Cloud-Based Security Operation Center (SOC) Automation via Security Orchestration, Automation, Response (SOAR), With Threat Intelligence Platform (TIP) Capabilities

> By Victor Coil

### Table of Contents

Table of Contents	1
Project Objectives	2
Reflection and Future Improvements	2
Section 1 - Wazuh XDR solution initial setup	
Subsection - Wazuh Firewall	7
Subsection - Initial commands in Wazuh	13
Section 2 - TheHive Case Management Solution Initial Setup	18
Subsection - TheHive Firewall	19
Subsection - Initial Commands in TheHive	21
Section 3 - TheHive Additional Configurations	26
Subsection - Cassandra Configurations	26
Subsection - ElasticSearch Configurations	30
Subsection - TheHive Configurations	32
Section 4 - Linux Victim Honeypot Initial Setup and Agent Deployment	35
Subsection - Honeypot Firewall	36
Subsection - Agent Deployment	
Section 5 - Wazuh XDR Server Configurations	44
Subsection - Wazuh Logs, Archives, and Filebeat	46
Section 6 - Wazuh Detection Rule Creation	49
Subsection - SSH Bruteforce Rule	50
Section 7 - MISP Threat Intelligence Platform Solution initial setup	52
Subsection - Creating a persistent service	57
Subsection - MISP login, Organization and User Creation	59
Subsection - MISP Server Settings & Maintenance	63
Subsection - Manual Enrichment	68
Section 8 - Shuffle SOAR solution deployment	72
Subsection - Webhook	77
Subsection - HTTP widget	81
Subsection - VirusTotal Widget	84
Subsection - TheHive Widget	86
Subsection - User Input Widget	95
Subsection - Wazuh Active Response Widget	97
Section 9 - Integrating TheHive into MISP	101
Section 10 - Atomic Threat Intelligence Gathered	106

#### **Project Objectives**

The objective of this project was to gain hands-on experience with the SOAR tool Shuffle for automated active response, as well as to become familiar with how a threat intelligence platform can be used to enrich observables tied to an alert. Overall, the project focuses on detecting SSH brute-force attempts using Wazuh XDR via custom detection rules, then beginning the Shuffle workflow that performs preliminary enrichment of observables with the Virustotal API, case creation on TheHive, further enriching and storing observables in MISP, and executing approval-based responses.

#### **Reflection and Future Improvements**

In future iterations, I plan to expand detection beyond bruteforce activity to include broader MITRE ATT&CK techniques, potentially interlink multiple cloud-based SOC environments under a unified MISP instance for threat correlation, and automate rule creation based on the enriched observables.

#### Section 1 - Wazuh XDR solution initial setup

The first thing on the to-do list for this project is to set up the Wazuh main Server. In this project, I will be using DigitalOcean. They generously offer \$200 credits to first-time users. You can use them or any other cloud provider.

If you are using the same provider and have created your account, you should see the dashboard as shown below. Let us set up a droplet, which is the name for a Virtual Machine.

Click on the "Create" button, then select "Droplets" from the dropdown menu.



On the "Create Droplets" page, select the Region closest to you.

I selected the "**New York**" Region

As for the Image, I chose Ubuntu, version "22.04 (LTS) x64" as the OS

# For the Droplet Type, select "**basic**". For the CPU options, select "**Premium Intel**". Then the \$48 a month option as shown below.

Choose Size	Need help picking a plan? Help me choose 🗹					
Droplet Type						
SHADED CDU	DEDICATED CPU					
Basic (Plan selected)	General Purpose	CPU-Optimized	Memory-Optimized	Storage-Optimized		

Basic virtual machines with a mix of memory and compute resources. Best for small projects that can handle variable levels of CPU performance, like blogs, web apps and dev/test environments.



#### \$48.00/month

\$0.071/hour

CREATE VIA COMMAND LINE

**Create Droplet** 

Scroll down a bit to find the "**Choose Authentication Method**" and select the "**Password**" option and input a strong password for the root account.

Choose Authentication Method ?



After inputting a strong password, move on down and change the "**Hostname**" to "**Wazuh**". Then click on the "**Create Droplet**" button.

