

# ThreatFusion: Wazuh + TheHive SOAR Integration

---

VISHWA PANCHOLI

SEMESTER-6

BSCIT IMS & CS



# Index

---

- ❖ Introduction
- ❖ Project Overview
- ❖ Flowchart Design
- ❖ Shuffle Workflow
- ❖ Conclusion

# Introduction

---

❑ Welcome to our presentation on "Threatfusion: Wazuh + TheHive SOAR Integration." Today, we'll explore how the integration of key security tools enhances our organization's cybersecurity capabilities. Let's dive in and take a closer look at the components driving our project.

- ❑ Components:
- Wazuh
  - TheHive
  - SOAR & SIEM
  - Sysmon & Mimikatz
  - Shuffle
  - Virustotal

# Wazuh

---

## ❖ Wazuh

- Wazuh is an open-source security monitoring platform renowned for its real-time threat detection and incident response capabilities. Its distributed architecture includes lightweight agents deployed on endpoints, a centralized manager for processing security events, and an optional Elasticsearch cluster for scalable storage and search.
- Wazuh offers features such as real-time threat detection, file integrity monitoring, and log analysis, complemented by services like threat intelligence integration and automated incident response. With its scalability and flexibility, Wazuh caters to organizations of all sizes, providing comprehensive security solutions for on-premises and cloud environments.

# TheHive

---

## ❖ TheHive

- TheHive is a robust Security Orchestration, Automation, and Response (SOAR) platform that centralizes incident response and threat intelligence activities. It enables rapid response to security events through features like case management, task automation, and collaboration tools.
- With its integration capabilities, TheHive connects with diverse security tools, facilitating automated response actions and enrichment with external threat intelligence feeds.
- Its user-friendly interface and customizable workflows empower organizations to streamline incident response processes and bolster their cybersecurity defenses.

# SIEM & SOAR

---

## ❖ SIEM (Security Information and Event Management)

- SIEM is a security solution that combines security information management (SIM) and security event management (SEM) capabilities to provide real-time analysis of security alerts and logs.
- Wazuh is a SIEM solution that collects and analyzes security data from various sources, including logs, network traffic, and endpoints, to detect and respond to security threats.

## ❖ SOAR (Security Orchestration, Automation, and Response)

- SOAR is a security solution that integrates security tools, automates response actions, and orchestrates incident response workflows to improve the efficiency and effectiveness of security operations.
- TheHive is a SOAR platform that centralizes incident response activities, automates response actions, and facilitates collaboration among security teams to streamline the investigation and remediation of security incidents.

# Sysmon & Mimikatz

---

- ❖ Sysmon is a tool for Windows systems that keeps track of activities like process creations, network connections, and file changes. It helps detect suspicious behavior on computers, aiding in identifying potential security threats.
- ❖ Mimikatz is a software tool used by hackers to steal passwords and other sensitive information from computer systems. It can retrieve passwords stored in memory, allowing attackers to gain unauthorized access to accounts and systems.

# Shuffle

---

- ❖ Shuffle is an automation tool designed to streamline and enhance security operations by integrating various security tools and platforms. Shuffle is like a conductor for security tools, helping them work together smoothly.
- ❖ It automates tasks and makes security operations more efficient by connecting different tools and coordinating their actions. With Shuffle, security teams can respond to threats faster and with less manual effort.



# Virustotal

---

- ❖ Virustotal is an online service that checks files and URLs against multiple antivirus engines and other security tools to assess whether they are safe or malicious. It provides valuable insights into the reputation and potential threats associated with digital assets, helping users make informed decisions about their security.

# Project Overview

---

- ❖ "Threatfusion" is an innovative project that aims to enhance our organization's cybersecurity capabilities through the integration of two powerful security technologies: Wazuh and TheHive SOAR.
- ❖ Key Objectives:
  - 1. Real-time Threat Detection: Leverage Wazuh's advanced threat detection capabilities to identify and mitigate security threats in real-time.
  - 2. Automated Incident Response: Implement TheHive SOAR to automate incident response workflows and streamline security operations.
  - 3. Enhanced Collaboration: Foster collaboration among security teams by centralizing incident management and facilitating information sharing.

