TrustIoT Framework for Industry 4.0

"IDS/IPS Deployment: Real-time threat detection and response"

|  |  |
| --- | --- |
| 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](#_Toc176333210)

[2. Purpose 4](#_Toc176333211)

[3. Scope 4](#_Toc176333212)

[4. Policy Statement 4](#_Toc176333213)

[4.1. Deployment Strategy 4](#_Toc176333214)

[4.2. Configuration and Tuning 4](#_Toc176333215)

[4.3. Incident Response 4](#_Toc176333216)

[5. Responsibilities 5](#_Toc176333217)

[6. Breaches of Policy 5](#_Toc176333218)

[7. Document Management 5](#_Toc176333219)

# Introduction

The proliferation of Internet of Things (IoT) devices has significantly expanded the attack surface of organisational networks. These devices, often with diverse functionalities and varying levels of security maturity, can be exploited to gain unauthorised access, propagate malware, or disrupt critical operations. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) play a crucial role in safeguarding the network and its connected devices by detecting and preventing malicious activity in real-time.

# Purpose

The purpose of this policy is to establish guidelines and requirements for the deployment, configuration, and management of IDS/IPS within the organisation's IoT infrastructure. This policy aims to:

* Detect and alert on suspicious or malicious activity targeting IoT devices and networks.
* Prevent unauthorised access and exploitation of vulnerabilities.
* Enable rapid response and mitigation of security incidents.
* Ensure the confidentiality, integrity, and availability of data and systems connected to the IoT network.

# Scope

This policy applies to all IDS/IPS deployed within the organisation's network, including those specifically dedicated to protecting IoT devices and segments.

# Policy Statement

## Deployment Strategy

* **Network-based IDS/IPS:** Network-based IDS/IPS shall be strategically deployed at key points in the network, such as the perimeter, between network segments, and in front of critical IoT systems, to monitor and analyse network traffic for signs of malicious activity.
* **Host-based IDS/IPS:** Where appropriate, host-based IDS/IPS may be installed on critical IoT devices or servers to detect and prevent intrusions at the endpoint level.
* **Hybrid Deployment:** A combination of network-based and host-based IDS/IPS may be employed to provide comprehensive protection across the IoT infrastructure.

## Configuration and Tuning

* **Signature and Rule Management:** IDS/IPS shall be configured with appropriate signatures, rules, and policies to detect known attack patterns, vulnerabilities, and suspicious behaviour.
* **Regular Updates:** Signatures and rules shall be regularly updated to address new threats and vulnerabilities.
* **Tuning:** IDS/IPS shall be tuned to minimise false positives and negatives, ensuring accurate and actionable alerts.

## Incident Response

* **Incident Response Plan:** A well-defined incident response plan shall be in place to address security incidents detected by IDS/IPS, including containment, eradication, and recovery procedures.
* **Alert Prioritisation:** Alerts generated by IDS/IPS shall be prioritised based on their severity and potential impact.
* **Timely Response:** Security incidents shall be investigated and responded to in a timely manner to minimise damage and disruption.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **Security Operations Centre (SOC):** Responsible for monitoring IDS/IPS alerts, analysing threats, and coordinating incident response.
* **Network Administrators:** Responsible for deploying, configuring, and maintaining IDS/IPS.

# 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