Analysis on Demand

This service ("Analysis On Demand") may also be referenced as:
AOD, Active Response, Active Response Team, or ART

1. Introduction

This Service Description outlines the scope, deliverables, and parameters of the **Analysis on Demand (AoD)** offering ("Services") provided by Binary Defense. The AoD service is designed to support Clients who require immediate expert assistance with a suspected or confirmed cybersecurity compromise, all in the quantities and volumes defined in, and subject to, your quote through which you purchased the Services. Services include validation, forensic investigation, and response recommendations to reduce risk and impact ,as described below.

2. Scope of Services

The Services provide on-demand access to incident response and compromise assessment expertise. Binary Defense will perform investigation and containment activities to help validate suspected cybersecurity incidents. AoD hours (with such quantity identified in the applicable quote) may also be used proactively to search for indicators of compromise (IOCs), assess malicious activity, or enhance threat visibility.

- Typical activities include:
    - Scoping calls with Client for triage
    - Collaborative incident response coordination
    - Digital forensics and malware analysis
    - Tactical containment and remediation guidance
    - Written technical reporting documenting timelines and root cause based on information made available to Binary Defense
    - Optional compromise assessments to uncover dormant threats

2.1. Service Definitions and Parameters

- **Hours of Service**:
    - Defined in the quote associated with the Services. Initial hours are estimates only; additional hours may be necessary depending on the incident complexity.
- **Validity**:
    - Purchased hours are valid for 12 months from acceptance of the quote and do not roll over. If the purchased hours are part of the MDR Bundle, in which

case hours quoted are quoted annually for the term length and do not roll over into subsequent contract years.

- **Supported Operating Systems for Digital Forensics**:
  - Microsoft Windows
  - macOS
  - Linux
  - IBM AIX
  - VMware ESXi
  - Chrome OS
- **Compromise Assessment**:
  - An optional proactive review of systems to detect signs of compromise. This can be scoped broadly across the enterprise or targeted to specific high-risk assets.

2.1.1. Options

- **Additional Hours**
  - Additional hours available as stand-alone purchase
- **Agent Deployment**:
  - Client may opt to allow deployment of forensic agents (e.g., Binalyze) to expedite data collection. If declined, Client must provide access to equivalent tooling.
  - With respect to the agents deployed to Client endpoints, Client agrees that (1) such agents may include services and products provided by Binalyze OÜ ("Binalyze Agents"); (2) the terms and conditions set forth at https://www.binalyze.com/terms and https://www.binalyze.com/resources/end-user-license-agreement apply to the use and deployment of the Binalyze Agents; and (3) Binary Defense is not responsible, and disclaims all liability, for the Binalyze Agents, including, without limitation, for any loss, damage, or liability relating or (or arising from) Binalyze or the Binalyze Agents.
- **Scope of Assessment**:
  - The Client may choose between comprehensive endpoint analysis or focused assessment on high-priority systems (e.g., domain controllers, VIP endpoints, internet-facing systems).
- **Escalation Option**:
  - Findings from compromise assessments may be escalated into a deeper investigation upon request, subject to the number of hours contracted for.

2.2. Planning, Governance, & Implementation

2.2.1.1. Planning Activities & Responsible Parties:

- Conduct initial scoping calls with Client to verify alerts or events and identify systems of interest
- Schedule coordination calls to align on response strategy, deliverables, and access requirements

2.2.2. Governance Activities:

- Daily updates will be provided to Client during active engagements
- Summary reports and findings shared throughout engagement lifecycle

2.2.3. Implementation Activities:

- Collection of forensic artifacts (host-based artifacts, memory images, live response data)
- Deployment of forensic agents (if permitted)
- Review and analysis of Client-provided telemetry (SIEM, EDR, firewall logs, etc.)
- Contextual interviews with Client personnel
- Tactical containment recommendations (e.g., isolation, blocking malicious domains/IPs)

2.3 Client Obligations & Assumptions

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

2.3.1. Client Obligations:

- Provide remote access to systems and required security tooling
- Enable permissions for analysis tools (e.g., SIEM, EDR, NDR, SOAR, firewalls)
- Grant access to key personnel for context and incident response coordination
- Provide contact information for escalation and daily updates
- If opting out of agent deployment, ensure access to equivalent tooling

2.3.2. Assumptions

- All services will be conducted remotely
- Services will be delivered in English
- Client's environment is available, accessible, and stable
- Analysis will be limited to data and systems made available to Binary Defense
- AoD Team operates Monday–Friday, 9:00 a.m. – 5:00 p.m. Eastern Time

2.4 Exclusions

- Onsite incident response or forensic acquisition
- Real-time malware reverse engineering
- Expert witness services or legal support
- Participation in live calls with insurance providers
- Remediation execution beyond advisory and tactical guidance

2.5 Service Level Targets and SLA Commitments

- **SOC Hotline Availability**:
  - 24x7 availability to report incidents via phone, email, or BD platform
- **AoD Response Window**:
  - Investigative work occurs during normal business hours (M–F, 9 a.m. – 5 p.m. ET)
- **Daily Engagement Updates**:
  - Provided throughout the active engagement period
- **Final Reporting**:
  - A written investigative report will be provided upon request at the conclusion of each engagement

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.