Sify Managed Security Services Proposal

Submitted To: <Customer Name>

Sify Technologies Ltd.

Contents

[Document History 4](#_Toc168670758)

[Sign-Off 4](#_Toc168670759)

[Document Title 4](#_Toc168670760)

[Preparation 4](#_Toc168670761)

[Release 4](#_Toc168670762)

[Distribution List 4](#_Toc168670763)

[Statement of Confidentiality 4](#_Toc168670764)

[Executive Summary 5](#_Toc168670765)

[About <CUSTOMER NAME> 5](#_Toc168670766)

[About Sify Technologies Ltd. 5](#_Toc168670767)

[Business Units 5](#_Toc168670768)

[Managed Network Services Portfolio 6](#_Toc168670769)

[Scale of Operations 6](#_Toc168670770)

[What does Sify bring to the table? 6](#_Toc168670771)

[Sify Managed Security Services 8](#_Toc168670772)

[Sify Managed Security Services (MSS) 10](#_Toc168670773)

[24X7 near Real Time Security Event Monitoring 10](#_Toc168670774)

[Sify’s Solution Delivery Architecture 11](#_Toc168670775)

[Sify’s Shared Tools Architecture 11](#_Toc168670776)

[Sify’s Shared Service Delivery Framework 11](#_Toc168670777)

[Service Delivery Using ITIL/Best Practices 11](#_Toc168670778)

[Service Window 11](#_Toc168670779)

[Services in Scope 12](#_Toc168670780)

[Firewall Management 12](#_Toc168670781)

[Sify’s Firewall Management Capability 13](#_Toc168670782)

[Service Deliverables for Firewall Management 14](#_Toc168670783)

[IDS/IPS Management 15](#_Toc168670784)

[Sify’s IDS/IPS Management Capabilities 16](#_Toc168670785)

[Service Deliverables for IDS/IPS Management 17](#_Toc168670786)

[DDoS Attack Mitigation 18](#_Toc168670787)

[Sify’s DDoS Mitigation Capability 19](#_Toc168670788)

[Service Deliverables for DDoS Attack Mitigation 20](#_Toc168670789)

[Secure Access Service Edge (SASE) Management 22](#_Toc168670790)

[Sify’s SASE Management Capability 22](#_Toc168670791)

[Service Deliverables for SASE Management 23](#_Toc168670792)

[Security Information and Event Management (SIEM) 25](#_Toc168670793)

[Service Deliverables for SIEM 26](#_Toc168670794)

[Security Orchestration, Automation, and Response (SOAR) 28](#_Toc168670795)

[Service Deliverables for SOAR 29](#_Toc168670796)

[Service Level Agreements 30](#_Toc168670797)

[SIEM Service SLAs 30](#_Toc168670798)

[Incident Definition/classification for SIEM service 31](#_Toc168670799)

[SLA Exceptions and Exclusions 31](#_Toc168670800)

[Service Level Conditions 32](#_Toc168670801)

[Site Uptime SLA – Service Credits 32](#_Toc168670802)

[Site Uptime SLA - Penalty Exclusion 32](#_Toc168670803)

[Service Request 33](#_Toc168670804)

[Severity Level Definitions 33](#_Toc168670805)

[Ownership of Firewalls Post Contract Period 34](#_Toc168670806)

[Faulty Firewalls Caused by Customer Site Conditions 34](#_Toc168670807)

[Addition of New Sites, Firewalls Post Contract Period 34](#_Toc168670808)

[RMA Process 35](#_Toc168670809)

[Device Warranties 35](#_Toc168670810)

[Pre-Requisites 36](#_Toc168670811)

[Internet Bandwidth 36](#_Toc168670812)

[Access Requirements 36](#_Toc168670813)

[System Requirement 36](#_Toc168670814)

[<Customer Name>’s Requirement 37](#_Toc168670815)

[Requirement Understanding 38](#_Toc168670816)

[Proposed Solution 39](#_Toc168670817)

[Solution Components 39](#_Toc168670818)

[Detailed Solution 39](#_Toc168670819)

[Reviews 40](#_Toc168670820)

[Commercial Proposal 41](#_Toc168670821)

[Information Security Policy 42](#_Toc168670822)

[Standard Terms & Conditions 43](#_Toc168670823)

[General T&Cs 43](#_Toc168670824)

[Payment Terms 45](#_Toc168670825)

# Document History

## Sign-Off

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Company** | **Name** | **Designation** |
| **Author** | Sify Technologies Limited |  | Solution Architect |
| **Client Management** | Sify Technologies Limited |  | Account Manager |
| **Project Owner** | <CUSTOMER NAME> |  |  |
| **Project Sponsor** | <CUSTOMER NAME> |  |  |

## Document Title

|  |  |
| --- | --- |
| **Customer** | <CUSTOMER NAME> |
| **Title** | Sify Managed Security Services Proposal |
| **Document Name** | <CUSTOMER NAME> - Security Approach v1.0.pdf |

## Preparation

|  |  |  |
| --- | --- | --- |
| **Action** | **Name** | **Date** |
| **Prepared By** | Solution Architect | June 2024 |
| **Reviewed By** |  |  |
| **Distributed By** |  |  |

## Release

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ver.** | **Release Date** | **Change Notice** | **Pages Affected** | **Remarks / Changes** |
| **v1.0** |  | NA | NA | NA |

## Distribution List

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Company** | **Name** | **Sections to Read** | **For Info** | **For Action** | **Released By** |
| <CUSTOMER NAME> |  | All |  | 🗹 |  |
| Sify Technologies Limited |  | All | 🗹 | 🗹 |  |
| Sify Technologies Limited |  | All | 🗹 | 🗹 |  |

## Statement of Confidentiality

|  |
| --- |
| This document contains proprietary trade secret and confidential information to be used solely for evaluating Sify Technologies Limited [“Sify”]. The information contained herein is to be considered confidential. <CUSTOMER NAME> by accepting this document, agrees that neither this document nor the information disclosed herein, nor any part thereof, shall be reproduced or transferred to other documents, or used or disclosed to others for any purpose except as specifically authorized in writing by Sify Technologies Limited. |

# Executive Summary

## About <CUSTOMER NAME>

< Content about the Customer>

## About Sify Technologies Ltd.

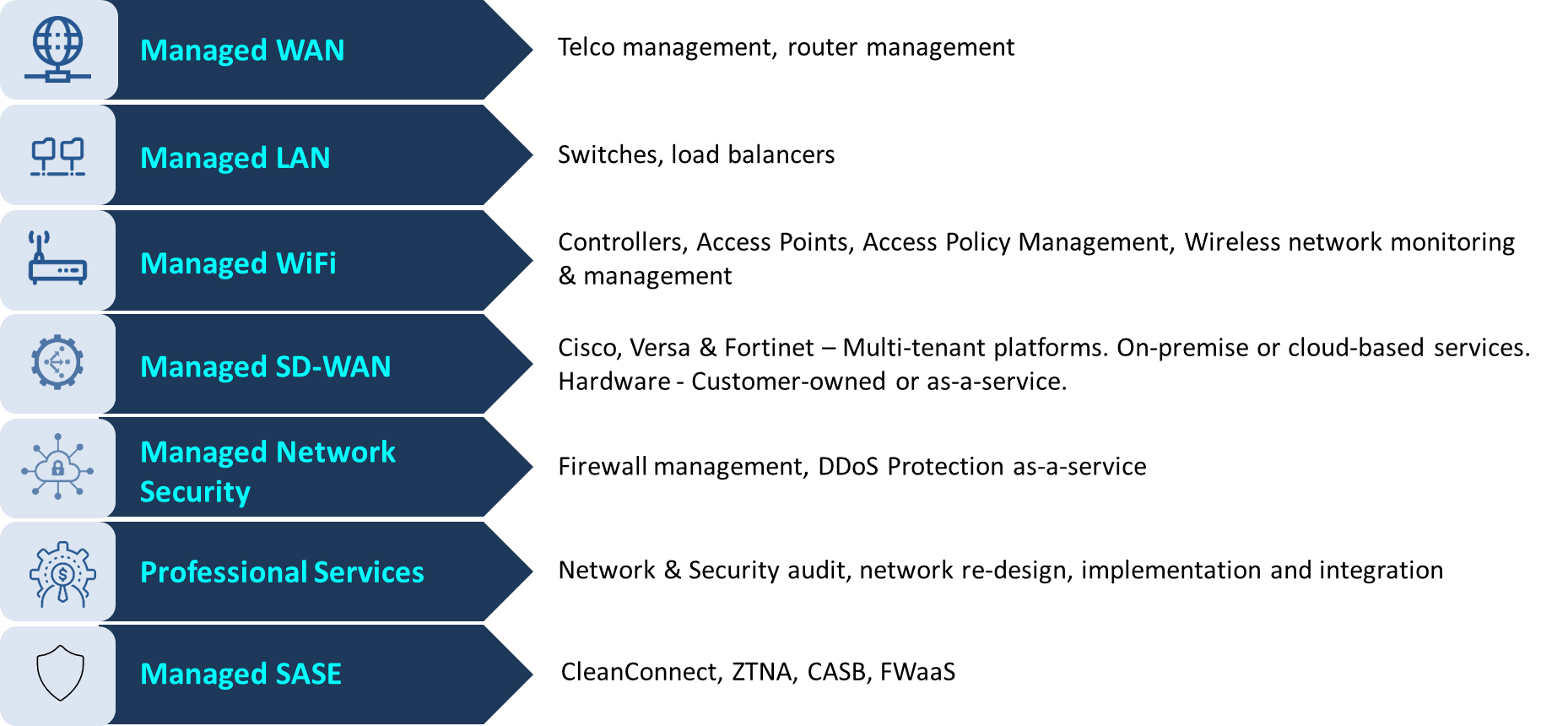
A Fortune 500 India company, Sify Technologies is India’s most comprehensive ICT service & solution provider. Sify being Digital at Core in our solutions portfolio, Sify is focused on the changing ICT requirements of the emerging Digital economy and the resultant demands from large, mid and small-sized businesses. Sify’s infrastructure comprising the largest MPLS network, top-of-the-line DCs, partnership with global technology majors, vast expertise in business transformation solutions modelled on the cloud make it the first choice of start-ups, incoming Enterprises, and even large Enterprises on the verge of a revamp,

