# Terms and Conditions

## 24×7 SOC Services (Monitoring + Remediation) - Schedule CS-6

Effective Date: October 14, 2025 | Supersedes prior versions.

**Service Summary**
Service Provider shall provide 24/7 Security Operations Center ("SOC") Services ("24/7 SOC Services") to continuously monitor, analyze, and remediate security alerts generated by the Extended Detection & Response (XDR) platform selected under Schedule 3A. These services extend Service Provider's XDR monitoring capabilities by adding continuous human-led remediation during and outside of business hours, including evenings, weekends, and holidays.

**Scope of Services**
- Continuous monitoring of security alerts from the Client's Adlumin/N-able XDR platform (Mailbox-Only, Standard Agent, or Advanced Agent, as applicable).
- Initial triage and classification of detected XDR events.
- Execution of approved containment and remediation actions supported by the XDR platform (e.g., disabling user accounts, forcing sign-outs, resetting credentials, isolating endpoints).
- Escalation of high-severity XDR events to Client-designated contacts for decision-making.
- Documentation of alerts, actions taken, and escalation activities in Service Provider's ticketing system.
- Periodic reporting of significant XDR events and trends.

**Exclusions**
- Security alerts or remediation outside the scope of the Adlumin/N-able XDR platform (e.g., Harmony Checkpoint Email Security, DNSFilter, or other third-party tools not integrated with XDR).
- Full incident response (IR), forensic investigation, or legal/regulatory reporting (available separately).
- Guarantee of prevention or detection of all attacks, including zero-day exploits or advanced persistent threats.
- Responsibility for business, regulatory, or legal obligations following a security incident.
- Remediation of non-security infrastructure issues (covered under NOC or other Schedules).

**Client Responsibilities**
- Maintain valid licensing and coverage under Schedule 3A – Extended Detection & Response (XDR), which is a prerequisite for 24/7 SOC Services.
- Provide Service Provider with necessary permissions and administrative access to execute remediation actions supported by the XDR platform.
- Keep escalation contacts current and available for high-severity event notifications.
- Act on recommendations for long-term remediation or policy changes following escalations.
- Retain responsibility for executing business, legal, or regulatory actions required after a security incident.

**General Terms**
- 24/7 SOC Services extend Service Provider's XDR monitoring by adding continuous human-led remediation. These services are limited to alerts and actions supported by the Adlumin/N-able XDR platform and expressly exclude other security platforms not integrated with XDR.
- Client acknowledges that 24/7 SOC Services are one element of a layered defense strategy. While continuous monitoring and remediation significantly reduce risk, no service can guarantee prevention of all security incidents. Even the most advanced SOC operations remain subject to bypass or compromise.
- All response times for SOC-related service requests are governed by the Service Level Objectives in Schedule A of the Master Service Agreement, unless otherwise specified in writing.
- Fees for this Schedule are billed in accordance with the Payment Terms of the Master Service Agreement. Required platform licensing is included in Service Provider's standard service fees unless otherwise specified. Additional costs (e.g., extended log retention, custom integrations, or specialized response services) may apply and will be billed separately.