WAZUH TO SOAR AUTOMATION/ SOC HOME LAB
BY Pranav Rao

OBJECTIVE

The objective of the Wazuh to SOAR automation project is to fortify the security posture of Windows servers by implementing an automated process for detecting and responding to potential Mimikatz activity. The objective entails:

1. Detection: Develop and deploy system monitor rules within Wazuh to identify suspicious Mimikatz activity on Windows servers.
2. Integration: Configure Wazuh to generate alerts upon detecting Mimikatz activity and forward them to the SOAR platform, Shuffle.
3. Alerting: Establish automated workflows within Shuffle to promptly notify a Security Analyst via email upon receiving a Mimikatz alert from Wazuh.
4. Incident Management: Enable Shuffle to create an incident in the case management system, TheHive, containing pertinent details of the Mimikatz detection.
5. Analysis and Response: Empower the Security Analyst to assess the severity of the Mimikatz activity based on the received email notification and determine appropriate action.
6. Automated Response (Optional): If the Security Analyst opts to stop the malicious activity, configure Shuffle to trigger an automated response to block the IP address of the Mimikatz server host at the firewall level.

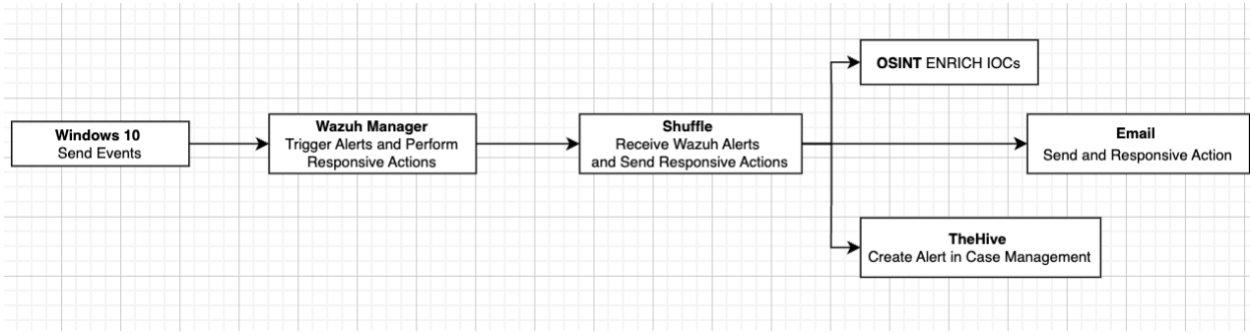


Figure 1: Displaying the path events.

By achieving these objectives, the project aims to enhance the organization's capability to swiftly detect and respond to Mimikatz attacks on Windows servers, thereby reinforcing cybersecurity defenses and mitigating potential risks effectively.

TOOLS AND APPLICATIONS:

- **Wazuh:** An open-source security monitoring platform that collects, analyzes, and responds to security data from various sources, including logs, file integrity monitoring, and system monitoring.

- **TheHive:** An open-source security incident response platform designed to streamline collaboration and management of security incidents and alerts, enabling effective incident response workflows.

- **Sysmon (System Monitor):** A Windows system service and device driver that monitors and logs system activity to provide comprehensive visibility into potential security threats and suspicious behavior.

- **Mimikatz:** A powerful post-exploitation tool used for extracting plaintext passwords, hashes, and other sensitive information from memory, credential caches, and authentication mechanisms in Windows environments.

- **Shuffle:** A SOAR (Security Orchestration, Automation, and Response) platform that integrates various security tools and facilitates automated workflows for incident response, including email notifications and user input prompts.

- **Digital Ocean:** A cloud infrastructure provider offering scalable and flexible cloud computing solutions, which could be utilized for hosting and deploying various components of the project.

