BINARY DEFENSE

Managed Theat Hunting

This Service ("Managed Threat Hunting") may also be referenced as: Managed Threat Hunting Services, MDR Threat Hunting.

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the *Managed Threat Hunting* offering ("Services") provided by Binary Defense and in the quantities and volumes defined in, and subject to, your quote through which you purchased the Services.

2. Scope of Services

The Services include the proactive building and execution of hypothesis-driven threat hunts by Binary Defense using the Client's existing security platform(s).

Binary Defense develops and executes threat-informed hunts designed to identify indicators of malicious or suspicious activity associated with known adversary tactics, techniques, and procedures (TTPs). Hunts are informed by current threat intelligence, emerging attack patterns, and observed threat actor behavior across various industry verticals.

Threat hunting activities are performed on an ongoing and recurring basis throughout the term of the Service. Hunting efforts are continuously prioritized to maximize coverage, effectiveness, and relevance.

Results will be analyzed and findings requiring investigation or determined as malicious are escalated to the Client with supporting context and recommendations.

Typical activities include:

- Development of threat-informed hunting hypotheses
- Creation and execution of hunting queries across in-scope platforms
- Analysis of hunt results
- Identification of suspicious or malicious activity as well as policy or behavior observations that may become an enabler of a future attack

- Escalation of findings requiring further investigation via NightBeacon platform
- Alignment with threat intelligence and adversary tradecraft

These services are performed during Business Hours throughout the term of the service.

2.1 Service Definitions and Parameters

- **Threat Hunt:**
  - A structured process using threat intelligence to develop a hypothesis to proactively identify threats.
- **Tactics, Techniques, and Procedures (TTP):**
  - Behavior and operational methods of threat actors.
- **Hunting Queries:**
  - Structured search parameter to identify signs of malicious and anomalous activity, tuned to a clients environment baseline.
- **Platform**
  - The SIEM and/or EDR solution in scope for the Managed Threat Hunting Service
- **Business Hours**
  - Monday through Friday from 9:00am ET to 5:00pm ET

2.1.1. Options

- **Supported Platforms**
  - Binary Defense currently supports Microsoft Sentinel, Palo Alto Networks XSIAM, Google SecOps, Splunk Cloud, Palo Alto Cortex XDR, Sumo Logic, Microsoft Defender for Endpoint, SentinelOne, and CrowdStrike NG-SIEM.

2.2 Planning, Governance, & Implementation

2.2.1. Planning Activities & Responsible Parties:

Binary Defense Responsibilities:

- Kick-off call for onboarding planning
- Conduct initial platform assessment and capability review

Client Responsibilities:

- Provision requisite access (web interface and API access) to in-scope SIEM and EDR platforms to deliver the Managed Threat Hunting service
- Provide complete inventory of deployed EDR platforms and versions
- Identify key stakeholders and technical contacts
- Define priority assets

2.2.2. Governance Activities:

- Governance calls as needed until onboarding is complete

2.2.3. Implementation Activities:

- Validate requisite access to in-scope SIEM and EDR platforms
- Provision customer access to NightBeacon

2.3 Client Obligations & Assumptions

2.3.1. Obligations:

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

Clients must:

- Credential Provisioning: Client must provide and maintain valid UI and API credentials with appropriate permissions for all in-scope SIEM and EDR platforms. Service delivery is contingent upon continuous availability of these credentials.
- Platform Licensing: Maintain active licensing and support agreements for all in-scope platforms
- Change Notification: Provide minimum 30-day advance notice of any planned in-scope platform changes, upgrades, or migrations. Where a planned or unplanned platform change, upgrade, or migration results in a configuration, version, or environment not supported by Binary Defense, Binary Defense reserves the right to suspend or modify the Services until such time as compatibility is restored or a mutually

agreed transition plan is established. Binary Defense shall not be liable for any degradation or interruption of Services arising from such unsupported transitions. Binary Defense will use commercially reasonable efforts to notify the Client promptly upon identifying any supportability concern arising from a platform change.
- Incident Context: Share relevant incident data and threat intelligence to inform threat hunting priorities

2.3.2. Assumptions:

- All services delivered remotely
- All communication in English
- In-scope platforms are 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
- Client has appropriate licensing levels for custom detection creation on all in-scope platforms
- Client infrastructure can support the processing requirements of threat hunting queries
- Platform API functionality remains consistent with documented capabilities
- Network connectivity between Binary Defense and in-scope platforms remains stable
- EDR agents are properly deployed and functioning across the client environment. Client understands that EDR detection effectiveness depends on proper EDR agent deployment and configuration
- Threat Hunting is not 24x7; activities occur during business hours

2.4 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
- Custom threat hunts or a collaborative approach to designing threat hunts
- Summary reports or dedicated meetings to discuss findings
- Ongoing communications during threat hunts
- Incident response or investigation of suspected breaches

- Reverse engineering of malware
- Real-time monitoring or detection tuning (covered by MDR service)
- Any legal support or expert witness work
- Services outside of stated business hours
- Configuration of unsupported third-party tools
- Initial platform deployment and architecture
- MSSP alert monitoring or triage (unless separately scoped)
- Remediation activities or IR (unless separately scoped)
- Platform installation, configuration, administration, or management
- Endpoint agent deployment, troubleshooting, or maintenance
- Incident response or forensic analysis activities
- Performance tuning or optimization of platform infrastructure
- Training or certification of client personnel on platforms
- 24x7 threat hunting services
- Compliance audit support or regulatory reporting
- Management of prevention policies or endpoint hardening configurations
- Support for end-of-life or unsupported platform versions

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.