

NxtGen Managed Services

- for ECS, On-Premise / Dedicated Hosting

NxtGen Managed Services (NMS)

NxtGen managed services offer enterprises a choice for secure and round the clock monitoring and service management inline with ITIL framework of structured and seamless incident, change and problem management for supported platforms, hybrid clouds, networks and database systems deployed on ECS & On-Premise Cloud.

Why Managed Services?

NxtGen Managed Services offers you an option of outsourcing entire data center management with adaptive support and governance for operations such as ongoing support for production systems, backups, data protection / archival / replications, audit readiness for regulatory compliance for ISO27k, PCI-DSS as per the business needs.

The shared expertise pool deployed at NMS ensures availability of skills and coverage manned **24x7x365** for helpdesk, monitoring and technical management to ensure proactive monitoring and remediation of incidents and issues and provide seamless service management and support for BAU / BCP / DR needs.

Managed Services – Platform/OS, Network & DB



- 24 x 7 Infrastructure Service Desk, ITIL framework based Structured and experienced L1, L2 and L3 Remote Support teams
- Proactive monitoring tools for monitoring the infrastructure and services, Well defined Incident and Change Management Process, Defined Escalation Process, Severity 1 and 2 call handling procedure & Escalation Management

Managed Services - ITIL Process & Reporting



ITIL Process Groups

- Incident Management
- Change Management
- Problem Management
- Availability Management
- Capacity Management
- Release Management
- Patch Management
- Report & metrics Management
- Service Improvement Management

Incident Management

- Standard Operating Model (SOP)
- Service Outage Notification Management
- Update Notification
- Alert Handling Assistance
- RCA / CMDB / KEDB

Change Management

- Predefined maintenance calendar
- Forward schedule of change
- CAB/ECAB
- Change Category
- Post Change Implementation review
- Change Management Notification Mgmt
- CMDB

Problem Management

- Proactive Problem Management

Availability Management

- Service Availability
- HW/SW Resources Availability
- DR Availability

Capacity Management

- Monitoring Resources
- Reporting resources utilization
- Capacity Enhancement

On Demand Reports & Metrics Management

- SLA report on Incident/Change/Problem
- Trend Analysis report
- MTBF / MTTA Report
- Availability Report
- Capacity Utilization Report
- RCA Report
- Risk Status Report

Service Improvement Management

- Metric Baseline Report
- Metric Analysis & RCA
- Alert/Trend Analysis
- Productivity Report
- Improved Efficiency
- Training Programs
- Process Compliance
- CSAT

Key Advantages..

- Improved service levels** due to centralized expertise and tools, and quick adaptation / implementation of new technologies, support upgrades / downgrades etc
- LOW CAPITAL / OPERATIONAL OUTLAY AND PREDICTABLE MONTHLY SERVICE COSTS** – dial up, dial down services, scale expertise without boundaries of technologies
- Increased Efficiency and productivity of services** thus Competitiveness, reduces risk of downtimes and quicker enablement of BCP/DR plans and execution, migrations
- Flexible, optimized and Converged services with 24x7 coverage and access to expertise and centralized collaborations for service management**
- Compliance and Security** due to process standardization and service management principles and audit support

NxtGen Managed Services

- Availing Support - FAQ

How do I avail the support from NxtGen?

NxtGen managed services support helpdesk operates 24x7x365 and can be reached via sending email to support@nxtgen.com, the service request once received via email will be logged in the NxtGen ticketing tool and ticket number is shared with customer within 15-30 minutes based on the type of service request and severity / priority thereof.

What are the SLA targets and escalation matrix?

