Dedicated Resource

This service ("Dedicated Resource") may also be referenced as: Dedicated Security Analyst and Engineer Service, DA, DE, Embedded Analyst, Embedded Engineer, Staffing

1. Introduction

This Service Description outlines the scope, deliverables, and operational parameters of the **Dedicated Resource offering** ("Services"). This offering provides the Client with dedicated cybersecurity personnel from Binary Defense who will assist Client with its enhancement of it's security operations through full-time Analyst and/or Engineer resources (as specified in your applicable quote) assigned specifically to their environment. The Services are provided in the quantities and volumes defined in, and subject to, your quote through which you purchased the Services.

For clarity, the parties agree that Binary Defense personnel and resources provided hereunder in the performance of the Services shall not be deemed employees of Client.

2. Scope of Services

The Services include the allocation of dedicated Binary Defense personnel to support Client's security operations, platform optimization, and incident management functions within the Client's environment. Services may include:

- Dedicated Analyst
    - Tier 1 and Tier 2 incident response and analysis
        - Level one referring to assisting Client with initial intake and high-level triage of a security incident
        - Level two referring to assisting Client with initial escalation and further technical analysis
    - Collaboration on security process optimization and playbook development
    - Collaboration on projects related to strategic objectives
    - Collaboration on maturity improvement efforts
    - Detection rule creation, tuning, and deployment
    - On-call support (as needed and defined within the parameters set forth herein, the quote, and the Agreement)
- Dedicated Engineer
    - SIEM platform management, configuration, and troubleshooting
    - Collaboration on security process optimization and playbook development
    - Collaboration on projects related to strategic objectives

- Collaboration on maturity improvement efforts
- Detection rule creation, tuning, and deployment
- On-call support (as needed and defined within the parameters set forth herein, the quote, and the Agreement)

2.1. Service Definitions and Parameters

- **Dedicated Analyst**
  - A Binary Defense resource who assists Client with Tier 1 and Tier 2 incident triage, escalation, analysis, and incident response coordination.
- **Dedicated Engineer**
  - A Binary Defense resource who assists Client with platform management, log source analysis, detection engineering, and tuning.
- **Client Standard Business Hours**
  - Monday through Friday, 9:00 AM – 5:00 PM EST, unless otherwise agreed to between the parties.
- **On-Call Support Threshold**
  - If on-call engagements occur >10% of off-hour periods over a rolling 2-month span, Client and Binary Defense will reevaluate staffing needs and a change order must be agreed to for continued off-hour support.
- **HR Policy Adherence**
  - All Binary Defense personnel (including, without limitation, Dedicated Analysts and Dedicated Engineers) are subject to internal company HR policies including, without limitation, PTO, holidays, and sick leave.
- **Temporary Coverage**
  - In case of personnel departure, Binary Defense will work in good faith to supply interim or alternative resources to minimize service disruption.

2.1.1. Options

- **Dedicated Analyst**
  - Available in full-time equivalent units; supports incident response and triage, and operational maturity improvement efforts as defined above.
- **Dedicated Engineer**
  - Available in full-time equivalent units; supports SIEM configuration and detection engineering, and operational maturity improvement efforts as defined above.
- **On-Call Support**

- Optional, subject to capacity and prior agreement; not billed separately unless otherwise scoped.

2.2. Planning, Governance, & Implementation

2.2.1. Planning Activities & Responsible Parties:

- Initial onboarding session with Client stakeholders
- Knowledge transfer and access provisioning sessions from Client to Binary Defense
- Weekly or bi-weekly check-ins to prioritize analyst/engineer focus areas

2.2.2. Governance Activities:

- Monthly status reporting on performance and key deliverables (if applicable)
- Participation in QBRs (if reasonably requested by Client)

2.2.3. Implementation Activities:

- Access validation and environment walk-through provided by Client
- Setup of analyst/engineer workspace (remote or hybrid)
- Workflow alignment with Client security operations team(s)

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 necessary access credentials, VPN access, and endpoint visibility
- Coordinate internal stakeholder availability for issue resolution
- Maintain a stable platform environment suitable for security operations work
- Inform Binary Defense of changes to business hours, holidays, or work expectations

2.3.2. Assumptions

- All Services are delivered remotely
- Client's internal teams will collaborate with Binary Defense resources
- English is the default language for service delivery

- Analysts/Engineers follow and are subject to only Binary Defense HR policies (vacation, sick leave, etc.)

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:

- MSSP services such as alert monitoring or 24x7 response
- Legal, expert witness, or compliance advisory services
- Onsite staffing unless specifically scoped and contracted for separately

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.