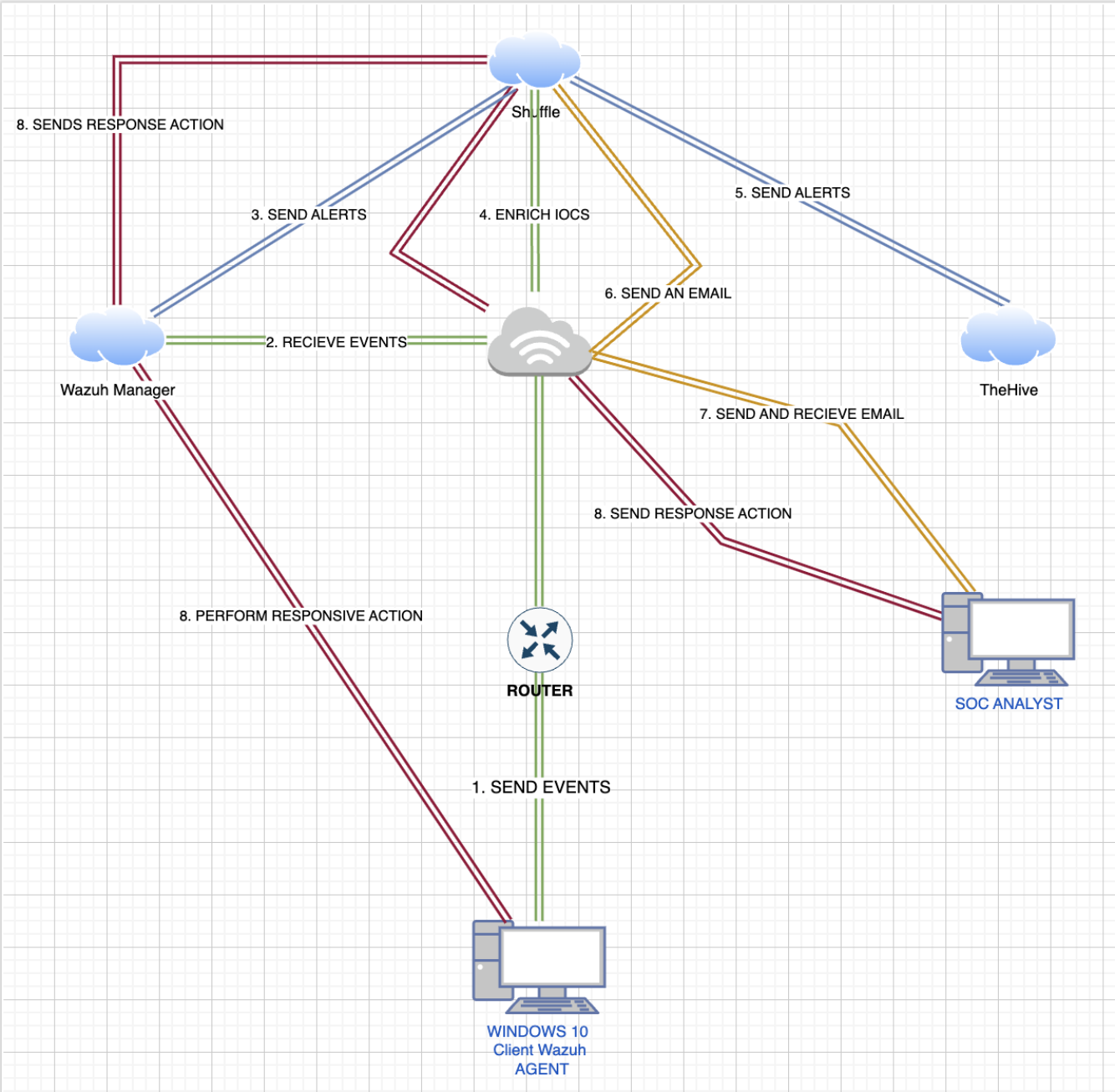
- **Windows 2019 ISO:** The official installation image for Windows Server 2019, used for setting up Windows server instances to emulate production environments for testing and analysis.

- **VirusTotal:** An online service that analyzes files and URLs to detect malicious content and provides insights into potential threats by aggregating results from multiple antivirus engines and other security tools.

- **Termius:** A cross-platform SSH client that allows secure remote access to servers and devices, facilitating configuration, management, and monitoring tasks.

- **VNC Viewer:** A remote desktop access application that enables users to control and interact with remote desktop environments, facilitating graphical access to servers and workstations for administration and troubleshooting purposes.

Figure 2: Holistic Network Architecture of the SOC Lab



VIRTUAL MACHINE TO HOST WINDOWS 2019 SERVER:

-Created droplet/instance in **Digital Ocean**

Figure 3

-Temius enabled SSH root login into the **Windows 19 server**

Figure 4

-**VNC viewer** to login remotely to the windows server by displaying the graphical contents of the window's server.

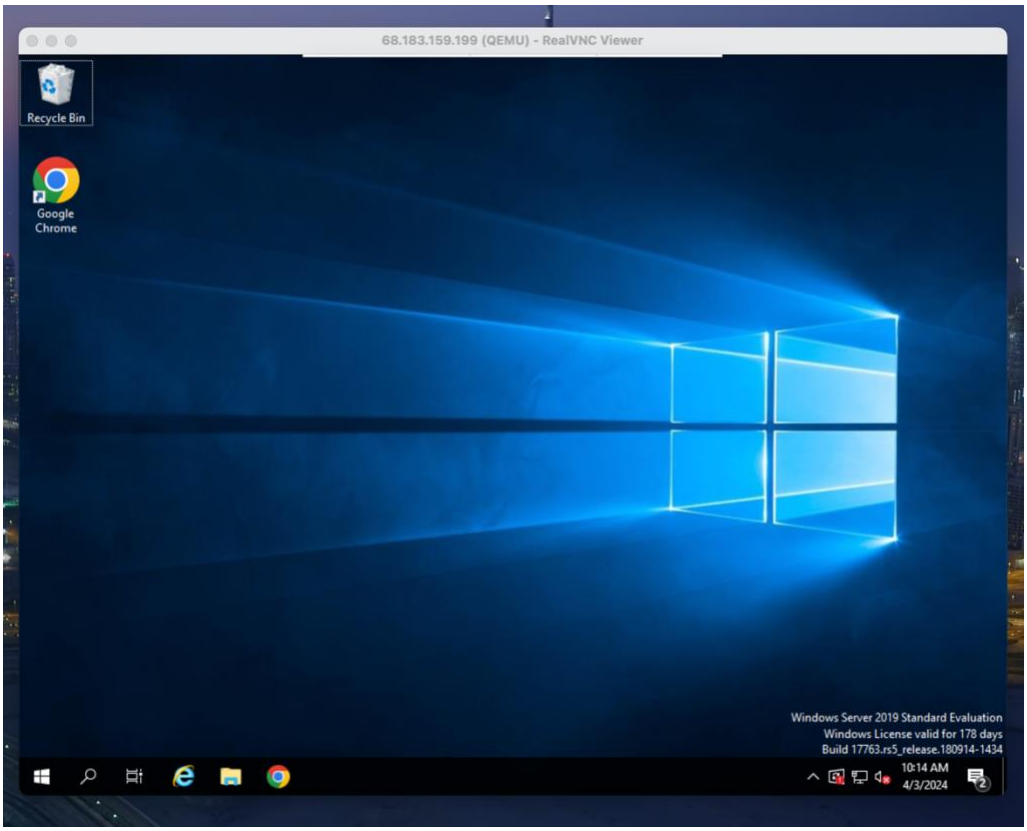


Figure 5

-Using **Sysmon** to monitor and track processes taking place on the systems activity

