|  |
| --- |
| SQ1 Security & Technology |
| WAZUH-MISP Integration Documentation |
| Mohamedshahrukh.s@sq1.security |

|  |
| --- |
| Mohamed Shahrukh  6-19-2025 |

# Table of Contents

## Introduction

## Objectives

## Architecture Overview

## Prerequisites

## Wazuh installation

## MISP Installation

## Wazuh Configuration

## References

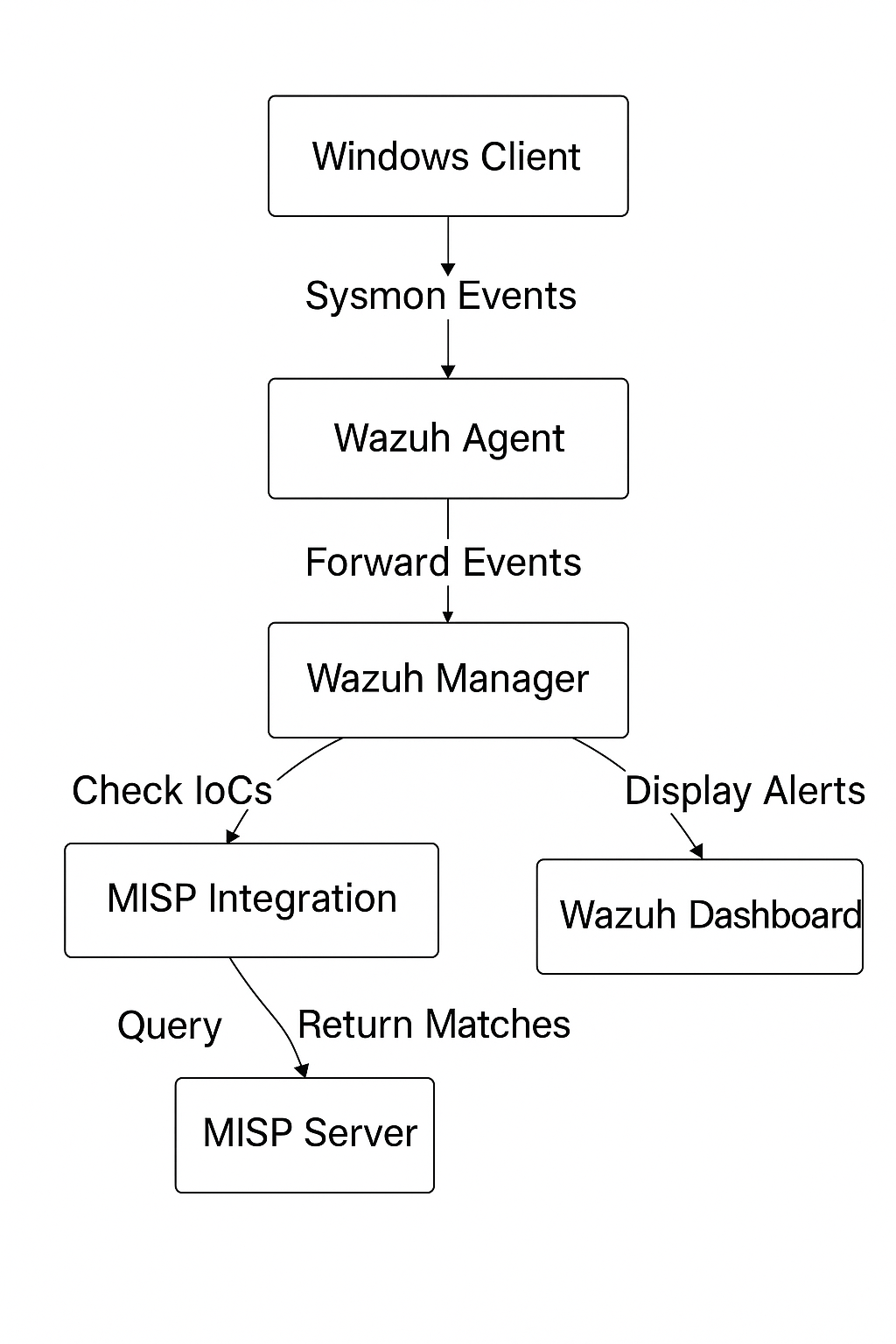
## Introduction

This document provides step-by-step instructions to integrate Wazuh (version 4.11) with MISP for real-time IOC enrichment and alerting. This integration enables automated querying of MISP for Indicators of Compromise (IOCs) and generation of enriched alerts in Wazuh.

## Objectives

* Enable Wazuh to automatically enrich alerts with MISP IOCs in real time.
* Reduce false positives by leveraging MISP’s verified IOC repository.
* Log all enrichment actions for audit and forensic review.

## Architecture Overview



## Pre-requisites

Before starting the integration, ensure you have the following:

* Two machines with Ubuntu Server 22.04 installed (for MISP and Wazuh installation)
* VMware or another virtualization platform (if using a VM)
* Basic knowledge of Linux command line.
* Python 3 and pip3 installed (for the integration script).

## Wazuh Installation

Kindly verify the wazuh documentation in the below reference link.  
[Getting started with Wazuh · Wazuh documentation](https://documentation.wazuh.com/4.11/getting-started/index.html)

Install Sysmon:

* Download Sysmon from the Microsoft Sysinternals [page](https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon).
* Download the Sysmon configuration file from this [link](https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml).
* Extract the Sysmon zip file and place the downloaded configuration file in the extracted folder.
* Install Sysmon with the configuration file using PowerShell (as administrator):

“.\sysmon64.exe -i .\sysmonconfig-export.xml”

* Edit the Wazuh agent's ossec.conf file: C:\Program Files (x86)\ossec-agent\ossec.conf
* Add the following configuration to collect Sysmon logs:

<localfile>

<location>Microsoft-Windows-Sysmon/Operational</location>

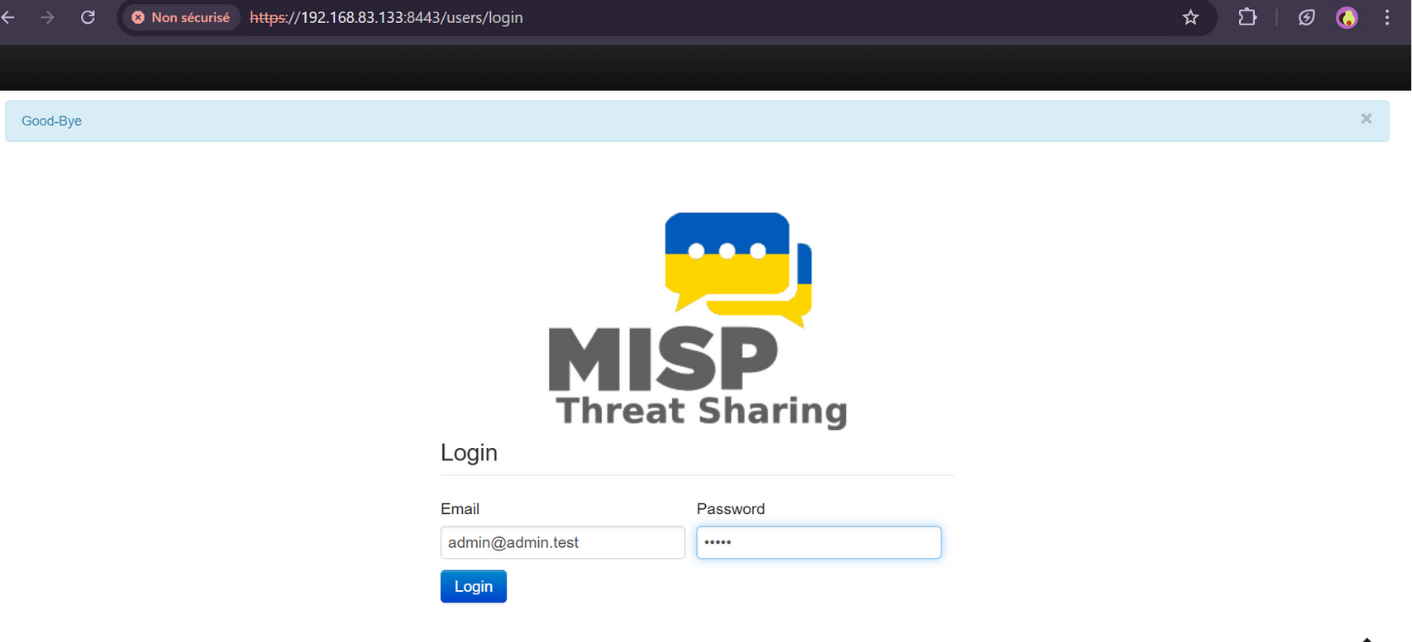
<log\_format>eventchannel</log\_format>

</localfile>

## Misp Installation

* wget --no-cache -O /tmp/INSTALL.sh https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh
* bash /tmp/INSTALL.sh
