SERVICE DESCRIPTIONS

Exhibit E to the Master Subscription Agreement

Version 1.3

H&A Security Solutions, LLC d/b/a Tellaro — 12178 N 1450th Street, Effingham, Illinois 62401

SERVICE DESCRIPTIONS

This Service Descriptions exhibit (this "Exhibit E") describes the Plans, the Tellaro Security Operations Platform, and the add-ons and standalone services available for purchase. The Service purchased by Customer is identified on the applicable Order Form. This Exhibit is incorporated into the Master Subscription Agreement and, for self-hosted deployments, into the End User License Agreement — On-Prem.

Customer purchases one of the following Plans, identified on the Order Form:

- **Platform Plan.** The Platform (Section 1), operated by Customer's own personnel. Available on SaaS, Hybrid, and self-hosted deployments.
- **Managed Plans: Identity, Protect, Defend, and Command.** The Platform together with the 24/7 MSOC service, with the scope for each Plan set out in Section 2. Available on SaaS and Hybrid deployments.

Add-ons and standalone services are described in Section 3. Fees are set out on the Order Form.

1. THE TELLARO SECURITY OPERATIONS PLATFORM

1.1 Overview.

The Tellaro Security Operations Platform (the "Platform") is an extended detection and response solution that collects, correlates, and analyzes telemetry from across Customer's IT environment. The Platform provides log ingestion, parsing and normalization, correlation, real-time alerting, dashboarding, and historical search capabilities.

1.2 Capabilities.

- Log Data Collection and Aggregation across servers, network devices, applications, security tools, and cloud services.
- Parsing and Normalization to a common naming schema, ensuring searchability.
- Real-Time Monitoring and Alerting on configured detection rules.
- Correlation and Analytics to identify patterns and prioritize alerts.
- Dashboards and Reporting (predefined and customizable).
- Authentication via local accounts, SAML, or SSO.

- Web-based access for Authorized Users.
- Tellaro-managed platform monitoring (SaaS and Hybrid deployments) or operational telemetry (self-hosted deployments).
- Onboarding support and training during initial deployment (up to four (4) remote sessions during the first sixty (60) days).

1.3 Retention.

SKU	Retention Period	Searchable Window	Archived Window
Extended (SaaS only)	1 year	365 days	—
Standard	1 year	90 days	275 days

Searchable data is available through interactive query within the Platform. Archived data is recoverable upon request, with retrieval time as set forth in the Documentation. Retention is calculated from the date data is ingested.

Standard retention applies unless the Order Form lists Extended retention. Extended retention is available on SaaS deployments of the Defend, Command, and Platform Plans. Endpoint agent telemetry is retained for fourteen (14) days.

On self-hosted and Hybrid deployments, data is stored on infrastructure Customer provides and Customer controls retention. Tellaro configures Standard retention as a default, which Customer may change; Extended retention does not apply.

The Service is not a system of record or backup service. Customer is responsible for retaining any data it must keep for legal, regulatory, litigation-hold, or audit purposes beyond the retention period of its Plan, and Tellaro will have no liability for data deleted in accordance with the applicable retention period.

1.4 Ingest Allowance.

For SaaS deployments of the Defend, Command, and Platform Plans, the Service includes an ingest allowance of 0.5 GB per Workstation per day and 1 GB per Server per day, pooled across Customer's environment. Network security monitoring sensor traffic counts toward the allowance. Tellaro will report ingest above the allowance to Customer. Ingest above the allowance on those deployments is billed at the overage

rate set forth on the Order Form. No ingest allowance or overage applies to self-hosted or Hybrid deployments, where data is stored on infrastructure Customer provides.

1.5 What Is Included.

- Onboarding assistance for sensor deployment and initial input configuration.
- Unlimited Authorized User accounts (no per-user fees; subject to the AUP and Customer's obligation not to share credentials).
- Access to Tellaro default detection rules, case templates, and Intel Lists, and the ability to create custom detection rules, case templates, and Intel Lists.
- Standard support during onboarding and ongoing platform maintenance.