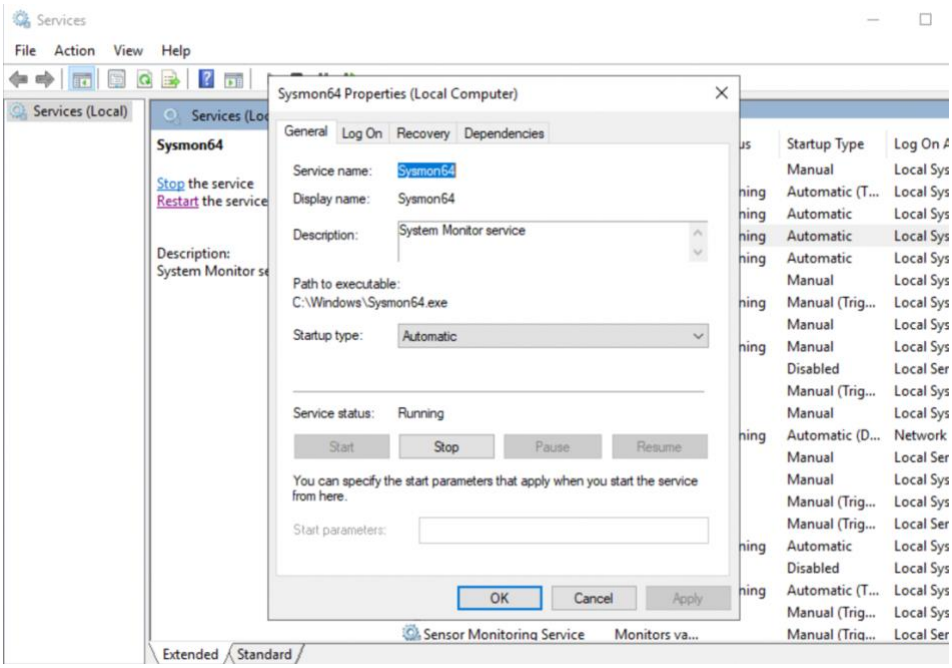


Figure 6

-**Wazuh Window Agent** installed and the **OSSEC.CONF** files configured on the window's server and tracks when a PowerShell script is executed

.

