

### SentinelOne EDR - Schedule CS-1

#### Service Summary

Service Provider will provide Endpoint Detection and Response (“EDR”) services through SentinelOne, deployed on Client’s covered endpoints. The service detects, contains, and remediates malicious activity using real-time monitoring and automated response. SentinelOne EDR enhances but does not replace Client’s overall cybersecurity posture and is limited to the functions described in this Schedule.

#### Included Services

- Deployment and licensing of SentinelOne agents on covered endpoints.
- Continuous monitoring for malware, ransomware, and other suspicious activity.
- Automated response actions (e.g., process termination, file quarantine, rollback) per SentinelOne capabilities and policy settings.
- Alert generation and integration into Service Provider’s ticketing system.
- Incident triage and remediation of SentinelOne alerts.
- Regular agent updates, policy configuration, and threat intelligence feeds.

#### Exclusions

- Security monitoring or log management beyond endpoints (covered under separate MDR or SOC Schedules).
- Support for third-party or Client-owned security solutions not managed by Service Provider.
- Guaranteed prevention of incidents, breaches, or data loss.
- Root-cause analysis or forensic investigation unless separately contracted.
- Response to threats outside SentinelOne’s scope (e.g., network intrusion, email compromise, cloud breaches).
- Data recovery or restoration (covered under Backup/DR Schedule).

#### Client Responsibilities

- Ensure covered endpoints meet SentinelOne requirements.
- Permit installation, updates, and management of EDR agents.
- Promptly report suspected threats or unusual activity.
- Maintain compliance with Service Provider security policies (e.g., MFA, patching).
- Authorize escalation to Project or MDR services when broader remediation is required.

#### General Terms

- Services are limited to SentinelOne capabilities as configured by Service Provider. No guarantee of complete threat prevention is provided.
- Incident response times are governed by the Service Level Objectives in Schedule A of the Master Service Agreement.
- Fees are billed in accordance with the Master Service Agreement’s Payment Terms. Vendor pass-through costs may apply.