NxtGen Managed Services have following SLA targets for availability and uptime, the managed services SLAs are measured against response and resolution times as per the agreed scope, subscribed services availed by the customer with good standing in the NxtGen books of accounts (no outstanding invoices or over dues payable as on the date)

Service	Metric	Deliverable
Asset Life-Cycle Management	Total Cost of Ownership	Quarterly report (First report from 3 rd Quarter)
Server Monitoring & Administration	Server Uptime	99.5% measured quarterly
Storage and SAN Monitoring & Management	Storage Uptime	99.5% measured quarterly
Network Administration & Management	Network uptime	99.5% measured quarterly
Security Management	Compliance	90% measured quarterly
Back-up Management	Compliance & restore	99% compliance & restore
Incident Management	On-Time-First-Time-Fix	90% of incidents measured quarterly
Escalation Management	Impacts other deliverables	Measured on basis on other parameters
Change Management	Compliance	90% measured quarterly
Audit Services	Compliance	90% measured quarterly
DR support	Compliance	2 Drills per Annum
VCEverywhere	Avaiability	99.5% measured quarterly

Service / Change Request	Definition	Response	Restoration
Severity 1 Critical (S1/P1) - Incidents	The Service is not available or not reachable due to cloud platform /device / resource down or network / internet access with no acceptable workaround resulting in a loss of service affecting entire setup or data centre and/or requires emergency changes to be deployed for service restoration	Within 15 Minutes	4 Hours
Severity 2 High (S2/P2) - Incidents	The service is running and operating with severely reduced functionality of cloud platform /device / resource down or network / internet access issues causing high impact to the usage, or the loss of partial service impacting affecting entire setup or data centre usage and possible workaround is available and/or requires emergency changes to be deployed for service restoration	Within 30 Minutes	8 Hours
Severity 3 High (S3/P3) Incidents & change requests etc.	The service is running and operating with reduced functionality causing little or no impact to of cloud platform /device / resource or network / internet access usage causing no impact or loss of service, new service request for provisioning and / or maintainace currently not in scope.	Within 60 Minutes	24 Hours

Escalation Matrix > <https://nxtgen.infinitevaults.com/index.php/s/3wY3kqLWPxdth2K>

NxtGen Managed Services – Backup as a Service (BKaaS) - Service Scope and SLA Definitions

Monitoring

- Backup Job Monitoring (when subscribed)
- Backup Policy Monitoring (when subscribed)
- Failed Backup / Job monitoring
- Backup Server / Storage Availability Monitoring

Scope of Activities / Services

- Backup policy documentation – Backup form
- Backup Agent Install, Configure and Support
- Backup Server - Install, Configure and support
- Backup Job / path configuration and Support
- License management
- Backup jobs failure – Incident management
- Group backup policy configuration and management
- Backup network configuration
- Restoration of backups – as per service request
- Backup Path Disk and Storage Management
- Backup reports & policy setup views / screenshots
- Resource utilization analysis
- OS Setup and configuration Support (if required)
- Media Server setup and support
- Backup troubleshooting for identifying performance bottlenecks or failure trends if any
- Patch Upgrades
- OS services for backup Configuration and Support

Out of Scope

- Tape Backups – media handling, tape drives and management
- Application backup configuration & troubleshooting, Support, External backup sources or tools and loss of data due to wrong backup path / data inconsistency, custom reports and data recovery
- Data integrity of backups and restored data
- Application Services, Source code and API Support etc
- Third party backup tools and integrations
- Custom backup policies and management

Technologies / Tools Supported

Commvault / Symantec

Standard Policy

Daily Incremental (one week), Weekly full backup , four weekly copies

Severity Definitions

SLA - S1/P1/Error - 15 minutes Response, 4 hours Restoration

- Backup Server Down - Impacting entire service
- Backup Services down or unresponsive
- Production data –priority restoration for other P1/S1 issue

SLA - S2/P2/Error – 30 minutes response, 12 hours restoration

- Backup Job failure due to service unavailable
- Failed restore, policy or jobs
- Data loss – priority restoration request

SLA - S3/P3/Error – 60 minutes response, 24 hours Restoration

- Share Backup media / Drive / storage access issues
- local policy reset
- group policy issues, new policy request
- windows firewall configuration
- local restoration of data being backed up reset
- Backup report and policy related queries
- Backup path change (requires backup form resubmission)

Change Request (OTC Applicable)

