NETSURIT SECURITY OPTIMIZATION SERVICE (NSOS): Scope and Benefits

COMPREHENSIVE OVERVIEW OF SECURITY ENHANCEMENT SOLUTIONS

Agenda:
NSOS Key Topics

- Overview and Purpose of NSOS
- Scope of NSOS: Services and Protected Infrastructure
- Core Activities and Functions of NSOS
- Reporting and Deliverables
- Out-of-Scope Activities and Limitations
- Engagement Parameters and Service Delivery
- Pricing Structure and Cost Details
- Netsurit Value Proposition and Benefits

OVERVIEW AND PURPOSE OF NSOS

Background and Need for Security Optimization

Evolving Cyber Threats

Constantly evolving cyber threats require periodic review to maintain effective security posture and protection.

Netsurit Security Optimization Service

NSOS offers monthly automated security assessments and proactive vulnerability remediation for continuous protection.

Continuous Improvement Approach

NSOS identifies opportunities for enhancement to ensure maximal protection using latest features and improvements.

Introduction to NSOS and its Approach

Continuous Security Optimization

NSOS delivers ongoing monthly security assessments to continuously optimize customers' security posture.

Proactive Risk Identification

NSOS identifies potential risks early, allowing remediation before issues arise.

Enhancement and Feature Implementation

NSOS proactively suggests improvements and new features to ensure maximal protection.

SCOPE OF NSOS: Services and Protected Infrastructure

Managed Security Service Components and NSOS Role

NSOS Core Functions

NSOS manages security infrastructure with proactive maintenance, risk remediation, incident response, and monitoring services.

Microsoft Security Stack Management

NSOS administers and monitors Microsoft 365, Entra ID, Defender XDR, Sentinel, and Defender for O365 security controls.

Security Optimization Roadmap

NSOS drives ongoing security improvements by implementing new functionalities and enhancements aligned with vendor updates.

Infrastructure Components Monitored and Secured by NSOS

Microsoft 365 Services

NSOS secures Microsoft 365 services including Exchange Online, SharePoint, OneDrive, and Teams to protect communication and collaboration.

Identity and Access Management

Entra ID and Active Directory services are monitored to ensure secure user authentication and hybrid integration.

Device and Server Security

NSOS protects Windows clients, Windows and Linux servers to ensure endpoint security across the infrastructure.

Cloud Subscription Security

Microsoft Azure subscriptions and resources are monitored and optimized to secure cloud infrastructure and services.

CORE ACTIVITIES AND FUNCTIONS OF NSOS

Microsoft Defender XDR and Microsoft 365 Security Activities

Defender XDR Workload Management

Manage, monitor, and secure Microsoft Defender XDR workloads continuously for robust protection.

Microsoft Defender Services

Operationally oversee Defender services including Endpoint, Office 365, Identity, and Cloud Apps security features.

Ongoing Security Enhancement

Continuously assess, plan, and implement security improvements for Microsoft 365 infrastructure.

Security Architecture and Monitoring

Update security designs, participate in forums, and monitor security posture for Microsoft 365 and Azure tenants.

Identity Solutions and Risk Management

Identity Solutions Management

Monitor and manage identity solutions including Entra ID tenant, Active Directory, ADFS, and Entra ID Connect.

Security Compliance Verification

Ensure all identity solutions comply with established security standards and organizational policies.

Risk Investigation and Remediation

Investigate security risks and recommend remediation steps to safeguard identity infrastructures.

Azure Workload Security and Optimization

Infrastructure Assessment

Evaluate Azure infrastructure for business suitability, operational efficiency, cost, and security risks.

Security Review and Enhancement

Review security configurations and develop remediation plans to align with best practices.

Proactive Security Monitoring

Monitor, respond to security alerts, and notify teams to resolve incidents proactively.

Ongoing Security Management

Continuously assess and enhance security posture with planned changes and regular reporting.

Administrative Role Management and Privileged Access

- **Apply Least Privilege Principle**

  Ensure users have only the necessary permissions to reduce security risks and maintain control.

- **Custom Administrative Roles**

  Design and implement tailored admin roles when built-in roles do not meet organizational requirements.

- **Access Review and Reporting**

  Regularly review privileged access and provide reports to management to ensure correct entitlements.

- **Manage Privileged Identity Management**

  Oversee configuration and approval processes of temporary privileged access via PIM to enhance security.

