Network Operations Center (NOC) - Definition of Services and Components (DSC)

Introduction

This document describes the services delivered by Tigunia, LLC, according to the relevant Statement of Work and Tigunia's Master Services Agreements ("MSA").

The descriptions, features, and scope of Tigunia's Network Operations Center ("NOC") are referenced below. This service has three separate tiers of features available. The Standard and Premium tiers are built on the features of the lower tier(s) and have increased service depth and complexity. The offerings herein are collectively referred to as the "Services."

Objective (Mission Statement)

The Network Operations Center ("NOC") supports the availability, integrity, and security of a Client's systems, networks, and essential technology operations.

Service Tiers & Definitions

Tigunia offers three tiers of NOC service, each with distinct levels of support and performance. Each tier delivers the services of the prior tiers plus additional services. Client retains the right to elect in to or out of any of the features listed under each service and their corresponding service tiers defined herein.

NOC Core

NOC Core is the basic NOC Service Tier. Clients in this tier are provided with the tooling and configurations for an NOC but self-manage the servers and monitoring.

- **Remote Monitoring and Management—Alert Monitoring and Auto Remediation:** Tigunia NOC services are backed by proprietary monitors and automation that ensure Client systems continue running as expected. Tigunia's automation will automatically remediate many alerts without user interruption. All generated alerts are available in the Client Portal for review and remediation.
- **Managed Windows OS Patching:** RMM automatically handles patch deployment, and Client manages system reboots for patches that require a system restart.

- **Managed Detection and Response for Endpoints:** The NOC services Clients use Tigunia's Managed Detection and Response (MDR) platform for any Windows or Mac OS device enrolled in RMM. MDR provides antivirus, anti-malware, foothold detection for potentially risky software, and ransomware detection.
- **Access to Client Management Portal:** This portal provides Clients with a centralized platform to create and review cases and access all Tigunia-provided reporting. Its user-friendly interface streamlines access to Tigunia services.
- **Basic Service Reporting:** Tigunia delivers reporting for the services that Client uses, including case metrics, agent health, and more. These reports will help you to understand how IT resources are utilized, identify areas for improvement, and make informed decisions about possible future investments and strategies.
- **Service Availability Commitment:** This is a **tooling-only** service. No support SLAs are provided, and only the availability of the tooling is guaranteed. The SLA for **tooling availability** is **99.9%**, ensuring the monitoring tools are functional and accessible.

NOC Standard

Standard Clients no longer self-manage and monitor their servers; instead, NOC manages these services. In addition to managing alert monitoring and response, NOC will begin performing maintenance and providing Client custom alert responses as requested. This includes all features of NOC Core.

- **24/7 NOC Support:** NOC Services are 24x7x365, and Endpoints and Infrastructure are monitored continuously for warnings and errors.
- **Remote Monitoring and Management—Alert Management and Custom Response:** Tigunia's NOC Team will manage the initial response to alerts and attempt to remediate any issues not addressed by scripted automation. At Client's discretion, we can defer issues to a contact at any point. Please refer to the Service Level Agreement document for more specific information.
- **Remote Monitoring and Management—Tailored Scripting:** Custom Scripts can be developed at Client's request. Depending on the complexity and requirements of the request, this may require resources from outside of NOC systems.
- **Pre/Post Reboots & Validation:** Tigunia's NOC team will manually initiate reboots at an agreed-upon cadence to ensure automated patches are properly applied. Service functionality will be validated before and after reboots and patching.
- **Monthly Server Maintenance: The NOC team reviews servers receiving maintenance manually** every month for issues not detected by Automation. They also validate that

the automation is running correctly, review system performance, and perform system scanning.