- Re-work on policy, Re-installation of OS client, Disk management-Drive Expand, Shrink for backup storage / destination path / share etc
- New Backup policy for new datasets/ locations and setups
- Any maintenance activity which is not covered in scope

NxtGen Managed Services – Replication as a Service (RPaaS)

- Service Scope and SLA Definitions

Monitoring

- Replication Job Monitoring (when subscribed)
- Replication Policy Monitoring (when subscribed)
- Failed Replication / Job Monitoring
- Replication Service & Storage Availability Monitoring

Scope of Activities / Services

- Replication policy - documentation – Replication setup
- Replication Services - Install, Configure and Support
- Replication Storage - Configure and support
- Replication Job / path configuration and Support
- Failed Replication remediation
- Group policy configuration and management
- Replication network configuration
- Restoration of images – as per service request
- Replication Path Disk and Storage Management
- Replication reports & policy setup views / screenshots
- Resource utilization analysis
- OS Setup and configuration Support
- Media Server setup and support
- Recovery from replicated images & troubleshooting for identifying service bottlenecks or failure trends if any
- Patch Upgrades
- OS services for replication - Configuration and Support

Out of Scope

- Custom Replication Requests – media handling, tape drives and management
- Application servers, software load balancers configuration & troubleshooting for replication, Support, External sources or tools
- Loss of data due to corrupt images / data inconsistency and data recovery
- Data integrity of images and restored data / image
- Application Services, Source code and API Support etc
- Third party backup tools and integrations
- Custom replication request for policies and management

Technologies / Versions Supported

HyperV / Vmware / Openstack

Standard Policy

Full VM Replication at 15 minute interval with 24 hourly checkpoints

Severity Definitions

SLA - S1/P1/Error - 15 minutes Response, 4 hours Restoration

- Replication Server Down - Impacting entire service
- Replication Services down or unresponsive
- Production data –image restoration for other P1/S1 issue

SLA - S2/P2/Error – 30 minutes response, 12 hours restoration

- Backup Job failure due to service unavailable
- Failed restore, policy or jobs
- Data loss – priority restoration request

SLA - S3/P3/Error – 60 minutes response, 24 hours Restoration

- Share Backup media / Drive / storage access issues
- local policy reset
- group policy issues, new policy request
- windows firewall configuration
- local restoration of data being backed up reset
- Backup report and policy related queries
- Backup path change (requires backup form resubmission)

Change Request (OTC Applicable)

- Re-work on policy, Re-installation of OS client,
- Disk management-Drive Expand, Shrink for backup storage / destination path / share etc
- New Backup policy for new datasets/ locations and setups
- Any maintenance activity which is not covered in scope

NxtGen Managed Services for Platforms – Windows

- Service Scope and SLA Definitions

Monitoring

Replication Monitoring (when subscribed)
 Backup Monitoring (when subscribed)
 Server Uptime / Availability Monitoring
 CPU, Memory and Disk - Threshold and alerts
 Ping based uptime
 Historical performance reporting

Scope of Activities / Services

OS Setup, Install and Support
 HyperV and VMware Install, Configure and Support
 Clustering - Install, Configure and support
 Replication and Backup configuration and Support
 License management
 Remote Desktop Services
 Group policy configuration and management
 DNS configuration
 DHCP Configuration
 Active Directory - Install, Configure and Management
 Server role install and configuration
 Disk and Storage configuration and Management
 OS Hardening and management
 Antivirus Management - Install, updates and support
 Resource utilization analysis
 Windows Cluster Setup and configuration Support
 FTP Server setup and support
 OS troubleshooting for identifying performance bottlenecks
 Patch Upgrades
 Windows Firewall Configuration and Support

Out of Scope

Application configuration & troubleshooting, Support
 website construction, Domain or Web services
 Middleware - install, configure and support
 Application Services, Source code and API Support etc
 Third party application install & support