# Project Overview

---

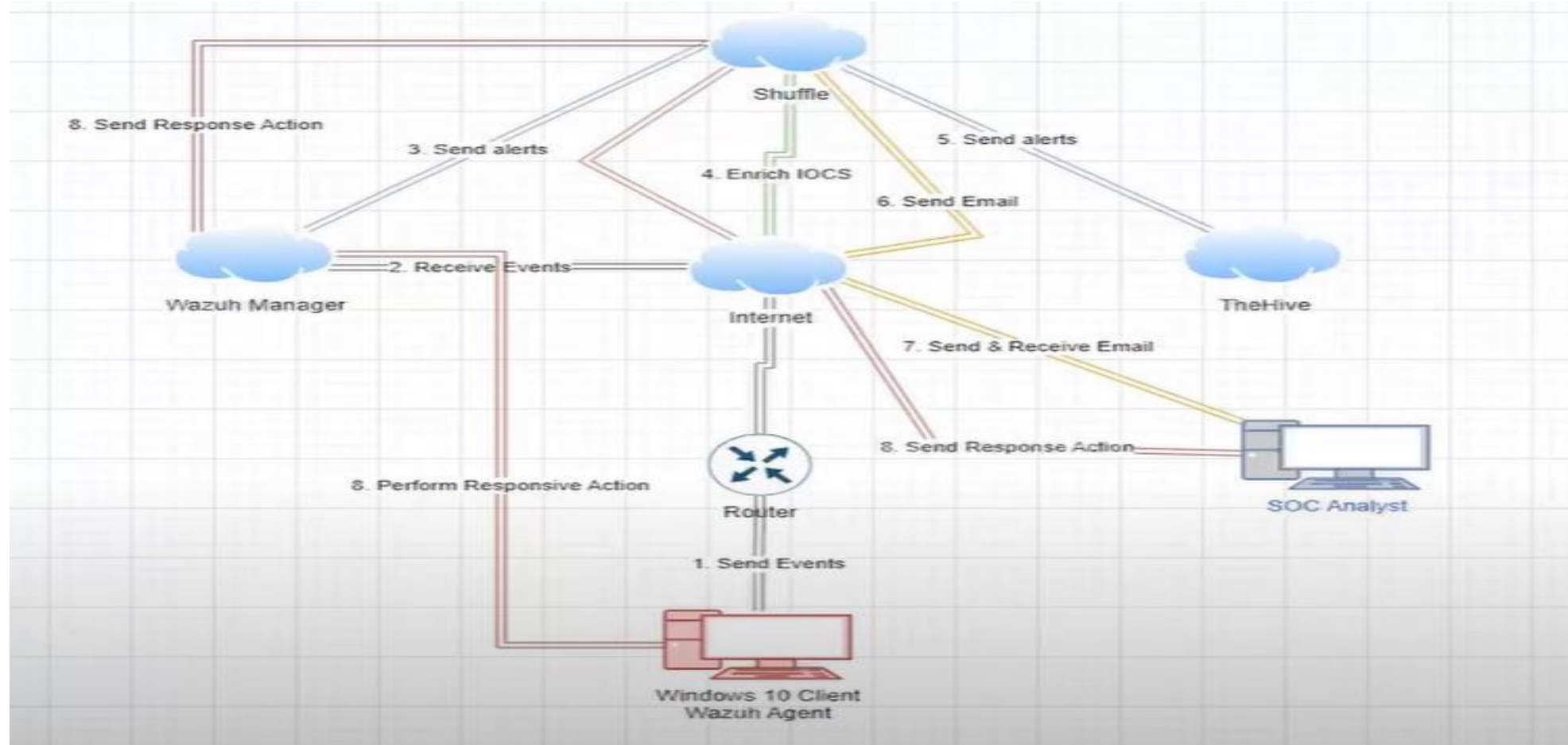
## ❖ Components:

- Wazuh: Acts as the primary SIEM solution, providing real-time monitoring, threat detection, and log analysis capabilities.
- TheHive: Serves as the central hub for incident response, orchestrating automated response actions and facilitating collaboration among security teams.

