TRIANZ℠

Threat Intelligence Procedure

TRIANZ INTERNAL

trianz.com

Statement of Confidentiality

The information contained in this document is internal to Trianz. It shall not be disclosed, duplicated, or used for any purpose other than that stated herein, in whole or in part, without the express written consent of Trianz.

Information Classification

☐	Public
☒	Internal
☐	Confidential
☐	Restricted

Table of Contents

1. Introduction

- Threat Intelligence is a discipline of obtaining and analyzing information about those who would do us harm in cyber space to understand how to make our defenses as effective as possible.
- Threat Intelligence (TI) is crucial for Trianz to proactively identify, assess, and mitigate cybersecurity risks. By systematically collecting, analyzing, and reporting intelligence, Trianz can detect emerging threats, including those from global adversaries.

2. Objectives

- Proactive Threat Identification – Continuously gather intelligence to detect and analyze potential cyber threats before they impact the organization.
- Risk Assessment & Prioritization – Evaluate the severity and relevance of identified threats to prioritize response efforts based on risk levels.
- Incident Response & Mitigation – Provide actionable intelligence to enhance incident response, containment, and mitigation efforts.
- Continuous Monitoring & Reporting – Regularly monitor the threat landscape and generate reports to keep stakeholders informed about emerging risks.
- Regulatory Compliance & Governance – Align the TI process with regulatory requirements and industry best practices to ensure compliance.

3. Scope

This Control applies to all systems, people and processes that constitute the organization's information systems, including board members , directors , employees, suppliers, and other 3rd party who has access to Trianz systems.

4. Entry Criteria

- Access to reliable threat intelligence sources.

- Established tools and platforms for collecting and analysing intelligence.
- Trained personnel with defined roles and responsibilities.

5. Inputs

- **Internal sources:** Logs, incident reports, and security events.
- **External sources:** OSINT (Open-Source Intelligence), commercial threat intelligence feeds, regulatory bodies, and industry ISACs.
- **Technical sources:** Indicators of compromise (IoCs) such as Unusual outbound traffic, abnormal DNS requests, Phishing email patterns, suspicious attachments, domains associated with cyber threats etc., malware analysis reports, vulnerability databases, and dark web monitoring.

6. Process Description (Procedure)

In Accordance with our policy Threat intelligence is gathered and reported at three levels.

1. **Strategic:**

   Focused on the collection and analysis of high-level information regarding groups of attackers, their motivation, typical targets, types of attack and current levels of activity.

2. **Tactical:**
   Concerned with specific attackers or types of attackers and the tactics, techniques, and procedures (TTPs) that they are currently using to gain access to systems or otherwise pose a threat to our organization.

3. **Operational:**
   Relating to specific and potentially ongoing attacks, including IOC's which may allow us to identify cases where we have suffered a breach.

This process is intended to be used in its basic form and below are the steps.

4. **Direction/Planning:**

It is important that clear objectives are defined for threat intelligence in general and for the specific topics for which information is to be collected and analyzed. These objectives should consider the context of the organization, in terms of our industry, locations, technology and interested parties.

Collection:
Threat intelligence is gathered from various sources, including:

- **Internal sources:** Logs, incident reports, and security events.
- **External sources:** OSINT (Open-Source Intelligence) such as Shodan, Maltego, the MITRE ATT&CK framework, and Open Threat Exchange (OTX), commercial threat intelligence feeds, regulatory bodies, and industry ISACs.
- **Technical sources:** Indicators of compromise (IoCs), malware analysis reports, vulnerability databases, and dark web monitoring.

The information must be stored appropriately, and its source clearly recorded for future reference.

5. **Processing and Analysis**
   - Collected intelligence is filtered, correlated, and validated for relevance.
   - Threats are categorized based on their severity, impact, and likelihood.
   - Analysis tools such as SIEM (Security Information and Event Management) and TIP (Threat Intelligence Platforms) are used to enrich intelligence data.
6. **Dissemination and Reporting**
   - Threat intelligence reports are shared with relevant stakeholders.
   - Critical threats are escalated immediately to the Incident Response Team.
   - Regular briefings and updates are provided to senior management.
7. **Response and Mitigation**

- Security teams apply threat intelligence to improve monitoring, detection, and response.
- Action plans are developed to mitigate risks associated with identified threats.
- Changes to security controls, patches, or policies are implemented as necessary.

8. **Continuous Improvement**
   - The effectiveness of the threat intelligence process is reviewed periodically.
   - Lessons learned from incidents and threat trends are incorporated into the TI process.
   - New intelligence sources and analytical tools are evaluated for potential integration.

7. Exit Criteria and Output

- Intelligence has been analyzed and disseminated.
- Relevant security controls have been implemented or updated.
- Reports have been provided to stakeholders, and mitigation actions have been taken.

8. Roles and Responsibilities

Roles	Responsibilities	Internal/External
IS Operations Team	• Collects and analyses intelligence from internal and external sources. • Monitors threat intelligence platforms, security feeds, and regulatory advisories. • Reports relevant threats to stakeholders and recommends mitigation strategies.	Internal

	• Utilizes threat intelligence to enhance incident detection and response. • Coordinates with other teams to remediate and mitigate identified threats. • Implements security controls based on intelligence findings. • Assists in closing vulnerabilities associated with identified threats. •	
InfoSec & Data privacy assurance Team	• Ensures that threat intelligence activities align with business and security objectives. • Provides necessary resources and approves threat intelligence policies.	Internal

9. ISO Control Mapping(s)

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Organizational Control	5.7 Threat intelligence Control Information relating to information security threats shall be collected and analyzed to produce threat intelligence.	Threat Intelligence Procedure

Document Control

Owner:	CISO	**Release ID:**	THR_PROC_0171

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	2/1/2024	Aishee	Balu/Vijaya	Shrikant	New Document	Mapped to New ISO 27001 2022 control 5.7
1.0	23-Feb-24	Aishee	Balu/Vijaya	Shrikant	For Approval	Approved and Baselined
1.1	06-Mar-25	Krutideepta Barik	Vijaya R, Beniyel S, Balu Nair		For Yearly Review	All Sections have been Modified. Migrated to a new Template.
2.0	14-May-25	Krutideepta Barik	Vijaya R, Beniyel S, Balu Nair	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com

The content in this document is copyrighted; any unauthorized use – in part or full – may violate the copyright, trademark, and other laws. This document may not be modified, reproduced, or publicly displayed, performed, or distributed, or used for any public or commercial purposes. The Trianz name and its products are subject to trademark and copyright protections, regardless of how and where referenced.