Technologies / Versions Supported

Windows Server 2008, 2012
 Microsoft HyperV
 VMware 5, 6

Severity Definitions

SLA - S1/P1/Error - 15 minutes Response, 4 hours Restoration

Instance down - Impacting Business
 OS Cluster / critical services down or unresponsive
 Loss of connectivity - Production servers

SLA - S2/P2/Error – 30 minutes response, 12 hours restoration

Server up but unable to connect via RDP
 OS Services down
 virus/ malware issues

SLA - S3/P3/Error – 60 minutes response, 24 hours Restoration

Share Drive / storage access issues
 local administrator password reset
 group policy issues
 windows firewall configuration
 local administrator password reset
 Driver install, OS Hardening
 Event analysis, Task Scheduling
 Resource utilization analysis
 performance counters

Change Request (OTC Applicable)

Patch Upgrades, Reinstallation of OS, service packs
 Disk management-Drive Expand, Shrink
 HyperV /Vmware ESX Configuration
 FTP / IIS Service, Cluster Setup Configuration
 Any maintenance activity which is not covered in scope

NxtGen Managed Services for Platforms – Linux

- Service Scope and SLA Definitions

Monitoring

Replication Monitoring (when subscribed)
 Backup Monitoring (when subscribed)
 Server Uptime Monitoring
 CPU, Memory and Disk - Threshold and alerts
 Ping based uptime
 Historical performance reporting

Scope of Activities / Services

Package Installation (Webservers, Database servers, php, Java etc.). Graphical installation. Provide access via 'mstsc/vnc-viewer' and ssh.

Disk Management - LVM configuration, volume resizing, file system management, checking file system corruption and rectifying.

OS hardening (Harden the OS against unauthorized access includes changing default ports, IPS configuration, selinux/apparmor configuration etc.)

Resource utilization analysis (Provide analysis on resource utilization of different applications and find the bottleneck. Provide suggestions for better performance based on the analysis.)

Network configuration (IP/Network configuration as per requirement. Configuring multiple Ips, IP binding, configuration of multiple routes etc.)

OS firewall configuration (Configure ip tables/firewall as per the client requirement to secure/route.)

OS security analysis (Perform log analysis and provide suggestions based on the findings, Filesystem scan for malicious scripts using scanners like maldet/clamd etc.)

Log monitoring. Provide RCA from Logs. Syslog configuration/ Log rotation

Out of Scope

Application configuration/troubleshooting
 Web Services and IP Tables etc
 User creation, end user support

Technologies / Versions Supported

RHEL
 CentOS
 Ubuntu
 OpenSUSE
 Debian
 Oracle Linux
 RHEL

Severity Definitions

SLA - S1/P1/Error - 15 minutes Response, 4 hours Restoration

Server down/not accessible

SLA - S2/P2/Error – 30 minutes response, 12 hours restoration

Package installation
 Disk management
 resource utilization analysis
 OS firewall configuration

SLA - S3/P3/Error – 60 minutes response, 24 hours Restoration

Network configuration
 OS hardening
 OS security scan/analysis
 IPS configuration
 Hardware Integration

Change Request (OTC Applicable)

Patch Upgrades, Reinstallation of OS, service packs
 Disk management-Drive Expand, Shrink
 Network Services Configuration
 FTP / Web Services, Cluster Setup Configuration
 Any maintenance activity which is not covered in scope

NxtGen Managed Services for Database Management – MySQL

- Service Scope and SLA Definitions

Monitoring

- MySQL Instance Uptime
- MySQL Query status
- Replication stats
- MySQL engine stats.
- MySQL Connections stats
- Galera Stats.

Scope of Activities / Services

- Installation & Setup
- Replication
- Upgrades
- Galera Setup
- MySQL Standardisation
- OS Tuning for MySQL
- MySQL Optimization.
- Optimizer Tuning.
- Engine Optimization .

Out of Scope

- MySQL Query Optimization.
- Schema Optimization and Query review.
- Transaction Support / optimization
- MySQL Firewall *
- Drop tables, delete records / data purge etc

Change Request (OTC Applicable)

- Upgrades (version / memory / disk swap etc.)
- Re-configuration of cluster or replication
- SELinux and Apparmor Support.
- Hot Backup encryption.
- MySQL Tablespace encryption (5.7)
- SSL based data replication to remote data centres.
- MySQL Audit logs for critical tables.
- MySQL user Restrictions and Frequent MySQL security Audits.

