JS Global IT Consultancy Services

www.jaishglobal.in

SERVICE CATALOGUE

SECURITY OPERATIONS CENTER

"Securing You Digitally with Expertise and Innovation."

Phone Number
+91-920-576-0111

Email Address
info@Jaishglobal.in

WELCOME TO JS GLOBAL

JS Global IT Consultancy Services is an ISO-certified and NSIC approved organization renowned for its extensive range of services and solutions in the realm of cybersecurity consulting.

Additionally, the company is committed to enhancing cybersecurity awareness through various educational programs and initiatives, ensuring clients stay informed and protected against emerging threats.

COMPANY’S VALUES

Commitment to Excellence

We strive for the highest standards of quality and precision in all our cybersecurity solutions, ensuring robust protection for our clients.

Client-Centric Focus

Our clients' security needs are at the forefront of our mission, and we tailor our services to provide bespoke, comprehensive protection.

Integrity and Transparency

We uphold the principles of honesty and openness in all our operations, ensuring our clients are well-informed and confident in our services.

Innovation and Adaptability

We continuously innovate and adapt our technologies to stay ahead of emerging threats, providing cutting-edge security solutions.

WHY YOUR BUSINESS NEEDS A SOC?

A company needs a SOC to ensure continuous, real-time monitoring and response to cyber threats, safeguard critical data, maintain regulatory compliance, and mitigate risks, thereby protecting its assets and maintaining operational integrity.

Enhanced Threat Detection and Response

Continuous Monitoring and Protection

Incident Management and Mitigation

Regulatory Compliance and Audit Readiness

Proactive Risk Management

OUR SERVICES

1

Manage Detection & Respond

Utilizing advanced solutions, our experts quickly identify and mitigate security incidents, ensuring your organization remains protected 24/7 * 365.

2

Managed SIEM

Our team of experts manages, monitors, & maintains your SIEM solution, ensuring it operates efficiently and effectively to detect and respond to security events.

3

SIEM Solution

Expert guidance & support throughout the process, from initial planning design to implementation and optimization, helping you build a robust and effective SOC.

