Security Services

PRODUCTS & SERVICES

Security Consultation & Implementation of Industry Standards

Security Programs

Managed Security Services

Vulnerability Management & Penetration Testing

Security Product Development

Security Consultation & Implementation of Industry Standards

ISO/IEC 27001 International standard to manage information security

NESA Compliance- National Electronic Security Authority

PCI-DSS Payment Card Industry Data Security Standard

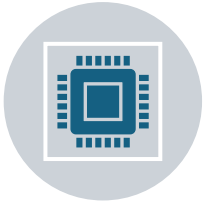
Security Consultation & Implementation of Industry Standards

Assessment Methodology

Comprehensive Assessment → **Regulatory Compliance** → **Security Controls Implementation** → **Continuous Monitoring and Improvement**

Deliverables:

Security Assessment Report: This report summarizes the findings of the security assessment conducted on the client's systems, networks, and infrastructure. It includes an analysis of vulnerabilities, risks, and gaps in the existing security posture.



Security Controls Implementation Plan: A detailed plan for implementing security controls and technologies is developed. This plan includes specifications for hardware/software installations, configuration guidelines, and deployment strategies.

Security Strategy and Roadmap: Based on the assessment findings, a comprehensive security strategy and roadmap are developed. This document outlines the recommended security measures, prioritized action items, and a timeline for implementation.

Monitoring and Reporting Mechanisms: Recommendations are made for implementing continuous monitoring tools and reporting mechanisms to track security events, detect anomalies, and generate security reports.

Compliance Documentation: If the client needs to comply with specific industry standards or regulations, compliance documentation is prepared. This may include a gap analysis report, risk treatment plan, and evidence of compliance with relevant standards (e.g., ISO 27001 certification).

Documentation and Handover: All deliverables are documented and organized for easy reference. A final handover meeting is conducted to review the deliverables with the client's stakeholders and address any questions or concerns.

Security Programs

Security Programs

Data classification / DLP Implementation

Data classification is the process of categorizing data based on its sensitivity, value, and criticality to the organization. This classification enables organizations to apply appropriate security controls, ensure compliance with regulations, and manage data effectively throughout its lifecycle.

Identify Data Owners: Assign ownership of data to individuals or departments within the organization. Data owners are responsible for determining the sensitivity and value of the data they manage.

Define Data Classification Levels: Establish a classification scheme that defines different levels of sensitivity or confidentiality for data. Common classification levels include:

- Public: Data that is intended for unrestricted access and does not contain sensitive information.
- Internal Use Only: Data that is restricted to employees and authorized personnel within the organization.
- Confidential: Data that is sensitive and requires protection from unauthorized access or disclosure.
- Restricted: Highly sensitive data that is subject to strict access controls and additional security measures.

Inventory Data Assets: Identify and catalog all data assets within the organization, including databases, files, documents, and other data repositories.

Assign Classification Labels: Apply appropriate classification labels to each data asset based on its sensitivity and value. This labeling may be manual or automated, depending on the organization's capabilities and tools.

Establish Handling Procedures: Develop and communicate procedures for handling, storing, transmitting, and disposing of data based on its classification. This ensures that employees understand their responsibilities for protecting sensitive information and complying with data protection policies.

Monitor and Audit Access: Implement monitoring and auditing mechanisms to track access to sensitive data and detect any unauthorized or suspicious activities. Regularly review access logs and audit trails to ensure compliance with security policies and regulations.

Review and Update Classification: Regularly review and update the classification of data assets as their sensitivity or value changes over time. This may be triggered by changes in business requirements, regulatory requirements, or the data itself.

Provide Training and Awareness: Conduct training and awareness programs to educate employees about the importance of data classification, their roles and responsibilities in protecting sensitive information, and the procedures for handling classified data securely.

Deliverables:

Data Classification Policy: A formal policy document that defines the objectives, scope, roles and responsibilities, and procedures for data classification within the organization. This policy serves as a foundation for the data classification program and outlines the criteria for classifying data, classification levels, and the handling of classified information.

Data Classification Scheme: A structured framework or taxonomy that defines the classification levels and criteria for categorizing data based on its sensitivity, value, and criticality to the organization. This scheme provides consistency and clarity in how data is classified across the organization.

