BSE
The Power of Vibrance

Market Security Operations Center

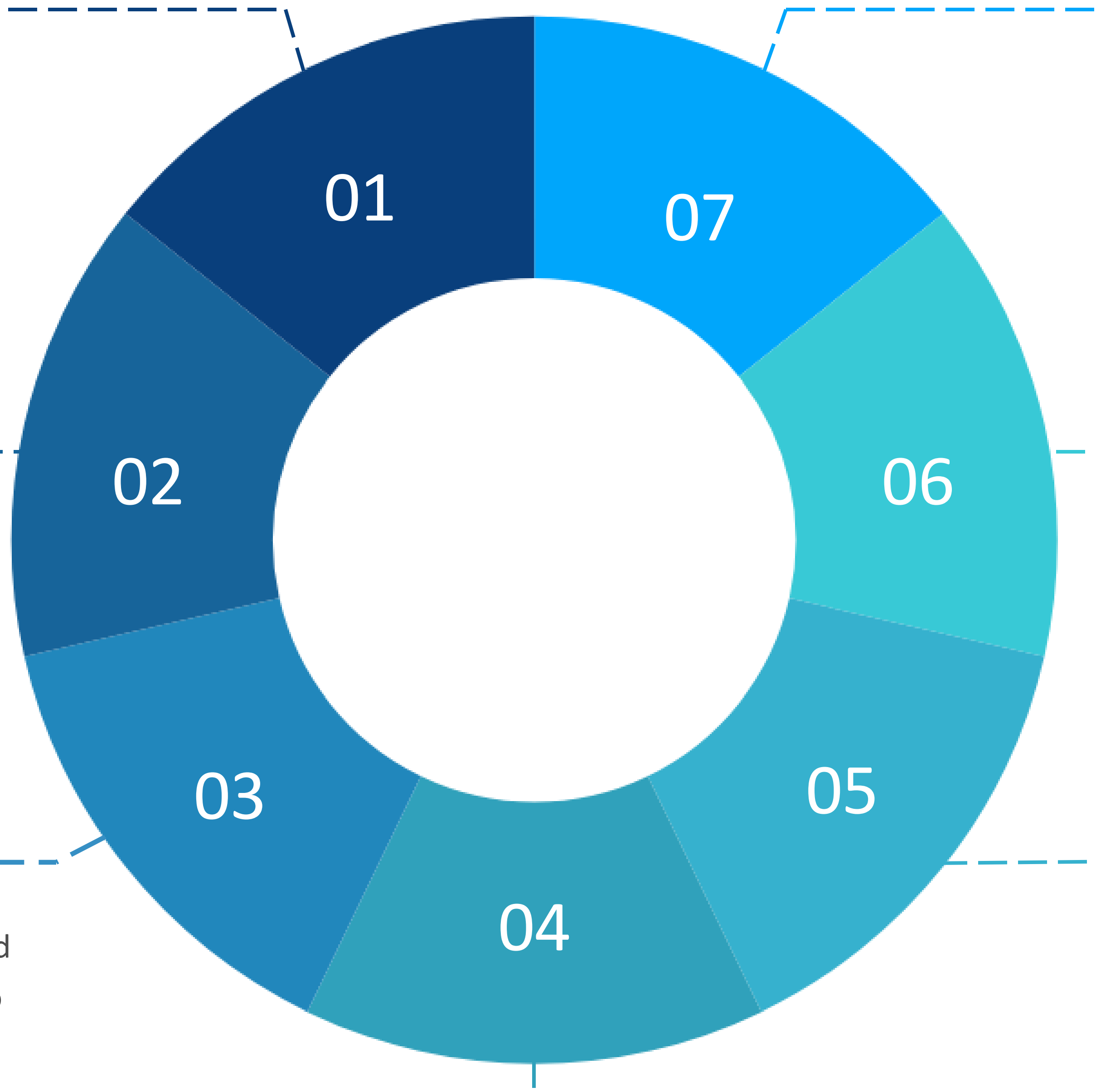
POWERED BY BluSapphire
Governed By BSE

Empowering Your Business with
Advanced Cybersecurity Measures
Powered by BluSapphire

Born, Built and Headquartered In India.

