Client: All

Service Level Agreement (SLA) for SOC Services

Provided by Waterleaf International LLC
April 30, 2021

Table of contents

1 Document information and history

1.1 Version history

Version	Change Date	Changes and description	Editor	Approval date	Approver
1.0	10/07/20	Added backup services	Marshall Howard		
1.1	2/14/21	Modified to turn into template form	Marshall Howard	3/3/21	
1.2	4/29/21	Final Edits	David Levitan	4/30/21	MKH

1.2 Distribution

New approved versions of this document must be distributed to the functions listed below. It is the responsibility of the document owner to initiate (re)approval processes and thereafter the responsibility of the approver to approve the changes to the SLA.

Permanent Network Operations members:

Function
Director of Information Technology
EVP
COO

2 Introduction

This document will describe the services delivered to Client (as designated on cover page of the document) by the Waterleaf International, LLC ("WL") as part of a master services agreement ("MSA") or Customer Service Agreement ("CSA"). Such services may be marketed and sold under the Cyberleaf (SM) brand.

3 SIEM/SOAR/SOC Services

3.1 SIEM

Security Information and Event Management (SIEM) is a single security management system that offers deep visibility into activity within Client network and devices which empowers real time response to events.

A SIEM solution ingests and analyses a high volume of data in mere seconds to detect and alert on unusual behaviour, offering real-time insight to protect Client business; a task that would be impossible to execute manually.

3.2 SOAR

SOAR stands for Security Orchestration, Automation, and Response. The term is used to describe three software capabilities – threat and vulnerability management, security incident response, and security operations automation. SOAR allows companies to collect threat-related data from a range of sources and automate responses to threats.

SOAR systems can define, prioritize and standardize functions that respond to cyber incidents. In other words, a SOAR enables organizations to automate the response to issues based on data collected and analyzed by the SIEM. By removing the need for human assistance, threats and vulnerabilities are addressed quicker and IT staff can better prioritize their time.

The software also allows security teams to gain attacker insights with threat rules derived from knowledge of attacker tactics, techniques and procedures (TTPs) and known indicators of compromise (IOCs). The SOAR uses multiple threat intelligence feeds (organized and analysed information on potential and current threats) to supplement threat detection.

3.3 SOC

A Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to manage and continuously optimize the SEIM and SOAR systems to improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

Essentially, the SOC is the correlation point for every event logged within the organization that is being monitored. For each of these events, the SOC determines how they will be managed and acted upon.

4 General

4.1 Purpose of this document

The purpose of this SLA is to establish the service levels agreed upon between the parties.

The SLA must describe which services the SLA includes, how they must be delivered and how reporting of the delivery must be performed.

5 Responsibility And Formal Organization

Responsible individuals will be defined below: Individuals can perform more than one of the below roles when required.

Role	Responsibility	Owner
SOC Team Lead	Manage the SOC services and report to the Client	WL
SOC Analysts	Deliver the SOC services to the Client	WL
Incident Manager	Can be the SOC team lead. Manages incidents and escalation of incidents when required (e.g. when manual handling of incidents is required).	WL and Client
Contract Manager	Responsible for the contract at the Client and for arranging periodic status meetings	Client
	Monitors SOC service delivery and follow up	WL
Change Manager	Coordinates delivery of services during change management	Client
	Responsible for communicating with Client when implementation of changes is required	WL

6 Services To Be Delivered By The SOC

6.1 Operating Security System

For SLA purposes, the core system services will be operational 99.99% of the time as measured in minutes on a calendar month basis. These core systems services consist of:

6.1.1 Log management via SIEM which includes:
1. Ensuring the comprehensiveness of logs added continuously to the SIEM; and
2. Ensuring the uninterrupted addition of logs to the SIEM including end point agent services

6.1.2 Timely analysis and response generation by the SOAR system including;
1. Analysis of SIEM logs;
2. Incident reporting; and
3. Automated notifications and actions per system design.

6.1.3 SOC Operations including 24/7/365 correlation of system events

For calculation purposes, WL will use a standard calendar month of 30 days thus a 99.99% uptime corresponds to 5 or less downtime per month. On a monthly basis, WL will report the

minutes of downtime excluding time that arise directly or indirectly from the exclusions listed in Section 7.1.3 below.

6.2 Incident Response:

WL will respond to incidents and threat events within defined timeframes based on the severity of the issue.

6.2.1 Definitions based on NIST:

- Threat Event: An event or situation that has the potential for causing undesirable consequences or impact.

- Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

6.2.2 Incident classification:
Events and Incidents are classified based on potential impact to Client. WL uses 4 classification levels as outlined in the table below:

Level	Description	Threat Event Example(s)	Incident Example(s)
Critical	Immediate action necessary to mitigate current malicious activity	- System Downtime - Lack of data receipt from client location -	Information Leak
3	High potential for incident if preventive action is not taken	- Significant change in SEIM data traffic volume indicating degraded performance potential	Lack of confirmation of SOAR action
2	Low potential for incident,	- A user has not updated password at required interval	Virus found on user computer, though no data leak
1	Informational or maintenance type activities	-	Incident reporting

6.2.3 SLA Initial Response Intervals

WL will respond within the below timeframes based on the classification and type of event per the intervals below. SLA credits will be given should WL not meet the SLA standards as defined later in this document.

.

