Security Services - Service Level Agreement (SLA)

Introduction

This Service Level Agreement ("SLA") outlines the performance standards, response times, and support expectations for the Tigunia Security Services provided by Tigunia to Client (collectively referred to as the "Services"). **To avoid doubt, this SLA applies solely to the availability and performance of the Service itself, not the availability or performance of the systems or assets that the SOC monitors. Tigunia's Security Services do not guarantee, ensure, or warranty against any potential threats but instead assist in responding to them.** This document and the related services are subject to the Tigunia Security Services – Definition of Services and Components ("DSC") and our Master Services Agreement ("MSA"). This SLA governs all SOWs for this service.

Purpose of this Document

This SLA document establishes the agreed-upon service levels between Tigunia and the Client.

This SLA describes which services are included, how they are delivered, and how the delivery must be reported. Each objective stated herein will be defined as a Service Level Objective ("SLO") with explicitly defined targets. Any statement of service effort established in the DSC is only rendered on a best-efforts basis if it does not relate to an established SLO.

Services Delivered by SOC

Tiers of Service: Tigunia provides three levels of service for each category, *i.e.,* system/network devices and user/identity security. The tiers define the scope and depth of services available for different types of endpoints:

SOC Services Tiers

- **Core**: Basic monitoring of system and network device endpoints.
- **Standard**: Enhanced monitoring with response actions for system and network device endpoints.
- **Premium**: Full monitoring and incident response with proactive security measures for system and network device endpoints.

User and Identity Security Services Tiers

- **Core**: Basic user access management and monitoring.
- **Standard**: Enhanced identity protection with alerting and role-based access controls.

- **Premium**: Full identity management with advanced detection and remediation capabilities.

Definition of Services and Components ("DSC")

This is a separate document that outlines the specific features and capabilities provided under each service tier. As defined in the DSC, all commitments in this SLA apply to the relevant tier selected by the Client.

Service Scope

This section covers the scope of service that the DSC defines.

Definitions based on NIST

- **Security Services Availability:** The operational uptime during which Tigunia's SOC, tools, and platforms remain accessible to provide monitoring, alerting, and incident response for system and network device endpoints, as well as user and identity security services.
- **Endpoint Agent:** Software agents deployed on system or network device endpoints for monitoring, detection, and telemetry purposes or managed identity software for user and identity security services.
- **Incident:** Any detected or reported event related to the security of Client's systems, network devices, or user identities, classified according to Tigunia's Incident Classification Policy.
- **Threat Event:** An event or situation that can cause undesirable consequences or impact.
- **Incident:** An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system, the information the system processes, stores, or transmits, or constitutes a violation or imminent threat of a breach of security policies, security procedures, or acceptable use policies.

Operating System Security

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:

- Log Management via SIEM includes:
  - Confirming the comprehensiveness of logs added continuously to the SIEM.
  - Confirming the uninterrupted addition of logs to the SIEM, including end-point agent services.
- Timely analysis and response generation by the SOAR system, including:
  - Analysis of SIEM logs.
  - Incident reporting.

  - Automated notifications and actions per system design.
- SOC Operations, including 24/7/365 reporting of system events.

For calculation purposes, Tigunia will use a standard calendar month of 30 days, with a 99.99% uptime corresponding to 5 or fewer minutes of downtime per month. Every month, Tigunia will report downtime minutes and exclude time that arises directly or indirectly from the exclusions listed below.

Monitoring and Detection

Tigunia provides real-time monitoring and detection services for endpoints and identity services according to the selected service tier. Tigunia monitors telemetry data and responds to system and network device endpoint alerts. Tigunia will manage software that enforces identity security policies and responds to threats to user and identity services.

Endpoint Vulnerability Scanning

The SOC Service includes endpoint vulnerability scanning and remediation using the telemetry data from managed SIEM. Telemetry data is gathered from the XDR solution and integrated directly from endpoints.

Incident Response and Escalation

Incident Classification

Tigunia will classify incidents based on the severity and impact according to Tigunia's Incident Classification Policy and prioritize response actions depending on the service tier selected.

Classification Levels

Incidents are classified according to the severity of impact on Tigunia or Client data and their respective operations. Each classification level reflects the type of data involved and its classification, as per the Tigunia Data Classification Policy.

