SERVICE LEVEL AGREEMENT

AUZA IT Services and Consultancy Inc.
Service Level Agreement – Managed Security Operations (SOC)
Document Version: 1.1
Last Updated: 01 January 2026

1. Purpose

This Service Level Agreement ("SLA") defines the service performance standards applicable to Managed Security Operations Center ("SOC") and Managed Security Service Provider ("MSSP") services provided by AUZA IT Services and Consulting Inc. ("AUZA").

The SLA establishes response-based service commitments relating to monitoring, detection, analysis, notification, and escalation of security events for covered services.

2. Relationship to the Master Service Agreement

This SLA forms part of, and is governed by, the Master Service Agreement for Managed SOC / MSSP Services ("MSA") between AUZA and the Client.

This SLA applies only to services expressly designated as subject to service level commitments in an applicable Statement of Work, Service Schedule, or Service Order.

In the event of a conflict, the following order of precedence applies:

1. Applicable Statement of Work or Service Schedule
2. This Service Level Agreement
3. Master Service Agreement

3. Scope of SLA Coverage

This SLA applies only to covered services, covered assets, covered tools and telemetry, and covered service tiers (L1, L2, and L3) as explicitly defined in the applicable Statement of Work or Service Schedule.

Services, systems, data sources, or activities not expressly included are excluded from SLA commitments.

4. Shared Responsibility Model

Consistent with the MSA, Managed SOC services operate under a shared responsibility model.

AUZA is responsible for monitoring agreed telemetry, performing alert triage and analysis, investigating security events based on available data, and notifying and escalating incidents in accordance with defined timelines.

The Client remains responsible for executing remediation and containment actions, maintaining systems and configurations, implementing security recommendations, and managing business continuity and disaster recovery.

Nothing in this SLA transfers operational control or decision-making authority to AUZA unless expressly agreed in writing.

5. Service Availability

SOC operating hours, availability targets, and maintenance windows are defined in the applicable Service Schedule.

Availability calculations exclude scheduled maintenance, client-initiated outages, force majeure events, failures of third-party tools or infrastructure, and telemetry gaps outside AUZA's reasonable control.

6. Incident Classification and Response

Security events are classified according to severity levels defined in the applicable Service Schedule or Incident Classification Matrix.

AUZA's SLA commitments relate to detection, analysis, notification, and escalation only. This SLA does not guarantee incident resolution, containment, or prevention.

7. Managed SOC Service Levels (L1 / L2 / L3)

7.1 SOC Tier Definitions

Level 1 (L1) – Monitoring and Triage

Includes continuous monitoring, alert validation, severity tagging, and escalation.

Level 2 (L2) – Analysis and Investigation

Includes in-depth investigation, event correlation, threat validation, and impact assessment.

Level 3 (L3) – Advanced Analysis and Advisory Support

Includes advanced threat analysis, incident advisory support, root-cause analysis, and strategic recommendations.

L3 services exclude hands-on remediation unless separately contracted.

7.2 SOC Service Scope by Tier

Tier	Activities
L1	Monitoring, triage, false-positive identification, escalation
L2	Investigation, correlation, incident confirmation
L3	Advanced analysis, advisory guidance, detection improvement

7.3 Response and Escalation Targets

Response targets apply only to covered services and are measured from the time an alert is generated within the monitored environment.

Severity	L1 Response	L2 Escalation	L3 Engagement
Critical	≤ 15 minutes	≤ 30 minutes	≤ 4 hours
High	≤ 30 minutes	≤ 1 hour	≤ 8 hours
Medium	≤ 2 hours	≤ 4 hours	As required
Low	≤ 1 business day	As required	Not applicable

Response targets represent initiation of analysis and notification, not resolution guarantees.

8. Support and Communication

Communication channels, escalation paths, and authorized contacts are defined in the applicable Service Schedule.

Notifications may be delivered through agreed channels such as email, ticketing systems, or client portals.

9. SLA Exclusions

SLA commitments do not apply to incidents arising from client-controlled systems or configurations, unsupported or unmanaged tools, third-party service failures, data quality or telemetry limitations, client delays in providing access or information, or force majeure events.

10. Service Credits (if Applicable)

Where service credits apply, eligibility and calculation methods shall be defined in the applicable Service Schedule.

Service credits, if provided, are capped, constitute the sole and exclusive remedy for failure to meet service levels, and do not modify liability limitations under the MSA.

11. Continuous Improvement

AUZA may refine detection logic, workflows, and analytical processes to improve service quality.

Such improvements do not alter contractual service level commitments unless formally agreed in writing.

12. Changes to the SLA

This SLA may be updated to reflect changes in service offerings, operational processes, or legal requirements.

Material changes affecting service commitments require mutual agreement or must follow the amendment provisions of the MSA.

13. Availability of the SLA

The official and current version of this Service Level Agreement is made available in PDF format through a secure download mechanism, ensuring controlled access to the authoritative service standards applicable to the engagement.