Quantity			Hostname		
Deploy multiple Droplets with the same configuration.		9	Give your Droplets an identifying name you will remember them by.		
_	1 Droplet	+	Wazuh		
Tags					
Type tag	gs here	_			
Project		T	his project has been selected as you only have one project		
🔽 first	-project				

\$48.00/month	Croate Droplet
\$0.071/hour	Create Dioplet

Subsection - Wazuh Firewall

After creating your droplet, it is time to create a firewall to stop any traffic from trying to get into the machine. On the left-hand side, expand "**Manage**", then click on "**Networking**".



### Select the "Firewall" Tab, and then click on the "Create Firewall" button.

# Networking

Domains	Reserved IPs	Load Balancers	VPC	Multi-cloud integrations	Firewalls	PTR records
			_			
				Firewalls		
Firewa	alls allow you to e	easily secure your in organize your i	nfrastruc infrastru	ture by explicitly defining w cture and apply Firewall rule	hich type of tr es to multiple	affic is allowed to reach it. Use tags to resources.
				Create Firewall		

On the "Create Firewall" page, input the firewall's name. I selected "Wazuh-Firewall."

Change the type from "SSH" to "All TCP," clear the sources, and enter your IP Address.

You can get it from this site:

https://whatismyipaddress.com/

## Create Firewall

Learn 🖻

Name	
Name Wazuh-Firewall	~

#### **Inbound Rules**

Set the Firewall rules for incoming traffic. Only the specified ports will accept inbound connections. All other traffic will be dropped.

Туре		Protocol	Port Range	Sources	
All TCP	~	ТСР	All ports	Add a source	Delete
New rule	~				

Add a new rule and do the same for "All UDP", with sources being your IP address.

No changes need to be made for the "Outbound Rules."

Scroll down and click on the "Create Firewall" button.

Apply the firewall to the Droplet.

Click on "Droplets" on the left-hand side. Then click on your droplet's Name.



On the left-hand side, click on "networking".



Then scroll down to the bottom to find the "Firewalls" section. Click on "Edit."

Click on your Wazuh Firewall.

# Networking

Domains	Reserved IPs	Load Balancers	VPC	Multi-cloud integrations	Firewalls	PTR records	
							Create Firewall
Name		ſ	Droplets	Rules	Cre	ated	
( w	'azuh-Firewall	(	D	5	7 m	inutes ago	More ∨

Select the "Droplets" tab, then click on the "Add droplet" button.



Type in "Wazuh", select it, then click on the "Add Droplet" button.

Add Droplet	×
Wazuh Search for a Droplet or a tag	Add Droplet

Subsection - Initial commands in Wazuh

Log in to the Wazuh server using SSH on your Windows terminal/command prompt. You can use Putty as well.

# The command format is "ssh <user>@<IP>
# Capitalization matters
# ssh root@<IP>

Name	IP Address	State	Added
Wazuh 8 GB / 2 Intel vCPUs / 160 GB / NYC1	137.184.97.114	Up-to-date	Just now
C:	Command Prompt		
Mic (c)	rosoft Windows [Versio Microsoft Corporation	on 10.0.19045.5854] n. All rights reserved.	
C:\	Users\ssh r	root@137.184.97.114	

Input "**yes**" to continue with the connection. Input your password.

Run an APT update and upgrade as shown below.



When you get these next two screens, just hit "ENTER" on your keyboard.

🖭 root@Wazuh: ~ 🗌
Package configuration
Configuring openssh-server
A new version (/tmp/tmp.QAkwwvLyd4) of configuration file /etc/ssh/sshd_config is available, but the version installed currently has been locally modified.
Sat the version installed carrently has been locally modified.
What do you want to do about modified configuration file sshd_config?
install the package maintainer's version
keep the local version currently installed
show a side-by-side difference between the versions
show a 3-way difference between available versions
do a 3-way merge between available versions
(UK)

🖦 root@Wazuh: ~		—	
Package configuration			
	Daemons using outdated libraries Which services should be restarted? (*) cron.service [ dbus.service [ getty@tty1.service [*] irqbalance.service [*] multipathd.service [ networkd-dispatcher.service [ ] polkit.service [*] serial-getty@ttyS0.service [ ] systemd-logind.service [ ] unattended-upgrades.service [ ] user@0.service		
	<ok> <cancel></cancel></ok>		