More than 10000 businesses across multiple verticals have taken advantage of our unassailable trinity of Datacentres, Networks and Security services and conduct their business seamlessly from more than 1600 cities in India. Internationally, Sify has presence across North America, the United Kingdom and Singapore.

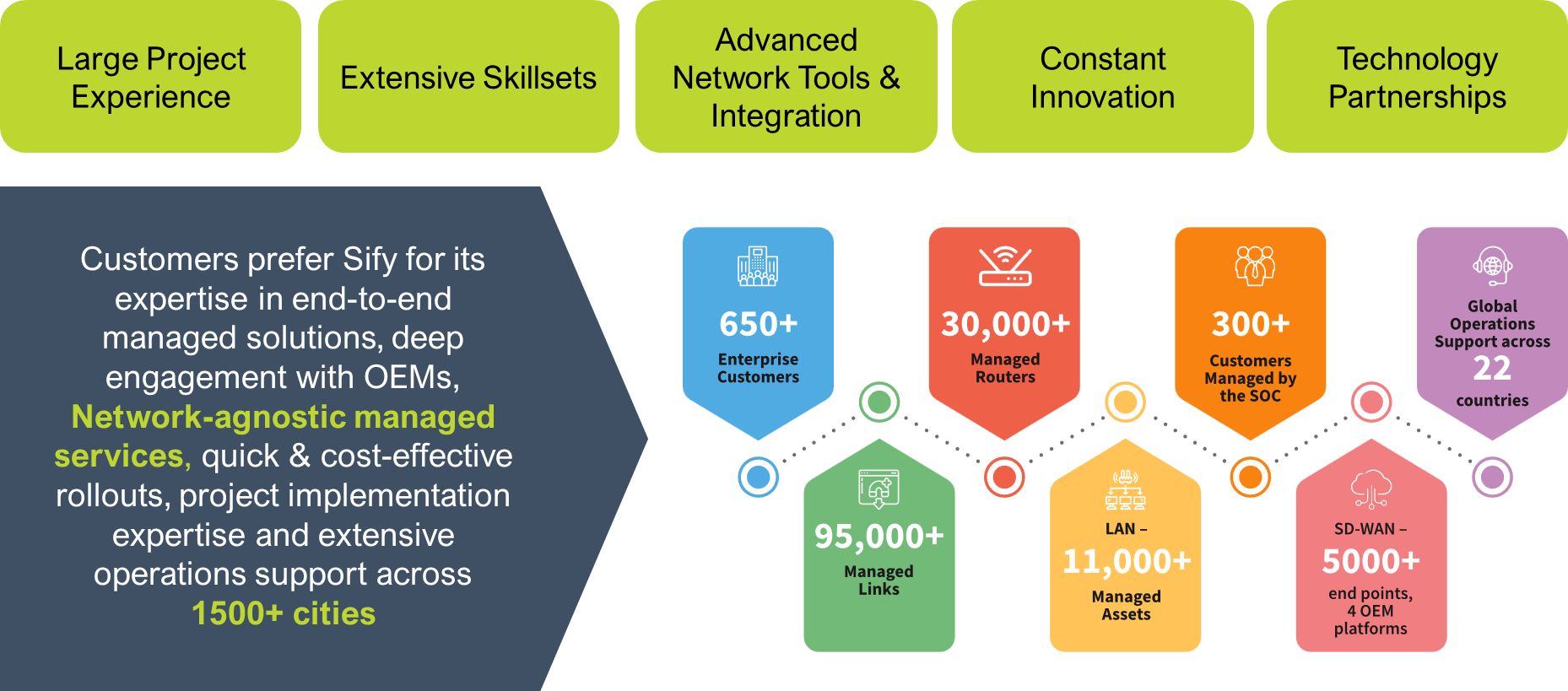
## Business Units



## Managed Network Services Portfolio



## Scale of Operations



## What does Sify bring to the table?

* Adherence to industry standards like ITILv3, ISO27001, ISO9001 and ISO20000 based service delivery
* Over 400 man-years of experience in management contributing to our core business
* Sify has optimal and right mix of services involved in system integration services including Network services, IT and security management, SOC
* Sify brings a strong Operational and Technical expertise in complex Infrastructure Management
* Extensive experience in delivering end-to-end network services concept creation – managing and delivering SLA adherence
* Sify has strategic relationships with OEM’s & Service Provider’s in the field of Compute, Network, Storage, Security, Operating Systems, Unified messaging & Applications, Enterprise Management Systems, Disaster Recovery Management & Replication, Power, Cooling, Building Management Systems, Passive components, MPLS Network, VPNoBB, Internet Bandwidth, Digital Certificates, etc.

Sify Technologies Limited (referred herein as “Sify”) has thoroughly understood the requirement and is pleased to submit the proposal to this. We are delighted at the possibility of partnering with <CUSTOMER NAME> in enhancing the adoption of technologies for efficient functioning of crucial business operations.

Sify is confident of offering a high-quality solution at a competitive price. We are equally confident that Sify’s awareness of the managed network services marketplace, its pioneering achievements in the field of providing high-quality managed network services to the Indian Corporate World, together with its unmatched expertise and experience in managing some of the country’s largest and mission-critical infrastructures can offer to <CUSTOMER NAME> a very unique and a distinct advantage which will clearly differentiate us and our solution from the rest of the competition. As a specialist and a leader in infrastructure management and services, we have also established our market leadership in the delivery of Managed Network Services, Data Center and Disaster Recovery services. It is this advantage of being a proven solution provider, which Sify wants to bring on board to <CUSTOMER NAME>.

To summarize this proposal, the response is divided into 2 parts, which addresses the following aspects of <CUSTOMER NAME> requirements as mentioned in the proposal.

Part 1: Technical Proposal

Part 2: Commercial Proposal

This document includes only Part 1 of the proposal. The document captures complete and comprehensive information about the proposed technical solution, its delivery capabilities and the support infrastructure/tools in place for management of the proposed solution offering based on adoption of industry-accepted ITIL standards. Part 2 is explained in a separate document, which is being submitted along with Part 1 to <CUSTOMER NAME>.

# Sify Managed Security Services

IT Infrastructure has become the lifeline for any business and there is a relentless drive towards automation and the focus on reducing manual intervention in processes, thereby achieving significant performance and productivity levels. Organizations are increasingly moving towards outsourcing their management of CPEs to Application Services to the service providers so that they can concentrate on their core business and thereby increase efficiency and productivity within the organization. Service provider not only brings rich and diversified experience but also enables a process-oriented approach ensuring smooth operations.

