Professional Services - Security Engineering

This service ("Professional Services - Security Engineering") may also be referenced as: SIEM Health Check, Tuning & Engineering, SIEM Platform Migration, SIEM Management Support Ad-Hoc

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the **Professional Services – Security Engineering** ("Services"). These services are designed to enhance the effectiveness, visibility, and operational maturity of the Client's SIEM deployment, and may be consumed across four categories: health check, detection engineering, management support, and platform migration; all 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 a flexible block of hours (in the amount set forth in the quote) that may be applied to any of the following activities:

- **SIEM Health Check Review:**
  - A structured assessment of the Client's current SIEM platform configuration, performance, and alignment to best practices.
- **SIEM Tuning and Detection Engineering:**
  - Hands-on development, deployment, and refinement of both custom and vendor-provided detection content.
- **SIEM Management and Support:**
  - Platform maintenance and monitoring activities, vendor coordination, issue resolution, and detection maintenance.
- **SIEM Migration:**
  - Transitioning log sources and detection content from one SIEM platform to another (e.g., SIEM A to SIEM B).

2.1. Service Definitions and Parameters

- **SIEM Platform**
  - The third-party SIEM solution deployed by the Client (e.g., Devo, Sumo Logic, Palo Alto Cortex, etc.).
- **SIEM Vendor**

    - The provider of the SIEM Platform, responsible for the platform's software and infrastructure.
- **Block of Hours**
    - The quantity of professional services hours purchased by the Client under the quote and tracked against service consumption.
- **1:1 Log Transition**
    - Transition of log sources from the current SIEM to a new SIEM in a like-for-like format (meaning the events are sending from the same log sources).
- **Custom Ruleset**
    - Detection logic authored by Binary Defense, tailored to the Client's specific risk profile and logging environment.
- **Out-of-the-Box (OOTB) Ruleset**
    - Detection content provided natively by the SIEM Vendor.
- **Vendor Terms**
    - The SIEM Vendor's standard terms and conditions for use of the platform, available on the vendor's website. With respect to the SIEM Platform and SIEM Vendor, Client agrees that such SIEM Platform and services provided by the SIEM Vendor are subject to the Vendor Terms and that Binary Defense is not responsible or liable for the SIEM Platform or SIEM Vendor.

2.1.1. Options

- **SIEM Migration Support**
    - Optional service available for transition from one SIEM platform to another (requires adequate hours in block as separately agreed to by the parties).
- **Custom Detection Engineering**
    - Included where platform access and ingestion allow.

2.2. Planning, Governance, & Implementation

2.2.1. Planning Activities & Responsible Parties:

- Initial scoping call to define use of service block
- Planning sessions for rule creation, SIEM tuning, or migration roadmap
- Regular check-ins for prioritization and progress tracking

2.2.2. Governance Activities:

- Delivery of in scope services
- Periodic progress updates (biweekly/monthly cadence based on block size)

2.2.3. Implementation Activities:

As determined by Client's selection of the four activity categories identified above in Section 2:

- SIEM Setup/Configuration
- Custom rule development and deployment
- Tuning of OOTB and custom rulesets
- Dashboard/report development
- SIEM A to SIEM B transition planning and execution

2.3 Client Obligations & Assumptions

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

2.3.1. Obligations:

Client must:

- Provide administrative access to the SIEM Platform(s)
- Remain responsible for obtaining and maintaining licensing required for such SIEM Platform(s)
- Ensure availability of technical contacts for each log source
- Support coordination with the SIEM Vendor as needed
- Approve work scope and use of block hours in writing

2.3.2. Assumptions

- Services will be conducted remotely
- All work will be performed in English
- Client infrastructure and access will be ready prior to service start
- SIEM Vendor provides stable and accessible platform
- Services apply only to supported SIEM Platforms that are licensed separately by Client

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:

- Raw data export, which must be handled by Client in coordination with the applicable SIEM Vendor

- Onsite support
- 24/7 MSSP alert monitoring
- Incident Response or Threat Hunting
- Any legal support or expert witness work
- Full re-architecture or SIEM re-implementation
- Migration of raw data or cold storage logs
- Use case development requiring third-party tooling not integrated with SIEM

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. Notwithstanding anything to the contrary, Binary Defense is not responsible for any loss, damage, or liability arising from the unavailability of the SIEM Platform.