TrustIoT Framework for Industry 4.0

"Integration of IDS/IPS with automated response systems"

|  |  |
| --- | --- |
| 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](#_Toc176333230)

[2. Purpose 4](#_Toc176333231)

[3. Scope 4](#_Toc176333232)

[4. Policy Statement 4](#_Toc176333233)

[4.1. Real-time Monitoring and Alerting 4](#_Toc176333234)

[4.2. Automated Response Actions 4](#_Toc176333235)

[4.3. Incident Response Integration 4](#_Toc176333236)

[4.4. Continuous Improvement 5](#_Toc176333237)

[5. Responsibilities 5](#_Toc176333238)

[6. Breaches of Policy 5](#_Toc176333239)

[7. Document Management 5](#_Toc176333240)

# Introduction

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are essential components of a robust network security infrastructure. They monitor network traffic and/or system activity to identify and potentially block suspicious or malicious behaviour. However, the effectiveness of these systems can be significantly enhanced by integrating them with automated response mechanisms. This integration enables swift and decisive action to be taken in response to detected threats, minimising the impact of security incidents.

# Purpose

The purpose of this policy is to establish guidelines and requirements for the integration of IDS/IPS with automated response systems within the organisation's network. This policy aims to:

* Enable rapid and effective response to security threats detected by IDS/IPS.
* Reduce the reliance on manual intervention for incident response, improving efficiency and minimising potential damage.
* Contain and mitigate the impact of security breaches by automating containment and remediation actions.
* Enhance the overall security posture of the organisation's IT infrastructure.

# Scope

This policy applies to all IDS/IPS deployed within the organisation's network, as well as the automated response systems integrated with them.

# Policy Statement

## Real-time Monitoring and Alerting

* **Event Collection:** IDS/IPS shall be configured to generate real-time alerts for detected security events, including intrusion attempts, policy violations, and suspicious activity.
* **Alert Correlation:** Alerts from multiple IDS/IPS sensors shall be correlated to identify patterns and potential attacks.
* **Notification:** Security alerts shall be promptly communicated to the Security Operations Centre (SOC) or designated personnel for further investigation and response.

## Automated Response Actions

* **Predefined Actions:** A set of predefined automated response actions shall be established, triggered by specific security events or threat indicators. These actions may include:
  + Blocking malicious IP addresses or traffic patterns
  + Isolating compromised or suspicious devices or network segments
  + Terminating malicious processes or connections
  + Triggering data backup or recovery procedures
* **Severity-Based Response:** The type and intensity of automated response actions shall be commensurate with the severity and potential impact of the detected threat.
* **Human-in-the-Loop:** Critical or high-impact automated actions may require human approval before execution.

## Incident Response Integration

* **Seamless Integration:** IDS/IPS and automated response systems shall be seamlessly integrated with the organisation's incident response processes and workflows.
* **Incident Creation:** Security alerts that require further investigation or response shall automatically trigger the creation of incidents in the incident management system.
* **Information Enrichment:** Relevant information from IDS/IPS and automated response systems shall be included in incident records to facilitate investigation and analysis.

## Continuous Improvement

* **Regular Reviews:** Automated response actions and associated policies shall be periodically reviewed and updated to ensure their continued effectiveness and alignment with evolving threats and security requirements.
* **Lessons Learned:** Post-incident analysis shall be conducted to identify areas for improvement in automated response capabilities and incident response procedures.

# Responsibilities

* **Information Security Officer:** Responsible for overseeing the implementation and enforcement of this policy.
* **Security Operations Centre (SOC):** Responsible for monitoring security alerts, analysing threats, and coordinating incident response.
* **Network Administrators:** Responsible for configuring and managing IDS/IPS and automated response systems.
* **Incident Response Team:** Responsible for investigating and responding to security incidents, including those triggered by automated response actions.

# 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