Data Inventory: An inventory or catalog of all data assets within the organization, including databases, files, documents, and other repositories. This inventory serves as a baseline for the data classification process and helps identify where sensitive information is stored. Based on this DLP can be configured and identify the sensitive document in electronic format.

Access Control Policies: Policies and procedures for controlling access to classified data based on its classification level. This includes defining access controls, permissions, and authentication mechanisms to restrict access to authorized users and protect sensitive information from unauthorized disclosure or misuse.

Handling and Storage Guidelines: Guidelines and procedures for handling, storing, transmitting, and disposing of classified data securely. This includes specifying encryption requirements, physical security measures, and protocols for data transfer and sharing.

Training and Awareness Materials: Training programs, educational materials, and awareness campaigns to educate employees about the importance of data classification, their roles and responsibilities in protecting classified information, and the procedures for handling classified data securely.

Architecture Review & Assessment

Architecture Review (On-premises)

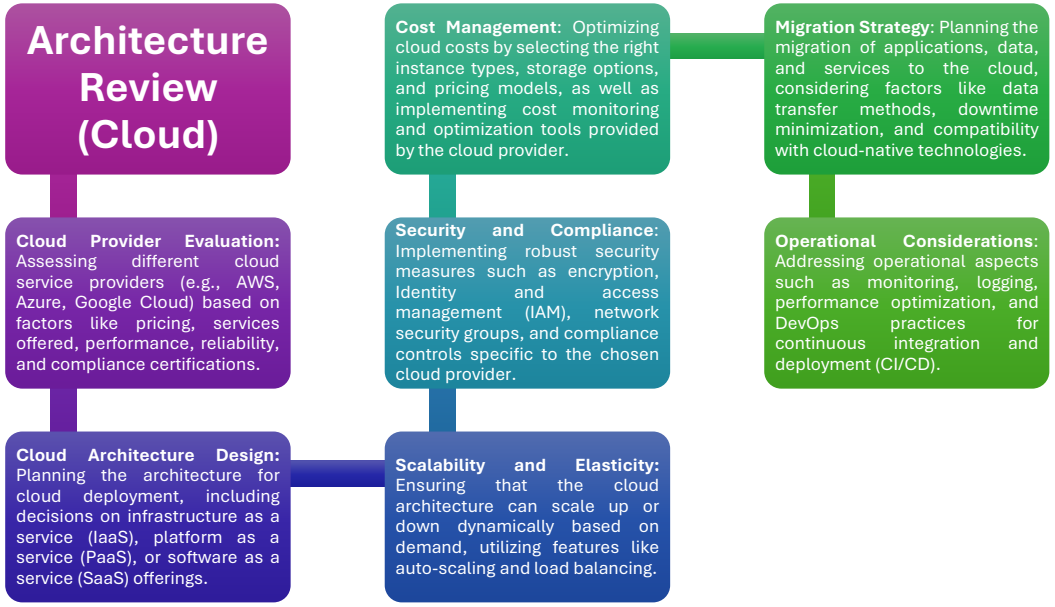
Assessment of Current Infrastructure: This involves understanding the existing hardware, software, network configurations, and data storage systems in the on-premises environment.

Scalability and Performance: Evaluating whether the current architecture can accommodate growth in terms of users, data volume, and transactions without compromising performance.

Security and Compliance: Reviewing security measures such as firewalls, intrusion detection systems, access controls, and compliance with industry standards and regulations (e.g., GDPR, HIPAA).

High Availability and Disaster Recovery: Analysing the resilience of the system to failures and disasters, including backup strategies, redundancy, failover mechanisms, and recovery procedures.

Cost Optimization: Identifying areas where costs can be reduced, such as optimizing resource utilization, licensing, and maintenance expenses.



Deliverables

Architecture Assessment Report: This report provides a detailed analysis of the current architecture, including hardware, software, network configurations, and data storage systems. It outlines the strengths, weaknesses, opportunities, and threats (SWOT analysis) of the existing setup.

Scalability and Performance Recommendations: Based on the assessment, recommendations are provided on how to improve scalability and performance to meet current and future demands. This may involve suggestions for hardware upgrades, optimization of resource utilization, or architectural changes.