BLUSAPPHIRE
ENTERPRISE SECURITY SIMPLIFIED

MSOC Scope of Services



24x7 Monitoring (Logs & EDR)

24x7 monitoring of RE endpoint security logs. Qualified Security Analysts review and escalate incidents. EDR Agent is optional. REs may use any EDR agent of their choice.

Incident Management

MSOC to share Incident Management Process with all RE(s).

Native Case Mgmt.

Native built-in Case Management allow RE(s) to view and manage incidents. Regulator/auditors will have access to cases.

Centralized Dashboarding/Report

Ongoing deliverables/KPIs dashboarding and reporting

Log Retention & Compliance Reports

Six (6) months Online, and Eighteen (18) months offline (Optional) .

Weekly & Monthly automated reports.

Multi- Tenancy

RE(s) can view only their data. Regulators and auditors can view and monitor all RE(s) cases and data for compliance.

Threat Intelligence

Threat Intelligence from multiple sources including CERT-IN and NCIIPC

MSOC

TECHNOLOGIES OFFERED BY MSOC

MANDATORY

- **Log Management**
  - Log Collection & Forwarding
  - Log baselining
  - Log Search
- **Log Collection**
  - Collect multiple Log formats
  - Collect in multiple log protocols (syslog, TCP, UDP)
  - Compress
  - Filter
  - De-Duplicate
  - Encrypt
  - Transmit to MSOC
- **Next Gen SIEM**
  - Security Incident & Event Management (SIEM)
  - Compliance Rule Management
  - Alert handling (forwarding)
  - Incident Management
- **Threat Intelligence**
  - Out of box TI included
  - Integration with CERT-IN, NCIIPC included
- **Dashboarding & Reporting**
  - Compliance Reports
  - Weekly & Monthly reports
- **Case Management**
  - Case creation
  - Case status & analyst notes
  - Case SLA tracking
  - Case closure(s) & Reporting

OPTIONAL

- **EDR Agent**
  - In-memory attach behavior detection
  - Prevent malicious attacks like Ransomware
  - Respond to malicious attacks with responses like clean, delete and quarantine.

