Threat & Vulnerability Management (TVM)
Solution Description

The following is included as part of the Threat & Vulnerability Management (TVM) Cyvatar Cybersecurity Solution, which shall be delivered in accordance with and subject to the terms of this Solution Description and the terms and conditions of the Agreement:

- Vulnerability Management
- Patch Management
- Internal & External Vulnerability Scanning
- Automated External Network Penetration Assessment

1. Member Delivery.

1.1. Security Engineer. As part of the Threat & Vulnerability Management (TVM) Solution, the Client will get access to a Cyvatar "Security Engineer" who will oversee the delivery of the solution.

1.2. Security Engineer Schedule & Tasks. The Security Engineer shall create a mutually agreed upon schedule to facilitate the delivery of the events/tasks set forth below. Notwithstanding the foregoing, all timelines, deliverables, and implementation efforts outlined in any mutually agreed schedule are estimates only.

1.2.1. Installation and Configuration of Third-Party Product (s). Cyvatar shall oversee the installation and configuration of the relevant Third-Party Product(s) which are approved by Client for installation into Client's environment. The potential list of Third-Party Product(s) which may be relevant to the delivery of the Solution is listed in Section 4 below. The actual Third-Party Product(s) installed/configured shall be approved by Client.

1.2.2. Assessment. Cyvatar shall continuously assess the risks identified by the relevant Third-Party Product(s) available and shall also assess gaps based on security best practices. Risks and gaps identified by the relevant Third Party Product(s) shall be documented with recommendations for remediation.

1.2.3. **Remediation.** Cyvatar shall continuously review the risks and gaps identified through the assessment and shall work with Client to develop a remediation plan and schedule. Cyvatar shall lead the remediation until identified risks and gaps are remediated, to the extent reasonably possible and approved by Client. Remediation work shall only be conducted after Client has agreed to recommended actions.

1.2.4. **Maintenance of Remediated Status.** Once all identified risks and gaps are remediated through the remediation plan (as defined in Section 1.2.3. above), to the extent reasonably possible and approved by Client, Cyvatar shall assist in maintaining that remediated status throughout the Subscription Term. Any remediation work shall only be conducted after Client has agreed to recommended actions.

1.2.5. **Monthly Executive Reporting.** Cyvatar shall deliver monthly reporting; the specific parameters reported shall be as mutually agreed.

2. **Client Obligations.** Client understands and agrees that in order for Cyvatar to provide the Threat & Vulnerability Management (TVM) Cyvatar Cybersecurity Solution, including relevant Professional Services, Cyvatar will need access to certain Client resources, personnel, and systems. As such, Client agrees to the following:

2.1. Client shall identify an internal point of contact for this engagement.

2.2. Client shall provide relevant information on proposed applications and computing systems, users, and data.

2.3. Client is responsible for the initial installation of the Third-Party Product(s) with the remote targeted assistance of Cyvatar.

2.4. Client is responsible for network, host, or cloud availability at all times; lack of network, host, or cloud readiness may result in lack of productivity and ability to provide Threat & Vulnerability Management (TVM) Cyvatar Cybersecurity Solution.

2.5. Client shall provide Cyvatar with necessary documentation, as needed.

2.6. Client will schedule any interviews with the appropriate individuals, as requested by Cyvatar.

3. **Included Third Party Product Licenses.** The Threat & Vulnerability Management (TVM) Cyvatar Cybersecurity Solution shall include reselling of licenses to certain of the following Third-Party Products listed below. The specific Third-Party Product(s) to be licensed, resold, and installed shall be determined by the number and type of assets monitored and/or managed as part of the solution, technical requirements, and recommendations of Cyvatar after discussions with Client. The final list of Third-Party Product(s) shall be approved by the Client after Cyvatar recommendation. The Third-Party Terms that are relevant to the Third-Party Products are listed below. Client agrees that as part of approving the Third-Party Product for installation, it agrees that it has reviewed and is approving the Third-Party Terms relevant to the use of the Third-Party Product.

Third Party Product (Resale)	Third-Party Terms
NinjaOne	https://www.ninjaone.com/license-agreement/
Automox	https://www.automox.com/legal/terms-of-use
Tenable.io	https://cloud.tenable.com/print-eula.html
Vonahi Security (A Kaseya Company)	https://www.kaseya.com/legal/kaseya-master-agreement/

4. **Exclusions**.
   - **4.1.** None of the above shall be performed onsite by Cyvatar.
   - **4.2.** None of the above shall include Cyvatar acting as an incident response team.
   - **4.3.** Notwithstanding anything to the contrary in this Agreement, Cyvatar shall

not be required to provide end user access to the Third Party Product or any component of the Solutions to the Client.