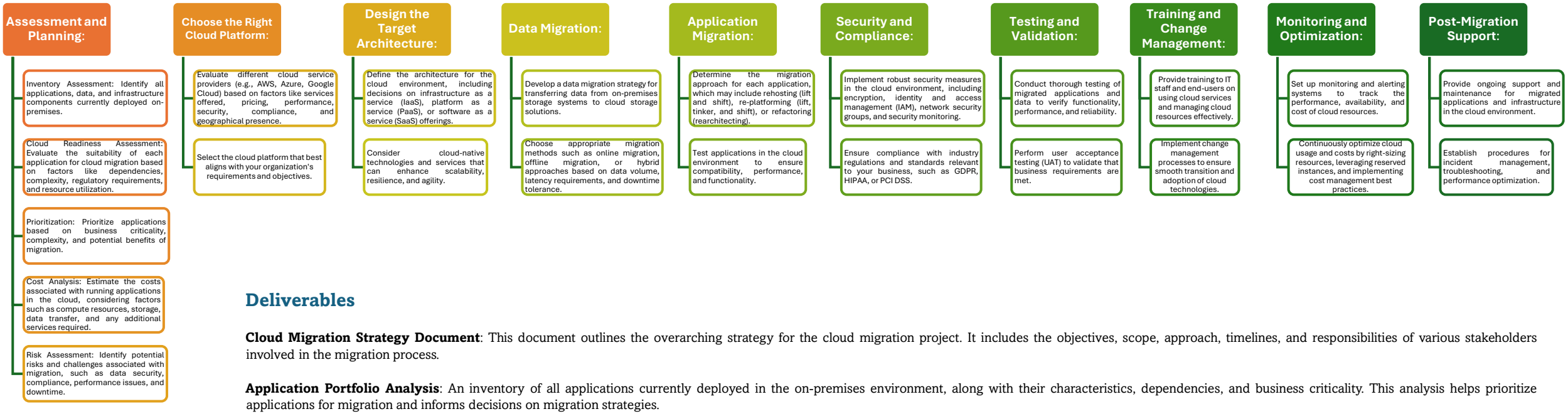
Security and Compliance Assessment: A comprehensive evaluation of the security measures in place, including firewalls, intrusion detection systems, access controls, encryption mechanisms, and compliance with industry standards and regulations. Recommendations are provided to enhance security posture and ensure compliance.

High Availability and Disaster Recovery Plan: An assessment of the resilience of the system to failures and disasters, along with recommendations for improving high availability and disaster recovery capabilities. This may include suggestions for implementing redundancy, failover mechanisms, backup strategies, and recovery procedures.

Roadmap and Action Plan: A roadmap is developed outlining the prioritized initiatives and actionable steps for implementing the recommended changes. This includes timelines, resource requirements, and dependencies for each initiative.

Executive Summary: A concise summary of the key findings, recommendations, and proposed action plan tailored for executive stakeholders. This summary highlights the business impact of the proposed changes and the expected return on investment (ROI).

Cloud Migration



Deliverables

Cloud Migration Strategy Document: This document outlines the overarching strategy for the cloud migration project. It includes the objectives, scope, approach, timelines, and responsibilities of various stakeholders involved in the migration process.

Application Portfolio Analysis: An inventory of all applications currently deployed in the on-premises environment, along with their characteristics, dependencies, and business criticality. This analysis helps prioritize applications for migration and informs decisions on migration strategies.

Cloud Provider Evaluation Report: An evaluation of different cloud service providers (e.g., AWS, Azure, Google Cloud) based on factors such as services offered, pricing, performance, security, compliance, and geographical presence. The report helps in selecting the most suitable cloud platform for the organization's needs.

Target Architecture Design & Implementation: A design document detailing the target architecture for the cloud environment. This includes decisions on infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS) offering, as well as cloud-native technologies and services to be utilized.

Data Migration Plan: A comprehensive plan for migrating data from on-premises storage systems to cloud storage solutions. This includes data discovery, assessment, classification, migration methods, scheduling, and validation procedures to ensure data integrity and consistency.