#### # Once done updating and upgrading, we can install Wazuh with this curl command.

curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a

#### # After installing Wazuh, take note of the username and password

💽 root@	Wazuh: ~		- 🗆
23/05/20	25 22:27:15	INFO:	Wazuh web interface port will be 443.
23/05/20	25 22:27:29	INFO:	Wazuh repository added.
23/05/20	25 22:27:30	INFO:	Configuration files
23/05/20	25 22:27:30	INFO:	Generating configuration files.
23/05/20	25 22:27:32	INFO:	Created wazuh-install-files.tar. It contains the Wazuh cluster key, cer
icates,	and passwor	ds nec	essary for installation.
23/05/20	25 22:27:32	INFO:	Wazuh indexer
23/05/20	25 22:27:32	INFO:	Starting Wazuh indexer installation.
23/05/20	25 22:28:50	INFO:	Wazuh indexer installation finished.
23/05/20	25 22:28:51	INFO:	Wazuh indexer post-install configuration finished.
23/05/20	25 22:28:51	INFO:	Starting service wazuh-indexer.
23/05/20	25 22:29:10	INFO:	wazuh-indexer service started.
23/05/20	25 22:29:10	INFO:	Initializing Wazuh indexer cluster security settings.
23/05/20	25 22:29:22	INFO:	Wazuh indexer cluster initialized.
23/05/20	25 22:29:22	INFO:	Wazuh server
23/05/20	25 22:29:22	INFO:	Starting the Wazuh manager installation.
23/05/20	25 22:30:15	INFO:	Wazuh manager installation finished.
23/05/20	25 22:30:15	INFO:	Starting service wazuh-manager.
23/05/20	25 22:30:35	INFO:	wazuh-manager service started.
23/05/20	25 22:30:35	INFO:	Starting Filebeat installation.
23/05/20	25 22:30:42	INFO:	Filebeat installation finished.
23/05/20	25 22:30:43	INFO:	Filebeat post-install configuration finished.
23/05/20	25 22:30:43	INFO:	Starting service filebeat.
23/05/20	25 22:30:44	INFO:	filebeat service started.
23/05/20	25 22:30:44	INFO:	Wazuh dashboard
23/05/20	25 22:30:44	INFO:	Starting Wazuh dashboard installation.
23/05/20	25 22:31:32	INFO:	Wazuh dashboard installation finished.
23/05/20	25 22:31:32	INFO:	Wazuh dashboard post-install configuration finished.
23/05/20	25 22:31:32	INFO:	Starting service wazuh-dashboard.
23/05/20	25 22:31:32	INFO:	wazuh-dashboard service started.
23/05/20	25 22:32:03	INFO:	Initializing Wazuh dashboard web application.
23/05/20	25 22:32:04	INFO:	Wazuh dashboard web application initialized.
23/05/20	25 22:32:04	INFO:	Summary
23/ <mark>05/26</mark>	25 22:32:04	TNFO:	You can access the web interface https:// <wazuh-dashboard-ip>:443</wazuh-dashboard-ip>
User	r: admin		
Pass	word: 8Z0xf	apRTGX	qCUcwoLmbAx0AjSjDXW9+
23/ 35/ 26		TNEO	Installation finished
root@Waz	uh:~# _		

#### # Navigate to the IP address of your droplet

Use either https://<IP> or the <IP>:443 to confirm you can reach the Wazuh dashboard



# with "<IP>" being the public IP of your Wazuh server.

#### Section 2 - TheHive Case Management Solution Initial Setup

To start setting up TheHive, let us create a new droplet. Screenshots are omitted as these steps mirror the Wazuh Server setup process.

Back in the dashboard, click on "Create", then select "Droplets."

Select the region closest to you. I selected "New York".