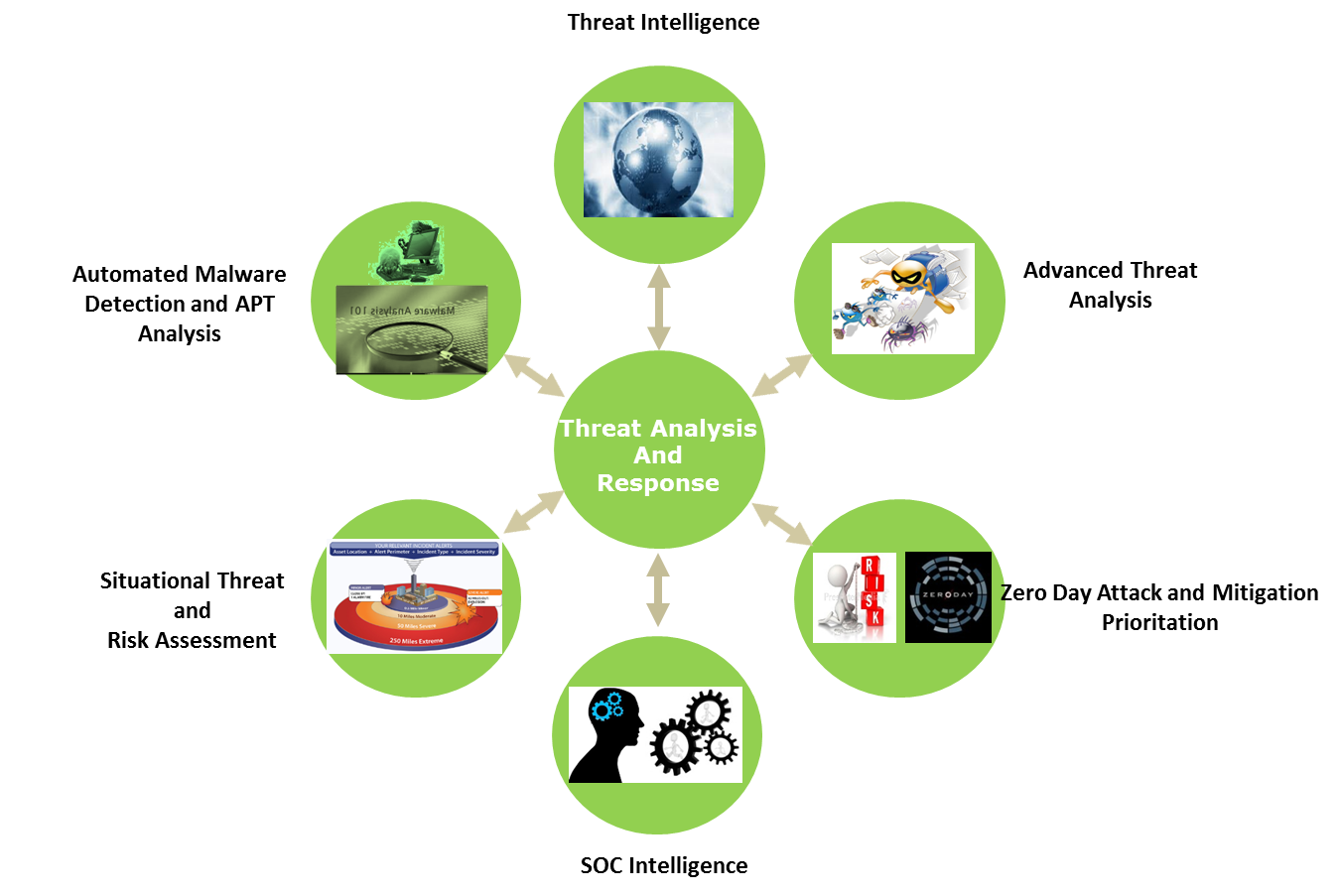
Sify monitors, manages, and administers customer’s infrastructure through redundant state-of-art Centralized Operations Centre at Mumbai, Chennai & Bangalore. Sify will manage the infrastructure proactively 24x7x365 days through the state-of-the-art Network Operations Centre. All the events will be proactively captured; analyzed and necessary actions will be taken through proper channel to rectify the errors, if any.

Proactive Monitoring and Management Service provided 24x7 proactive monitoring and management of WAN network, Security elements to offer performance and reporting with assured guarantees to Sify customers.

SIFY proposes to provide Managed Security Services for the deployed Information Security infrastructure. SIFY would provide best in class monitoring services for the security devices in scope.

SIFY would carry out near real-time event monitoring using state of the art tools including Security Information and Event Management correlation framework. The Security Information and Event Management framework which Sify has deployed is the best in class and provides proactive mitigation strategy for the emerging threats. The SIFY service Operations team consists of highly trained and experienced professionals who will identify the security incidents as and when they occur and proactively address them with structured ITIL V3 based service delivery & support processes.

To combat the advanced threat Sify brings in its Cyber Threat Intelligence Framework to help customers in mitigating known and un-known threats even before they enter the customer’s network. Below is Sify’s Cyber Threat Intelligence Framework which can be leveraged to customers in a phased manner for combating the emerging threats.



# Sify Managed Security Services (MSS)

Sify will provide its managed security services to meet the stated requirement and vision in a cost effective and efficient manner to enable <CUSTOMER NAME> to meet their security and compliance objectives.

With industry accepted process and tested technology, Sify would provide real-time detection and protection for <CUSTOMER NAME> security infrastructure in scope. Sify would use state of the art tools including Security Information and Event Management framework and advance correlation algorithms for monitoring of the security infrastructure in real time and detection of security events. Our highly trained and experienced consultants will identify the real threats from the midst of several Megabytes of data using several automated processes and tools, and proactively tackle them with structured escalations before they turn into problems.

By leveraging Sify’s Security service offerings, <CUSTOMER NAME> will realize the strategic value of their IT investments in mitigating the associated security risks in their infrastructure landscape. The key benefits on which <CUSTOMER NAME> can leverage upon are:

* Decade long experience in service delivery with Defined Processes, qualified people and in-depth expertise.
* Large Pool of Security Resources: 100+ having security domain expertise.
* Dedicated Sify Technology innovation Centre which would provide Proof of concept, Technology refresh and Optimization process.
* Presence of strong collaborative partnership with all leading security OEMs.
* Sify developed Security Visibility Portal would provide 360-degree view of Information security maturity and compliance level.
* Improve security posture and compliance adherence.
* Ensure business continuity and effective incident management.
* Reduces operational cost and increases return on security investments.
* Well streamlined Sify’s processes that continuously improve delivery processes.

## 24X7 near Real Time Security Event Monitoring

By using state of the art technology and Sify’s Security Operations Center and Threat Intelligence Framework, <CUSTOMER NAME> will be able to detect potential threats and attacks in early stages before they impact <CUSTOMER NAME> environment.

## Sify’s Solution Delivery Architecture

By leveraging Sify’s multi-tenant integrated tools framework combined with the robust service delivery framework, Sify would enable <CUSTOMER NAME> to manage their Information Security maturity in a cost-effective manner.

## Sify’s Shared Tools Architecture

<CUSTOMER NAME> will be able to leverage on the investment made by SIFY in Integrated Security Information and Event management tools for advanced event and vulnerability correlation technology combined risk simulation and threat modeling to provide optimum protection to <CUSTOMER NAME> IT assets.

## Sify’s Shared Service Delivery Framework

Sify’s Shared Services framework with the right resources at each level would provide <CUSTOMER NAME> having experienced resources in each Security technology in a cost-effective way. This combined with the Sify’s Crisis management framework would enable <CUSTOMER NAME> to avail Rapid response during any Security incident mitigation strategy.

## Service Delivery Using ITIL/Best Practices

SIFY would follow ITIL V3 based processes for service support and service delivery. This coupled with SLA’s will ensure SIFY is able to provide services which will be consistent and predictable. This will also provide an opportunity to <CUSTOMER NAME> to standardize and improve their processes by alignment with ITIL & industry best practices.

## Service Window

SIFY would provide security incident monitoring services round the clock. Resources will be available 24 x 7 for services.

## Services in Scope

The below are the services in scope for <CUSTOMER NAME>,

In DC,

|  |  |  |
| --- | --- | --- |
| **#** | **Devices** | **Quantity** |
| 1 | Firewall | XX |
| 2 | IPS | XX |
| 3 | SSL Box | XX |

In DR,

|  |  |  |
| --- | --- | --- |
| **#** | **Devices** | **Quantity** |
| 1 | Firewall | XX |
| 2 | SSL Box | XX |

* Firewall Management and security event monitoring
* IPS Management and security event monitoring
* Reverse Proxy Management and Security event monitoring

As per the understanding the below services would be in-scope for delivering 24x7 Managed Security Services,

# Firewall Management

In the realm of network security, the management of firewalls plays a pivotal role in safeguarding sensitive data and ensuring the integrity of digital communications. A firewall acts as a barrier between a trusted internal network and untrusted external networks, such as the internet. By monitoring and controlling incoming and outgoing network traffic based on predetermined security rules, firewalls serve as the first line of defence against cyber threats.

Effective firewall management involves a comprehensive approach to configuring, monitoring, and maintaining firewall systems to protect an organization’s network from unauthorized access, malware, and other security threats. This process includes setting up rules and policies that define what traffic is permitted or denied, continuously monitoring firewall activity, and regularly updating the firewall to respond to emerging threats.

The importance of firewall management cannot be overstated in today’s digital landscape. With the increasing sophistication of cyber-attacks and the growing complexity of network infrastructures, robust firewall management practices are essential for maintaining the security and functionality of network operations. This includes not only the technical aspects of firewall configuration but also the strategic alignment of firewall policies with the organization’s overall security posture.

Moreover, effective firewall management demands a proactive stance. This involves regular audits and assessments to ensure that firewall configurations remain optimal and aligned with current security requirements. It also requires staying informed about the latest threats and vulnerabilities to adapt firewall settings accordingly.

Firewall management is a critical component of network security that requires a blend of technical expertise, strategic planning, and ongoing vigilance. By implementing robust firewall management practices, organizations can significantly enhance their defences against cyber threats and ensure the resilience of their network infrastructures.