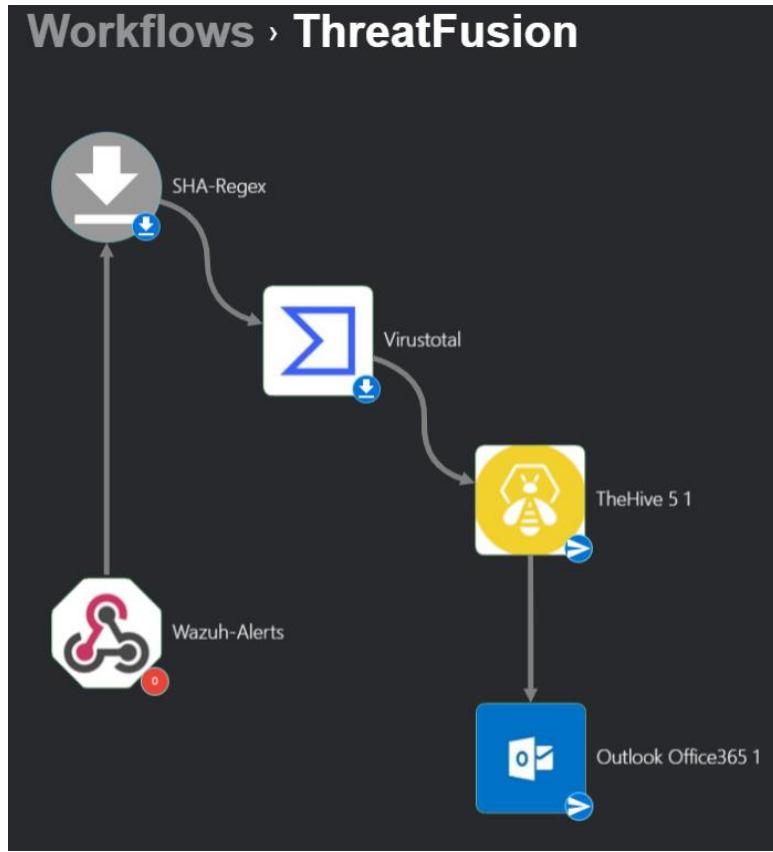
## ❖ Benefits:

- Improved Threat Visibility: Gain comprehensive visibility into security events and incidents across the organization's infrastructure.
- Efficient Incident Response: Automate response actions and workflows to respond rapidly to security incidents and minimize their impact.
- Streamlined Collaboration: Enhance communication and collaboration among security teams to effectively manage and mitigate security threats.

# Flowchart Design



# Shuffle Workflow



## ❖ Workflow Creation:

- Mimikatz Alert Sent to Shuffle
- Shuffle receives Mimikatz Alert
- Check Reputation Score with Virustotal (Extract SHA256 Hash from file)
- Send Details to TheHive to Create Alert
- Send Email to SOC Analyst to Begin Investigation

# Shuffle Workflow

```
PS C:\Windows\system32> cd "C:\Users\Vishwa Pancholi\Downloads\mimikatz_trunk\x64"
PS C:\Users\Vishwa Pancholi\Downloads\mimikatz_trunk\x64> ls

Directory: C:\Users\Vishwa Pancholi\Downloads\mimikatz_trunk\x64

Mode                LastWriteTime         Length Name
----                -
-a----          28-04-2024   11:10           37208 mimidrv.sys
-a----          28-04-2024   11:10        1355264 mimikatz.exe
-a----          28-04-2024   11:10           37376 mimilib.dll
-a----          28-04-2024   11:10           10752 mimispool.dll

PS C:\Users\Vishwa Pancholi\Downloads\mimikatz_trunk\x64> .\mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
## ^ ##.  "A La Vie, A L'Amour" - (oe-oe)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##  > https://blog.gentilkiwi.com/mimikatz
'## v ##'  Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'  > https://pingcastle.com / https://mysmartlogon.com ***

mimikatz #
```


Security Alerts					
Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Apr 28, 2024 @ 11:41:46.857	T1003	Credential Access	Mimikatz Usage Detected	15	100002
Rows per page: 10 ▾					
< 1 >					


```
Execution Argument
Execution Argument

Status SUCCESS

"Results for Execution Argument": { 8 items }
"severity": 3
"pretext": "WAZUH Alert"
"title": "Mimikatz Usage Detected"
"text": { 1 item
  "win": { 2 items
    "system": { 16 items
      "providerName": "Microsoft-Windows-Sysmon"
      "providerGuid": "{5778385f-c22a-43e0-bf4c-06f5698ffbd9}"
      "eventId": "1"
      "version": "5"
      "level": "4"
      "task": "1"
      "opcode": "0"
      "keywords": "0x8000000000000000"
      "systemTime": "2024-04-30T14:54:57.9778411Z"
      "eventRecordID": "5452"
      "processID": "3608"
      "threadID": "5056"
      "channel": "Microsoft-Windows-Sysmon/Operational"
      "computer": "DESKTOP-HPTAS3F"
      "severityValue": "INFORMATION"
      "message":
```