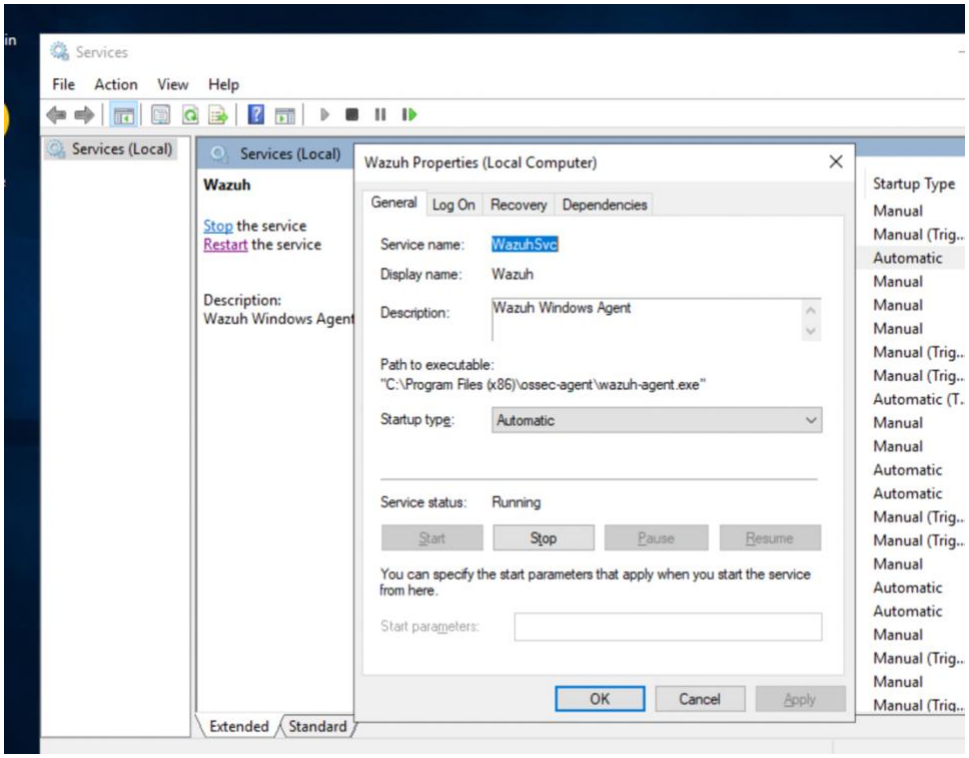


Figure 7

-Running a **Mimikatz executable** for credential Harvesting

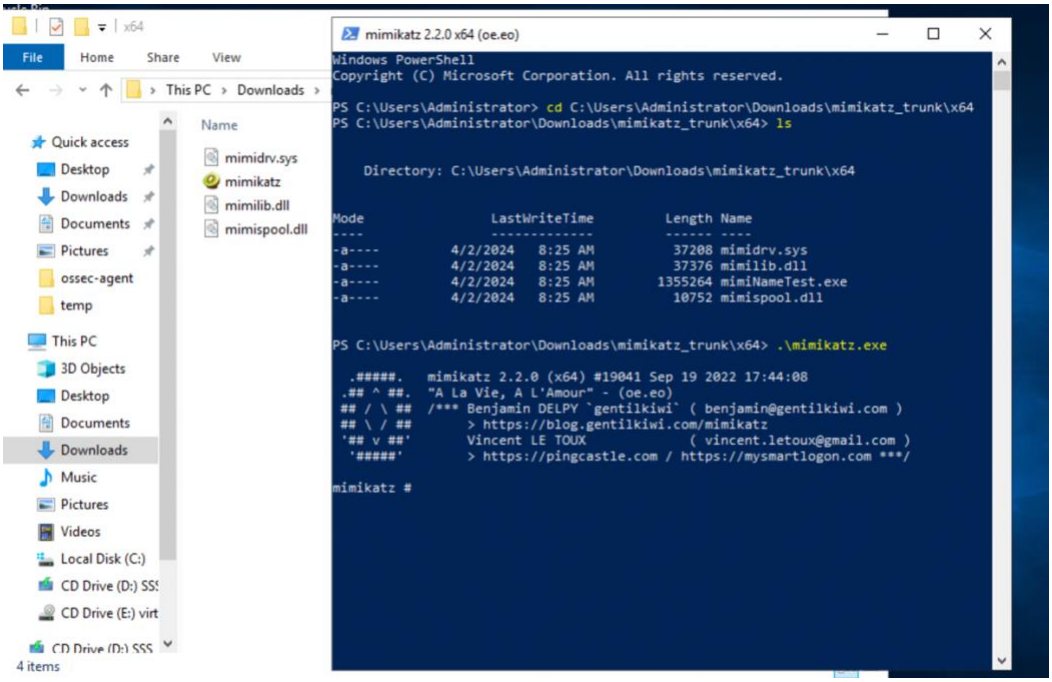


Figure 8

WAZUH INTEGRATION

-Created a **Wazuh Sever** on **Digital Ocean**

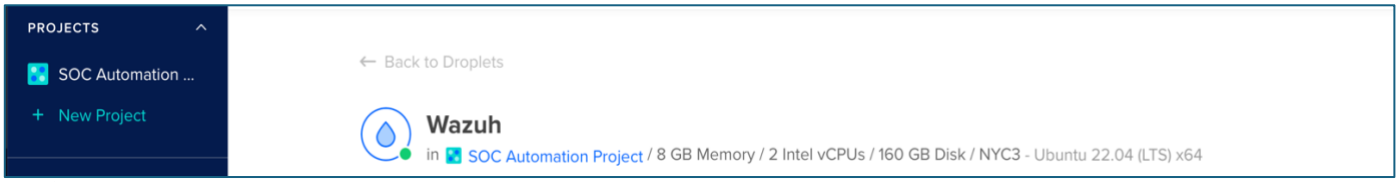


Figure 9

-Used Termius to SSH to root to the Wazuh-Manager server

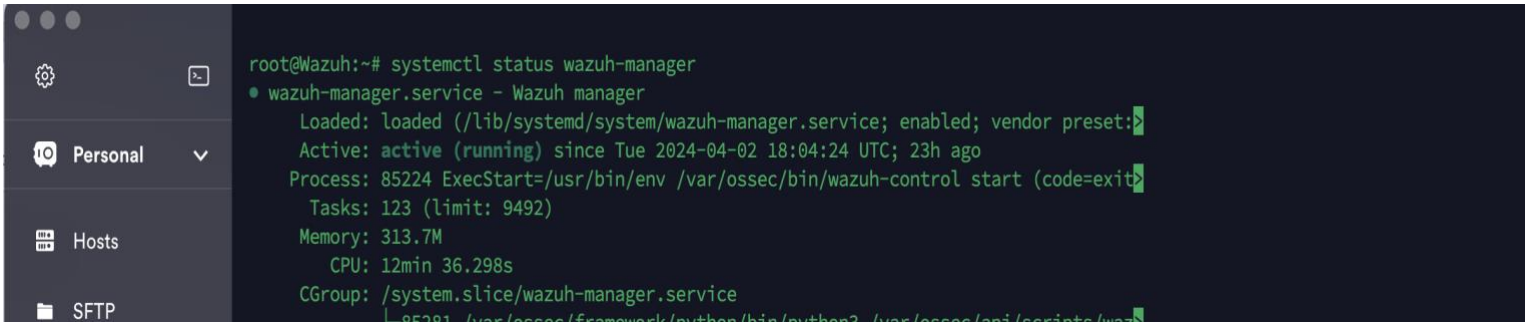


Figure 10

-Events and Agents have been populated on the **Wazuh SEIM Dashboard** indicating T003 and Mimikatz Usage Detected.