## Sify’s Firewall Management Capability

Sify’s Firewall Management Service provides robust and comprehensive protection for your network by ensuring continuous, proactive defence against unauthorized access and cyber threats. Our expert team handles the deployment, configuration, and ongoing management of firewall solutions tailored to your specific needs. Key capabilities include:

* **Real-Time Monitoring and Management**: Continuous monitoring of firewall activity to detect and respond to security events promptly, ensuring minimal disruption to your operations.
* **Policy Configuration and Enforcement**: Development and application of security policies to control traffic flow and enforce compliance with organizational and regulatory requirements.
* **Regular Updates and Patching**: Timely updates and patches to firewall systems to protect against emerging threats and vulnerabilities.
* **Advanced Threat Detection**: Utilization of advanced threat intelligence and analytics to identify and mitigate sophisticated cyber threats.
* **Comprehensive Reporting and Analytics**: Detailed reporting on firewall performance, security events, and compliance status, providing actionable insights for enhanced security posture.

With Sify’s Firewall Management, you can be assured of a secure, resilient network environment, safeguarded by industry-leading practices and technologies.

## Service Deliverables for Firewall Management

Firewall management is a crucial aspect of network security, encompassing a variety of deliverables that collectively ensure the protection and integrity of an organization's network.

The deliverables for Firewall management form the foundation of a robust firewall management strategy, aimed at protecting network assets, ensuring regulatory compliance, and maintaining high levels of operational efficiency. Key deliverables include:

|  |  |  |  |
| --- | --- | --- | --- |
| **Service** | **Task** | **Deliverables** | **Service Trigger** |
| 24x7 Monitoring | SIFY will monitor the following parameters through Sify owned monitoring tools | Reports on Device Availability | On alerts |
| Customer managed monitoring tools |  |
| Device Availability | Reports on CPU and memory utilizations |
| CPU Utilization Threshold |  |
| Memory Utilization for Threshold |  |
| Link Availability |  |
| System events monitoring | SIFY will monitor for system events which are critical | Notification to customer through Email/Phone | On alerts |
| Troubleshooting issues | SIFY will troubleshoot any of the issues which are causing business disruption by firewall. | Notification to customer through Email/Phone | On customer request. |
| Changes to firewall | SIFY will do configuration changes when required | Notification to customer through Email/Phone | Change request through ServiceNow. |
| Create/changes rule base |
| NAT/PAT configuration changes |
| User accounts |
| IPSec / VPN |
| DNS |
| ACLs |
| QoS |
| Protocol Inspection. |
| Integrating firewall with SIEM |
| Authentication Configuration | SIFY will configure or change the authentication configuration established at user, client, and session levels. | Notification to customer through Email/Phone | Change request through ServiceNow. |
| AAA configuration. |
| VPN Tunnels | SIFY will troubleshoot/configure site to site and client to site VPN tunnels | Notification to customer through Email/Phone | As needed. |
| Virtualization | SIFY will configure multiple device contexts (Virtual firewall) as per the customer requirement | Notification to customer through Email/Phone | As needed |
| Vendor coordination | We will do vendor coordination for hardware replacements and software issues | Notification to customer through Email/Phone | As needed |
| Backup Management | SIFY will ensure the automated backups are happening or not. | Notification to customer through Email/Phone |  |
| Rule base analysis | SIFY will analyze the existing rule base and fine tune them to increase the performance of firewall | Report sent to the customer | As needed |
| Virtualization | SIFY will configure multiple device contexts (Virtual firewall) as per the customer requirement | Notification to customer through Email/Phone | As needed |
| Up gradation | SIFY will do the Up gradation whenever the newer version is available. | Notification to customer through Email/Phone | As needed |
| Alerting | Alert customer on high and critical alerts getting generated on SIEM | Notification to customer through Email/Phone | As needed |
| Reporting | Reporting based on Reporting tools | Notification to customer through Email/Phone | As needed |
| Top Bandwidth |
| Top User |
| Top Threats |
| Admin failure attacks |
| VPN reporting |
|  |

# IDS/IPS Management

In the landscape of network security, the management of Intrusion Prevention Systems (IPS) is a cornerstone of proactive defence strategies. An IPS is a network security technology that monitors network traffic to detect and prevent identified threats. It not only alerts administrators to potential security breaches but also takes immediate action to block malicious activities, thereby safeguarding the network from a wide array of cyber threats.

Effective IPS management encompasses the deployment, configuration, and continuous oversight of IPS solutions to ensure they operate efficiently and effectively. This involves setting up detection and prevention policies, fine-tuning the system to reduce false positives and false negatives, and integrating the IPS with other security measures to create a cohesive defence mechanism.

The significance of IPS management in network security cannot be overstated, given the increasing sophistication of cyber-attacks. Modern IPS solutions are designed to detect complex threats, such as zero-day exploits, Advanced Persistent Threats (APTs), and various forms of malware, making them vital components in an organization's security arsenal. By actively blocking threats in real-time, an IPS helps to minimize the potential impact of security incidents and maintain the integrity of critical data and systems.

A robust IPS management strategy includes regular updates and patches to keep the system current with the latest threat signatures and detection algorithms. It also involves continuous monitoring and analysis of IPS alerts to refine the system's accuracy and effectiveness. Additionally, IPS management requires detailed logging and reporting to facilitate incident response, forensic investigations, and compliance with regulatory requirements.

Furthermore, IPS management is not a one-time task but an ongoing process that demands vigilance and adaptability. As new threats emerge and network environments evolve, IPS configurations and policies must be regularly reviewed and adjusted to ensure optimal protection.

IPS management is a crucial element of network security that requires a blend of technical expertise, strategic planning, and continuous improvement. By effectively managing IPS solutions, organizations can enhance their defence against cyber threats, ensuring a resilient and secure network infrastructure.

## Sify’s IDS/IPS Management Capabilities

Sify's IDS/IPS Management Service offers a powerful and proactive defence against network intrusions and cyber threats. Our comprehensive management of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) ensures that your network remains secure and resilient. Key capabilities include:

* **Real-Time Threat Monitoring**: Continuous surveillance of network traffic to detect and identify suspicious activities and potential threats.
* **Automated Threat Response**: Immediate response mechanisms to block and mitigate detected threats, preventing them from causing harm to your network.
* **Advanced Analytics and Correlation**: Utilization of sophisticated analytics and correlation techniques to enhance threat detection accuracy and reduce false positives.
* **Regular System Tuning and Updates**: Ongoing optimization of IDS/IPS configurations and timely application of updates to address new vulnerabilities and threats.
* **Detailed Reporting and Incident Analysis**: Comprehensive reporting on detected threats, response actions, and overall security posture, providing insights to strengthen defences.

With Sify’s IDS/IPS Management, your network benefits from expert oversight and advanced technologies, ensuring robust protection against intrusions and maintaining the integrity of your critical assets.

## Service Deliverables for IDS/IPS Management

Intrusion Prevention System (IPS) management is a critical aspect of network security, focusing on the proactive detection and prevention of potential threats. This ensures that the IPS management is comprehensive and effective, providing robust protection against cyber threats and maintaining the security and integrity of the network. Key deliverables of IPS management include:

|  |  |  |  |
| --- | --- | --- | --- |
| **Service** | **Task** | **Deliverables** | **Service Trigger** |
| 24x7 Monitoring | SIFY will monitor the following parameters through Sify owned monitoring tools | Reports on Device Availability | On alerts |
| Customer managed monitoring tools |  |
| Device Availability | Reports on CPU and memory utilizations |
| CPU Utilization Threshold |  |
| Memory Utilization for Threshold |  |
| Incident notification | Email alert for low correlated, medium, and high events. Phone call will also be placed for critical incident | Notification to customer through Email/Phone | On alerts |
| Security Analysis | Alarm analysis Event Correlation & Analysis Root Cause Analysis for High Level Alerts | Notification to customer through Email/Phone | On alerts |
| Signature updates | SIFY will make sure the latest signatures are up to date to protect against the latest vulnerabilities. | Notification to customer through Email/Phone | On customer request. |
| Changes to IPS | SIFY will do configuration changes when required | Notification to customer through Email/Phone | Change request through ServiceNow. |
| Create/changes rule base |
| Protocol Inspection. |
| Block rules based on signatures/Geo location, IP address |
| Configuring global correlation rules |
| Integrating IPS to third party SIEM tools |
| Signature Fine tuning | SIFY will fine tune signatures based on the customer infra. | Notification to customer through Email/Phone | Change request through ServiceNow. |
| Signature customization | SIFY will create custom signatures based on the customer need. | Notification to customer through Email/Phone | As needed |
| Virtualization | SIFY will configure multiple device contexts (Virtual IPS) as per the customer requirement | Notification to customer through Email/Phone | As needed |
| Vendor coordination | We will do vendor coordination for hardware replacements and software issues | Notification to customer through Email/Phone | As needed |
| Backup Management | SIFY will ensure the automated backups are happening or not. | Notification to customer through Email/Phone |  |
| Reporting | Create Reports based | Report sent to the customer | As needed |
| Top critical alerts |
| Top Victims |
| Top attacks |
| Top Risks |
| Top Blocked |
| Web based attacks |
| Alerting | Fine tuning the false alerts based on the alert generation. | Notification to customer through Email/Phone | As needed |
| Up gradation | SIFY will do the Up gradation whenever the newer version is available. | Notification to customer through Email/Phone | As needed |

# DDoS Attack Mitigation

Distributed Denial of Service (DDoS) attacks represent one of the most significant threats to network security, capable of overwhelming online services and causing extensive disruptions. These attacks involve multiple compromised systems, often distributed across various locations, which flood a target with an excessive amount of traffic, rendering it inaccessible to legitimate users. Effective DDoS attack mitigation management is essential for protecting network infrastructure, maintaining service availability, and ensuring business continuity.