Technologies / Versions Supported

- MySQL[®] by Oracle
- MySQL[®] by Oracle
- MariaDB[®]
- Galera Cluster
- Percona Server for MySQL
- MySQL HA Solutions (MHA, MMM, DBDRD etc.,)
- MySQL Engines (InnoDB, TokuDB , XtraDB, MyISAM , Memory , Sphinx , Maria)

Severity Definitions

SLA - S1/P1/Error - 15 minutes Response, 4 hours Restoration

- MySQL server / Host server not reachable.
- Galera Cluster failure.
- Replication Failure.
- Abnormal DB Usage pattern / Spikes.
- MySQL Locking
- High CPU usage by MySQL

SLA - S2/P2/Error - 30 minutes response, 12 hours restoration

- Memory Exhaustion Replication lag > 200 secs.
- Increased Dead locks
- High Disk waits / IO waits.
- Disk Utilization beyond normal threshold 1 Hour

SLA - S3/P3/Error – 60 minutes response, 24 hours Restoration

- Long running reads on slave.
- Memory Swap.
- New error on MySQL logs and SYS logs.
- Backup failures
- Backup mount points not available
- Re-Installation

NxtGen Managed Services for Database Management – MsSQL

- Service Scope and SLA Definitions

Monitoring

- Availability & Performance Monitoring
- Backup/Space Monitoring
- Scripted Health Checks
- Fragmentation checking & defragmentation
- Log Shipping status

Scope of Activities / Services

- Installation
- Upgrade
- Migration
- Log Shipping(two locations)
- Mirroring
- Clustering with log shipping/mirroring (when subscribed)
- Backup and Recovery
- OS Tuning for MSSQL
- Service Patch, cumulative upgrade
- Always on Availability

Out of Scope

- SQL queries Performance tuning
- Transaction Support/ Production Release Implementation
- Drop / delete records / data purge etc
- Transaction Support / optimization

Change Request (OTC Applicable)

- Database upgrade
- Re-configuration of cluster or replication
- Log shipping configuration/reconfiguration
- Mirroring
- Index rebuild
- reinstalltion(emergency request)
- Database restart (emergency request)

Technologies / Versions Supported

- MsSQL 2008 Web, Std, Enterprise
- MsSQL 2012 Web, Std, Enterprise
- MsSQL 2014 Web, Std, Enterprise
- OS window 2008, 2012 std, R2 etc

Severity Definitions

SLA - S1/P1/Error - 15 minutes Response, 4 hours Restoration

- Database not reachable
- Replication Failure
- Abnormal DB uage(spikes)
- High CPU usage by MSSQL
- Memory utilization

SLA - S2/P2/Error - 30 minutes response, 12 hours restoration

- High CPU and I/O, Wait events, Mermory usage.
- High Disk Waits
- Locks, Blocking session
- Disk utilization beyond normal threshold 1 hour

SLA - S3/P3/Error – 60 minutes response, 24 hours Restoration

- Long running reads and writes on disks and memory.
- Backup failure
- Re-installation

NxtGen Managed Services for Database Management – Oracle

- Service Scope and SLA Definitions

Monitoring

Availability & Performance Monitoring.
 Backup/ISpace Monitoring.
 OEM, GRID Performance Monitoring.
 AWR, ADDM and ASH reports. Explain Plan, Gather stats, SQL profiling.
 Fragmentation checking & defragmentation.
 Automate daily Replication materialized views and Status Check.
 Index Management(index creation and rebuild).
 Table Partitioning.
 Data Purge, table and index tuning.
 Tablespace Management.
 User security Management(create roles and Profiles).

