TrustIoT Framework for Industry 4.0

"Dynamic network segmentation based on real-time threat assessment"

|  |  |
| --- | --- |
| 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](#_Toc176333091)

[2. Purpose 4](#_Toc176333092)

[3. Scope 4](#_Toc176333093)

[4. Policy Statement 4](#_Toc176333094)

[4.1. Real-Time Threat Assessment 4](#_Toc176333095)

[4.2. Dynamic Segmentation 4](#_Toc176333096)

[4.3. Access Control and Isolation 5](#_Toc176333097)

[4.4. Monitoring and Logging 5](#_Toc176333098)

[5. Responsibilities 5](#_Toc176333099)

[6. Breaches of Policy 5](#_Toc176333100)

[7. Document Management 5](#_Toc176333101)

# Introduction

The dynamic and evolving nature of cyber threats, coupled with the proliferation of Internet of Things (IoT) devices, necessitates a more adaptive and proactive approach to network security. Traditional static network segmentation, while providing a baseline level of protection, may not be sufficient to address the rapidly changing threat landscape. Dynamic network segmentation, based on real-time threat assessment, enables the network to respond and adapt to potential threats by automatically isolating compromised or suspicious devices and systems, thereby limiting the lateral movement of attacks and minimising their impact.

# Purpose

The purpose of this policy is to establish guidelines and requirements for implementing dynamic network segmentation based on real-time threat assessment within the organisation's IoT infrastructure. This policy aims to:

* Enhance the security and resilience of the IoT network by dynamically adapting to evolving threats.
* Proactively isolate compromised or suspicious devices and systems to prevent the spread of malware and lateral movement of attacks.
* Minimise the impact of security breaches by containing them within isolated network segments.
* Enable rapid response and remediation of security incidents.

# Scope

This policy applies to all IoT devices and systems connected to the organisation's network, regardless of their function or manufacturer. This includes, but is not limited to:

* Sensors, actuators, and controllers
* Gateways and edge devices
* Industrial control systems (ICS)
* Wearable and embedded devices

# Policy Statement

## Real-Time Threat Assessment

* **Threat Intelligence:** Real-time threat intelligence feeds shall be integrated into the network security infrastructure to provide up-to-date information on emerging threats, vulnerabilities, and indicators of compromise (IOCs).
* **Behavioural Analytics:** User and entity behaviour analytics (UEBA) shall be employed to establish baseline patterns of normal activity and identify deviations that may indicate malicious intent or compromised devices.
* **Anomaly Detection:** Network traffic and device behaviour shall be continuously monitored for anomalies that may signify potential threats or security breaches.

## Dynamic Segmentation

* **Automated Segmentation:** Based on real-time threat assessment, network segmentation shall be dynamically adjusted to isolate compromised or suspicious devices and systems.
* **Policy-Based Segmentation:** Segmentation decisions shall be based on predefined policies that consider factors such as threat severity, device criticality, and data sensitivity.
* **Adaptive Response:** The network segmentation architecture shall be capable of adapting to changing threat conditions and evolving attack patterns.

## Access Control and Isolation

* **Micro-segmentation:** Micro-segmentation techniques may be employed to create highly granular network segments, isolating individual devices or groups of devices as needed.
* **Access Control Lists (ACLs):** ACLs or firewall rules shall be dynamically updated to enforce isolation and restrict communication between compromised or suspicious segments and the rest of the network.
* **Quarantine:** Compromised or suspicious devices shall be quarantined in isolated network segments to prevent further spread of malware or lateral movement.

## Monitoring and Logging

* **Comprehensive Logging:** All security events, including threat detections, segmentation changes, and access control actions, shall be logged in a centralised and secure manner.
* **Real-time Monitoring:** Network traffic and device behaviour shall be continuously monitored to detect potential threats and security incidents.
* **Alerting:** Automated alerts shall be generated for suspicious activity or policy violations, triggering timely investigation and response.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **Network Administrators:** Responsible for configuring and managing the network infrastructure to support dynamic segmentation.
* **Security Operations Centre (SOC):** Responsible for monitoring security events, analysing threats, and responding to incidents.
* **Incident Response Team:** Responsible for investigating and containing security breaches, including isolating compromised devices and segments.

# 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