1.6 Not Included in the Platform Plan.

- 24/7 alert triage, incident response services, or analyst review of alerts (available in the Managed Plans).
- Managed vulnerability scanning (available as Tellaro VMS; see Section 4).
- Endpoint detection and response or managed detection and response of endpoint telemetry (available in the Protect, Defend, and Command Plans).
- Custom rule development or threat-hunting engagements beyond those included in Customer's Plan (available via Statement of Work under the Professional Services Agreement).

2. MANAGED PLANS: 24/7 MSOC

2.1 Overview.

Each Managed Plan includes the Managed Security Operations Center ("MSOC") service, which provides around-the-clock alert monitoring, triage, and incident response support delivered by Tellaro analysts. Managed Plans are available on SaaS and Hybrid deployments. On Hybrid deployments, the MSOC works through the Tellaro search proxy described in the Hybrid Deployment Exhibit (Exhibit H).

2.2 Included Services.

- 24/7 Continuous Monitoring of alerts and other security telemetry within the scope of Customer's Plan (Section 2.2A).
- Alert Triage / Review: Tellaro analysts establish an initial assertion (true positive vs. false positive) for each alert and recommend next steps.

- Incident Response Level 1 (detection and analysis; recommendations for containment).
- Incident Response Level 2 (remote only; a dedicated analyst for each confirmed incident, providing deeper analysis and guidance through containment, eradication, and recovery, up to forty (40) analyst hours per incident and one hundred twenty (120) analyst hours per contract year, with additional hours available under a Statement of Work or incident response retainer at Tellaro's then-current rates).
- Regular reporting on security posture and alert dispositions.

2.2A Scope by Plan.

In addition to the services in Section 2.2, each Managed Plan includes the following. Each Plan includes everything in the Plans listed before it.

- Identity: monitoring of Microsoft 365, Entra ID, and on-premises Active Directory, with account containment.
- Protect: managed detection and response on every Device through the EDR Provider (Sections 5 and 5A); creation and validation of detection rules on EDR and Microsoft 365 data; EDR policy management, device control, and endpoint firewall control; and, where the EDR provides application inventory and vulnerability data, prioritization of vulnerable software on covered endpoints.
- Defend: monitoring of firewall, server, cloud, and Microsoft 365 logs; creation and validation of detection rules based on common or emerging threats facing Customer; an annual MITRE ATT&CK gap assessment identifying visibility and detection gaps; managed vulnerability scanning through Tellaro VMS (Section 4); and vulnerability and compliance baselines.
- Command: monitoring of all connected logs, including workstation logs; threat hunting; monitoring of Customer's network security monitoring sensors; file integrity monitoring and application inventory; and custom dashboards.

Threat hunting, phishing triage, and the other add-ons available for each Plan may be purchased on an Order Form. A MITRE ATT&CK gap assessment may be purchased as a one-time service with the Identity, Protect, or Platform Plan.

2.3 Response Targets.

MSOC response targets are set forth in the Service Level Agreement (Exhibit A), Section 3.

2.4 HIPAA-Regulated Customers.

Where Customer is a Covered Entity or Business Associate under HIPAA, MSOC analysts may encounter Protected Health Information (PHI) within the alerts, case data, and telemetry they review. A signed Business Associate Agreement (Exhibit D) is required before MSOC service begins for HIPAA-regulated Customers. Tellaro MSOC analysts are bound by the BAA terms with respect to PHI, including limitations on Use and Disclosure, safeguards, breach notification, and Subcontractor controls. Customer is responsible for configuring data sources and detection content to avoid sending unnecessary PHI to the Service.

2.5 Out of Scope.

The MSOC service does not include: legal representation; data-breach notification services; collection or preservation of forensic evidence for legal proceedings; on-site response; ransomware negotiation, ransom or extortion payment, or other dealings with threat actors; determinations of whether a breach-notification obligation exists; communications with regulators, law enforcement, insurers, or the media on Customer's behalf; or restoration of systems or data from backup. Tellaro will not facilitate any payment that would violate U.S. sanctions laws. Such services may be procured under a separate Statement of Work.