- **Low:** Minimal risk incidents involving data of lower sensitivity (*e.g.,* public or internal data).
- **Medium:** Moderate risk incidents that involve more sensitive or confidential data (*e.g.,* Client business data).
- **High:** Significant impact incidents involving sensitive data can potentially disrupt operations or damage the reputations of the Client or Tigunia.
- **Critical:** Incidents involving the highest-risk data (*e.g.,* personally identifiable information, financial data) that pose an existential threat to Tigunia or the Client.

Mapping of Incident Types to Classification Levels

Incident Type	Low	Medium	High	Critical
Undefined Security Incident			✓	
Data Exposure	✓	✓	✓	
Data Vulnerability	✓	✓	✓	
Information Disclosure		✓	✓	
Data Exfiltration		✓	✓	✓
Data Breach		✓	✓	✓
Ransomware			✓	✓

Incidents will be considered “Undefined” at the point of alert generation until they can be classified.

Incident SLA Initial Response Levels

Incident Response

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

The SOC will respond within the timeframes below, based on the classification and type of alert, per the intervals below.

Priority Level	Alert Acknowledgement	Response Interval / Escalation	SLA
P1 Critical	Within 15 Minutes	30 Minutes	96%
P2 Major	Within 30 Minutes	1 Hour	96%
P3 Intermediate	Within 1.5 Hours	4 Hours	96%
P4 General	Within 6 Hours	24 Hours	96%
P5 Informational	Within 1 Day	7 Days	96%

Limitations on Response

Tigunia’s response is limited to the features provided under the selected service tier. Tigunia is not responsible for resolving underlying vulnerabilities in systems, network devices, or identities beyond the detection and reporting obligations outlined for each service level.

Client Responsibilities

Endpoint Agent and Managed Software Maintenance: The Client will ensure that endpoint agents and managed identity software are installed, configured, and operational. Tigunia is not liable for service delays or failures due to malfunctioning software, systems, or user misconfigurations.

Data Classification and Compliance: Client agrees to comply with Tigunia's Data Classification Policy and will provide updated information on its data classification. Tigunia relies on accurate data classification to prioritize incidents.

Provision of Information: Client is responsible for providing Tigunia with any information, access, or credentials required to monitor the environment, respond to incidents, or manage identity services.

SOC Service Level

A specific list of use cases and the standard assigned priority levels will be agreed upon and issued to the Client before or during our onboarding process.

Based on the performance levels provided below, Client may receive a service credit that can be used against future purchases. Such credits will only be applied to charges for SOC services.

Alert Acknowledgement and Responses

Percentage of Time Meeting SLA	Service Credit
96% and Above	0
>=95% and <96%	5%
>=92% and <95%	10%
>=90% and <92%	15%
<90%	20%

SLA credit for Acknowledgment and Responses are tracked together per alert.

Exclusions

Acknowledgment and Responses will not be measured if due to the following:

- Connectivity issues between Client systems and the SOC.
- Emergency scheduled maintenance.

- Actions caused by Client staff or third parties that interrupt service.
- Events or conditions beyond Tigunia's control. Such events include, but are not limited to:
  - Acts of government authorities are not due to Tigunia's prior lack of conformance with regulations or law.
  - Natural disasters.
  - War, insurrection, riot, terrorism, or similar unlawful actions.
  - Suspension or termination of services provided under this agreement per our Master Services Agreement.

SLA Metrics for Reporting

All incidents and threat events are tracked and available for reporting on demand. Client and its agent must correctly configure and manage all Client devices. This includes:

- Daily verification that devices or applications receive signature updates.
- Monitoring the availability of new firmware or software versions.
- Changing default passwords and community strings.
- Documenting passwords in password managers.
- Documenting asset configurations with the agreed-upon level of configuration item detail.
- Confirming the separation of duties between production systems and backup systems that backup data.
- SNMP configuration or other API integrations to ingest data back to the SIEM.
- SIEM agent configuration and operation.

All security devices must pass an initial configuration audit before applying the Threat Event and Incident SLAs. Tigunia or its designated agent will perform this audit, and the results will be presented to Client within five business days of completion.

