SISL-IT-POL-Threat Intelligence Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-Threat Intelligence Policy
Abstract	This document describes Threat intelligence at Share India Group
Security Classification	Internal
Location	Share India Group– Delhi

Authorization		
Document Owner	Reviewed by	Authorized by
IT Team	Head – IT	Head – IT

Amendment Log				
Version	**Modification Date DD MMM YYYY**	**Section**	**A/M/D**	**Brief description of change**
1.0	30th October 2025	Initial Version	A	Final

Distribution list
Designated Officer (DO)
Information Security Steering Committee (ISSC)
ISMS Core Team
Auditors (Internal & External)
All users at Share India Group

Table of Content

1 Introduction

The term threat intelligence covers the need for Share India Securities Limited (SISL) to collect, analyze and produce threat intelligence relating to information security threats.

2 Policy Statement

Threat intelligence is the process of gathering, analyzing and contextualizing information about current and future cyberattacks, providing SISL with a deeper understanding of threats.

For example, threat intelligence can be used to identify the tactics, techniques and procedures (TTPs) attackers are using to gain entry into networks or compromise their targets. This can make it easier for SISL to defend against those specific attacks.

In addition to helping SISL understand how they might be targeted by hackers, threat intelligence can also help SISL learn about the types of data attackers are looking for, as well as what they do with that data once it's been stolen.

3 Scope

The policy applies to

- Security incidents that include, but are not limited to viruses, worms, and Trojan horse detection.
- Unauthorized use of computer accounts and computer systems.
- Complaints of improper use of Information Resources as outlined in the acceptable usage policy
- All information assets
- All employees
- All third-party vendors working with SISL assets

4 Roles and Responsibilities

Sr. No.	Role	Responsibility
1.	Designated Officer (DO)	Owns the process
2.	IT HOD	Ensure that this policy is effectively implemented.
3.	IT Team (Infrastructure and Application)	Comply to this policy.

5 Standard and Guidelines

Information about existing or emerging threats shall be collected and analyzed in order to:

- Facilitate informed actions to prevent the threats from causing harm to the SISL
- Reduce the impact of such threats.

5.1 Threat intelligence layers

Threat intelligence can be divided into three layers.

5.1.1 Strategic threat intelligence

Involves exchange of high-level information about the changing threat landscape (e.g. types of attackers or types of attacks). It is high-level intelligence, and it provides insight into cybersecurity also concerning real-life factors such as economic and political climates. Common topics are, for example, trends and patterns in threat actor tactics and targets as well as relevant geopolitical events. It is typically aimed at non-technical audiences, mostly decision makers such as board members. These individuals are responsible for threat response, and it is, therefore, vital for them to know about the business impact of online risks and to comprehend emerging environmental patterns.

5.1.2 Tactical threat intelligence

Involves provision of information about attacker methodologies, tools and technologies involved. It intends to cater to technical audiences who work in system and cybersecurity defense. This intelligence outlines how malicious actors operate (their techniques, tactics, and procedures). It involves tracking internal threat information feeds like network traffic data. Tactical threat intelligence allows security professionals to detect direct attacks on systems or understand prominent attack strategies.

5.1.3 Operational threat intelligence

Details about specific attacks, including technical indicators. It refers to technical data about the tools and infrastructure threat actors deploy. Typical examples include subject lines or email content from phishing campaigns or maliciously registered URLs. So, if threat actors use business emails as a way into an organization (tactical info), the actual email subject lines used would qualify as technical Threat Intelligence. It also indicates to cybersecurity teams how an unauthorized user executes a particular cyberattack. Using external sources, such as dark web forums, it gathers information directly from threat actors to piece together details such as timing, motives, and specific techniques.

SISL shall consider all three layers for action:

5.2 Threat intelligence enablers

- Relevant (i.e. related to the protection of the organization);

- Insightful (i.e. providing the organization with an accurate and detailed understanding of the threat landscape);
- Contextual, to provide situational awareness (i.e. adding context to the information based on the time of events, where they occur, previous experiences and prevalence in similar organizations);

5.3 Actionable

SISL shall act on information quickly and effectively.

5.3.1 Threat intelligence activities

SISL shall consider the following activities to safeguard its information systems:

- Establishing objectives for threat intelligence production
- Identifying, vetting and selecting internal and external information sources that are necessary and appropriate to provide information required for the production of threat intelligence.
- Collecting information from selected sources, which can be internal and external.
- Processing information collected to prepare it for analysis (e.g. by translating, formatting or corroborating information) in line with incident management.
- Analyzing information to understand how it relates and is meaningful to the organization
- Communicating and sharing it to relevant individuals / interested parties in a format that can be understood.

5.4 Analysis

Threats shall be analyzed and later used by SISL as follows:

- Implementing processes shall include information gathered from threat intelligence sources into SISL's information security risk management processes.
- Serve as an additional input to technical preventive and detective controls like firewalls, intrusion detection system, or anti malware solutions.
- Provide input to the information security test processes and techniques.

5.5 Continuous Improvement

SISL shall share threat intelligence with relevant interested parties on a mutual basis in order to improve overall threat intelligence.

The lessons learnt from threat intelligence can be used for:

- For user awareness training
- For improving the policies and procedures

5.6 Tooling and Automation

To improve the efficiency, scalability, and reliability of threat intelligence processing and integration, SISL shall adopt appropriate security tools and automation platforms. These include:

5.6.1 Threat Intelligence Platform (TIP)

- SISL may integrate a Threat Intelligence Platform to aggregate feeds from multiple sources (e.g., CERT-In, CSIRT-Fin, ISACs, commercial providers).
- TIP shall enable correlation, normalization, and prioritization of threat indicators (IOCs, TTPs).

5.6.2 Security Information and Event Management (SIEM)

- The SIEM system shall be configured to:
  - Ingest threat intelligence feeds (IPs, domains, file hashes, etc.)
  - Trigger alerts for matches found in system logs or network activity.
  - Support real-time detection based on updated threat indicators.

5.6.3 Integration with SOC/SOAR

- SISL's Security Operations Centre (SOC) shall use the threat intel feeds for event correlation and incident triage.
- If applicable, integration with a Security Orchestration, Automation and Response (SOAR) system shall be used to:
  - Automate blocking of IOCs at the firewall or endpoint level.
  - Trigger playbooks based on threat intel (e.g., for phishing or ransomware indicators).

5.6.4 Threat Feed Sources

SISL shall consider the following internal and external sources for automated ingestion:

- CERT-In Advisories
- CSIRT-Fin Circulars
- National Critical Information Infrastructure Protection Centre (NCIIPC) alerts
- Industry-specific ISACs (e.g., BFSI-ISAC)
- Reputed open source threat feeds (Abuse.ch, AlienVault OTX)
- Commercial threat intel providers (optional)

5.6.5 Review and Testing

- All automation scripts, connectors, and enrichment rules shall be tested before production deployment.
- The effectiveness of automated detection and response mechanisms shall be reviewed annually by the DO/ISM.

6 Reference

Ref: - SISL-IT-PRO-Threat Intel and Incident Management Procedure

7 Policy Review Frequency

The policy shall be reviewed annually or when there is a major change within Share India Securities Limited environment.

8 Policy Exception

In case of any deviation against policy guidelines, Risk Acceptance form should be submitted to Designated Officer for approval.

9 Policy Violation Reporting Matrix

Any violation to the policy should be reported to Reporting Manager/Designated Officer

Level	**Designation**
Level 1	Employee's Reporting Manager
Level 2	Designated Officer
Level 3	MD & CEO