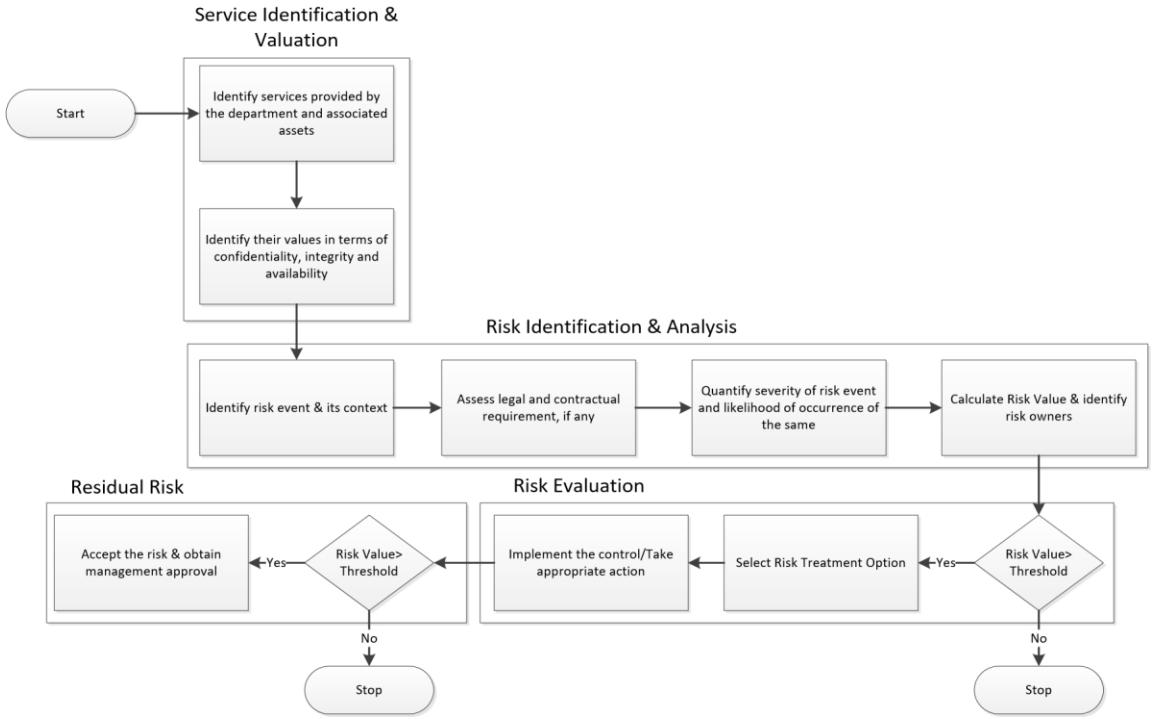
Application Migration Plan: Individual migration plans for each application, outlining the migration approach (e.g., rehosting, re-platforming, refactoring), migration steps, dependencies, testing procedures, rollback strategies, and post-migration validation criteria.

Security and Compliance Framework: A framework for implementing robust security measures in the cloud environment, including encryption, identity and access management (IAM), network security, compliance controls, and security monitoring. This ensures data protection and regulatory compliance in the cloud.

Training and Adoption Plan: A plan for providing training and support to IT staff and end-users on using cloud services effectively. This includes training programs, documentation, knowledge transfer sessions, and ongoing support mechanisms to facilitate smooth adoption of cloud technologies.

Post-Migration Support Plan: A plan for providing ongoing support and maintenance for migrated applications and infrastructure in the cloud. This includes procedures for incident management, troubleshooting, performance optimization, and continuous improvement initiatives.

Risk Assessment & Risk Management



Deliverables

Risk Assessment Report

A comprehensive document that outlines the identified risks, their potential impact, and the likelihood of their occurrence. This report includes methodologies, tools used, and detailed findings from the risk assessment process.

- Executive summary
- Scope and objectives
- Methodology
- Risk identification.
- Risk analysis and evaluation.
- Recommendations and mitigation strategies
- Appendices (if any, such as data sources or detailed analysis)

Risk Register

A centralized repository that captures all identified risks, including details about their status, priority, and mitigation measures. It serves as a reference for ongoing risk management activities.

- Risk ID
- Description of the risk
- Risk owner
- Likelihood and impact ratings
- Mitigation measures
- Status (open, in progress, closed)
- Review dates

Risk Treatment Plan

A detailed plan outlining the actions to be taken to mitigate identified risks. It specifies the risk treatment options chosen (e.g., accept, transfer, mitigate, avoid) and assigns responsibilities and timelines for implementation.