Level	Threat Event	Incident	SLA
Critical	1 Hour	1 Hour	96%
3	24 hours	2 Hours	96%
2	72 hours	8 Hours	96%
1	5 days	24 Hours	96%

SLA Metrics for reporting:

All Incidents and Threat Events will be tracked in WL's systems and reported monthly to client. Client reported trouble tickets or issues will also be tracked by WL.

The client must not hinder the uninterrupted addition of logs to the SIEM, which includes ensuring that end point log forwarding agents are running, maintaining Internet connectivity, and ensuring any on-site WL devices are kept in an operational environment.

6.3 Security device configuration and management

6.3.1 Configuration

Unless contracted to WL, all Client devices must be correctly configured and managed by the Client and/or its agent. This includes:

- Daily verification that devices or applications that need signature updates receive them.
- Monitoring for new firmware or software version availability
- Changing default passwords and community strings
- Documenting passwords in password managers
- Documenting asset configurations for inclusion in the WL system with the agreed upon level of configuration item detail.
- Ensuring separation of duties between production systems and backup systems holding backup data
- SEIM agent configuration and operation

All security devices must pass an initial WL configuration audit after Client has configured them before application of the Threat Event and Incident SLAs. This audit will be performed by WL or its designated agent and results presented to Client within 5 business day of completion.

6.3.2 Change Management

Proper SEIM/SOAR/SOC operation depends on maintaining up to date information in WL and Client will work together on system changes that affect system operations. Examples include but are not limited to:

1. Client installs new devices or software packages
2. Client location changes
3. WL software changes that affect reporting

7 SOC/SIEM/SOAR Service Level Agreement

A specific list of use cases and the standard assigned priority levels will be agreed and issued to the Client prior to or during onboarding of Client. This may be reviewed and amended during service review.

Client will receive a Service Credit that can be used against future purchases based on performance levels provided in Section 7.1 below. Such credits will only be applied to charges for the SOC/SIEM/SOAR service charges.

Client is responsible for ensuring that credits are applied when the SLA has been invoked.

In the event that more than one service level within each specific SLA is breached during an SLA period then WL will only be liable to pay out against the highest value Service Credit. Multiple breaches within each category will not be cumulative.

7.1 Service level credit levels:

7.1.1 Service Availability

Downtime Minutes Per Month	Service Credit
Less than 5	0
Greater than 5 Less then 10	10%
Greater than 10 less than 20	15%
Greater then 20	20%

7.1.2 Threat Event and Incident Responses

Percentage of Time Meeting SLA	Threat Event	Incident
96% and above	0%	0%
>= 95% and < 96%	5%	5%
>= 92% and < 95%	8%	8%
>= 90% and < 92%	10%	10%
< 90%	15%	15%

SLA credit for Threat Events and Incidents will be tracked separately.

7.1.3 Exclusions: Downtime minutes and delays in Response Intervals will not be measured if due to the following:

1. Issues arising from Client or a third party including not providing current and accurate data to WL;
2. Connectivity issues between Client location(s) and WL SEIM/SOAR/SOC not attributable to WL;
3. Force Majeure: Events or conditions beyond WL's reasonable control. Such events include, but are not limited to:
    a. Acts of government authorities not due to WL's prior lack of conformance with regulations or law;
    b. Natural disasters;
    c. War, insurrection, riot, or similar unlawful actions; or
    d. Other Acts of God.
4. Emergency or scheduled maintenance

5. Suspension or termination of services provided under this agreement in accordance with the Customer Service Agreement.

8 Additional Services – As Applicable

8.1 Backup Services – Provided Through Wasabi

8.1.1 WL will use commercially reasonable efforts to ensure the Wasabi Service is available for in accordance with the Monthly Uptime Percentage. The "Monthly Uptime Percentage" is calculated by subtracting from 100% the average of the Error Rates from each five-minute period in the monthly billing cycle. "Error Rate" means: (i) the total number of internal server errors returned by Wasabi as error status "Internal Error" or "Service Unavailable" divided by (ii) the total number of requests for the applicable request type during that five-minute period. WL will calculate the Error Rate for each account as a percentage for each five-minute period in the monthly billing cycle. The calculation of the number of internal server errors will not include errors that arise directly or indirectly as a result of any of the SLA Exclusions listed below

8.1.2 Exclusions: This SLA does not apply to any unavailability, suspension or termination of the Backup Service, or any other related performance issues: (i) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of the Backup Service; (ii) that result from any actions or inactions of Client or any third party; (iii) that result from Client equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (iv) that result from scheduled or emergency maintenance activities for the Services; (v) arising from our suspension and termination of Client right to use the Backup Services in accordance with the Customer Service Agreement, or (vi) scheduled maintenance, as well as any unscheduled emergency maintenance. Further, all test, development, beta, sandbox and other non-production environments are expressly excluded from this SLA, and no Service Credits shall be available for unavailability of any such environment.

8.1.3 Credits
Upon written request, Client will receive a Service Credit that can be used against future purchases based on performance levels provided directly below. Such credits will only be applied to charges for the Backup Service charges.

Monthly Uptime Percentage	Service Credit
Greater than 99.0% but less than 99.9%	10%
Less than 99.0%	25%

8.2 EDR

No SLA applies to individual installations of EDR as EDR is provided on multiple machines and is subject to many factors outside WL's control. Questions and issues regarding performance and operation will be addressed through trouble tickets.

8.3 RMM & Patch Management

No SLA applies to individual installations as RMM & Patch Management systems are machine specific and performance is subject to many factors outside WL control. Questions and issues regarding performance and operation will be addressed through trouble tickets.