DDoS attack mitigation management involves a comprehensive set of strategies and technologies designed to detect, respond to, and neutralize the impact of DDoS attacks. It starts with robust monitoring and early detection mechanisms that can identify unusual traffic patterns and distinguish between legitimate spikes in traffic and malicious activities. Advanced threat intelligence and analytics play a crucial role in this phase, providing real-time insights and predictive analytics to pre-emptively identify potential threats.

One of the primary components of DDoS mitigation is traffic filtering and rate limiting. By employing sophisticated algorithms and rules, organizations can filter out malicious traffic before it reaches critical resources, ensuring that only legitimate traffic is allowed through. Rate limiting helps to control the flow of traffic, preventing servers from being overwhelmed by excessive requests.

Another critical aspect of DDoS mitigation is the use of scrubbing centres. These are specialized facilities equipped with the necessary infrastructure to handle large volumes of traffic. When an attack is detected, traffic is rerouted through these centres, where malicious packets are filtered out, and clean traffic is forwarded to the destination. This approach ensures that the impact of an attack is minimized, and normal operations can continue uninterrupted.

Cloud-based DDoS protection services offer an additional layer of defence, leveraging the scalability and distributed nature of cloud infrastructure to absorb and mitigate large-scale attacks. These services can dynamically scale to handle even the most substantial DDoS attacks, providing robust protection for both on-premises and cloud-based resources.

Collaboration and communication are also vital in DDoS mitigation management. Establishing clear protocols and communication channels with Internet Service Providers (ISPs), third-party security vendors, and internal stakeholders ensures a coordinated and timely response to attacks. Regular drills and simulations help organizations prepare for actual incidents, enhancing their ability to respond swiftly and effectively.

DDoS attack mitigation management is a crucial element of network security, requiring a proactive and multi-layered approach. By implementing advanced detection systems, traffic management techniques, and leveraging cloud-based solutions, organizations can protect their network infrastructure from the disruptive impact of DDoS attacks, ensuring the availability and reliability of their services.

## Sify’s DDoS Mitigation Capability

Sify offers a completely managed DDoS Mitigation service for Sify’s On-Net internet customers & operates DDoS scrubbing centres in four strategic locations globally: Mumbai, Chennai, London, and Singapore. These centres are equipped with advanced infrastructure and technologies to effectively mitigate DDoS attacks, ensuring the resilience and security of the Company's network and services.

Details of the DDoS scrubbing centres and their respective mitigation capacities are as follows:

* Location: Mumbai | Mitigation Capacity: 4Gbps
* Location: Chennai | Mitigation Capacity: 20Gbps
* Location: London | Mitigation Capacity: 72Gbps
* Location: Singapore | Mitigation Capacity: 72Gbps

These centres serve as critical components of the Company's network defence infrastructure, providing rapid detection and mitigation of DDoS attacks to safeguard against disruptions and ensure the availability and reliability of services for our customers.

Sify can protect customers against the following range of attacks –

|  |  |
| --- | --- |
| **Attack Type** | **Protection** |
| •  TCP SYN Flood |  |
| •  Spoofed TCP-SYN flood |  |
| •  SYN/ACK Reflection Flood |  |
| •  TCP ACK flood |  |
| •  Smurf attack |  |
| •  Ping flood |  |
| •  ping of death |  |
| •  ICMP Echo request flood |  |
| •  Teardrop attack |  |
| •  low-rate denial of service attack |  |
| •  Mydoom |  |
| •  UDP Flood |  |
| •  Nuke | (for volumetric attacks) |
| •  HTTP/HTTPS flood attack | (for volumetric attacks) |
| •  DNS amplification attack |  |
| •  IP fragmented attack etc. |  |

## Service Deliverables for DDoS Attack Mitigation

DDoS attack mitigation services provide essential protection for organizations against the disruptive impact of Distributed Denial of Service (DDoS) attacks.

This ensures that organizations can effectively manage and mitigate the risks associated with DDoS attacks, maintaining the availability and reliability of their online services and network infrastructure. The key deliverables of these services include:

|  |  |  |  |
| --- | --- | --- | --- |
| **Service** | **Task** | **Deliverables** | **Service Trigger** |
| Incident Management | * Rapid deployment of mitigation strategies to minimize the impact of detected attacks. * Coordination with ISPs and third-party vendors to reroute and manage traffic effectively. | * Incidents will be created by the customer or by Sify through Sify’s Delivery portal Aakash or through mail notification. * Periodicity: 24X7 | On alerts |
| Change Management | * Regular updates to mitigation technologies and strategies to address evolving threats. * Change in the hardware deployed to run the service. | * Any change to the existing infrastructure or configuration of the customer assets will be followed as per the SOW and as per the SOC’s Change management process. * Periodicity: 24X7 | Change request through ServiceNow. |
| Configuration Management | * Application of rate limiting to control the flow of incoming traffic, preventing server overload. * Continuous improvement of service capabilities to adapt to new attack methods and trends. | * Manage the configuration on all network security devices as per the design document and best practices if applicable * Periodicity: 24X7 | As needed |
| Vendor Management | * We will do vendor coordination for hardware replacements and software issues | * Sify NOC will interact with respective with corresponding vendor for any kind of replacement of customer asset as per the proposed SOW. * Periodicity: 24X7 | As needed |
| Device Management | * SIFY will do the upgradation whenever newer iOS versions are available. | * Check whether the Device management port could be reached; if so, take initial backup of the device configuration. * Periodicity: 24X7 | As needed |
| Email & Web Based Support | * Keeping customer’s updated & informed. | * Customers would have access to Sify’s security experts through email and web during regular working hours * Periodicity: 24X7 | On customer request. |
| Telephonic Support | * Keeping customer’s updated & informed. | * Skilled Network Security resources will be available during regular working hours to provide technical support over phone. * A toll-free number would be provided to the customer for this purpose. * Periodicity: 24X7 | On customer request. |

# Secure Access Service Edge (SASE) Management

The emergence of Secure Access Service Edge (SASE) represents a paradigm shift in network security, offering a holistic approach that integrates wide area networking (WAN) and comprehensive security services into a unified, cloud-delivered model. SASE management focuses on the administration and optimization of this architecture to ensure seamless, secure, and efficient access to applications and resources, regardless of user location.

SASE management is driven by the need to adapt to modern IT environments characterized by increasing cloud adoption, remote workforces, and the proliferation of edge devices. Traditional security models, which relied on perimeter-based defences, are no longer sufficient in this distributed landscape. SASE addresses this by converging network and security functions such as secure web gateways (SWG), cloud access security brokers (CASB), firewall as a service (FWaaS), and zero-trust network access (ZTNA) into a single, integrated service.

## Sify’s SASE Management Capability

Sify’s SASE solution aims to transform traditional network architectures into modern, cloud-centric models that prioritize security, flexibility, and user experience in the increasingly distributed and digitalized business environment.

Sify’s effective SASE management practice involves several key responsibilities such as:

* Policy Configuration and Enforcement
* User and Device Authentication
* Traffic Inspection and Threat Prevention
* Performance Optimization and QoS
* Continuous Monitoring and Analytics

## Service Deliverables for SASE Management

Sify’s Managed SASE offers a comprehensive and integrated approach to network security and connectivity, delivered from the cloud. This enables organizations to achieve a secure, agile, and scalable network infrastructure while simplifying management and reducing operational overhead. SASE as a Service empowers organizations to embrace digital transformation securely and adapt to evolving business requirements with confidence.

