IT Security & Infrastructure

Managed Services Portfolio

Comprehensive Engagement Overview · April 2026 · Confidential

11+	6+	3	24/7
Core Responsibilities	Value-Add Initiatives	Security Domains	Operational Coverage

SECTION 1 · CORE RESPONSIBILITIES

Identity, Directory & Access Management

- •Hybrid Active Directory / Azure AD / Entra ID environment administration
- •Azure AD Connect synchronisation, attribute mapping and conflict resolution
- •Identity Lifecycle Management — provisioning, de-provisioning, role assignment
- •Conditional Access policy design, testing and enforcement

Active Directory	Azure AD / Entra ID	Conditional Access	SSO / MFA

Microsoft 365 Security

- •Microsoft Defender XDR monitoring, alert triage and incident resolution
- •Phishing email analysis, quarantine actions and user notification
- •Data Loss Prevention (DLP) policy configuration and tuning
- •Email trace investigations for delivery failures and spoofing incidents

Defender XDR	DLP Policies	Exchange Online	Phishing Response

Endpoint & Device Management

- •Microsoft Intune — device enrolment, compliance policies, app deployment
- • EDR strategy planning and implementation oversight
- •Endpoint security baseline configuration and hardening
- •Patch management and vulnerability remediation tracking

Intune / MEM	Endpoint Hardening	EDR	Patch Management

Infrastructure & Virtualisation

- •VMware / ESXi hypervisor administration and capacity planning
- •Azure VM health monitoring, performance alerting and right-sizing
- •Veeam backup job management, recovery testing and DR runbooks
- •Azure Administration — subscriptions, resource groups, RBAC

VMware / ESXi	Veeam Backup & DR	Azure VMs	Azure RBAC

Network Security & Operations

- Firewall rule review, optimisation and change management
- Network anomaly detection and investigation via Vectra AI NDR
- VPN gateway administration and remote-access security
- Helpdesk supervision, escalation management and SLA-driven ticket closure

Firewall / VPN	Vectra AI NDR	Incident Response	Helpdesk Ops

SATYA TECHNOLOGIES
We Believe in Solutions

SECTION 2 · DAILY OPERATIONAL ACTIVITIES

Azure VM Health Monitoring

Continuous monitoring of Azure VM performance metrics, alert investigation, and root-cause analysis of CPU, memory, and disk anomalies using Azure Monitor and Log Analytics.

Phishing Email Analysis & Mitigation

End-to-end phishing triage: header analysis, URL detonation, attachment sandboxing, quarantine actions, and post-incident user communications.

Microsoft Defender Security Monitoring

Daily review of Defender XDR incidents, advanced hunting queries, false-positive tuning, and coordination with stakeholders for remediation.

Email Trace Investigations

Investigating mail flow failures, NDR analysis, SPF/DKIM/DMARC validation, and resolving delivery issues for end-users and business-critical mailboxes.

Network Anomaly Detection (Vectra AI)

Monitoring Vectra AI NDR detections, investigating lateral movement and exfiltration signals, and escalating confirmed threats through IR procedures.

SECTION 3 · ENHANCED SECURITY CONTRIBUTIONS (VALUE-ADD)

Beyond assigned responsibilities, the following security-focused capabilities are being actively introduced to elevate the organisation's overall security maturity and resilience posture.

Vulnerability Assessment & Penetration Testing (VAPT)

Structured VAPT engagements covering internal network, web applications, and AD/Azure attack surface. Findings documented with CVSS scoring and actionable remediation roadmaps.

VAPT	Burp Suite	Nessus	Nmap

Network & Application Security Strengthening

Architecture review of DMZ, segmentation policies, and east-west traffic controls. Web application firewall (WAF) tuning and API security hardening.

WAF	Network Segmentation	API Security	Zero Trust

Endpoint Security & EDR Strategy

Design and rollout of a unified EDR strategy across Windows and macOS endpoints. Behavioural detection rule authoring and threat hunting playbook development.

EDR / XDR	Threat Hunting	Behavioural Analytics	MITRE ATT&CK;

SOC-Oriented Monitoring & IR Improvements

SIEM use-case development, playbook automation, and SOAR integration planning to reduce mean-time-to-respond (MTTR) and analyst alert fatigue.

SIEM	SOAR	Playbooks	MTTR Reduction

Firewall & IDS/IPS Optimisation

Rule-base cleanup, geo-blocking policies, IDS/IPS signature updates, and performance benchmarking to ensure optimal throughput without security trade-offs.

Firewall Hardening	IDS/IPS	Geo-Blocking	Rule Optimisation

Security Awareness & User Training

Design and delivery of phishing simulation campaigns, security awareness training modules, and departmental risk briefings to build a human firewall layer.

Phishing Simulation	KnowBe4 / Proofpoint	Security Culture	Risk Briefings

SATYA TECHNOLOGIES
We Believe in Solutions