TrustIoT Framework for Industry 4.0

" Integration of endpoint protection with network-wide security monitoring"

|  |  |
| --- | --- |
| 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](#_Toc190894757)

[2. Purpose 4](#_Toc190894758)

[3. Scope 4](#_Toc190894759)

[4. Policy Statement 4](#_Toc190894760)

[4.1. Centralised Management and Monitoring 4](#_Toc190894761)

[4.2. Real-time Threat Intelligence Sharing 4](#_Toc190894762)

[4.3. Correlation and Analysis 4](#_Toc190894763)

[4.4. Automated Response and Remediation 5](#_Toc190894764)

[5. Responsibilities 5](#_Toc190894765)

[6. Breaches of Policy 5](#_Toc190894766)

[7. Document Management 5](#_Toc190894767)

# Introduction

In today's interconnected digital landscape, the security of endpoints, including IoT devices, is paramount. Endpoint protection solutions play a crucial role in safeguarding these devices from malware, unauthorized access, and other threats. However, the effectiveness of endpoint protection can be significantly enhanced by integrating it with network-wide security monitoring. This synergy allows for a more comprehensive and proactive approach to threat detection and response, enabling the organisation to identify and mitigate risks more effectively.

# Purpose

The purpose of this policy is to establish guidelines and procedures for integrating endpoint protection mechanisms with network-wide security monitoring systems. This integration aims to:

* Provide a holistic view of security events across the network and endpoints.
* Enable correlation of endpoint and network events to identify sophisticated attacks.
* Facilitate automated response and remediation actions to contain and mitigate threats.
* Enhance the overall security posture of the organisation's IT infrastructure.

# Scope

This policy applies to all endpoint protection solutions and network-wide security monitoring systems deployed within the organisation. This includes, but is not limited to:

* Anti-malware and antivirus software
* Endpoint detection and response (EDR) solutions
* Intrusion detection and prevention systems (IDPS)
* Security information and event management (SIEM) systems
* Network traffic analysis (NTA) tools

# Policy Statement

## Centralised Management and Monitoring

* **Integration Platform:** A centralised platform or solution shall be implemented to integrate endpoint protection and network-wide security monitoring systems, enabling unified management and visibility.
* **Real-time Data Collection:** Endpoint security events and network logs shall be collected in real-time and forwarded to the centralised platform for analysis.
* **Dashboard and Reporting:** A comprehensive dashboard and reporting capabilities shall be provided to visualise and analyse security events across endpoints and the network.

## Real-time Threat Intelligence Sharing

* **Threat Intelligence Feeds:** Threat intelligence feeds from reputable sources shall be integrated into the centralised platform to provide up-to-date information on emerging threats and vulnerabilities.
* **Endpoint and Network Correlation:** Threat intelligence shall be correlated with endpoint and network events to identify potential attacks and indicators of compromise.

## Correlation and Analysis

* **Event Correlation:** Events from endpoint protection and network security monitoring systems shall be correlated to identify patterns, anomalies, and potential threats.
* **Behavioural Analytics:** User and entity behaviour analytics (UEBA) shall be employed to detect deviations from normal activity that may indicate malicious intent.
* **Machine Learning:** Machine learning algorithms may be utilised to enhance threat detection and reduce false positives.

## Automated Response and Remediation

* **Automated Actions:** Predefined automated actions shall be triggered in response to specific security events or threat indicators, such as:
  + Isolating infected endpoints
  + Blocking malicious traffic
  + Quarantining suspicious files
* **Incident Response Integration:** The centralised platform shall be integrated with incident response workflows to facilitate efficient and coordinated response to security incidents.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **IT Department:** Responsible for integrating endpoint protection and network-wide security monitoring systems, configuring automated response actions, and managing the centralised platform.
* **Security Operations Centre (SOC):** Responsible for monitoring security events, analysing threats, and responding to incidents.

# 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