* wget --no-cache -O /tmp/INSTALL.sh https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh
* bash /tmp/INSTALL.sh -c

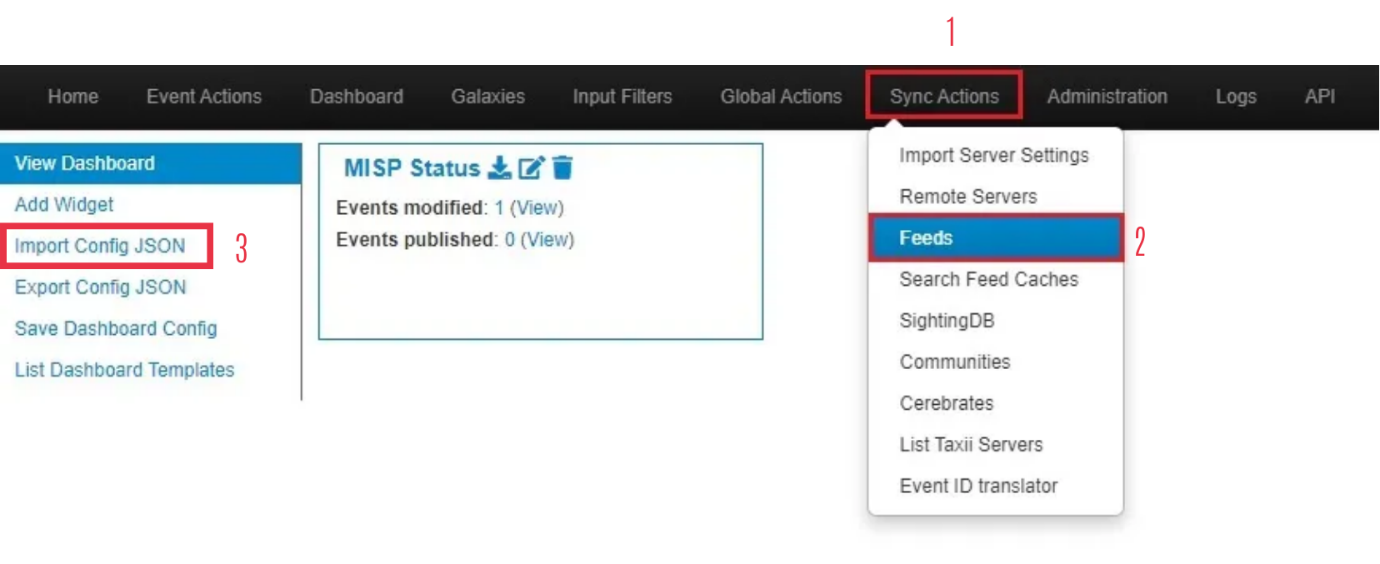
You can access your MISP instance through ports 80 and 443 on the machine hosting MISP. Accept the security certificate, then log in as the default Administrator using the credentials:

