Justin Lew

Security Operations Center (SOC) Service Level Agreement (SLA)

1. Introduction This Service Level Agreement (SLA) defines the expectations, response times, escalation procedures, and performance metrics for the Security Operations Center (SOC). This document ensures incident handling and a clear understanding between stakeholders regarding security monitoring and response obligations.

2. Scope of Services The SOC provides continuous security monitoring, threat detection, incident response, forensic investigation, and mitigation services. This SLA applies to all security incidents detected within the monitored network infrastructure. It covers both proactive and reactive threat management.

---

3. Response Time Commitments

Incident Severity	Description	Initial Response Time	Detection Time	Mitigation Timeframe
Critical-1	Active security breach affecting business continuity or sensitive data	15 minutes	5 minutes	4 hours
Critical-2	High-risk vulnerability exploitation with immediate risk	15 minutes	15 minutes	6 hours
High	Severe vulnerability exploitation with potential business impact	30 minutes	30 minutes	8 hours

Medium	Potential security threats requiring further investigation	1 hour	1 hour	24 hours
Low	Routine alerts and non-urgent vulnerabilities	4 hours	4 hours	72 hours

Additional Notes:

- The **Detection Time SLA** ensures that security threats are identified within a specific timeframe post-occurrence.
- **Response Times** are contingent upon the severity classification and SOC's monitoring capabilities.

---

4. Escalation Procedures

1. **Tier 1 (SOC Analyst):** Initial triage, validation, and classification of alerts. Escalates unresolved critical incidents within 10 minutes.
2. **Tier 2 (Incident Responder):** Deep investigation, containment, and remediation recommendations. Coordinates with internal IT and compliance teams.
3. **Tier 3 (SOC Manager/Security Engineer):** Handles advanced threat remediation, forensic investigation, and root cause analysis.
4. **Third-Party Coordination:** If applicable, the SOC engages with external cybersecurity vendors or law enforcement.
5. **Executive & Stakeholder Notification:** Critical-1 incidents must be reported to executives within 30 minutes.

---

5. Key Metrics for Performance Tracking

- **Mean Time to Detect (MTTD):** Average time taken to identify security incidents.
- **Mean Time to Respond (MTTR):** Average time taken to remediate and resolve security incidents.
- **False Positive Rate (FPR):** Percentage of alerts incorrectly classified as threats.
- **Incident Closure Rate:** Percentage of incidents resolved within the committed response time.
- **Dwell Time:** The total time an attacker remains undetected in the network.

- **Containment Time:** Time required to neutralize a security event.
- **Recovery Time:** Time taken to restore normal operations after an incident.

---

6. Example Incident Response: <u>Ransomware Attack</u>

Scenario:
At **2:00 AM**, the SOC detects unusual file encryption activity on an internal file server. The incident is classified as **Critical-1** due to potential business disruption.

Response Timeline (As per SLA Commitments)

Time	SOC Action	Responsible Team
2:05 AM	Detection triggered via SIEM	Tier 1 Analyst
2:10 AM	Initial triage confirms ransomware indicators	Tier 1 Analyst
2:15 AM	Escalation to Tier 2 for containment	Tier 1 → Tier 2
2:30 AM	Critical-1 notification sent to IT Security Lead	Tier 2
3:00 AM	Firewall rules updated to isolate infected machines	Tier 2
4:00 AM	Incident reported to executive stakeholders	SOC Manager

6:00 AM	Containment completed, forensic analysis begins	SOC Engineer

Performance Metrics Applied:

- **MTTD:** 5 minutes
- **MTTR:** 4 hours
- **Containment Time:** 3 hours
- **Dwell Time:** ~2 hours (based on logs)

Regulatory Actions:

- If PII was compromised, **GDPR notification must be filed within 72 hours**.
- Affected stakeholders must receive a **data breach disclosure**.

Post-Incident Report Template:

- **Incident Summary:** (Brief overview of the attack)
- **Root Cause Analysis:** (Entry point, vulnerabilities exploited)
- **Corrective Actions:** (Patching, system recovery, SOC improvements)
- **Recommendations:** (Additional security measures)

---

7. Service Scope & Responsibilities

- **Threat Hunting:** The SOC proactively searches for hidden threats beyond automated alerts.
- **Penetration Testing & Red Teaming:** Scheduled offensive security testing is conducted quarterly.
- **Forensics & Compliance:** Ensures compliance with GDPR, HIPAA, ISO 27001, and other industry regulations.
- **Incident Reporting:** All security incidents are documented in a standardized format within the SIEM system.
- **Stakeholder Communication:** SOC will provide detailed reports and updates based on incident severity levels.

---

8. Memorandum of Understanding (MOU) vs. Memorandum of Agreement (MOA)

Aspect	Memorandum of Understanding (MOU)	Memorandum of Agreement (MOA)
Definition	A non-binding document outlining general terms of cooperation	A legally binding document detailing specific responsibilities
Legal Enforceability	Not legally enforceable	Legally enforceable
Level of Detail	High-level understanding of roles	Detailed scope, responsibilities, and expectations
Use Case	Used for initial discussions and partnerships	Used for finalized agreements with detailed commitments
Example	Agreement between internal teams for security collaboration	Formal contract with third-party SOC provider to deliver security services

---

9. Compliance & Regulatory Considerations

- **Alignment with Security Frameworks:** This SLA follows **NIST 800-61, ISO 27001, CIS Controls**.
- **Data Retention Policy:** Incident logs and forensic reports are retained for **12-24 months**.
- **Regulatory Reporting:** If applicable, breaches must be reported per compliance requirements (e.g., GDPR within **72 hours**).

---

10. Review & Updates This SLA will be reviewed **quarterly** to ensure alignment with evolving security threats and business requirements.

---

11. Acknowledgment By signing this document, all parties agree to the terms and conditions outlined within the SOC Service Level Agreement.

Signatures

SOC Manager: _____ Date: _____

IT Security Lead: _____ Date: _____

Executive Sponsor: _____ Date: _____