Scope of Activities / Services

Installation
 Migration on database to unix/windows flavours
 Database and Version Upgrades
 Apply Patches(Bug, CPU, PSU and upgrade)
 Refreshes (expdb & impdb with/without data Mask)
 Cloning(cold, hot and RMAN)
 Dataguard(DR) setup
 RAC(4 node) configuration
 Materialized views replication(BO and BI)
 OEM, Grid configuration
 Controlfile Contention Management
 Backup and Recovery(Hot backup, cold backup, exp/expdb(database level, Schema level, tablespace level, table level), RMAN backup.

Out of Scope

SQL queries Performance tuning, DB recovery
 Transaction Support/ Production Release Implementation
 Transaction Support / optimization
 Drop tables, delete records / data purge etc
 Move Control file, Resize redo log file, add redo group
 Recreate Db_links, Jobs, schedules etc.

Technologies / Versions Supported

ORACLE 9i / 10g / 11g / 12C
 File system, Raw device and ASM
 Database Standalone, RAC, Ebz, Documentum, Infra etc

Severity Definitions

SLA - S1/P1/Error - 15 minutes Response, 4 hours Restoration

Oracle database not reachable
 RAC Services failover
 Replication Failure.
 Abnormal DB usage (spikes), high CPU
 Archive log filesystem utilization, undo/temp usage.
 DB Memory latches

SLA - S2/P2/Error - 30 minutes response, 12 hours restoration

High CPU and I/O, Wait events, Memory usage.
 High Disk Waits
 Locks, Blocking sessions and memory latches
 Disk utilization beyond normal threshold 1 hour

SLA - S3/P3/Error – 60 minutes response, 24 hours Restoration

Long running reads and writes on disks and memory.
 Memory swap.
 Backup failures
 Backup mount points not available.
 Tablespace space issue.

Change Request (OTC Applicable)

Database upgrade / reinstallation,
 Apply Patches, Oracle bug fix
 Archive log mode change, parameter changes
 Index Rebuild, Shrink data file, Defrag, partitioning
 Migration on database to unix/windows flavours
 Move Control file, Resize redo log file, add redo group
 Recreate Db_links, Jobs, schedules etc.
 Data guard Configuration

NxtGen Managed Services for Network Management

- Service Scope and SLA Definitions

Monitoring

Availability & Performance Monitoring.
Backup / HA Monitoring.
Sapphire - Interface / port monitoring
PRTG - Bandwidth Utilization & uptime
WAN / P2P Link - ISP interface monitoring
Firewall connection session logs
Monetis URL monitoring (license charges apply)

Scope of Activities / Services

NAT / PAT / VDOM Management
Configuration to network routing tables
IPsec VPN Configuration & Management
Troubleshoot Packet loss and slowness issues
Load Balancer Configuration & Management
SSL Offloading, iRule etc
Cluster / HA Support & Configuration
Load Balancer provisioning/SSL offloading
Stateful firewall
Correlation rules incorporate all security elements (white list, black list) to detect complex, multi-stage attacks
Support for SSL client certificates /SSL VPN Configuration
Web User Interface (HTTP/HTTPS)/Creation of user for Firewall
Configuration to alerts, monitoring & logging functions
Define a default gateway or default route
IP Details: IP Address, DNS Name, MAC Address, Alias Name
Add Subnets/Vlan Manually on the Firewall
Export report to PDF/CSV/XLS format

Out of Scope

LAN / Wifi Device Support (external)
End user support / ISP Nixie peering etc.
Security setups and configurations / troubleshooting
ISP Services / DDoS / IPS / UTM / IDS etc (on demand)
DNS / Web / Sockets etc. - Network Services

Technologies / Versions Supported

Fortigate, Cisco, PaloAlto Firewalls & SDN (Brocade)
Switching & Routing - LAN & WAN / VLANs
Load Balancers (Array / F5), SSL, VPN / IPSEC
PRTG / NAGIOS / CACTI Configuration for monitoring
TACACS / RADIUS (AAA)