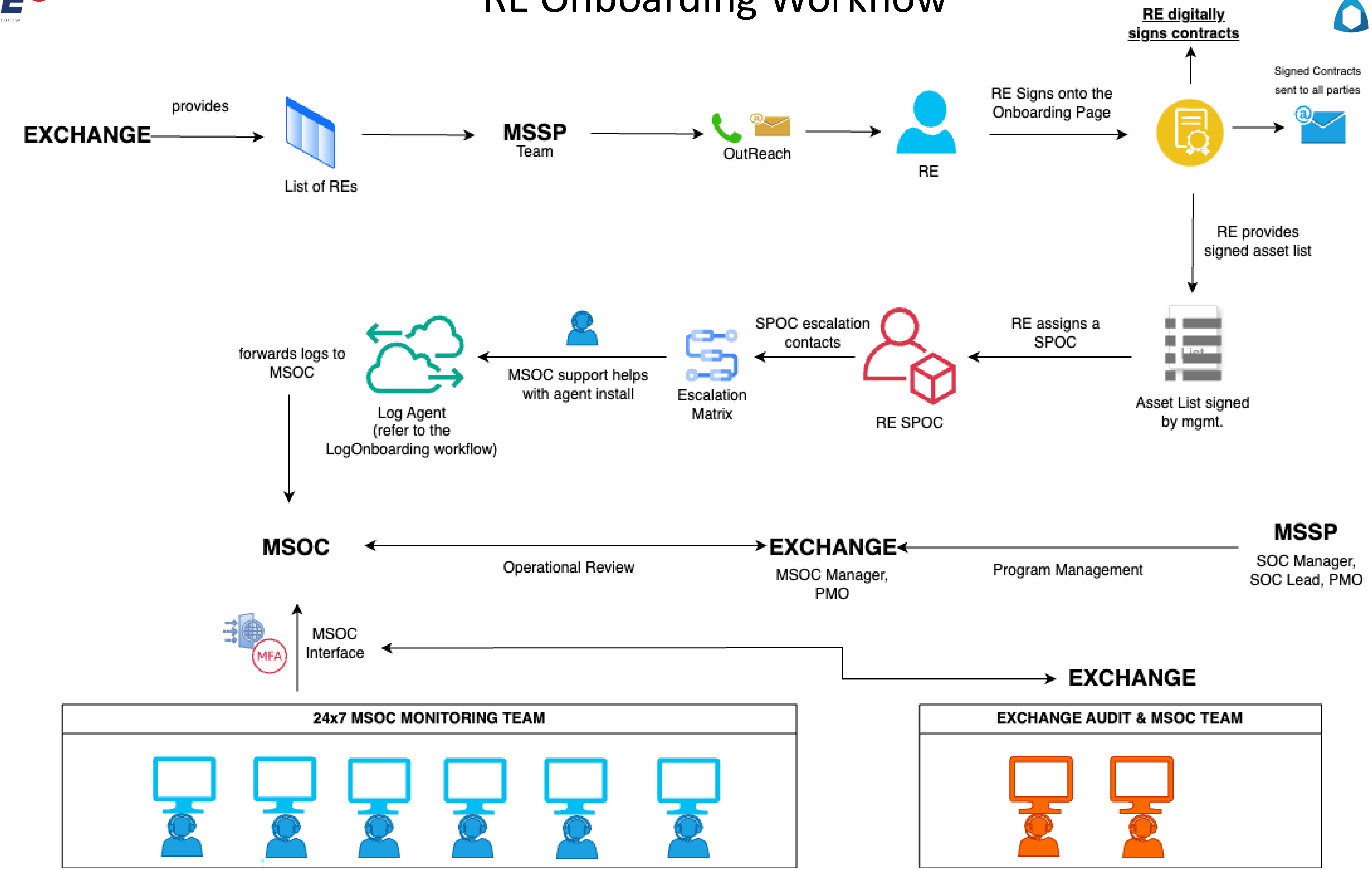
- **User Entity Behavior Analytics (UEBA)**

- **Network Behavior Anomaly Detection**
  - Monitor Netflow records
  - Detect anomalous behavior
  - ML based anomaly detection including geo-based traffic anomaly detection
- **Log Retention** (As per regulatory requirement)