3. ADD-ONS AND STANDALONE SERVICES

3.1 Add-Ons.

The following add-ons may be purchased on an Order Form with the Plans shown, on SaaS and Hybrid deployments. Where an add-on is included in Customer's Plan, it is not purchased separately.

- **Threat Hunting (included in Command; available with Identity, Protect, and Defend).** Tellaro analysts proactively search Customer's data for attacker activity that did not generate an alert, using current threat intelligence and the techniques observed in active campaigns. Findings are investigated and handled as incidents where warranted.
- **Phishing Triage (available with all Managed Plans).** Tellaro analysts review emails that Customer's users report as suspicious, determine whether they are malicious, and take or recommend action, including removal of matching messages where access allows.

- **Extended Retention (available with Defend, Command, and Platform; SaaS deployments only).** Logs are searchable for 365 days, and endpoint telemetry collected by the Tellaro agent is searchable for 30 days.
- **File Integrity Monitoring and Application Inventory (included in Command; available with Defend and Platform).** The Tellaro agent monitors critical system files and configuration for unauthorized change and maintains an inventory of installed applications across covered endpoints. Changes are visible in the Platform and, under a Managed Plan, reviewed by Tellaro analysts.
- **Vulnerability and Compliance Baselines (included in Defend and Command; available with Platform).** The Tellaro agent matches installed software against known vulnerabilities and checks covered systems against configuration baselines, including DISA STIG, the macOS Security Compliance Project, and Microsoft security baselines.
- **Network Security Monitoring Sensors (included in Command; available with Defend).** The MSOC monitors network security monitoring sensors that run the Tellaro agent's sensor role on hardware Customer provides.

3.2 Standalone Services.

The following services may be purchased with any Plan or on their own, including by self-hosted customers:

- **Tellaro VMS (included in Defend and Command).** Managed vulnerability scanning, as described in Section 4.
- **SentinelOne Licensing.** SentinelOne Singularity Complete licenses with Tellaro console administration and support, as described in Section 5.
- **MITRE ATT&CK Gap Assessment (one-time; included in Defend and Command).** Tellaro analysts map Customer's existing visibility and detections against the MITRE ATT&CK framework, considering both prevalent industry threats and those specific to Customer, identify gaps in visibility or detection that could be exploited, and provide a road map for addressing them.

4. MANAGED VULNERABILITY SCANNING (TELLARO VMS)

4.1 Overview.

Tellaro VMS is Tellaro's managed vulnerability scanning service. It provides regular vulnerability scanning of Customer assets using scanning software licensed and managed by Tellaro. Tellaro VMS is included in the Defend and Command Plans and may be purchased with the Platform Plan or on its own. Scan results are surfaced within the Platform alongside other security telemetry.

Customer does not need its own scanning software license. The scanning software is licensed to Tellaro, and Customer receives no rights in it.

4.2 Included Services.

- Deployment of a Tellaro VMS scanner within Customer's environment (or, where applicable, agent installation on portable assets).
- Scheduled scans of in-scope assets identified by Customer, on a schedule agreed during onboarding and at least monthly, with a prioritized remediation list after each scan cycle.
- Customizable scan policies tailored to Customer's environment.
- Detailed reports identifying vulnerabilities, severity, and remediation guidance.
- Integration of vulnerability data into the Platform.

4.2B Scan Scope and Impact.

Customer is responsible for identifying in-scope assets and represents that it owns or is authorized to permit scanning of each of them (MSA Section 3.5). Vulnerability scans can affect the performance or stability of some systems, including operational technology, medical devices, and legacy systems. Customer will identify any asset that should be excluded or scanned with restricted policies, and Tellaro is not responsible for any disruption resulting from scans performed within the agreed scope and schedule.

4.2A Optional Compliance Audit Scans.