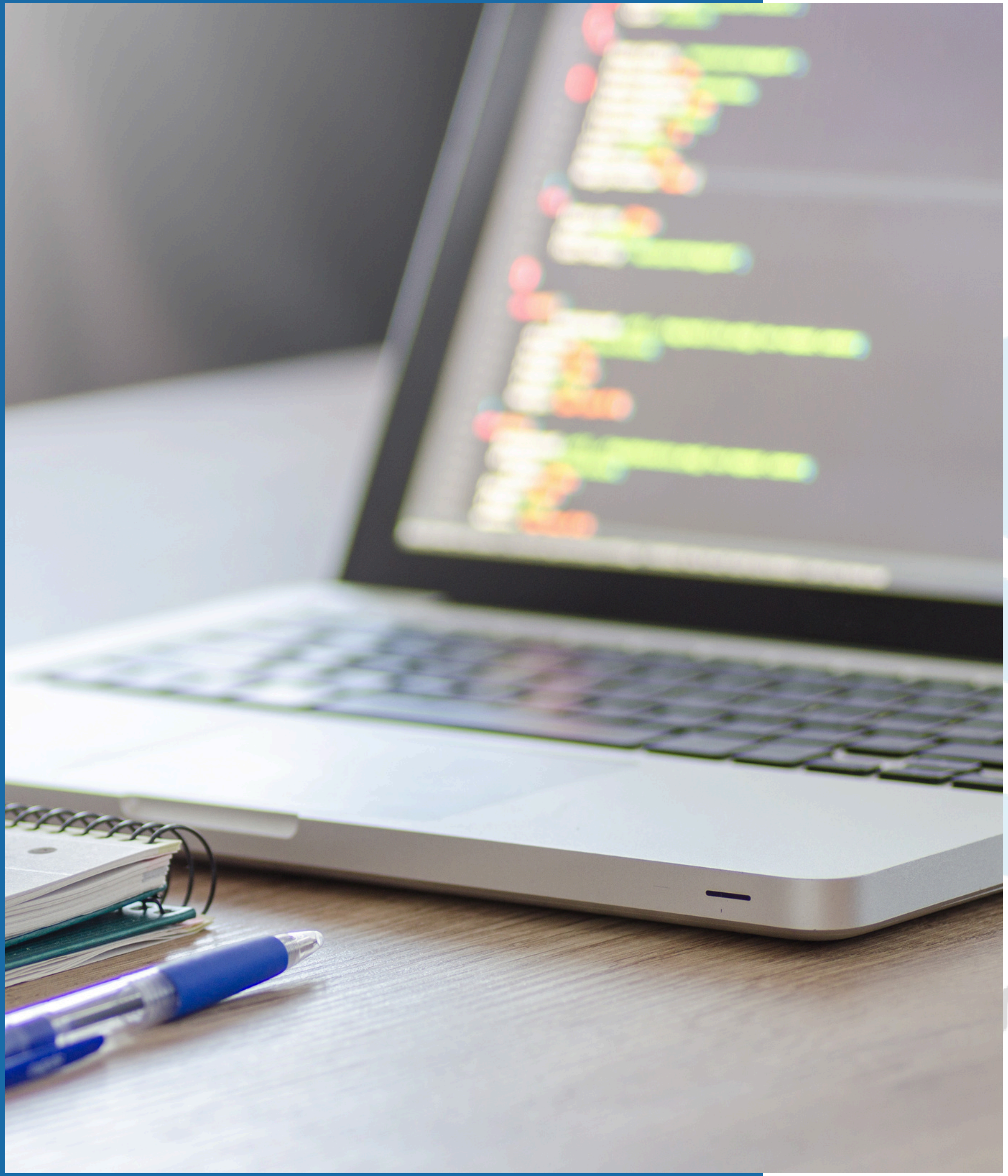
4

Dedicated SOC

We offer industry-leading SIEM solutions tailored to your specific needs, providing comprehensive security event collection, correlation, and analysis capabilities.

OUR MDR & DEDICATED SOC SERVICE INCLUDES:

- 24/7*365 Monitoring
- Incident Response
- Advanced Threat Intelligence
- Audit & Compliance Support
- Threat Hunting
- AI & ML Integration
- Real-Time Reporting
- Awareness Trainings



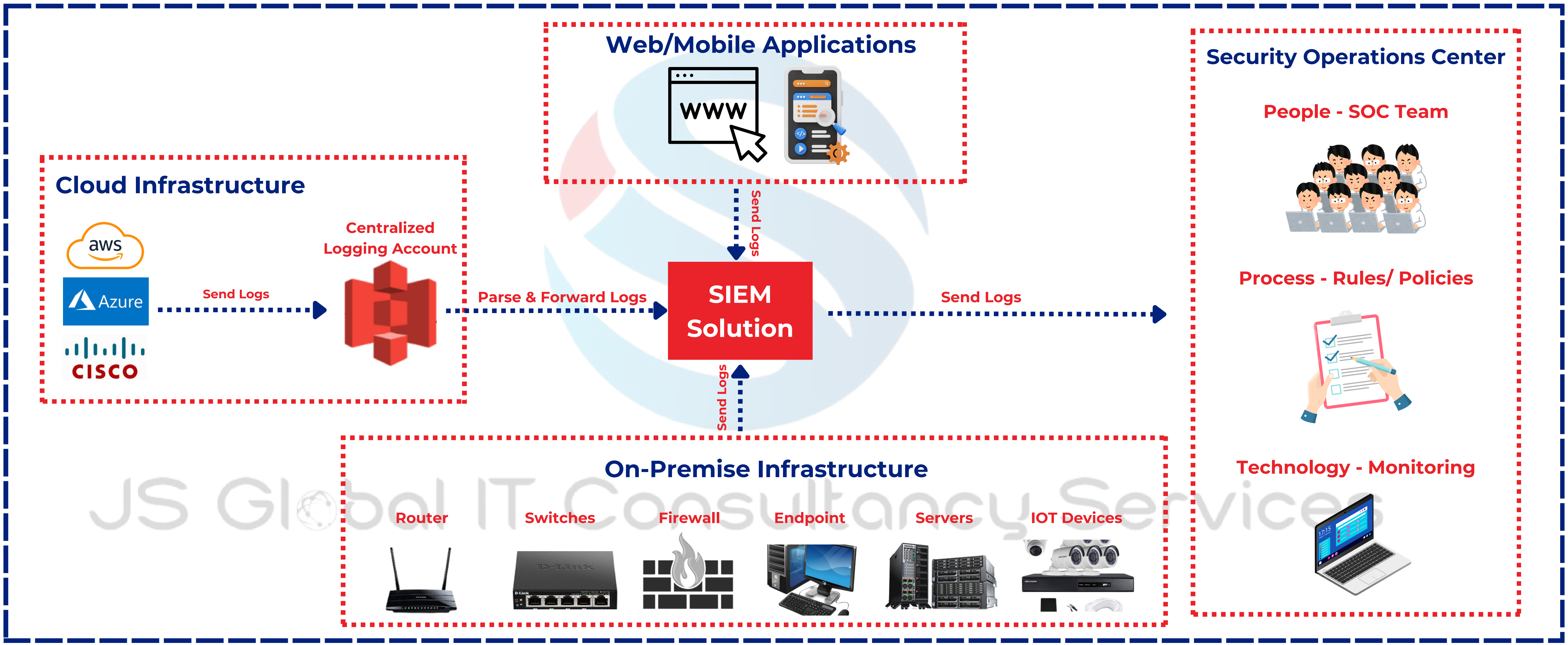
SIEM SOLUTIONS WE OFFER (Not limited to)