For the OS: Ubuntu, Version: 22.04 (LTS) x64

Droplet Type: Basic CPU options: Premium Intel \$48 option for 8GB of memory

Authentication Method: Password (Input a strong password)

Hostname thehive

Subsection - TheHive Firewall

After creating the droplet, you should be redirected to your project listing both droplets. Let us add "thehive" to a firewall group.

first-project DEFAULT Update your project information	→ Move Resources								
Resources Activity Settings	Resources Activity Settings								
DROPLETS (2)									
• 👌 thehive	● <b>()</b> thehive 165.227.197.170 + <b>()</b> Upsize ····								
• 👌 Wazuh	137.184.97.114	+ 🥹 + 👌 Upsize •••							
Create an Al agent         Fully-managed Al agent         development         Create a Managed Database         Worry-free database management         Spin up a Load Balancer         Distribute traffic between multiple         Droplets	Create a GPU Droplet         Virtualized GPUs available on demand         Start using Spaces         Deliver data with scalable object storage	Learn more Product Docs Technical overviews, how-tos, release notes, and support material Tutorials DevOps and development guidelines API & CLI Docs Run your resources programmatically Ask a question Connect, share and learn							

We can add TheHive to the Wazuh-Firewall by clicking on TheHive's droplet.

Select "networking" on the left-hand side.

Scroll down to find the "Firewall" section, then click on "Edit".

Click on the firewall, select the "Droplets" tab. Then click on the "Add Droplet" button.

Type in "**thehive**", click on it, then click on the "**Add Droplet**" button.

← Back to Firewalls								
Wazuh-Firewall 5 Rules / 2 Droplets								
Rules Droplets Destroy								
				Learn 🖻				
				Add Droplets				
Name	IP Address	State	Added					
Wazuh 8 GB / 2 Intel vCPUs / 160 GB / NYC1	137.184.97.114	Up-to-date	2 hours ago	More ∨				
8 GB / 2 Intel vCPUs / 160 GB / NYC1	165.227.197.170	Up-to-date	Just now	More ∨				

Subsection - Initial Commands in TheHive

Log in to TheHive server using SSH on your Windows terminal. You can use Putty as well.

# The command format is "ssh <user>@<IP>
# Capitalization matters
# ssh root@<IP>

Accept key fingerprints

Once connected via SSH, run an apt update and upgrade on the system.



Click "ENTER" on any red screens.

Once done updating, we need to get 4 components for this server. (Java, Cassandra, ElasticSearch, and TheHive) Run these commands one by one for these components.

#### # For Java, 6 commands, click ENTER on any red screens:

wget -qO- https://apt.corretto.aws/corretto.key | sudo gpg --dearmor -o /usr/share/keyrings/corretto.gpg

echo "deb [signed-by=/usr/share/keyrings/corretto.gpg] https://apt.corretto.aws stable main" | sudo tee -a /etc/apt/sources.list.d/corretto.sources.list

sudo apt update

sudo apt install java-common java-11-amazon-corretto-jdk

echo JAVA\_HOME="/usr/lib/jvm/java-11-amazon-corretto" | sudo tee -a /etc/environment

export JAVA\_HOME="/usr/lib/jvm/java-11-amazon-corretto"

#### # For Cassandra, 4 commands, click ENTER on any red screens:

wget -qO - https://downloads.apache.org/cassandra/KEYS | sudo gpg --dearmor -o /usr/share/keyrings/cassandra-archive.gpg

echo "deb [signed-by=/usr/share/keyrings/cassandra-archive.gpg] https://debian.cassandra.apache.org 40x main" | sudo tee -a /etc/apt/sources.list.d/cassandra.sources.list

sudo apt update

sudo apt install cassandra

#### # For ElasticSearch, 5 commands, click ENTER on any red screens:

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

sudo apt-get install apt-transport-https

echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list

sudo apt update

sudo apt install elasticsearch

#### # For TheHive, 4 commands, click ENTER on any red screens:

wget -O- https://archives.strangebee.com/keys/strangebee.gpg | sudo gpg --dearmor -o /usr/share/keyrings/strangebee-archive-keyring.gpg

echo 'deb [signed-by=/usr/share/keyrings/strangebee-archive-keyring.gpg] https://deb.strangebee.com thehive-5.2 main' | sudo tee -a /etc/apt/sources.list.d/strangebee.list

