TrustIoT Framework for Industry 4.0

"Real-time threat intelligence integration and automated reporting"

|  |  |
| --- | --- |
| Document Classification: | Internal |
| Document Ref. | *TrustIoT Framework for Industry 4.0* |
| Version: | *1* |
| Document Author: | *Jibran Saleem* |
| Document Owner: |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Revision Author** | **Summary of Changes** |
|  |  |  |  |
|  |  |  |  |

**Distribution**

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |

**Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

Table of Contents

[1. Introduction 4](#_Toc176333598)

[2. Purpose 4](#_Toc176333599)

[3. Scope 4](#_Toc176333600)

[4. Policy Statement 4](#_Toc176333601)

[4.1. Threat Intelligence Integration 4](#_Toc176333602)

[4.2. Real-time Monitoring and Analysis 4](#_Toc176333603)

[4.3. Automated Reporting 4](#_Toc176333604)

[4.4. Incident Response Integration 5](#_Toc176333605)

[5. Responsibilities 5](#_Toc176333606)

[6. Breaches of Policy 5](#_Toc176333607)

[7. Document Management 5](#_Toc176333608)

# Introduction

The dynamic and evolving nature of cyber threats necessitates a proactive and adaptive approach to security. Real-time threat intelligence provides up-to-date information on emerging threats, vulnerabilities, and attack patterns, enabling organisations to identify and respond to potential risks more effectively. Integrating this intelligence into the IoT ecosystem and automating reporting processes enhances the organisation's ability to detect, analyse, and mitigate security incidents in a timely manner.

# Purpose

The purpose of this policy is to establish guidelines and requirements for integrating real-time threat intelligence into the organisation's IoT security infrastructure and automating the reporting of security events and incidents. This policy aims to:

* Enhance the organisation's ability to detect and respond to emerging threats in real-time.
* Proactively identify and mitigate risks to IoT devices and systems.
* Streamline the reporting and communication of security events and incidents.
* Facilitate informed decision-making and incident response through automated reporting.

# Scope

This policy applies to all IoT devices, systems, and security solutions within the organisation's network.

# Policy Statement

## Threat Intelligence Integration

* **Threat Intelligence Sources:** Reputable and relevant threat intelligence feeds shall be identified and integrated into the organisation's security infrastructure.
* **Data Correlation:** Threat intelligence data shall be correlated with logs and events from IoT devices, network security tools, and other security solutions to identify potential threats and indicators of compromise.
* **Real-time Updates:** Threat intelligence feeds shall be updated in real-time to ensure that the organisation has access to the latest information on emerging threats.

## Real-time Monitoring and Analysis

* **Security Information and Event Management (SIEM):** A SIEM system or equivalent solution shall be utilised to collect, aggregate, and analyse security events and logs from various sources, including IoT devices, network infrastructure, and threat intelligence feeds.
* **Anomaly Detection:** Behavioural analytics and machine learning techniques shall be employed to identify deviations from normal patterns that may indicate security incidents or malicious activity.
* **Correlation Rules:** Correlation rules shall be defined and implemented within the SIEM to identify patterns and relationships between events that may indicate a potential threat.

## Automated Reporting

* **Incident Reports:** Security incidents detected through real-time monitoring and analysis shall trigger the automatic generation of incident reports, containing relevant details such as:
  + Date and time of the incident
  + Affected devices or systems
  + Description of the incident and observed indicators of compromise
  + Severity and potential impact assessment
* **Regular Reports:** Automated reports on security trends, vulnerabilities, and threat activity shall be generated and distributed to relevant stakeholders on a regular basis.
* **Customisation:** Reporting formats and content shall be customisable to meet the specific needs of different stakeholders and departments.

## Incident Response Integration

* **Incident Creation:** Detected security incidents shall automatically trigger the creation of incidents in the organisation's incident management system.
* **Workflow Automation:** Automated workflows shall be implemented to streamline incident response processes, including notification, escalation, and assignment of tasks to relevant personnel.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **Security Operations Centre (SOC):** Responsible for monitoring security events, analysing threats, and coordinating incident response.
* **IT Department:** Responsible for integrating threat intelligence feeds, configuring SIEM correlation rules, and setting up automated reporting mechanisms.

# Breaches of Policy

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contractual relationships.

# Document Management

This document is valid as of [dd/mm/yyyy].

This document is reviewed periodically and at least annually to ensure compliance with the following prescribed criteria.

* Compliant with the Internet of Things (IoT) Security Framework for Industry 4.0.
* Legislative requirements defined by law, where appropriate.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Name 1]

Manager