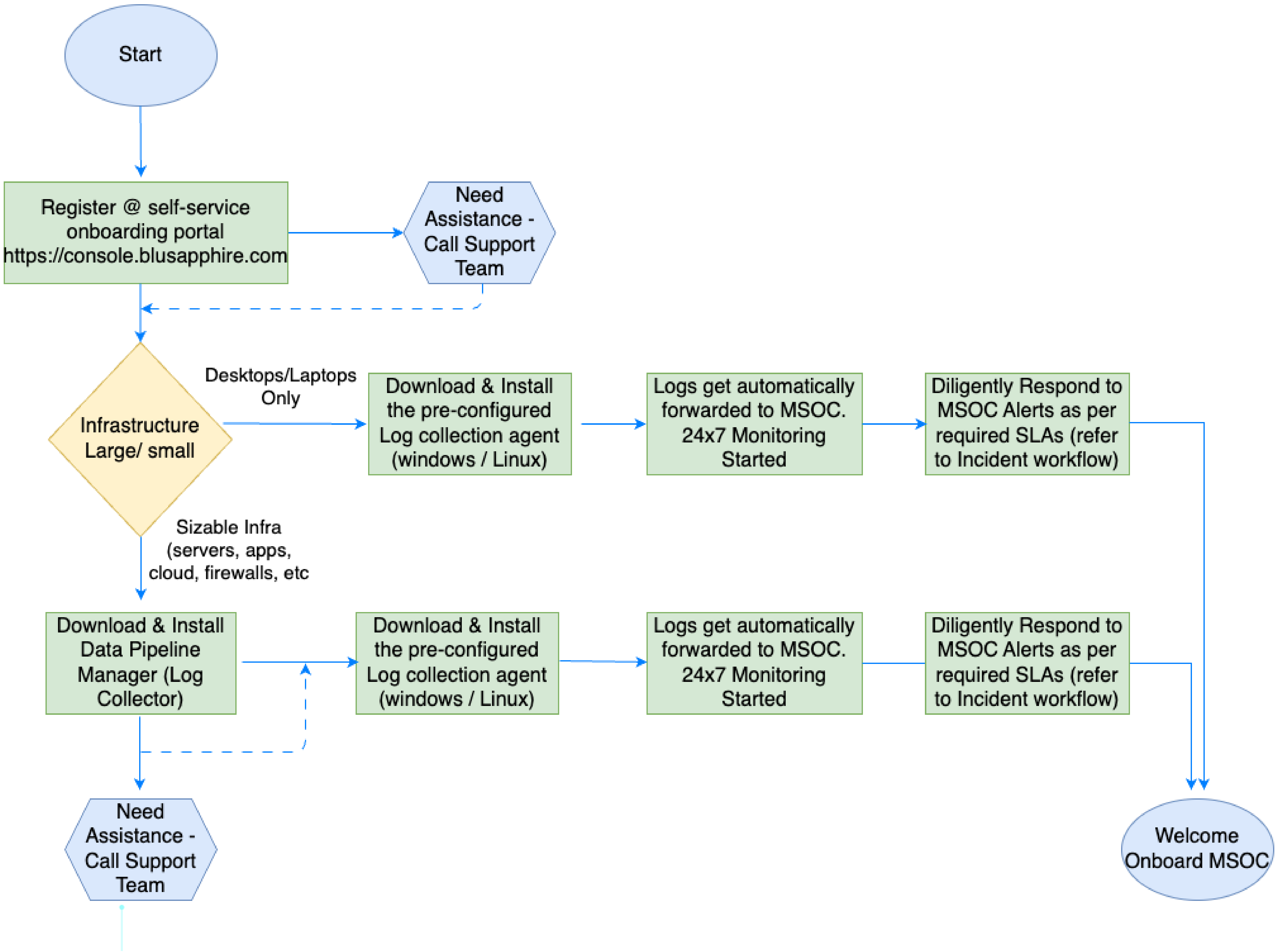
- **SOAR**
  - Automation of Triage
  - Automated Response to Industry standard tools (over 200 OpenAPI integrations supported)
  - Incident/Ticket Orchestration
  - Incident Response Playbooks

- VAPT
- CSCRF Audit

RE Onboarding Workflow


EXCHANGE
provides
List of REs
MSSP
Team
OutReach
RE
RE Signs onto the Onboarding Page
RE digitally signs contracts
Signed Contracts sent to all parties
RE provides signed asset list
Asset List signed by mgmt.
List
RE assigns a SPOC
RE SPOC
SPOC escalation contacts
Escalation Matrix
MSOC support helps with agent install
Log Agent (refer to the LogOnboarding workflow)
forwards logs to MSOC
MSOC
Operational Review
EXCHANGE
MSOC Manager, PMO
Program Management
MSSP
SOC Manager, SOC Lead, PMO
MFA
MSOC Interface
EXCHANGE
24x7 MSOC MONITORING TEAM
EXCHANGE AUDIT & MSOC TEAM