sudo apt-get update

sudo apt-get install -y thehive

#### # After running those commands, make a new file that will help with Elasticsearch.

Vim /etc/elasticsearch/jvm.options.d/jvm.options

#### # And here is what to put in that file

-Dlog4j2.formatMsgNoLookups=true -Xms2g -Xmx2g

-Dlog4j2.formatMsgNoLookups=true	
V0-	
-xmszg	
-Ymy2g	
-////28	
~	
~	
N	
~	
~	

# Press "Escape" on your keyboard, and type in ":wq" to save and exit Vim.

#### # After that, do these commands individually

Systemctl stop elasticsearch Rm -rf /var/lib/elasticsearch/\* Systemctl start elasticsearch Systemctl restart thehive

🕲 Wazuh X 🛞 TheHive - Login	x (+)	- 🗆 X
← → C බ ▲ Not secure 165.227.197.170:9000/log	jin 🖈 🍺 🗟 🖷 🕲 😽 🗘 🗌	[Cā   =J 🚥 :
🔡   💙 Titan 🗎 MySite 干 JobSheet 🖿 WCS 🖿 Index	🖬 Ln 👖 JFNG 🚔 THM 😧 XINTRA LABS 🎧 Ai 🎧 CTF-notes	💭 Nishang 🛛 »
	Hello, Sign in to start your session	Image: Without a start
	I forgot my password	

After that, we should be able to navigate to the public IP of our Hive server on port 9000.

#### Section 3 - TheHive Additional Configurations

Going back to the SSH terminal for TheHive, we need to change some configurations for the components of the server.

```
Subsection - Cassandra Configurations
```

The first changes will be tied to Cassandra.

#### # Nano into Cassandra's YAML file

Nano /etc/cassandra/cassandra.yaml

The first thing that I changed was the cluster name from "**Test Cluster**" to "**VCResearch**". You can leave it or change it to something you like.

	🔊 root@thehive: ~
	GNU nano 6.2 /etc/cassandra/cassandra.yaml *
;#	Cassandra storage config YAML
# # # #	NOTE: See https://cassandra.apache.org/doc/latest/configuration/ for full explanations of configuration directives /NOTE
# # C	The name of the cluster. This is mainly used to prevent machines in one logical cluster from joining another. Luster_name: 'VCResearch'
# # # # #	This defines the number of tokens randomly assigned to this node on the ring The more tokens, relative to other nodes, the larger the proportion of data that this node will store. You probably want all nodes to have the same number of tokens assuming they have equal hardware capability.
# # #	If you leave this unspecified, Cassandra will use the default of 1 token for legacy compa and will use the initial_token as described below.
* # # #	Specifying initial_token will override this setting on the node's initial start, on subsequent starts, this setting will apply even if initial token is set.
# # #	See https://cassandra.apache.org/doc/latest/getting_started/production.html#tokens for best practice information about num_tokens.
'n	m_tokens: 16

After changing the cluster name, click on the "**CTRL+W**" keys to activate the search functionality of Nano. Type in "**listen\_address**" and click "**ENTER**." This will take you to the spot as shown below.

Replace the localhost with the public IP address of TheHive.