The key deliverables of SASE as a Service include:

|  |  |  |  |
| --- | --- | --- | --- |
| **Service** | **Task** | **Deliverables** | **Service Trigger** |
| Service portal | * Develop and maintain a portal for customers to view, configure, and monitor WAN network performance for Sify and other providers. | * Portal to customer, able to view, configure, monitor WAN network performance of Sify and other providers | As needed |
| Capacity management | * Measure WAN link utilization trends, create baselines, and recommend actions for customers, including upgrades or downgrades. | * Measure WAN link utilization trends, create baselines and recommend customer on the actions taken – upgrade, downgrade | As needed |
| Transition and implementation services | * Conduct site surveys and prepare CRD, HLD, and LLD documents. | * Site survey, CRD, HLD and LLD. Deploy initial CPE devices across all sites. Perform MACD as and when changes required [bandwidth upgrade/downgrade, new features] | As needed |
| Proactive network monitoring | * Deploy initial CPE devices across all sites and perform MACD (Moves, Adds, Changes, and Deletions) as required. | * 24x7 Monitoring of network related faults and performance management. Able to view these alerts on self-service portal | As needed |
| Application visibility | * Provide 24x7 monitoring of network-related faults and performance management, with alerts viewable on a self-service portal. | * Identify applications and sub-applications, report the performance of applications | As needed |
| Incident reporting and management | * Identify applications and sub-applications, and report on their performance. | * Trouble ticketing for all network related issues including other SP links. Detection of alerts from fault and performance management systems | As needed |
| Problem management | * Manage trouble ticketing for all network-related issues, including those involving other service provider links, and detect alerts from fault and performance management systems. | * Diagnose, identify and isolate issues. Work on fix and workarounds with providers and SASE vendors | As needed |
| Configuration management | * Diagnose, identify, and isolate network issues, and work on fixes and workarounds with providers and SASE vendors. | * Configuration of managed CPE devices, auditing, backup of configuration, template-based config | As needed |
| Inventory management | * Configure managed CPE devices, perform audits, back up configurations, and implement template-based configurations. | * Manages inventory of CPE devices, resources – IP address, VLAN etc. | As needed |
| Vendor management | * Manage the inventory of CPE devices and resources, including IP addresses and VLANs. | * Co-ordinate with vendors for issue reporting and resolution, faulty hardware management, recommended best practices | As needed |
| Change management | * Coordinate with vendors for issue reporting and resolution, manage faulty hardware, and recommend best practices. | * Scheduled network changes – changing software based on EOL, proactive identification of network issues and resolution, MACD of WAN links and bandwidth | As needed |
| Service desk | * Implement scheduled network changes, including software updates based on EOL (End of Life) and proactive identification and resolution of network issues. | * 24x7 technical support team to co-ordinate with customer for issue reporting and resolution | As needed |
| Hardware replacement time | * Provide 24x7 technical support and coordinate with customers for issue reporting and resolution. | * Replacement of faulty hardware and components | As needed |
| Support systems | * Replace faulty hardware and components as needed. | * IAM, NTP, OOB management systems | As needed |
| Root cause analysis | * Manage IAM (Identity and Access Management), NTP (Network Time Protocol), and OOB (Out-of-Band) management systems. | * Analysis of issues and identify root causes – including CPE and provider links | As needed |

# Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) is a critical component of modern network security, designed to provide real-time analysis of security alerts generated by applications and network hardware. SIEM management involves the deployment, configuration, and continuous oversight of SIEM systems to detect, respond to, and mitigate security threats effectively.

SIEM systems integrate security information management (SIM) and security event management (SEM) functions into a comprehensive security solution. This integration allows for the collection, normalization, and analysis of log data from various sources across the network. By correlating this data, SIEM systems can identify patterns and anomalies that may indicate security incidents or breaches.

Effective SIEM management is essential for several reasons:

* **Centralized Monitoring and Visibility**:
  1. SIEM systems provide a centralized view of an organization’s security posture, aggregating data from firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus software, and other security tools.
  2. This holistic view enhances the ability to detect and respond to threats across the entire network.
* **Real-Time Threat Detection and Response**:
  1. SIEM systems enable real-time monitoring and analysis of security events, allowing for the immediate detection of suspicious activities.
  2. Automated response mechanisms can be configured to mitigate threats as they are detected, reducing the potential impact on the network.
* **Incident Investigation and Forensics**:
  1. SIEM solutions store and organize log data, making it easier to conduct thorough investigations following a security incident.
  2. Detailed logs and reports aid in forensic analysis, helping to determine the root cause of incidents and improve future defences.
* **Compliance and Reporting**:
  1. Many regulatory frameworks and standards require organizations to monitor and report on security events. SIEM systems facilitate compliance by providing the necessary logging and reporting capabilities.
  2. Customizable reports can be generated to meet specific regulatory requirements and demonstrate compliance to auditors.
* **Proactive Threat Management**:
  1. SIEM management involves continuous tuning and updating of the system to adapt to emerging threats and evolving network environments.
  2. Proactive threat hunting and regular review of SIEM alerts help identify vulnerabilities and mitigate risks before they can be exploited.
* **Resource Optimization**:
  1. By automating the correlation and analysis of security events, SIEM systems reduce the workload on security teams, allowing them to focus on more strategic activities.
  2. Efficient SIEM management ensures optimal performance and minimizes false positives, enhancing overall security operations.

## Service Deliverables for SIEM

Sify’s SIEM offering provides organizations with a comprehensive solution for managing and monitoring security events and information in real-time from the cloud. This enables organizations to enhance their security posture, detect and respond to security threats more effectively, and achieve regulatory compliance requirements while reducing the complexity and overhead associated with managing an on-premises SIEM solution. SIEM as a Service empowers organizations to strengthen their security defences and protect their valuable assets with confidence.

The key deliverables of SIEM as a Service include:

|  |  |
| --- | --- |
| **#** | **Sify’s SIEM Deliverables** |
| **1** | **Management** |
| i | Event Sources Integration with SIEM tool, whenever needed. |
| ii | Sify SOC provides solution to integrate a new data/event sources into existing collectors without disruption to the on-going data collection. |
| iii | The SIEM product have capability to collect, correlate, analyze, derive logical conclusion from logs, events, information received by it from heterogeneous systems including Networking and Security systems, OS, Web servers, databases, other infrastructure servers and Network devices etc.  Note: If a log source is not supported out of box, manually create customer parsers. |
| iv | Creation of Correlation Rules based on endpoint device, also provides solution which support the following correlation methods but not limited to: |
|  | Rules based Correlation – This is based on inherent and/or custom rules which would detect criteria when matched would result in a certain action. |
|  | Statistical Threat Analysis – To detect unknown threats and anomalies with immediate out-of-the-box value that can be improved through tuning. |
|  | Susceptibility Correlation – Raises visibility of threats against susceptible hosts, Reduces noise of threats against non-susceptible hosts |
| v | Setting up an alert Aggregation (baseline) and generating the events. |
| vi | Sify SOC provides a threat intelligence feed for identifying new global threats around the globe like DDoS (Slow Loris or LOIC etc.), Malicious IP Addresses, Known C&C (Command and Control) hosts etc. |
| vii | Manual Email notification would be created for alerts, based on rules applied and the same to be notified. |
| viii | Sify SOC provides SIEM solution to import the vulnerability information from scanning and assessment tools on real time basis and correlate them for all possible implications. |
| ix | The Security advisories to be shared on timely basis which suits the Customer computing network Infrastructure |
| **2** | **Security Event Monitoring** |
| i | 24x7x365 proactive event log monitoring of infrastructure and business applications. |
| ii | Incident creation in ticketing tool based on its criticality. |
| iii | Rapid response to Incidents and performing an in-depth analysis to identify whether it's a True positive/False positive alarm. |
| iv | Alert mechanism for immediate intimation / escalation and confirmation of remediation to the authorised / nominated officials |
| v | Continuous follow-up with IT support team until the issue gets resolved. |
| vi | Maintaining the False positive tracker to avoid further reiterations. |
| **3** | **Report Template** |
| i | Report Template Creation based on customer requirement. |
| ii | Submitting the Monthly report which summarizes the list of events / incidents reported correlation analysis, recommendations, status of actions and other security advisories. |
| iii | The monthly reports include the trend analysis comparing the present reporting cycle data with the previous reporting cycle data (Weekly, Monthly, Quarterly and Annually as what may be applicable). |
| iv | Monthly Review meeting will be arranged between Customer and Sify SOC, SOC Consultant would present the report of last one month status on security, vulnerabilities, Status of the ticket etc. |
| **4** | **Log Collection Methodology** |
| i | Sify SOC provides the solution which supports the collection of logs from devices/ servers/ applications etc., via the following methods but not limited to: |
| ii | Syslog over UDP / TCP and Syslog NG |
| iii | Secure XML |
| iv | Check Point LEA |
| i | SNMP |
| ii | ODBC (to pull events from a remote database) or Database Connection |
| iii | FTP (to pull a flat file of events from a remote device that can’t directly write to the network) |
| iv | Snare tool for Windows Event logs |
|  |  |
| **5** | **Log Retention** |
|  | Sify SOC providing the SIEM solution that can handle the log retention 30 days - Online |
|  | Sify SOC providing the SIEM solution that can handle the log retention 90 days - Online and custom storage requirement |

# Security Orchestration, Automation, and Response (SOAR)

Security Orchestration, Automation, and Response (SOAR) is a comprehensive approach in network security that combines various tools and processes to improve an organization's ability to respond to security incidents.

**Security Orchestration:** Connects disparate security tools and systems to work together seamlessly. Automates and coordinates workflows across different security technologies and teams, ensuring that all necessary steps in a response plan are executed efficiently.

**Automation:** Uses scripts and automated processes to handle repetitive and time-consuming tasks such as data collection, analysis, and initial threat response. Minimizes the need for human intervention in routine security operations, freeing up security personnel to focus on more complex tasks.