- Risk treatment options
- Action items and steps
- Responsible parties
- Timelines and deadlines
- Monitoring and review processes

Risk Management Policy

A formal document that outlines the organization's approach to risk management. It defines the principles, framework, and processes for managing risks.

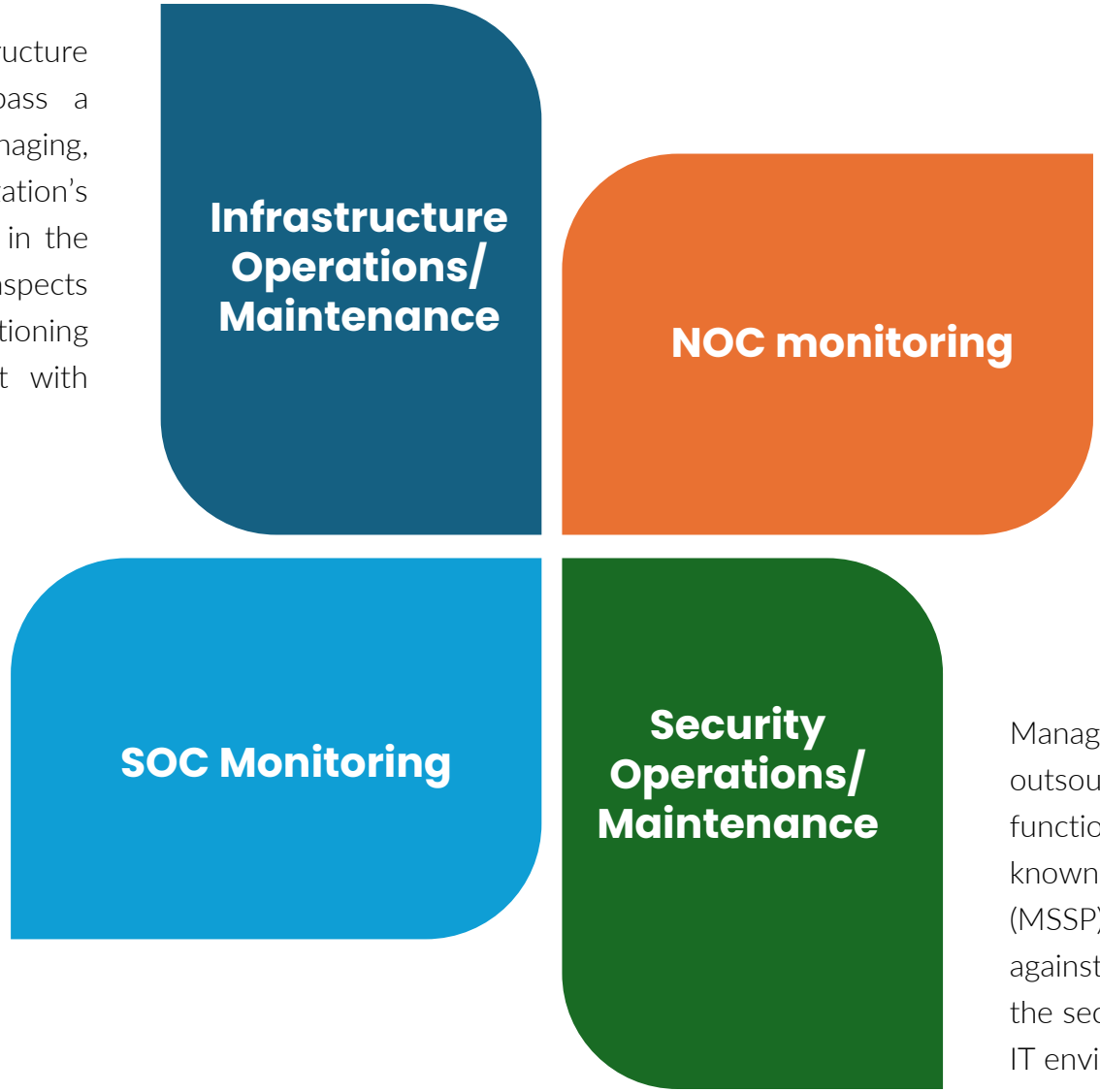
- Purpose and scope
- Definitions and terminology
- Risk management principles
- Roles and responsibilities
- Risk management process
- Monitoring and review

Reporting and documentation requirements

Managed Security Services

Managed Security Services

Managed services for infrastructure operations and maintenance encompass a comprehensive approach to managing, maintaining, and optimizing an organization's IT infrastructure, both on-premise and in the cloud. These services ensure that all aspects of the IT environment are functioning efficiently, securely, and in alignment with business goals.