Severity Definitions

SLA - S1/P1/Error - 15 minutes Response, 4 hours Restoration

Internet access impacted / RTOs
Network / Device / Services inaccessible / Interface / Port Down
Gateway Inaccessible
Dedicated P2P Link / Route down

SLA - S2/P2/Error - 30 minutes response, 12 hours restoration

Packet loss / IP / VLAN / Gateway issues
IPSEC-VPN connectivity / SSL VPN
HA failures or failovers

SLA - S3/P3/Error – 60 minutes response, 24 hours Restoration

ACL configurations & provisioning / upgrades etc
Bandwidth upgrades
backup restoration
Utilization reports
CR Preparation / Custom queries

Change Request (OTC Applicable)

Modification of Existing LB Configurations, new setup
Re-installation of firewalls, polices, firmware
VPN tunnel configurations
P2P / MPLS link termination and interconnects
Routing & Switching configuration changes
Cluster / HA Reconfiguration / DR-BCP services
Inter Vlan access / gateway setups

NxtGen Managed Services for Security Management – OS & Network - Service Scope and SLA Definitions

Monitoring

Antivirus & Endpoint protection alerts
Critical Alert Response on Intrusion detection
Brute force / DDOS monitoring (when subscribed)
Configuration Changes – Device / platform
DDoS / IPS / UTM / IDS Alerts (when subscribed)
Firewalls uptime and availability & Alerts
Risk Identification & escalations (SOP Driven)

Scope of Activities / Services

SOC – 24x7 Security incident management (DC infra)
VAPT Testing & Remediation (platforms & Networks)
Platform / OS Hardening / Configuration Management
Log management - Syslog / kiwi log & reporting
Support for SSL client certificates /SSL VPN
Configuration / off loading (when subscribed)
Spyware blocking / removal / Antivirus Enforcement
IPsec VPN Configuration & Management
Correlation rules incorporate all security elements
(white list, black list) to detect complex, multi-stage
attacks / Host Intrusion Prevention
Support for SSL client certificates /SSL VPN
Configuration Management
Audit Enablement – ISO27K / PCI-DSS / HIPPA
Configuration of alerts, monitoring & logging functions
TSR Implementation for platforms & networks
Network protection Services / DDoS / IPS / UTM / IDS
ISP Coordination & Vendor Management

Out of Scope

LAN / Wifi Device Support (external) Identity & access
management & transaction security / data encryption
End user support / Desktop / laptop support / PIM
Application / Web Security / API support / Fraud
Prevention / SSA & SSI
Security policy /procedures / Document updates
Third party tools & devices – HSM / Websense etc.
Forensics & security / data breach investigations / data
loss or data integrity (transactions) / Phishing / SQL
Injections / Ethical hacking / Identity Assurance etc.
Backups & Restoration of data / DLP Support
Physical Security & Asset Management / BMS etc.

Supported Areas & Coverage

SOC – Operations – 24x7x365
Platform Services – Logging (SIEM) HIPS
Network protection Services / DDoS / IPS / UTM / IDS
Compliance – ISO27K / PCI-DSS / HIPPA enablement
Dedicated Staffing - Security experts - Deployment

Severity Definitions

SLA - S1/P1/Error - 15 minutes Response, 4 hours Restoration

Intrusion detection / critical alerts response -
impacting entire setup or environment
Network / Device / Tools / Services inaccessible /
Interface / Instance Down or unavailable
Security incidents / data integrity issues
Major Risk Realization / BCP / DR related activities

SLA - S2/P2/Error - 30 minutes response, 12 hours restoration

Medium Risk Realization with partial impact
Configuration Recovery / Restoration
Failed login attempts

SLA - S3/P3/Error – 60 minutes response, 24 hours Restoration

ACL configurations & provisioning / upgrades etc
Audit Remediation activities / service requests
Logs / Utilization reports for investigations
CR Preparation / Custom queries / RCA Reports

Change Request (OTC Applicable)

Modification of Existing Configurations, new setup
Re-installation of firewalls, polices, firmware
Device Support / Vendor Engagement for fixes
Third party tools implementation support – racking /
stacking & interconnects