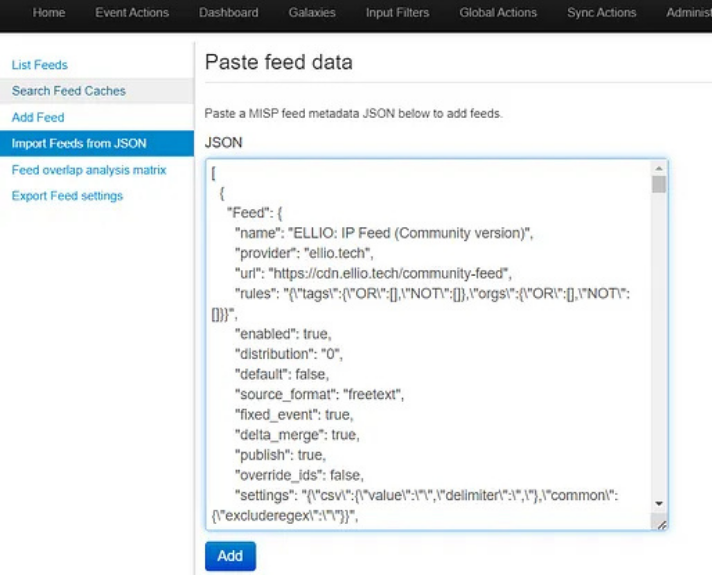


A screenshot of a login box

AI-generated content may be incorrect.

A MISP feed is a structured data source that automatically provides up-to-date information on cyber threats.





The feed script is mentioned in the below reference link:  
[MISP/app/files/feed-metadata/defaults.json at 2.4 · MISP/MISP · GitHub](https://github.com/MISP/MISP/blob/2.4/app/files/feed-metadata/defaults.json)

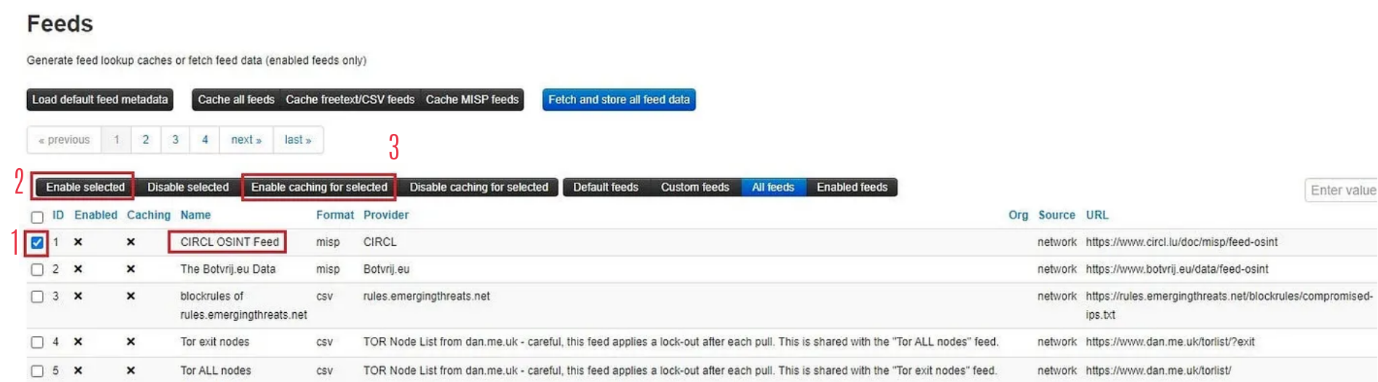
(Note: **IMPORTANT**: DON'T FORGET TO ACTIVATE AND COLLECT THE FEEDS)

A screenshot of a computer

AI-generated content may be incorrect.