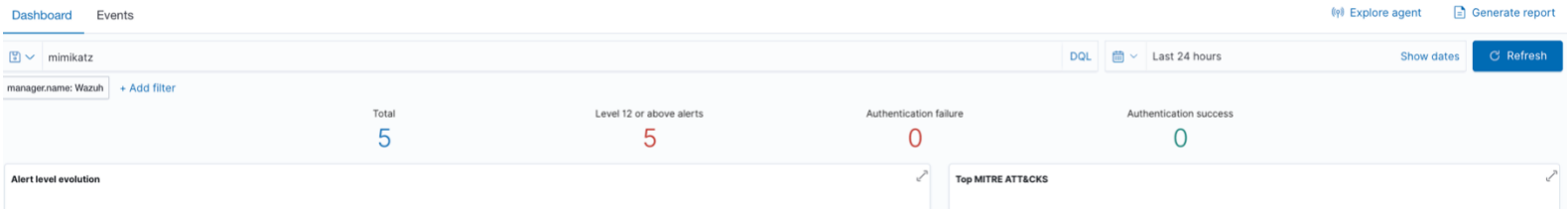


Figure 11

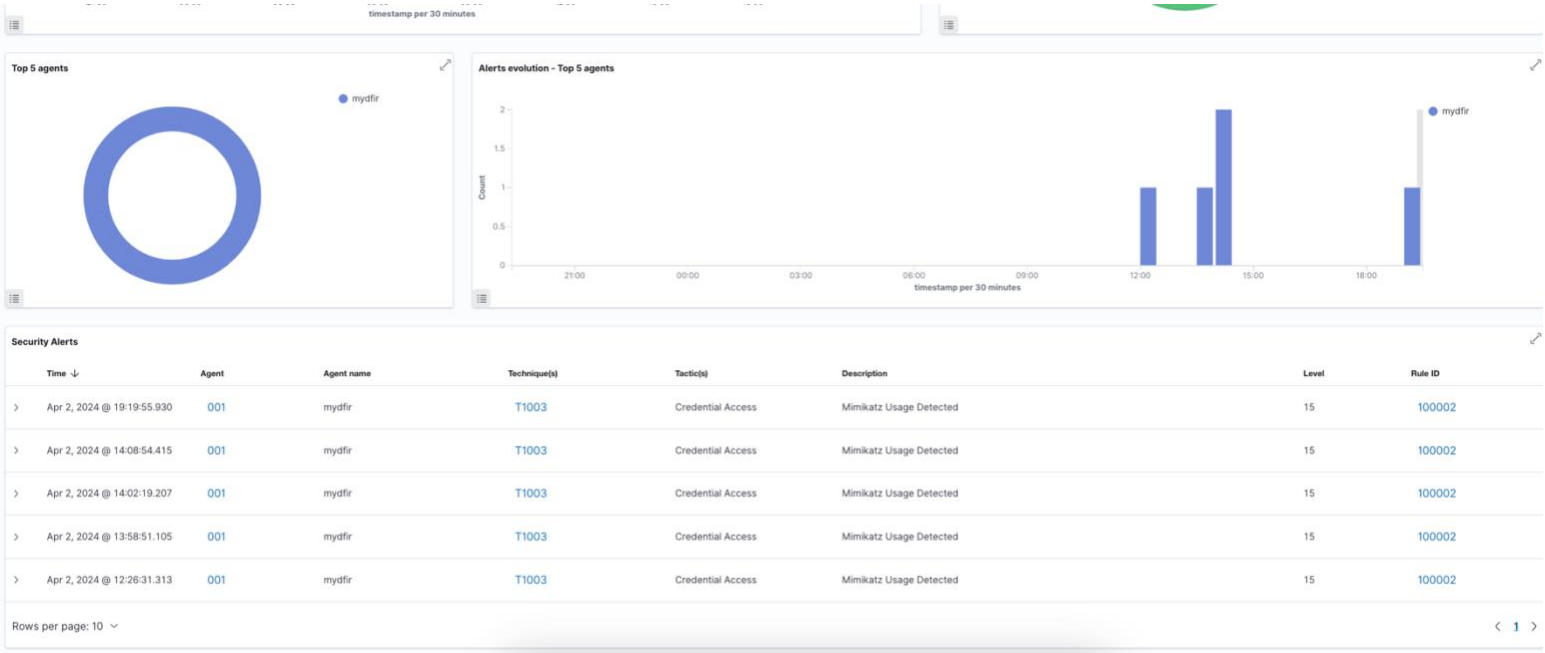


Figure 12

TheHIVE INTEGRATION

-Initiated theHive server on **Digital Ocean**; Need to install Java, Casandra, and Elastic search in order for theHive to work.

1. **Java:** TheHive is built on Java and requires Java Runtime Environment (JRE) to execute its code.
2. **Cassandra:** TheHive uses Apache Cassandra as its backend database to store and manage large volumes of security incident data efficiently.
3. **Elasticsearch:** Elasticsearch is used as the search and indexing engine for TheHive, enabling fast and flexible searching capabilities across the stored security incident data.

These components are essential for TheHive to function properly, providing the necessary infrastructure for storing, indexing, and retrieving security incident information efficiently.

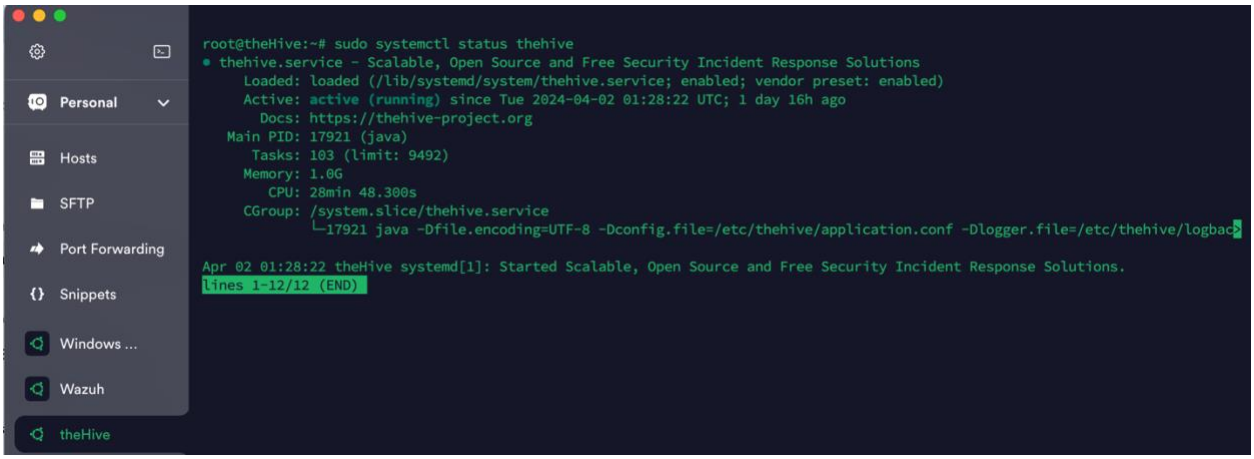


Figure 13

SOAR SHUFFLE IMPLEMENTATION

-The app layout on the **shuffle workflow for creating automated playbook** when alert is sent from the Wazuh Manager