**Response:** Provides structured response actions to mitigate and contain security threats, reducing the time and impact of an incident. Utilizes predefined response playbooks that guide the response process, ensuring consistency and effectiveness.

## Service Deliverables for SOAR

Sify’s deliverables w.r.t SOAR encompass a wide range of components and functionalities designed to enhance an organization's security posture. The key service deliverables are:

|  |  |
| --- | --- |
| **Service Deliverable** | **Description** |
| Security Orchestration | * Integration of Security Tools: Connecting existing security tools and systems into a unified SOAR platform. * Workflow Automation: Developing and implementing automated workflows. |
| Automation | * Automated Incident Response: Predefined actions for common security incidents. * Script and Playbook Development: Custom scripts and playbooks tailored to client’s needs. |
| Threat Intelligence Management | * Integration of Threat Feeds: Incorporation of multiple threat intelligence feeds. * Threat Correlation and Analysis: Automated correlation and analysis of threat data. |
| Incident Response | * Real-Time Monitoring: Continuous monitoring of security events. * Incident Triage and Prioritization: Automated triage. * Response Playbooks: Predefined playbooks for incident response. |
| Alert Management | * Alert Aggregation: Consolidation of alerts from multiple sources. * Alert Enrichment: Enrichment of alerts with contextual information. |
| Reporting and Analytics | * Dashboard and Visualization: User-friendly dashboards. * Automated Reports: Scheduled and on-demand reports. * Compliance Reporting: Generation of compliance reports. |
| Customization and Scalability | * Custom Playbooks and Workflows: Development of custom solutions. * Scalable Architecture: Ability to accommodate organizational growth. |
| Training and Support | * User Training: Training for effective use of SOAR platform. * Ongoing Support: Continuous support and maintenance services. |
| Post-Incident Review | * Incident Post-Mortem Analysis: Detailed analysis of incidents. * Lessons Learned: Documentation and dissemination of lessons learned. |
| Consulting and Advisory | * Security Assessments: Regular assessments of SOAR implementation. * Strategic Advice: Ongoing strategic advice for security operations optimization. |

# Service Level Agreements

Service level agreement for the steady state delivery stage is defined during the due diligence phase, after discussing with <CUSTOMER NAME> designated representatives. There would be definite SLA related to all the deliverables mentioned above.

Following is the standard SLA, committed to <CUSTOMER NAME>.

|  |  |  |
| --- | --- | --- |
| **Incident Priority** | **Response Time** | **Resolution Time** |
| Critical | 30 min | 2 hours |
| High | 30 Min | 4 hours |
| Medium | 2 hours | 8 hours |
| Low | 4 hours | 48 hours |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Criticality** | **Service Window** | **Measurement Target** | | **Measurement  Window** |
| Security Monitoring Service availability | 24x7 | 99.00% | | Monthly |
| **Service Management** | | | | |
| Security Monthly Reports | | | Previous Months Reports in 7 business days | Monthly |
| Provisioning Ad hoc operational report (Max 2 in a quarter) | | | 15 business days | Monthly |
| Availability of security correlated logs for 1 month for in scope devices | | | 95% | Monthly |
| Threat Advisory -Advisory for new vulnerabilities impacting Customer's assets | | | 90% | Monthly |

## SIEM Service SLAs

|  |  |
| --- | --- |
|  | **Service Level Agreement (SLA)** |
|  | **Raising Alerts** |
| i | Within 15 minutes of detection of Critical priority events / incidents. |
| ii | Within 30 minutes of detection of high priority events / incidents. |
| i | Within 45 minutes of detection of medium priority events / incidents. |
| ii | Within 60 minutes of detection of low priority events / incidents. |
|  |  |
|  | Note-High, medium, and low referred above would be defined as follows: |
| i | High: Event/Incident that affects the functioning of business operations / system being not operational. |
| ii | Medium: Event/Incident that does not result in non-functioning of business operations /systems but if not addressed could result in business operations being hampered/ System not operating with full capability but is still operational. |
| iii | Low: Event/Incident which does not hamper business operations/ System is up and running with limited or no significant impacts. |

## Incident Definition/classification for SIEM service

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Incident Type** | **Threshold Value** | **Severity** |
| 1 | Security Device Down / Connectivity | Complete setup / service down | P1 |
| 2 | Infected Server | >500 events in 120 Seconds | P2 |
| 3 | Brute Force attempt to critical servers | >5 failed attempts in 120 Seconds | P2 |
| 4 | Exploit attempt to critical servers | Single instance observed at internal NIDS / Arbor devices | P2 |
| 5 | Port Scan from Internal sources | <500 events in 180 Seconds | P3 |
| 6 | Abnormal traffic observed after a vulnerability announcement | New alarms observed | P3 |
| 7 | Voluminous traffic dropped from internal sources | >50000 dropped in 120 Seconds | P2 |
| 8 | Failed login attempts from multiple sources | >20 failed logins from different user ids in 180 Seconds | P2 |
| 9 | Reconnaissance from external (Port Scans, Host Queries, Mail Reconnaissance, DNS Queries etc.) | >350 events in 180 Seconds | P3 |
| 10 | Suggestive Vulnerability Assessment from Internal sources | >500 Events in 180 Seconds | P3 |
| 11 | Voluminous dropped packets from external sources | >50000 Events in 120 Seconds | P2 |
| 12 | Deviation from normal traffic | New alarms being observed | P3 |
| 13 | Failed login attempts from same source / User | >10 Failed attempts in 180 Seconds | P3 |
| 14 | Policy Violations i.e. peer to peer traffic etc. | >10 Events in 60 Seconds | P4 |

## SLA Exceptions and Exclusions

Sify is not responsible for failure to meet an SLA where Sify’s failure results, in whole or in part, from:

* Negligence of the Customer or its representatives.
* Any Force Majeure event that prevents Sify, or vendor from providing Service or affecting restore or repair.
* Failures in performance caused by any national or local holiday.
* Any case in which Sify or vendor agents are available to repair within the Service Level commitment, but Customer reschedules to a different time or date.
* No access (Sify or vendor Agents rare available to repair within the Service Level commitment but the Customer does not provide Site access)

Interruptions or delays caused by the failure of power, equipment, services, or systems (at Customer premises) not provided by Sify including, but not limited to UPS Backup power; Generators; or Air conditioning/Heating.

## Service Level Conditions

The Service Levels defined above are subject to the conditions that for all Service Level Types mentioned above, Customer must provide on-site personnel & hardware to replace the failed device with a replacement device.

## Site Uptime SLA – Service Credits

The total of all Service Credits provided by Sify is limited to a maximum of 5% of the Quarterly Service Charge for the affected Service and Location. The Site Uptime Service Credit will be applicable as per the Site Type deployment (as mentioned within SLA table). Service credits shall be Customer’s sole remedy for a breach of the applicable service level agreement.

## Site Uptime SLA - Penalty Exclusion

No Service penalty is payable by Sify, if the failure to meet the Service Level is attributable to:

* Suspension of Services due to the Customer’s breach of the Agreement
* Alleged Service Level failure which cannot be verified by Sify's systems.
* Acts or omissions of the Customer, its subcontractors or any third party acting on the Customer’s behalf.
* Scheduled Maintenance
* Emergency Maintenance (where the emergency has not been caused by the negligence or wilful misconduct of Sify)
* Previously identified Problem that is awaiting a Change Window to be approved by the Customer to Resolve the Problem
* Any malfunction, Incident, defect, or failure in the Customer’s equipment
* Power failure at the Customer Location
* Force Majeure Events

## Service Request

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Service Feature** | **Severity** | **Metric** |
| 1 | Mean Time to Respond | For Severity 1/2/3/4 | 15 mins/ 30mins / 60 mins/1 Business Day\* |
| 2 | Incident Response Rate |  | 99.90% |

\* Indicates all time mentioned as Business Hours

## Severity Level Definitions

* **Severity 1**: An existing infrastructure is down or there is a critical impact on the Customer’s business operation. (Business Critical or Emergency)
  + System Unusable
  + Immediate Action Needed
  + Critical Condition
* **Severity 2**: Operation of an existing infrastructure is severely degraded, or significant aspects of the Customer’s business operation are being negatively impacted by unacceptable infrastructure performance. Operational performance of the infrastructure is impaired, but most business operations remain functional. (Major)
  + Error Condition
  + Warning condition
  + Normal but significant condition
* **Severity 3**: Changes to the infrastructure elements to activate / provision new services to end users. (Minor)
  + Change management request.
* **Severity 4**: Information is required on software capabilities, installation, or configuration. There is clearly little or no impact on the Customer’s business operation. (Low)
  + Informational message only
  + Debugging

## Ownership of Firewalls Post Contract Period

* All Sify owned Managed CPE will continue to be under Sify’s ownership for the entire lifecycle of the product.
* Ownership of such devices will not change even if the project reaches the end of contract duration.
* Ownership of the Managed CPE can be transferred to the customer at the end of the contract only if the customer agrees to procure the device the residual value decided by Sify.
* Ownership of the Managed CPE can be transferred to the customer before the end of contract only if the customer agrees to procure the device at the transfer rate decided by Sify.