We provide industry-leading SIEM solutions that offer comprehensive security event collection, correlation, and analysis, tailored to meet your specific cybersecurity needs.

- **Seceon**
- **Wazuh**
- **Splunk**
- **IBM QRadar**
- **Palo Alto**
- **Manage Engine**
- **Securonix**
- **FortiSIEM**

SOC ARCHITECHTURE

High level diagram of SOC implementation!

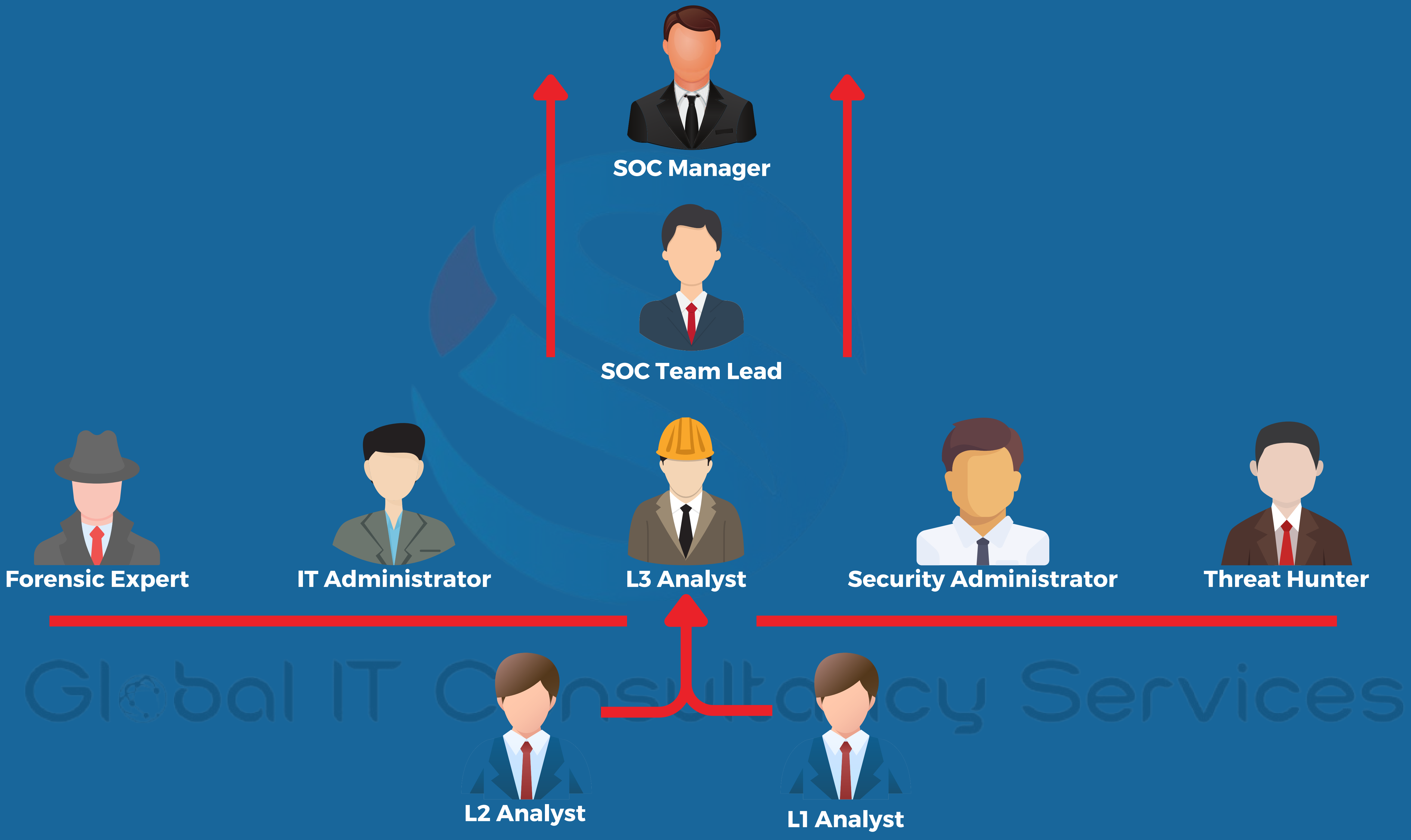


SOC FRAMEWORK

High level plan of SOC framework!