Check and click Enable feeds to enable data sources, and then click fetch and store all feed data to download the data provided by each feed source.

We can see the data taken from the feeds in the Event Actions.



A screenshot of a computer

AI-generated content may be incorrect.

And you can see the attributes that appear for each event in the Attributes List.

A screenshot of a computer

AI-generated content may be incorrect.

**Generate an API key**

* Click on administration >> list auth keys >> Add authentication key.
* We generate an authentication key to allow the API to recognize and authorize the user. Fields such as user, comment, and authorized IPs must be configured as needed before submitting.
* Please make sure to write down the authentication key.

**A screenshot of a computer

AI-generated content may be incorrect.**

## Wazuh Configuration

Place [this Python script](https://github.com/karelumair/MISP-Wazuh-Integration/blob/main/custom-misp.py) at /var/ossec/integrations/custom-misp.

(**Note:** Ensure that you didn't add extension .py)

Change the URL and the API key in the script.

A screenshot of a computer program

AI-generated content may be incorrect.

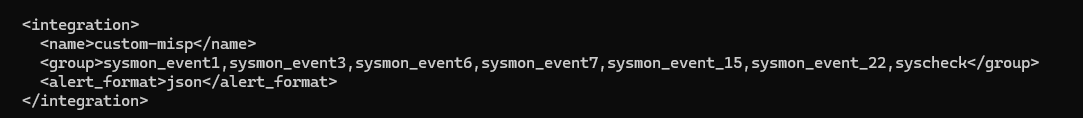
* Make sure to set the permissions:

cd /var/ossec/integrations/

sudo chown root:wazuh custom-misp && sudo chmod 750 custom-misp

* Make sure wazuh is already alerting for the desired sysmon events. You will likely need to create a custom rule if it isn't already alerting.
* For example, in our test we will need DNS queries from sysmon event 22
* We will change the under rule level from 0 to 4 in the file /var/ossec/ruleset/rules/0595-win-sysmon\_rules.xml
* Change the rule level of the alerts to more than 0 to desired rule level.

Edit the Wazuh manager's /var/ossec/etc/ossec.conf file to add the integration block:



* Restart the Wazuh manager.

Systemctl restart wazuh-manager

* Go to Server Management > Rules > Add New Rule file. Name it misp.xml, add the following and save.



* Create a new file in the mentioned location /var/ossec/integrations/misp.

A computer screen shot of a program code

AI-generated content may be incorrect.

* Enable the Sysmon rules in the mentioned location /var/ossec/ruleset/rules and set the rule levels as per the severity.

A screenshot of a computer

AI-generated content may be incorrect.

* Restart wazuh services

systemctl restart wazuh-manager

systemctl restart wazuh-indexer

systemctl restart wazuh-dashboard

## References

[GitHub - aymenmarjan/MISP-Wazuh-Integration: A comprehensive integration solution connecting MISP threat intelligence with Wazuh security monitoring for real-time threat detection. This project provides step-by-step instructions for deploying, configuring, and integrating MISP and Wazuh with Sysmon to automatically detect indicators of compromise (IoCs) in your environment.](https://github.com/aymenmarjan/MISP-Wazuh-Integration?tab=readme-ov-file)

[INSTALLATION INSTRUCTIONS | MISP](https://misp.github.io/MISP/xINSTALL.ubuntu2204.html)

[Wazuh And MISP Integration - Quickly Detect IoCs Within Your Wazuh Alerts With MISP!](https://www.youtube.com/watch?v=-qRMDxZpnWg)

[wazuh-custom-rules-and-decoders/integration at main · bayusky/wazuh-custom-rules-and-decoders · GitHub](https://github.com/bayusky/wazuh-custom-rules-and-decoders/tree/main/integration)