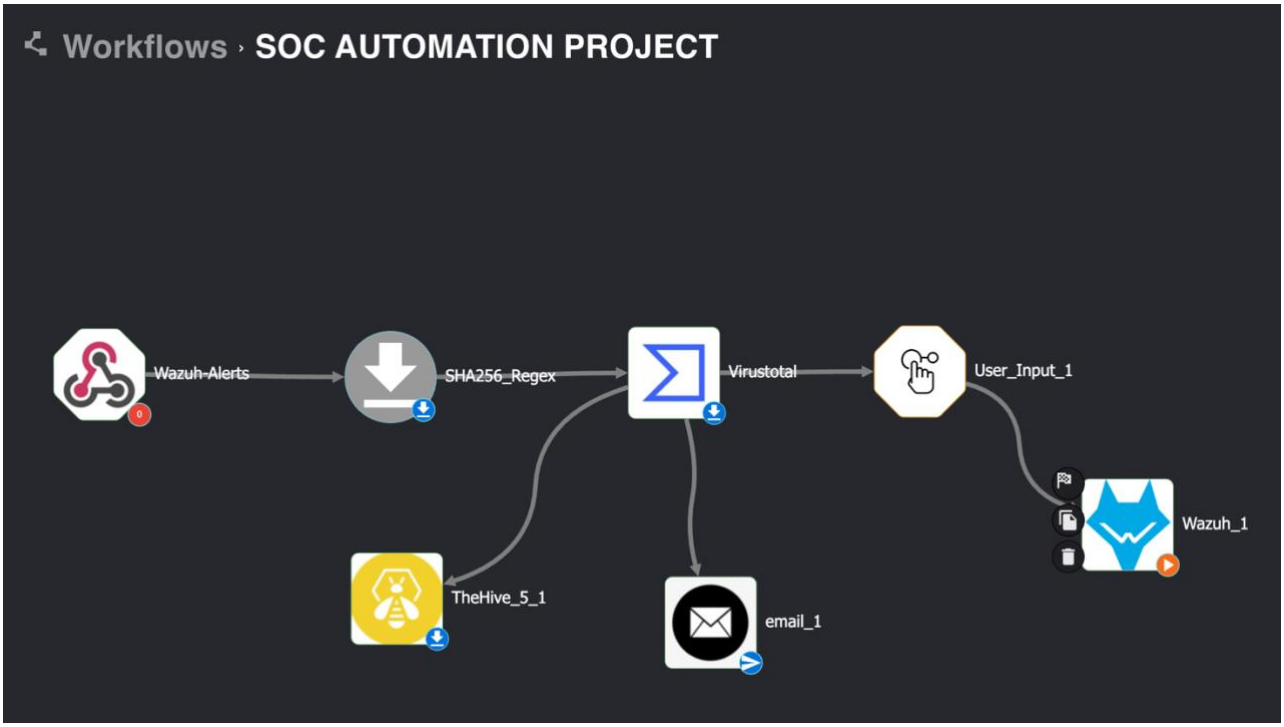


Figure 14

-The Wazuh alert containing Mimikatz data is sent to the **SHA256 Regex** to parse out the hash value.