# Shuffle Workflow

 **Change Me**  
regex\_capture\_group











Status SUCCESS




▼ "Results for Change Me" : { 3 items

```
"success" : true
  "group_0" : [ 1 item
    0 : "61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1"
  ]
  "found" : true
}
```

Variables (click to expand)

 61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1     Vishwa Pancholi 


 

**File distributed by Offensive Security**  Reanalyze  Similar  More

61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1

mimikatz.exe

Size: 1.29 MB | Last Modification Date: 53 minutes ago



pevte | direct-cpu-clock-access | runtime-modules | 64bits | assembly | known-distributor | idle

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 28

Crowdsourced YARA rules

- Matches rule HKTLMimikatzSkeletonKey\_in\_memory\_Aug20\_1 from ruleset gen\_mimikatz at <https://github.com/Neo23x0/signature-base> by Florian Roth (Nextron Systems)  
↳ Detects Mimikatz SkeletonKey in Memory
- Matches rule HKTLMimikatzIcon from ruleset gen\_mimikatz at <https://github.com/Neo23x0/signature-base> by Arnim Rupp  
↳ Detects mimikatz icon in PE file
- Matches rule MimikatzGenStrings from ruleset thor-hacktools at <https://github.com/Neo23x0/signature-base> by Florian Roth (Nextron Systems)  
↳ Detects Mimikatz by using some special strings
- Matches rule MimikatzStrings from ruleset gen\_mimikatz at <https://github.com/Neo23x0/signature-base> by Florian Roth (Nextron Systems)  
↳ Detects Mimikatz strings
- Matches rule WindowsHacktoolMimikatz\_1388212a from ruleset WindowsHacktoolMimikatz at <https://github.com/elastic/protections-artifacts> by Elastic Security
- Matches rule WindowsHacktoolMimikatz\_674fd079 from ruleset WindowsHacktoolMimikatz at <https://github.com/elastic/protections-artifacts> by Elastic Security  
↳ Detection for default mimikatz memssp module

See all

Crowdsourced Sigma Rules

# Shuffle Workflow

Mimikatz Usage Detected

Id ~42102856

Created by SOAR

Created at 03/05/2024 08:56

SEVERITY:MEDIUM

TLP:AMBER

PAP:AMBER

Assignee Assign to me

Unassigned

Source

WazuH

Reference

Rule: 100002

Type

Internal

Occurred date

03/05/2024 05:30

Status

New

General

Observables (0)

TTPs (0)

Attachments

Similar Cases

Similar Alerts

Res

Tags

T10003

Description

"Mimikatz Detected on host": "DESKTOP-HPTA53F" "from user": "DESKTOP-HPTA53F\Vishwa Pancholi"

Summary

"Mimikatz activity detected on host": "DESKTOP-HPTA53F" "and the process ID is": "3284" "and the Commi is": ""C:\Users\Vishwa Pancholi\Downloads\mimikatz\_trunk\x64\Hackerspace.exe""

Edit ?

1 of 149

< > ☰

Mimikatz Usage Detected !!!! Inbox x

Vishwa Pancholi

via outlook.com

to me

7:27 PM (0 minutes ago) ☆ 😊 ↶ ⋮

Be careful with this message

This may be a spoofed message. The message claims to have been sent from your account, but Gmail couldn't verify the actual source. Avoid clicking links or replying with sensitive information, unless you are sure you actually sent this message. (No need to reset your password, the real sender does not actually have access to your account!)

Report spam

Looks safe

?

"Title": "Mimikatz Usage Detected" "Host": "DESKTOP-HPTA53F" "Time": "2024-05-17 13:56:26.319"

↶ Reply

↷ Forward

😊



# Conclusion

---

- ❖ "Threatfusion: Wazuh + TheHive SOAR Integration" is a game-changer for our cybersecurity. By combining Wazuh's threat detection with TheHive's automated response, we're faster and smarter at spotting and stopping security threats. This project helps our teams work better together, saves time with automated tasks, and keeps our digital assets safe from harm. With "Threatfusion," we're stronger and more secure in today's ever-changing threat landscape.

THANK YOU