- **SQL Server Maintenance:** SQL Servers receiving maintenance are reviewed by hand monthly to configure and execute SQL maintenance jobs.
- **MDR For O365:** Tigunia Clients utilizing NOC services are entitled to use Tigunia's Managed Detection and Response (MDR) platform for any Windows or Mac OS Device enrolled in RMM. This provides antivirus, antimalware, foothold detection for potentially risky software, and ransomware detection.
    - **Endpoint Security – Extended Detection and Response (XDR):** Tigunia will utilize our Extended Detection and Response (XDR) platform to protect endpoints further, block malicious actions and files as they appear, and investigate potential threats.
- **Server Endpoints—Vulnerability Scanning and Remediation:** The NOC Team will review and attempt remediation for operating system (OS) and configuration vulnerabilities. Our system agents perform this to inform patching activities based on identified OS vulnerabilities. Some configuration changes may require Client consultation before they can be remediated. Non-line-of-business application patching (Web Browser Patching, Adobe Acrobat, etc.) will also be attempted when possible.
- **Public Key Infrastructure Management:** Tigunia's NOC will document and manage the rotation of SSL certificates, code signing certificates, and other Client secrets.
- **Fortified Monitoring ("FoMo")—Custom Solutions:** The NOC will deploy our Fortified Monitoring solution and provide in-depth performance logging and analytics dashboards for servers and services. The dashboards can be tailored to Client's reporting needs and preferences.
- **Managed Backups:** Whether Client already has a solution or is protecting Client's systems using one from Tigunia, the NOC Team will manage and monitor backups to ensure you meet Client's Recovery Time Objectives (RTO) and Recovery Repoint Objectives (RPO).
- **Service-Level Commitment: As detailed in this document, service-l**evel Objectives (SLOs) for response and resolution times are applied.

NOC Premium

Premium includes all previously listed services in addition to the following services:

- **Patching – Linux Operating Systems:** Tigunia's NOC Team supports patching a small subset of Linux operating systems, namely Ubuntu, following its stable release schedule.

- **Tailored Validation:** Tigunia's NOC team will coordinate, maintain, and update validation steps tailored to each service-included system's design and use case.
- **White Glove Administration of Systems:** NOC team members will engage with Client systems and maintenance windows and perform validation efforts and targeted testing as defined by the engagement process to ensure consistency.
- **Line of Business Application Patching:** If agreed upon, Line of Business Application patching will be supported on a per-application basis.
- **Remote Monitoring and Management - Tailored Scripting:** Custom Scripts can be developed at Client's request. Depending on the complexity and requirements of the request, this may require resources from outside of NOC systems.
- **Quarterly Security Assessment:** Tigunia's NOC will provide a quarterly security assessment. Systems covered by NOC Premium will be measured against one of several compliance standards (such as CIS 8.0, GDPR 4, NIST, and HIPAA). This assessment is not a replacement for security attestation.
- **Quarterly DR Testing:** Tigunia's NOC will perform a quarterly Backup and Disaster Recovery Test. This service involves a timed mock failover of Client's environment using Client's chosen backup solution, which will create documentation and demonstrate preparedness in a real disaster recovery scenario.
- **Azure Tenant Monitoring:** Expand FoMo Monitoring into Client's Azure/O365 Tenant. This effort requires that Tigunia have access to a Global Administrator. It allows monitoring of App Registrations, risky user sign-ins, SSO Certificates, Entra AD Connect Sync Errors, Entra AD Connect Health Alerts, Role Changes, and Security Notifications.

Maintenance actions are defined in the Service Definitions document and detailed during onboarding or in the respective service deployment SOW.

Scope of Service

The scope of this service is expressly limited to the locations, endpoints, systems, and infrastructure explicitly defined in the corresponding Statement of Work ("SOW"). Any services, support, or activities outside these designated areas are considered out of scope and will not be included in the particular or selected service offering. Modifications or extensions to the scope must be formally agreed upon and documented in an updated SOW or separate engagement agreement.

SLAs for Each Service Tier

All services provided herein are provided with the commitments contained in the corresponding “Network Operations Center (“NOC”) - Service Level Agreement (“SLA”)” and are provided with no further warranty or guarantee whatsoever.