Managed NOC monitoring services provide a comprehensive solution for overseeing and maintaining an organization's network infrastructure. These services offer continuous monitoring, proactive maintenance, and swift incident response, ensuring high network availability and performance. The deliverables from NOC monitoring include real-time alerts, detailed performance reports.

SOC (Security Operations Center) monitoring is a critical function within managed security services, focusing on the continuous surveillance, detection, and response to security threats across an organization's IT infrastructure. SOC teams utilize advanced technologies, skilled analysts, and standardized processes to protect the organization's data and assets from cyber threats.

Managed Security Services (MSS) involve the outsourcing of an organization's cybersecurity functions to a specialized third-party provider, known as a Managed Security Service Provider (MSSP). These services are designed to protect against a wide range of cyber threats, ensuring the security and compliance of an organization's IT environment.

Vulnerability Management & Penetration Testing

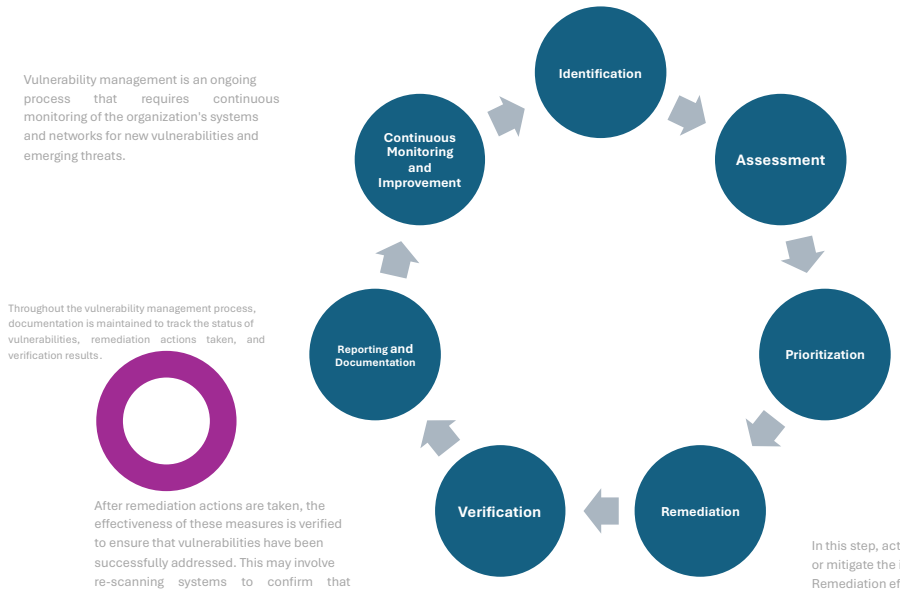
Vulnerability Management & Penetration Testing

- **Vulnerability Assessment Reports:** Detailed reports summarizing the findings of vulnerability scans, penetration tests, and security assessments conducted on the client's systems and networks.
- **Risk Prioritization Recommendations:** Recommendations for prioritizing remediation efforts based on the severity, impact, and risk posed by identified vulnerabilities, tailored to the client's risk tolerance and business objectives.
- **Remediation Action Plans:** Actionable plans outlining specific steps and timelines for addressing identified vulnerabilities, including recommendations for patching, configuration changes, and additional security controls.
- **Security Policy and Procedure Documentation:** Documentation of policies, procedures, and best practices for vulnerability management, tailored to the client's organizational structure, regulatory requirements, and industry standards.
- **Executive Briefings and Presentations:** Executive-level briefings and presentations to communicate the importance of vulnerability management, present findings, and recommendations, and secure buy-in from senior leadership for remediation efforts.
- **Continuous Monitoring and Maintenance Plans:** Plans for ongoing monitoring, maintenance, and optimization of vulnerability management processes and tools to ensure that the client's security posture remains robust and resilient to evolving threats.
- **Additional Deliverables:**

The below deliverables are subjected to the Microsoft licenses and deployment methodology.

Power BI Dashboards

Automation of Security finding assignment using Power automation.



Thank you