Discovery	Preliminary Investigation	Triage	Essential Investigation	Contain & Respond
External Threat Intelligence	Linking		Full Scoping	Quarantine
Logs, Endpoint Data, etc.: Correlation (via SIEM)	Scoring	Ranking	Visualization	Remediate
Logs, Endpoint Data, etc.: Anomaly Analytics	Merging			Update
Logs, Endpoint Data, etc.: Deception Technologies	Preliminary Scoping		Enrichment	Share (Optional)

OUR SOC TEAM STRUCTURE



OUR DELIVERY MODEL

SOC Manager & Team Lead

SOC Manager

Provides management oversight of the service

Incident Response Service

- Enables rapid investigation of incidents
- Invokes forensic investigation when required
- Effectively contains threat vectors and lateral movements
- Proactively eradicates indicators of compromise
- Facilitates risk-based recovery of business operations

Team Lead

- Acts as an extension of your team
- Primary contact for security, compliance, and general queries

SOC Analysts

Level 1 Analyst:

Monitors and triages alerts to identify potential security incidents.

Level 2 Analyst:

Investigates and analyzes incidents to determine their impact and scope.

Level 3 Analyst/ Threat Hunter:

Proactively hunts for threats and responds to complex security incidents.

OUR INCIDENT CATEGORIZATION

Unauthorized Access

When an individual gains unauthorized access to a client's network, system, application, data, or similar instance without permission.

Compromised Machine

When a corporate asset is compromised by intrusion attempts or access gained through compromised user account credentials.

Phishing

Incidents involving phishing emails in the client's network affecting its employees.

Exercise / Network Defense Testing

Approved exercises such as authorized penetration tests or vulnerability assessments.

Policy Violations or Improper Usage

Policy violations such as the use of corporate IT systems for non-business activities like using Bit Torrent to download movies or copyrighted content, abusing client's IT assets.

Data Theft

Any potential or suspicion of theft or misuse of client data.

Denial of Service (DoS/DDoS)

An attack successfully impairs the normal authorized functionality of networks, systems, or applications by exhausting resources.

Malicious Code or Malware

Successful installation of malicious software, such as viruses, worms, Trojan horses, or malicious entities, that infects an OS or application.

Scans/Probes/Attempted Access

Activities seeking to access or identify a client's computer, open ports, protocols, services, or any combination for a future attack.

Others or Uncategorized

Incidents that do not fall under the above-mentioned categories.

INCIDENT TRIAGE MATRIX

High level plan of SOC framework!

		CONCEQUENCES				
		Non Significant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain	Medium	High	Critical	Critical	Critical
	Likely	Medium	High	High	Critical	Critical
	Possible	Low	Medium	High	High	Critical
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Low	Medium

SERVICE LEVEL DESCRIPTION

Priority	Description
Urgent	Incidents requiring immediate action and attention. Client should respond within hours of receiving the incident notification.
Important	Incidents requiring prompt attention and should be addressed within a few days. If left unattended for a considerable time, these incidents may severely undermine the security of information assets.
Minor	Incidents requiring attention but can be attended to within an acceptable timeframe.

SERVICE LEVEL AGREEMENT

Priority Level	Category	TAT
Critical to High	Event Alert	Within 15 Minutes
Medium	Event Alert	Within 30 Minutes
Critical to High	Initial Response	Within 30 Minutes
Critical	First Response	Within 60 Minutes
Medium	Initial Response	Within 2 Hour
High	First Response	Within 4 Hour
Medium	First Response	Within 12 Hour
Mitigation of Security Events / Threats based on the priority of events		90 to 360 Minutes

Please Note: The color coding is based on the service level description. Kindly refer to the previous slide for the same.

Contact Information

Location :

India - Delhi NCR

MEA - Dubai

Phone :

+91-920-576-0111

Websites :

www.jaishglobal.in

Email:

info@jaishglobal.in

THANK YOU