Support for Security-Related Issues

Support Call Logging

Assist support teams in logging security-related calls efficiently to ensure timely issue resolution.

Security Issue Focus

Focus on security issues within Microsoft 365 and Azure services to maintain cloud infrastructure safety.

Collaboration with Microsoft

Collaborate closely with Microsoft support to address and resolve security concerns effectively.

REPORTING AND DELIVERABLES

Monthly Status Reports and Documented Outputs

Monthly Status Reporting

Monthly reports summarize key security and architecture status for ongoing support engagements.

Access and Role Reviews

Reports include summaries of access reviews for roles and resources to ensure compliant security.

Recommendations and Updates

Monthly deliverables outline recommendations, planned changes, and updates to designs and documentation.

Summary of Changes, Risks, and Recommendations

▶ Identified Issues and Risks

Key issues and risks were identified in the managed environment during the review period.

▶ Summary of Changes

A summary of important changes made in the preceding period highlights progress and adjustments.

▶ Recommendations Overview

Recommendations are provided to address risks and improve future management strategies.

OUT-OF-SCOPE ACTIVITIES AND LIMITATIONS

Excluded Services and Activities

Scope Limitations

Only explicitly stated services are in scope; all others are excluded from this engagement to ensure clarity.

Excluded Technical Services

Configuration and support of various Microsoft and third-party systems, endpoint management, and physical infrastructure are excluded.

No Onsite or Training Services

All managed service delivery is remote; no onsite work or instructor-led training will be provided during this engagement.

ENGAGEMENT PARAMETERS AND SERVICE DELIVERY

Service Duration, Hours, and Staffing

Managed Service Duration

The service agreement is based on a 12-month managed security services contract duration.

Managed Service Hours

Service staff are available 8 hours daily, 5 days per week, throughout the year for incident response.

Managed Service Staffing

Specialized security professionals staff the service, focusing on Microsoft security expertise.

Assumptions and Dependencies

- **Cloud Services Provision**

  All necessary cloud service subscriptions must be provided by the client for project success.

- **Connectivity Requirements**

  Reliable internet connectivity is essential for all devices involved in the managed security service.

- **Access and Permissions**

  The project team must receive Owner role delegation on relevant Azure subscriptions for management.

- **Pre-requisites and Contacts**

  All Microsoft cloud prerequisites must be met and a liaison person must be available for communication.

Microsoft Partner Association and Project Schedule

Microsoft Partner Association

The customer associates Netsurit to Microsoft 365 and Azure resources via CPOR and PAL processes to ensure proper deployment partnership.

Claiming Partner of Record (CPOR)

Netsurit is confirmed as deployment partner for Microsoft services and submits confirmation list to Microsoft before deployment.

Partner Admin Link (PAL)

PAL links partner network IDs to customer credentials for Azure service delivery, supporting multiple partners in the same environment.

Agile Project Schedule

Project implementation uses Agile methodology with short sprints, clear activities, and defined outcomes developed with the customer.

PRICING STRUCTURE AND COST DETAILS

Assessment and Optimization Cost Breakdown

▶ **Assessment Services Overview**

Services include assessments across Azure, Microsoft Security Stack, Microsoft 365, Endpoints, and Identity domains.

▶ **Optimization Services Scope**

Optimization covers Azure, Microsoft Security Stack, Microsoft 365, Endpoints, and Identity to improve efficiency and security.

▶ **Pricing Structure Details**

Pricing includes monthly and 12-month fees for the listed assessment and optimization services.

NETSURIT VALUE PROPOSITION AND BENEFITS

Microsoft Security Association and Specializations

Member of
Microsoft Intelligent
Security Association

Microsoft Security

Microsoft Verified
Managed XDR Solution

Microsoft Intelligent Security Association

Netsurit is a distinguished member of the Microsoft Intelligent Security Association, enhancing security collaboration.

Security Copilot Early Access

Netsurit participates in Microsoft's Security Copilot program, leveraging AI to boost security operations.

Advanced Microsoft Specializations

Netsurit holds multiple advanced Microsoft specializations demonstrating expert capabilities in cloud and security.

Conclusion

Comprehensive Security Approach

Netsurit provides a thorough and expert-driven approach to enhancing security through continuous monitoring and optimization.

Microsoft-Aligned Solutions

The service integrates solutions aligned with Microsoft technologies to improve overall security posture effectively.

Client Benefits

Clients receive clear scope definitions, detailed reporting, and strong partnership support for security optimization.