Where listed on the Order Form, Tellaro VMS includes compliance audit scans that check configuration settings of in-scope assets against published benchmarks for frameworks Customer identifies (for example, PCI DSS or HIPAA). Compliance audit scans report configuration findings only. They do not certify, attest to, or establish Customer's compliance with any law, regulation, or standard. Tellaro VMS is not an

Approved Scanning Vendor (ASV) scan under PCI DSS unless the Order Form expressly states otherwise, and Tellaro is not acting as a Qualified Security Assessor, auditor, or assessor of record. Compliance audit scans are part of Tellaro VMS only and are not part of the vulnerability and compliance baselines in the Platform.

4.3 HIPAA-Regulated Customers.

Tellaro VMS scanning is performed against Customer assets that may host Protected Health Information (PHI). Scan results, while typically configuration and vulnerability metadata, may incidentally include identifiers or other information that could be considered PHI in context. Where Customer is a Covered Entity or Business Associate under HIPAA, a signed Business Associate Agreement (Exhibit D) is required before Tellaro VMS begins. Tellaro will store and process scan results subject to BAA terms.

4.4 Out of Scope.

- Active exploitation, penetration testing, or social-engineering testing.
- Remediation of identified vulnerabilities (Customer is responsible for remediation; Tellaro can assist via Statement of Work).

5. SENTINELONE SINGULARITY COMPLETE LICENSING

5.1 Overview.

Tellaro holds SentinelOne Singularity Complete licenses and provides them to Customer as part of Tellaro's services. SentinelOne licensing is the default EDR Provider in the Protect, Defend, and Command Plans and is also available license-only as a standalone service, including to self-hosted Platform customers (with Tellaro console administration and support, without SOC monitoring). Monitoring, triage, and response on SentinelOne telemetry are performed by Tellaro analysts as part of the applicable Plan; SentinelOne does not provide managed detection and response under this section. SentinelOne licensing is subject to the SentinelOne Third-Party Terms (Exhibit F), which Customer agrees to as a condition of purchase.

5.2 Included (subject to SentinelOne's scope and policies).

- SentinelOne Singularity Complete platform with endpoint protection.
- Tellaro provisioning, console administration (agent deployment, policy management, and upgrades), and support.

5.3 Out of Scope.

- Warranties as to SentinelOne services beyond the Tellaro warranty in Exhibit F Section 3.1; SentinelOne services are otherwise subject to Exhibit F.
- Customer's direct contractual relationship with SentinelOne; the contractual relationship is between Tellaro and Customer, with SentinelOne as a Tellaro Sub-Processor or vendor.

5A. CUSTOMER-PROVIDED EDR

5A.1 Overview.

For the Protect, Defend, and Command Plans, Customer may use its own endpoint detection and response product instead of SentinelOne licensing through Tellaro (a "Customer-Provided EDR"), provided the product appears on Tellaro's list of supported EDR products in the Documentation. The Order Form identifies the Customer-Provided EDR and the applicable credit.

5A.2 Customer Responsibilities.

- Customer maintains the license, vendor contract, vendor support, and product coverage for the Customer-Provided EDR, and keeps its agent deployed and current on all Devices counted on the Order Form.
- Customer grants Tellaro analyst access to the product's management console and API sufficient to monitor, investigate, and triage alerts.
- For the Defend and Command Plans, Customer grants Tellaro response rights in the console for the pre-authorized actions (such as host isolation) agreed during onboarding. For the Protect Plan, response rights are optional.

5A.3 Limitations.

- Tellaro is not responsible for the Customer-Provided EDR's failure to detect, prevent, or carry out an action, or for the acts or omissions of its vendor.

If Customer does not maintain the Customer-Provided EDR on any counted Device, Tellaro's obligations for that Device under the Plan are suspended until coverage is restored, and fees continue to accrue.

- Where Customer has not granted response rights, or revokes them, any containment commitment in the Service Level Agreement does not apply; Tellaro will recommend response actions and Customer will carry them out.

6. DEPENDENCIES

Each add-on in Section 3.1 requires an active Plan with which it is available, under the same Agreement. Standalone services in Section 3.2 may be purchased without a Plan. Add-ons and services not described in this Exhibit are not offered under it.