## Faulty Firewalls Caused by Customer Site Conditions

The customer will be charged for any damage or fault occurring to a Sify owned device due to poor hygiene at location or device burnout due to insufficient Earthing & lack of UPS power. Customer will be charged for replacement of device even if the damage occurs due to unpredictable disasters such as fire or flooding. The price for replacement of the device will be decided by Sify and will depend on device type.

Addition of New Sites, Firewalls During Contract Period

Any new sites added over the course of the contract should have the same scope and deliverables as the original set of sites. Customer will need to release separate PO for the additional sites. Sify will aim to protect the price of new locations up to a maximum period of 6 months, post which any new sites added will be subject to price update.

Any change in solution will be treated as a separate opportunity & will have no bearing on the running contract.

## Addition of New Sites, Firewalls Post Contract Period

Addition of new sites, devices post the contract period will be considered as a new opportunity. The price of deliverables in the previous contract cannot be used as a reference even if there is no change in the solution.

## RMA Process

The scope of RMA will cover the services under Firewall with Proactive Network Monitoring and Management i.e. hardware provided by Sify & managed by Sify.

## Device Warranties

* The RMA process is undertaken to ensure the return of a faulty product to receive a replacement of repair during the product’s warranty period.
* As standard process, all managed CPE are procured with minimum 1 year of warranty. Any project specific procurements are done with warranty scope as per project.
* Faulty Firewalls are classified as Dead-on-Arrival (DOA) if a fault is detected during installation within specified period from date of delivery.
* RMA can only be raised when device is in-warranty. Devices are treated as in-warranty during the RMA process even if the actual warranty runs out before the RMA process ends.

# Pre-Requisites

## Internet Bandwidth

Sify would recommend <CUSTOMER NAME> to factor minimum 4 MB internet /MPLS bandwidth for the purpose of log forwarding.

## Access Requirements

Sify would need root / admin access to MSS Systems to be able to install MSS agents and then manage agent services. Specific Services / Ports and IP details will be shared during time of Integration of services.

## System Requirement

Customer is requested to provide server class hardware with the following specification for installation of SIEM agent.

* Windows server 2008 (Minimum)
* CPU – Dual Core, 2.1 GHz
* RAM – 8 GB
* HD – 500 GB

# <Customer Name>’s Requirement

**<<<<<<<<<<<<<<**

**INCLUDE DETAILED DESCRIPTION OF THE CUSTOMER’S REQUIREMENT**

**>>>>>>>>>>>>>>**

# Requirement Understanding

**<<<<<<<<<<<<<<**

**INCLUDE DETAILED DESCRIPTION OF SIFY’S UNDERSTANDING OF THE CUSTOMER’S REQUIREMENT**

**>>>>>>>>>>>>>>**

# Proposed Solution

## Solution Components

**<<<<<<<<<<<<<<**

**INCLUDE DETAILED DESCRIPTION OF SIFY’S UNDERSTANDING OF THE CUSTOMER’S REQUIREMENT**

**>>>>>>>>>>>>>>**

## Detailed Solution

**<<<<<<<<<<<<<<**

**INCLUDE DETAILED DESCRIPTION OF SIFY’S UNDERSTANDING OF THE CUSTOMER’S REQUIREMENT**

**>>>>>>>>>>>>>>**

# Reviews

<CUSTOMER NAME> & Sify shall conduct reviews with preset periodicity along with the Project In-charge, Support Engineers, and Account Manager to review & ascertain the performance of the team & in-scope infrastructure.

# Commercial Proposal

**<<<<<<<<<<<<<< INCLUDE CUSTOMER PRICING >>>>>>>>>>>>>>**

# Information Security Policy

Information is a critical asset for Sify, and it is essential to protect it from unauthorized access, disclosure, alteration, and destruction. This Information Security Policy outlines the principles, guidelines, and responsibilities necessary to maintain the confidentiality, integrity, and availability of information within the organization.

**Policy Scope:** This policy applies to all employees, contractors, third-party vendors, and any other personnel who have access to Sify's information resources.

**Information Classification:** All information assets must be classified based on their sensitivity and criticality. The classification levels are:

* Public: Information that can be freely shared with the public.
* Internal: Information for internal use only, not to be shared outside the organization.
* Confidential: Sensitive information requiring strict controls and limited access.

**Access Controls:** Access to information resources shall be based on the principle of least privilege. Access rights will be granted on a need-to-know basis, considering the employee's role and responsibilities. User access accounts must be promptly deactivated upon termination or change of roles.

**Physical Security:** Physical access to information assets, datacentres, and server rooms must be restricted and monitored. All devices containing sensitive information must be securely stored, and access to these areas must be logged and monitored.

**Network Security:** All network connections to the [Company Name] infrastructure must be secure and compliant with industry best practices. Firewalls, intrusion detection/prevention systems, and other security measures must be implemented and regularly updated.

**Data Encryption:** Sensitive data must be encrypted during transmission and storage. Encryption protocols must align with industry standards, and encryption keys must be securely managed.

**Malware Protection:** All endpoints must have up-to-date antivirus software, and regular scans should be conducted to detect and remove malware. Employees should be educated on the risks of phishing and other social engineering attacks.

**Incident Response:** A documented incident response plan shall be in place to address security incidents promptly. Employees must report any suspected security incidents to the IT department immediately.

**Security Awareness Training:** All employees must undergo regular security awareness training to stay informed about the latest security threats, policies, and best practices.

**Compliance with Laws and Regulations:** Sify is committed to complying with all applicable laws, regulations, and industry standards related to information security.

**Policy Review and Updates:** This Information Security Policy will be reviewed annually and updated as necessary to address emerging threats and changes in the business environment.

**Enforcement:** Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or legal action.

# Standard Terms & Conditions

## General T&Cs

* All pricing provided are exclusive of applicable taxes.
* The contract period will be applicable as per the PO.
* The project delivery timelines will be 12 - 14 weeks from the date of Sify’s acceptance of a customer PO. Any delays caused due to Customer premises or infrastructure not being ready will result in extension of delivery timelines.
* Additional Charges are applicable for any additional cabling requirements.
* Any physical hardware damage caused by customer will incur hardware charges for replacement of faulty hardware (OTC). Customer must provide UPS Power and earthing for the managed devices.
* Early Termination charges are applicable for any services terminated within the contract period.
  + In the event of performance degradation in Sify’s scope of work, which is brought to the notice of Sify in writing, Sify shall use all means available to rectify the same immediately and communicate to the customer on the action taken.
  + If the performance degradation is not rectified within one month (1 month) from the time Sify acknowledges the customer complaint in writing/mail and if this performance degradation is repeated for the same site / network element for 3 consecutive times within a calendar quarter after Sify has taken necessary corrective measures, Customer has the option of terminating the contract with 1 month notice period for the affected site / network element.
  + If the Customer chooses to terminate the entire contract for convenience or any other reason other than performance degradation of the service, the customer is liable to pay the annual recurring charges for the remaining period of the contract on a pro-rata basis. These charges will pertain to any Hardware and/or Software Licenses that have been specifically deployed for the use of the customer.
* Any requirement of changing the feature tier (if applicable) will result in associated change of commercials.
* Any changes to the Solution design and configuration will result in the design change along with the revised commercials.
* Cancellation or reschedule of site visits (for international locations) within 48 hours’ notice will incur additional charges.
* The provisioning/commissioning of any unmanaged or managed network security services (apart from anything included within the Solution) is considered out of scope.
* All Payment will be as per Sify's payment terms and conditions.
* 24\*7 proactive monitoring and management of the network as defined in the solution document is included.
* The customer will sign a scope of work document along with the PO and that will be considered as the reference for sign off on delivery of the project. Any scope not explicitly mentioned in the SOW will be considered out of scope of the project.
* Only one site visit is factored for all on-site deployments and implementation for international locations, any additional site visits required will incur additional charges.
* Installation SOW - basic rack & stack, uploading IOS/config file.
* For International locations, Field Engineering services are factored for during business hours (9 AM - 5.00 PM Local Time Business Days). Out of business hours and Weekends and holidays will incur additional charges.

All Internal Cabling needs to be completed within 5 business days from the date of Service Readiness communicated by Sify. Failure to comply with the timeline will lead to the initiation of the billing for the service automatically from the Sixth day.”

## Payment Terms

|  |  |  |
| --- | --- | --- |
| **Billing T&C** | **Notice Period** | **Billing Dispute** |
| Direct Sale: 100% on delivery | 30 days in advance | Billing Disputes to be raised within 15 days of invoice submission. No claims raised later would not be accepted |
| Recurring Charge: Quarterly in Advance | 30 days in advance | Billing Disputes to be raised within 15 days of invoice submission. No claims raised later would not be accepted |

**<<<<<<<<<<<<<<<<<<<<<<< END OF DOCUMENT >>>>>>>>>>>>>>>>>>>>**