🖭 root@thehive: ~	
GNU nano 6.2 /et	c/cassandra/cassandra.yaml *
<pre># impacting read latencies. Almost always a good id # necessarily on platters. trickle_fsync: false trickle_fsync_interval_in_kb: 10240</pre>	ea on SSDs; not
# TCP port, for commands and data # For security reasons, you should not expose this storage_port: 7000	port to the internet. Firewall it if needed.
<pre># SSL port, for legacy encrypted communication. Thi # server_encryption_options (see below). As of cass # as a single port can be used for either/both secu # For security reasons, you should not expose this ssl_storage_port: 7001</pre>	s property is unused unless enabled in andra 4.0, this property is deprecated re and insecure connections. port to the internet. Firewall it if needed.
<pre># Address or interface to bind to and tell other Ca # You _must_ change this if you want multiple nodes #</pre>	ssandra nodes to connect to. to be able to communicate!
<pre># Set listen_address OR listen_interface, not both. #</pre>	
<pre># Leaving it blank leaves it up to InetAddress.getL # will always do the Right Thing _if_ the node is p # (hostname, name resolution, etc), and the Right T # address associated with the hostname (it might no # it will fall back to InetAddress.getLoopbackAddre #</pre>	ocalHost(). This roperly configured hing is to use the t be). If unresolvable ss(), which is wrong for production systems.
# Setting listen_address to 0.0.0.0 is always wrong #	
.isten_address: localhost	
<pre># Set listen_address OR listen_interface, not both. # to a single address, IP aliasing is not supported # listen_interface: eth0</pre>	Interfaces must correspond
# If you choose to specify the interface by name an # you can specify which should be chosen using list	d the interface has an ipv4 and an ipv6 address en_interface_prefer_ipv6. If false the first i
<sup>∧G</sup> Help <sup>∧O</sup> Write Out <sup>∧W</sup> Where Is <sup>∧K</sup> Cut <sup>∧X</sup> Exit <sup>∧R</sup> Read File <sup>∧\</sup> Replace <sup>∧U</sup> Pas	^T Execute <sup>∧</sup> C Location M-U Under te <sup>∧</sup> J Justify <sup>∧</sup> / Go To Line M-E Rede

After inputting the listen address, scroll down or do the search feature again for "**rpc\_address**", and replace localhost with the public IP of TheHive.

🔤 root@thehive: ~	
GNU nano 6.2	/etc/cassandra/cassandra.yaml *
# nor writes for a time period. #	
# Clients may implement heartbeats by se # will reset idle timeout timer on the s # values for heartbeat intervals have to #	nding OPTIONS native protocol message af erver side. To close idle client connect be set on the client side.
<pre># Idle connection timeouts are disabled # native_transport_idle_timeout_in_ms: 6</pre>	by default. 0000
# The address or interface to bind the n #	ative transport server to.
<pre># Set rpc_address OR rpc_interface, not #</pre>	both.
<pre># Leaving rpc_address blank has the same # (i.e. it will be based on the configur #</pre>	effect as on listen_address ed hostname of the node).
<pre># Note that unlike listen_address, you c # set broadcast_rpc_address to a value o #</pre>	an specify 0.0.0.0, but you must also ther than 0.0.0.0.
<pre># For security reasons you should not e pc_address: localhost_</pre>	xpose this port to the internet. Firewa
<pre># Set rpc_address OR rpc_interface, not # to a single address, IP aliasing is no # rpc_interface: eth1</pre>	both. Interfaces must correspond t supported.
<pre># If you choose to specify the interface # you can specify which should be chosen # address will be used. If true the firs # ipv4. If there is only one address it</pre>	by name and the interface has an ipv4 a using rpc_interface_prefer_ipv6. If fal t ipv6 address will be used. Defaults to

After inputting the rpc\_address, use the search functionality to search for "**seed\_provider**". Replace the 127.0.0.1 with the public IP of TheHive. Keep the port after the IP.

os. root(	⊉thehive: ~	
GNU n	ano 6.2	/etc/cassandra/cassandra.yaml *
# Compr # Note #	ession to apply to SSTables as they f that tables without compression enabl	lush for compressed tables. ed do not respect this flag.
" # As hi # block # compr #	gh ratio compressors like LZ4HC, Zstd flushes for too long, the default is essor in those cases. Options are:	, and Deflate can potentially to flush with a known fast
# none # fast # # table #	<ul> <li>Flush without compressing blocks but</li> <li>Flush with a fast compressor. If the fast compressor that compressor is</li> <li>Always flush with the same compressor was the pre 4.0 behavior.</li> </ul>	t while still doing checksums. e table is already using a used. or that the table uses. This
# flush	_compression: fast	
# any c # const <u>s</u> eed_pr # A # C	lass that implements the SeedProvider ructor that takes a Map <string, strin<br="">ovider: ddresses of hosts that are deemed con assandra nodes use this list of hosts</string,>	interface and has a g> of parameters will do. tact points. to find each other and learn
# t # m	he topology of the ring. You must ch ultiple nodes!	ange this if you are running
- c	lass_name: org.apache.cassandra.locat	or.SimpleSeedProvider
	<pre># seeds is actually a comma-delimi # Ex: "<in1> <in2> <in3>" - seeds: "127.0.0.1:7000"</in3></in2></in1></pre>	ted list of addresses.
# For w # bottl # disk.	orkloads with more data than can fit eneck will be reads that need to fetc "concurrent_reads" should be set to	in memory, Cassandra's h data from (16 * number_of_drives) in