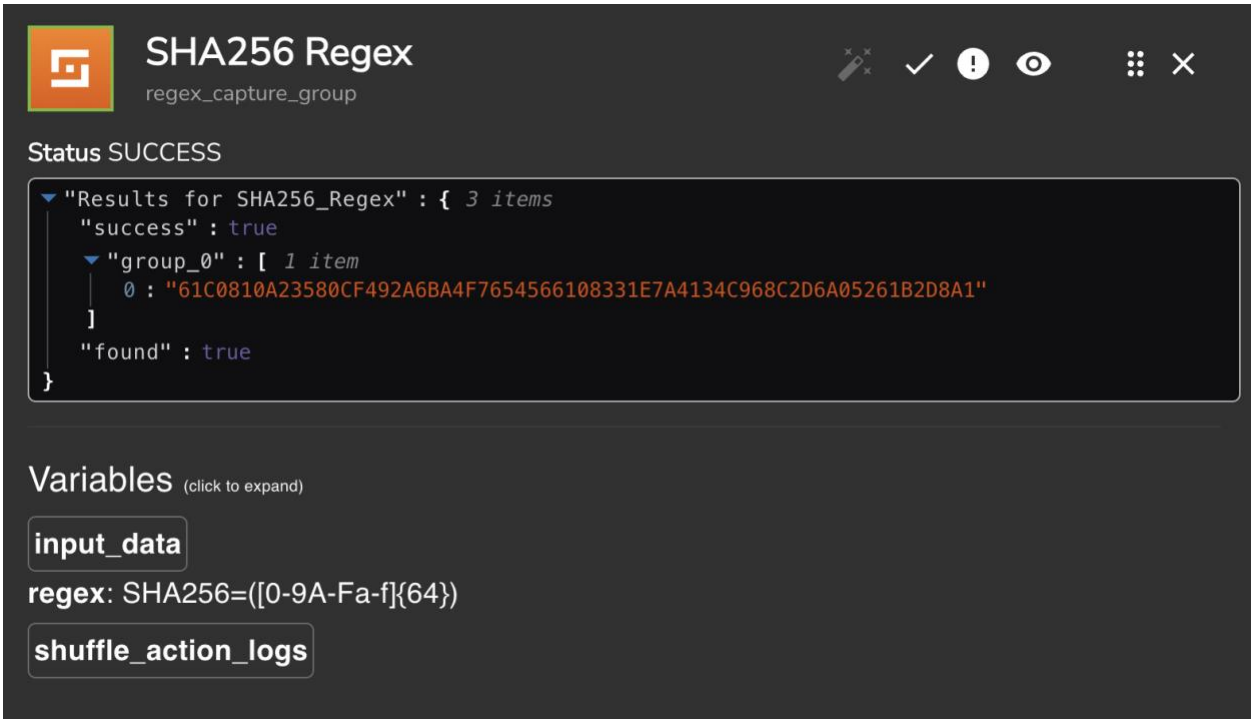


Figure 15

-The hash value is passe on to the **VirusTotal app** to check for integrity of the Hash and reports the **"malicious": 64**

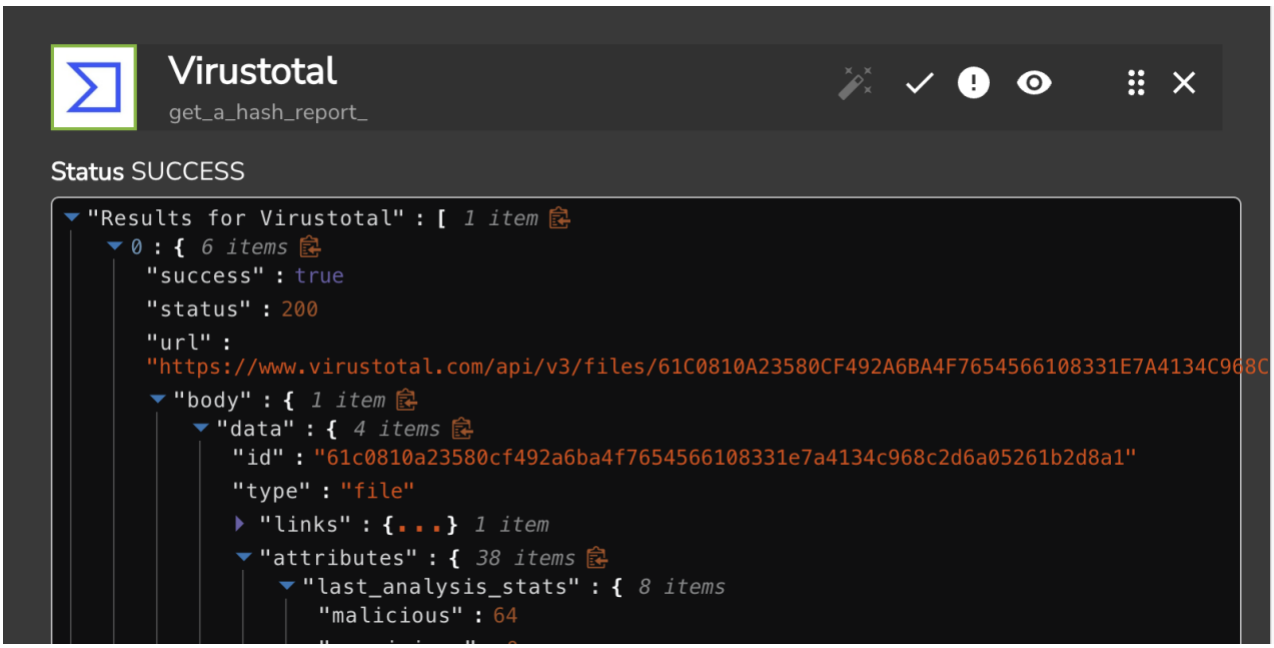


Figure 16

-After determining the Mimikatz is malicious through VirusTotal it is then sent to the **case management in the TheHive server**, and an email is also sent to the security analyst.

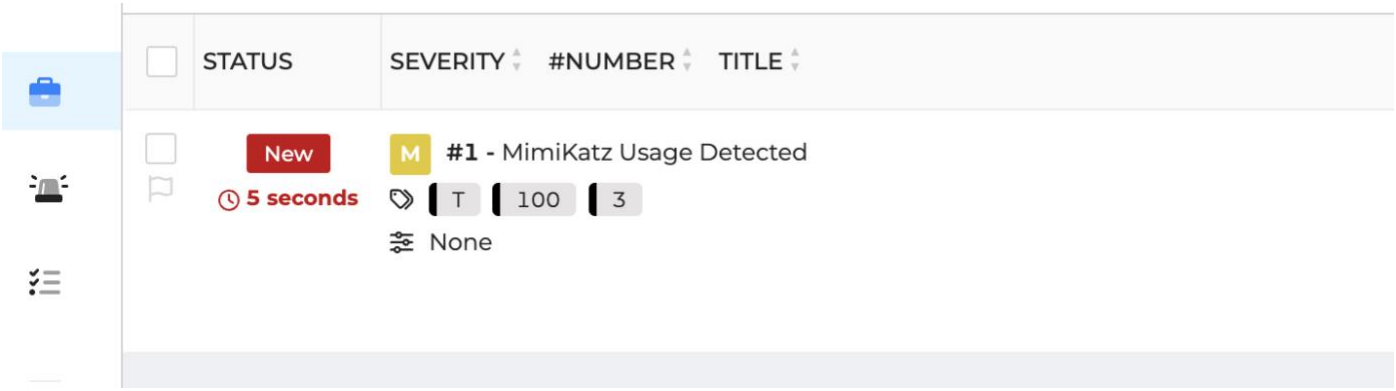


Figure 17

-Email indicating the source of the IP address as well as options for the analyst to take **actionable response**.

