



# Service Level Agreement

Version 1.5

## 1. Definitions

Unless otherwise defined in this Service Level Agreement (“SLA”), capitalized terms shall have the meanings assigned to them in the Terms of Service or their standard technical or common usage.

## 2. Service Levels

### 2.1. Alert Levels

Alerts from Customer Systems that are monitored by the Managed Detection and Response (MDR) Services of Eye are classified as either “High” or “Low” to determine the priority of response by Eye’s Security Operations Center (SOC). The threat level is assessed based on:

- i. The findings or analytics that triggered the Alert.
- ii. The confidence level regarding the malicious intent of the activity that led to the Alert.

The severity of Alerts can also vary depending on the type of category of the finding.

Level	Definition
High	Indicates a significant likelihood of resource compromise. There is a strong confidence in both the findings that prompted the Alert and the malicious intent. For instance, an Alert detecting the execution of a known malicious tool like Mimikatz, commonly used for credential theft.
Low	Suggests potentially suspicious activity that may indicate resource compromise. The confidence in the finding that prompted the Alert is medium, while the confidence in the malicious intent is low. These are typically machine learning or anomaly-based detections, such as sign-in attempt from an unusual location.

### 2.2. Reaction Time: Monthly Average Time To Assign (ATTA)

The ATTA metric evaluates whether the MDR Service meets the agreed-upon availability standards by separately assessing the responsiveness for different Alert categories and time periods. “Reaction Time” is defined as the duration, measured in minutes, from when an Alert is generated until it is acknowledged by the first Eye SOC analyst.

The ATTA is calculated monthly for each combination of Alert level and time period (during vs outside Business Hours) using the formula:

$$\frac{\text{Total Reaction Time}}{\text{Total Alerts Created}}$$



**2.3. Target ATTA**

Eye will make reasonable efforts to adhere to the following ATTA, based on their classification and the time of occurrence:

	During Business Hours	Outside Business Hours
High	60 minutes	120 minutes
Low	240 minutes	N/A

**2.4. Reporting**

Eye will make reasonable efforts to provide monthly reports that present key indicators such as endpoint and 2FA coverage and actionable recommendations. This provides the Customer with insights to enhance its cyber resilience.

**2.5. Annual Reviews**

Eye will make reasonable efforts to invite the Customer for an annual review call. This annual review aims to provide insights and recommendations, supporting a proactive approach to managing cyber risks and enhancing the Customer’s overall security strategy.

**3. Exclusions**

The service levels outlined in this SLA do not apply to performance issues or service level failures resulting from the following circumstances:

- a) periods during which Eye is performing scheduled maintenance;
- b) that result from any actions or inactions of the Customer or any third party acting on behalf of the Customer;
- c) resulting from the equipment, software or other technology of the Customer and/or equipment, software or other technology of third parties; or
- d) caused by the Customer’s use of the Services in a manner inconsistent with the Agreement or Eye’s written guidance.