After those changes, on your keyboard, click on "ctrl+x" and Y to save, and then click "ENTER" to exit

#### # Run these commands after exiting the YAML file.

Systemctl stop cassandra.service Rm -rf /var/lib/cassandra/\* Systemctl start cassandra.service Systemctl status cassandra.service Subsection - ElasticSearch Configurations.

# Nano into the Elasticsearch yml file

Nano /etc/elasticsearch/elasticsearch.yml

After opening the file, uncomment "cluster.name" and replace "my-application" with "thehive".

After that, uncomment "node.name".

ा. root@thehive: ~	
GNU nano 6.2	<pre>/etc/elasticsearch/elasticsearch.yml *</pre>
# ====================================	Elasticsearch Configuration =================================
<pre># NOTE: Elasticsearch comes # Before you set out # understand what are #</pre>	with reasonable defaults for most settings. to tweak and tune the configuration, make sure you you trying to accomplish and the consequences.
# The primary way of confi # the most important settin #	guring a node is via this file. This template lists ngs you may want to configure for a production cluster.
<pre># Please consult the docume # https://www.elastic.co/gu #</pre>	entation for further information on configuration options: uide/en/elasticsearch/reference/index.html
# #	Cluster
# Use a descriptive name fo #	or your cluster:
:luster.name: thehive	
# #	Node
# Use a descriptive name fo #	or the node:
node.name: node-1	
# Add custom attributes to #	the node:
#node.attr.rack: r1 #	
#	Paths

Scroll down a bit past the "**paths and memory**" sections to the "**Network**" section and uncomment "**network.host**" and replace the placeholder IP with the public IP of TheHive.

Then, uncomment "cluster.initial\_master\_nodes" and delete "node\_2" from the array.

🖭 root@thehive: ~						
GNU nano 6.2 /etc/elast	icsearch/elasticsearch.yml *					
# Elasticsearch performs poorly when the system is swa #	pping the memory.					
# Network #						
<pre># By default Elasticsearch is only accessible on local # address here to expose this node on the network: #</pre>	host. Set a different					
network.host: 192.168.0.1						
<pre># By default Elasticsearch listens for HTTP traffic on # finds starting at 9200. Set a specific HTTP port her #</pre>	the first free port it e:					
#http.port: 9200 #						
<pre># For more information, consult the network module doc #</pre>	umentation.					
# Discovery #						
<pre># Pass an initial list of hosts to perform discovery w # The default list of hosts is ["127.0.0.1", "[::1]"] #</pre>	# Pass an initial list of hosts to perform discovery when this node is started: # The default list of hosts is ["127.0.0.1", "[::1]"] #					
<pre>#discovery.seed_hosts: ["host1", "host2"] #</pre>						
# Bootstrap the cluster using an initial set of master #	-eligible nodes:					
<pre>cluster.initial_master_nodes: ["node-1"] #</pre>						
<pre># For more information, consult the discovery and clus #</pre>	ter formation module documentation.					
# Various #						
# Require explicit names when deleting indices: #						
<pre>#action.destructive_requires_name: true</pre>						

#### # After the changes, click "ctrl+x" and "Y" to save and click "ENTER" to exit

Systemctl start elasticsearch Systemctl enable elasticsearch Systemctl status elasticsearch

#### # Check the status of Cassandra and verify that it is running

Subsection - TheHive Configurations

#### # Check permissions on /opt/thp. If root is the owner of "thehive" change it

Is -la /opt/thp Chown -R thehive:thehive /opt/thp

root@thehive:~# ls -la /opt/thp							
total 12							
drwxr-xr-x 3	root roo	t 4096 M	lay 24	00:53			
drwxr-xr-x 5	root roo	t 4096 M	lay 24	00:53			
drwxr-xr-x 5	root roo	t 4096 M	lay 24	00:53	thehiv	'e	
root@thehive	:∼# cnown	-R theh	ive:t	nehive	/opt/t	:hp	
root@thehive	:~# ls -1	a /opt/t	hp				
total 12							
drwxr-xr-x 3	thehive	:hehive	4096 N	lay 24	00:53		
drwxr-xr-x 5	root	root	4096 N	lay 24	00:53		
drwxr-xr-x 5	thehive	:hehive	4096 N	lay 24	00:53	thehive	
root@thehive:~#							

