Binary Defense is not responsible or liable for a Platform Vendor's provision of the platform

2.4.1. Exclusions

Unless specifically set forth in this Service Description or reasonably related thereto as jointly determined by the parties, such activities are excluded, including, for example:

- Onsite support
- Initial platform deployment and architecture
- Any legal support or expert witness work
- MSSP alert monitoring or triage (unless separately scoped)
- Features not available within the selected platform
- Remediation activities or IR (unless separately scoped)

3. Terms and Conditions

The Services described herein are subject to the Binary Defense Terms and Conditions, unless you have a separate written agreement in place with Binary Defense ("Agreement"). In the event of a conflict, this Service Description shall control unless otherwise expressly agreed in writing.