Figure 18

ACTION RESPONSE

-The action response in this case is to **block the IP Address** of the local host that contains the malicious virus using a **firewall** which is the Windows's 2019 Server's IP. This is action response was configured by changing by modifying the **action responses on the ossec.conf file for Wazuh**.

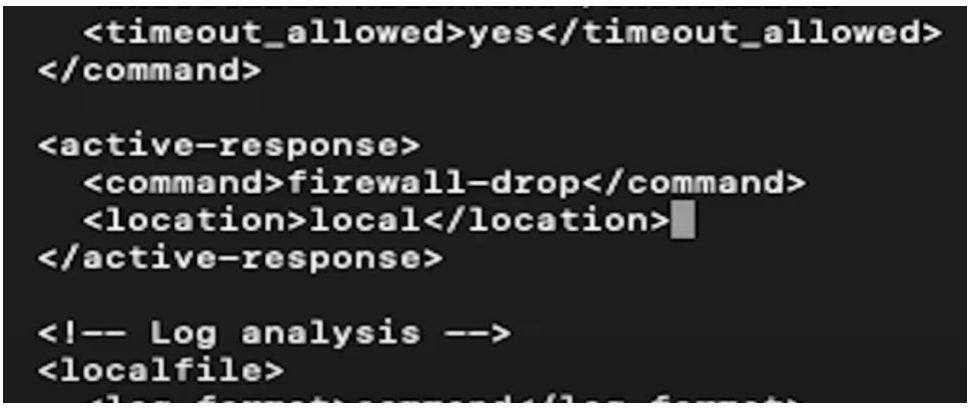


Figure 18

-Configuring the **Wazuh app on Shuffle** to run a command that was listed in the email

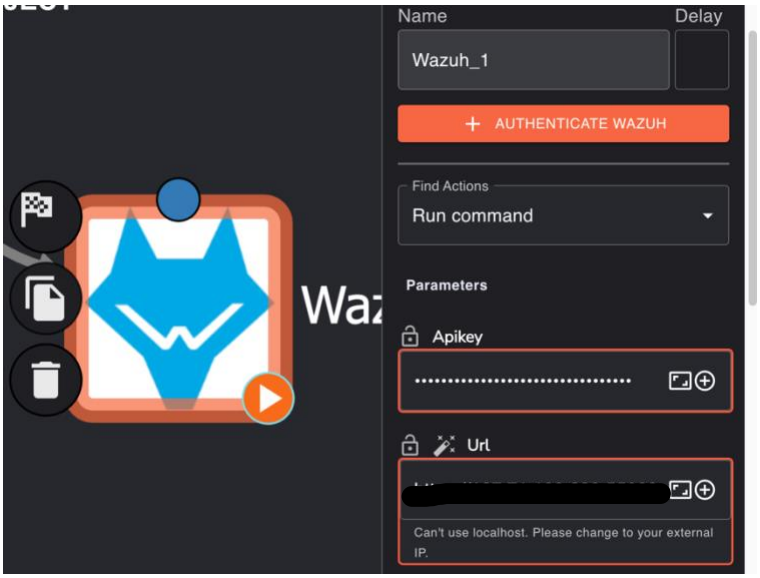


Figure 19

-If you ping the IP Address the target indicates that it has been **dropped**

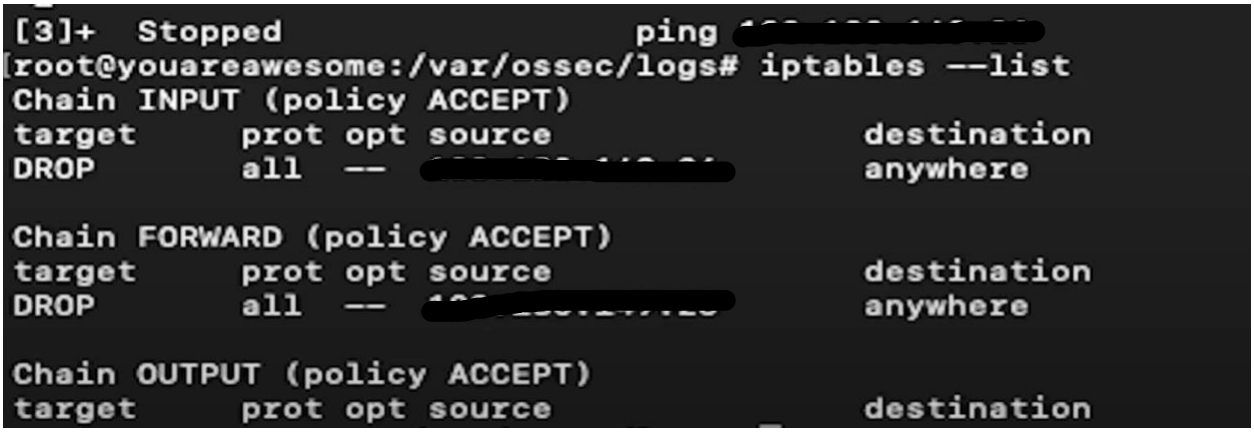


Figure 20

CONCLUSION

In conclusion, the SOC home lab project presents a comprehensive setup leveraging a combination of powerful tools and applications to bolster cybersecurity capabilities. Through integration of Wazuh for threat detection, TheHive for incident management, and Shuffle for automated response orchestration, the project streamlines incident detection, analysis, and response processes. With meticulous monitoring, analysis, and optimization, the lab not only enhances understanding of security operations but also equips practitioners with practical experience in combating real-world cybersecurity threats.