Log Collection Workflow



Start

Register @ self-service onboarding portal https://console.blusapphire.com

Need Assistance - Call Support Team

Infrastructure Large/ small

Desktops/Laptops Only

Download & Install the pre-configured Log collection agent (windows / Linux)

Logs get automatically forwarded to MSOC. 24x7 Monitoring Started

Diligently Respond to MSOC Alerts as per required SLAs (refer to Incident workflow)

Sizable Infra (servers, apps, cloud, firewalls, etc

Download & Install Data Pipeline Manager (Log Collector)

Download & Install the pre-configured Log collection agent (windows / Linux)

Logs get automatically forwarded to MSOC. 24x7 Monitoring Started

Diligently Respond to MSOC Alerts as per required SLAs (refer to Incident workflow)

Need Assistance - Call Support Team

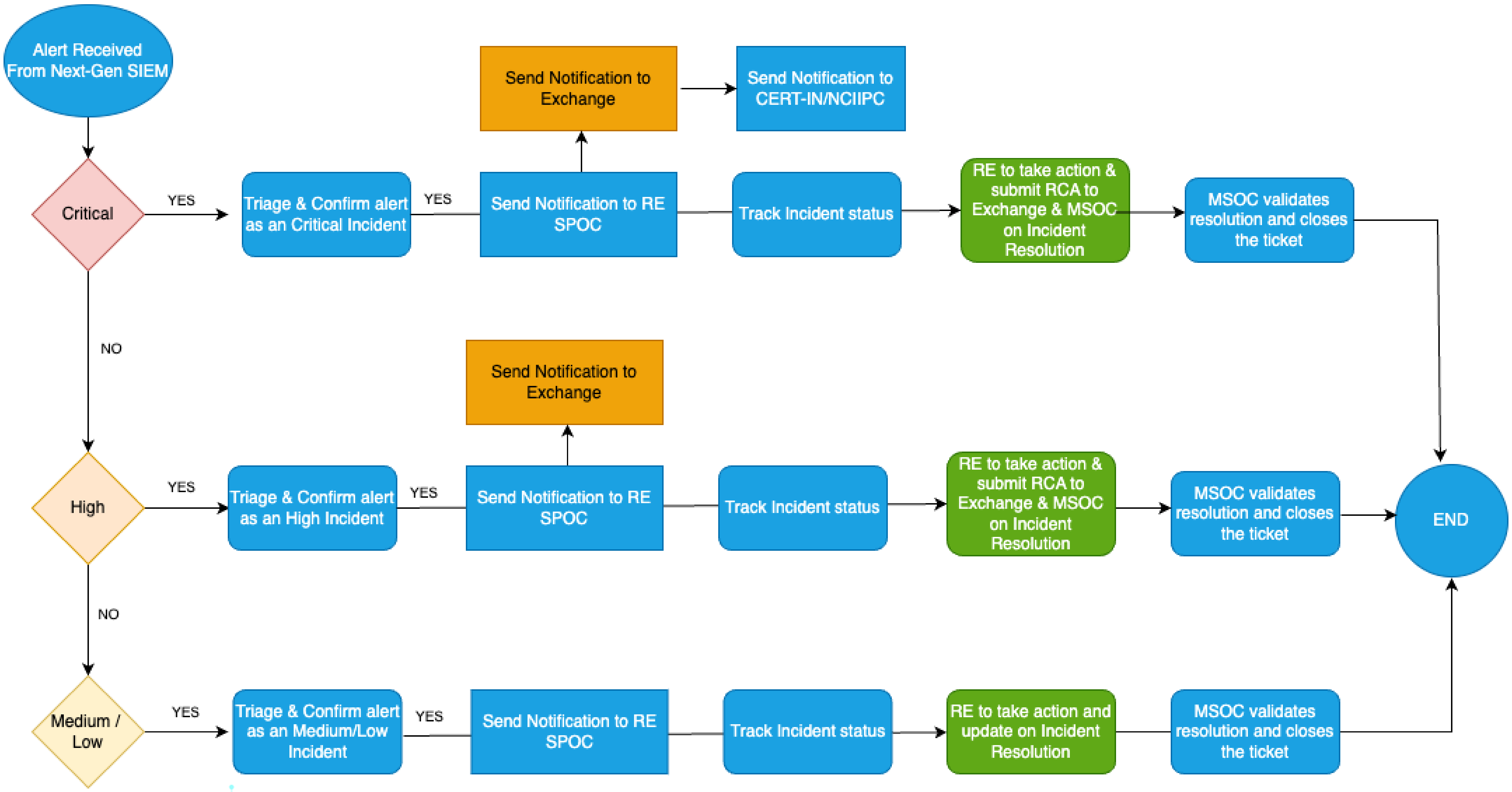
Welcome Onboard MSOC

Scope of MSSP (Managed SOC Service Provider)

Sr. No.	Endpoints	Logs to be collected
1	**Windows 11/10 (server and desktop)**	- OS / System & Security Event - AV / XDR / EDR / Windows Defender Logs - Network Connection - User Access Audit
2	**Unix (Linux, RHEL, Fedora, Ubuntu etc.,)**	- OS / System & Security Event - AV / XDR / EDR / Windows Defender Logs - Network Connection - User Access Audit
3	**Web server**	- Access logs - Traffic logs where applicable - IIS / Apache
4	**Database Server (As applicable)**	- DB Audit logs - DB Access logs
5	**Firewall(s)**	- Audit Logs - Access Logs - NetFlow - Traffic Logs
6	**Proxy (web/email)**	- Audit Logs - Access Logs - Traffic Logs
7	**DHCP**	- DHCP logs where applicable
8	**DNS**	- DNS logs where applicable
9	**Active Directory**	- AD logs
10	**Auth**	- Authentication logs