Service Credits

Service Credits are Client's sole and exclusive remedy for any performance or availability issues for any service under the Agreement and this SLA. You may not unilaterally offset Client's monthly service fees for performance or availability issues.

Service Credits apply only to fees paid for the Service, Service Resource, or Service tier for which a Service Level has not been met. In cases where Service Levels apply to individual service resources or to separate Service tiers, Service Credits apply only to fees paid for the affected service resource or Service tier, as applicable. The Service Credits awarded in any billing month for a particular service or service resource will remain within Client's monthly service fees for that Service or service resource in the billing month.

If Client purchased Services as part of a suite or other single offer, the applicable monthly service fees and Service Credit for each service will be pro-rated.

If Client purchased a service from another reseller, it could receive a service credit directly from that reseller.

Requesting Service Credits

The Client must request service credits within 5 days of the end of the affected month. The requests must be made in writing and include detailed documentation of the downtime.

Limitation of Service Credits

Service credits are the sole and exclusive remedy for failure to meet the uptime guarantee. Service credits are limited to the relevant invoice amount per calendar month.

Exclusions and Disclaimers

- **Service Credits**: Service Credits will not apply to any unavailability, suspension, or termination of services arising from:
  - Scheduled maintenance or system upgrades, provided Tigunia notifies the Client at least 24 hours in advance.
  - Client actions or omissions, including misconfiguration of endpoint agents or managed software.
  - Force majeure events, third-party disruptions, or circumstances outside Tigunia's control.

Disclaimer on Security Guarantees: Tigunia makes no guarantees that the Security Services provided will prevent any form of security incident, including but not limited to breaches, unauthorized access, or data loss. The services provided under this SLA are designed to reduce the risk of such events but cannot eliminate all risks. Tigunia shall not be held liable for any security incidents or resulting damages beyond the scope of the services explicitly provided.

Definitions

- **SIEM:** Security Information and Event Management (SIEM) is a single security management system that offers visibility into activity within the Client network and devices and empowers real-time response to events. The SIEM solution ingests and analyzes a high volume of data in seconds to detect and alert on unusual behavior and offers real-time insight to protect Client's business.
- **SOAR**: SOAR stands for Security Orchestration, Automation, and Response. The term describes three software capabilities – threat and vulnerability management, security

incident response, and security operations automation. SOAR allows companies to collect threat-related data from various sources and automate threat responses. 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 the 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 the knowledge of attacker tactics, techniques, and procedures (TTPs) and known indicators of compromise (IOCs). The SOAR uses multiple threat intelligence feeds (organized and analyzed information on potential and current threats) to supplement threat detection.

- **SOC**: A Security Operation Center (SOC) is a centralized function within an organization that employs 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. The SOC determines how each event will be managed and acted upon.
- **Security Incident**: Any event that compromises the confidentiality, integrity, or availability of information or information systems or violates security policies, standards, or practices of Tigunia or Client.
- **Breach**: An incident that results in the unauthorized acquisition, access, use, or disclosure of sensitive or protected information of Tigunia or Client.
- **Data Exposure**: A situation where sensitive or confidential information managed by Tigunia is unintentionally made accessible to unauthorized individuals or entities due to inadequate security measures.
- **Data Vulnerability**: A weakness or flaw in a system or process within Client's systems that could potentially allow unauthorized access to sensitive data belonging to the Client.
- **Information Disclosure**: The unauthorized or accidental release of Tigunia or Client confidential or sensitive information to individuals or entities that should not have access to it.
- **Data Exfiltration**: The unauthorized transfer or extraction of Client data from a system, network, or database to an external location controlled by an attacker.
- **Data Breach**: An incident with unauthorized access to, acquisition, or disclosure of sensitive, protected, or confidential data.
- **Ransomware**: A type of malicious software that encrypts Client data or locks users out of Client's systems and demands payment to restore access. Ransomware attacks can severely disrupt operations and cause significant damage.
- **Threat**: Any circumstance or event with the potential to cause harm to Client's information systems or data.
- **Vulnerability**: A weakness in Client's information systems, security procedures, or controls that a threat could exploit.

- **Impact**: The potential adverse effect on Client's operations, assets, or individuals, based on the severity of the incident.

Change Log

All changes are tracked by Tigunia's managed Governance Risk Compliance ("GRC") platform.