11	**Cloud**	- CloudWatch, CloudTrail, Guardduty - M365, Azure, EntraID, Defender

Ticket/Case Management Workflow

🟦 MSOC 🟩 RE 🟧 EXCHANGE



Alert Received From Next-Gen SIEM

Critical

YES

Triage & Confirm alert as an Critical Incident

YES

Send Notification to RE SPOC

Send Notification to Exchange

Send Notification to CERT-IN/NCIIPC

Track Incident status

RE to take action & submit RCA to Exchange & MSOC on Incident Resolution

MSOC validates resolution and closes the ticket

NO

High

YES

Triage & Confirm alert as an High Incident

YES

Send Notification to RE SPOC

Send Notification to Exchange

Track Incident status

RE to take action & submit RCA to Exchange & MSOC on Incident Resolution

MSOC validates resolution and closes the ticket

END

NO

Medium / Low

YES

Triage & Confirm alert as an Medium/Low Incident

YES

Send Notification to RE SPOC

Track Incident status

RE to take action and update on Incident Resolution

MSOC validates resolution and closes the ticket

Onboarding Overview Video

- M-SOC Self Service Onboarding Training Video Playlist
  - M-SOC Self Service Onboarding
  - M-SOC Contract Signing
  - M-SOC Billing Update
  - M-SOC Escalation Matrix
  - M-SOC Users & Roles
- M-SOC Frequently Asked Questions (FAQ)

Self Service Onboarding – Documentation Link

Self Service Onboarding – Documentation Link

msoc@blusapphire.com
msoc@bsetech.in

MSOC Support numbers
+91 81210 03126
+91 81210 03127

BSE
The Power of Vibrance

BLUSAPPHIRE
ENTERPRISE SECURITY SIMPLIFIED

Thank You

for joining us!

msoc@blusapphire.com
msoc@bsetech.in

MSOC Support numbers
+91 81210 03126
+91 81210 03127

Your presence and insights have made this a meaningful discussion

Self Service Onboarding – Documentation Link