#### # Confirm change

ls -la /opt/thp

#### # Nano into application.conf

Nano /etc/thehive/application.conf

Once inside of the application configuration file, scroll down to find the database and index configuration section.

Under "**db.janusgraph**", it will have a "**hostname**" with the IP of "**127.0.0.1**", change it to the public IP of TheHive.

A bit lower, it will have a "cluster-name" section. I changed it to "VCResearch" to match the cluster name I put in the other config files.

Under "index.search", it will have a "hostname" with the IP of "127.0.0.1", change it to the public IP of TheHive

🔤 root@thehive: ~	
GNU nano 6.2	<pre>/etc/thehive/application.com</pre>
<pre># # # # Secret key - used by Play # If TheHive is installed w # If TheHive is not install # command before starting t # cat &gt; /etc/thehive/secre # play.http.secret.key="\$ # _EOF_ include "/etc/thehive/secre</pre>	Framework ith DEB/RPM package, this is automatically genera ed from DEB or RPM packages run the following hehive: et.conf << _EOF_ (cat /dev/urandom   tr -dc 'a-zA-Z0-9'   fold -w t.conf"
<pre># Database and index config # By default, TheHive is co # local Elasticsearch servi db.janusgraph { storage { hostname = ["127.0.0.1"</pre>	uration nfigured to connect to local Cassandra 4.x and a ces without authentication. ]
<pre># Cassandra authenticat # username = "thehive" # password = "password" col {     cluster-name = thp     keyspace = chenive }</pre>	ion (if configured)
<pre>     }     index.search {         hostname = ["127.0.0.1"         index-name = chenive     } }</pre>	]
}	

After those changes, scroll down and look for "**application.baseurl**", it will have a URL pointing to localhost.

Change it to...

application.baseURL= "http://<TheHivePublicIP>:9000"

```
🖏 root@thehive: ~
 GNU nano 6.2
                                                /etc/thehive/application.co
   # password = "password"
   cql {
     cluster-name = VCResearch
     keyspace = thehive
 index.search {
   backend = elasticsearch
   hostname = ["165.227.197.170"]
   index-name = thehive
# Attachment storage configuration
 By default, TheHive is configured to store files locally in the folder.
 The path can be updated and should belong to the user/group running thehi
storage {
 provider = localfs
 localfs.location = /opt/thp/thehive/files
Define the maximum size for an attachment accepted by TheHive
play.http.parser.maxDiskBuffer = 1GB
Define maximum size of http request (except attachment)
play.http.parser.maxMemoryBuffer = 10M
Service configuration
pplication.baseUrl = "http://localhost:9000"
                                                          ay meep concert
 Additional modules
 TheHive is strongly integrated with Cortex and MISP.
```

#### # ctrl+x and Y to save and ENTER to exit

Systemctl start thehive Systemctl enable thehive Systemctl status thehive

# Check the status of Cassandra, Elasticsearch, and TheHive. Confirm all are running

#### Section 4 - Linux Victim Honeypot Initial Setup and Agent Deployment

Let us deploy our Victim machine on DigitalOcean.

Click on the "Create" Button and select "Droplets" from the drop-down menu.



Select the region closest to you. I selected "New York".

For the OS: Ubuntu, Version: 22.04 (LTS) x64

Droplet Type: Basic CPU options: Regular \$18 option

Authentication Method: Password (Input a strong password)

Hostname VCResearch-Linux
Subsection - Honeypot Firewall

Once you have created your droplet, let us make a firewall rule for it. Click on your new droplet.

first-project DEFAULT Update your project informat	first-project DEFAULT Update your project information under Settings					
Resources Activity Settings						
DROPLETS (3)						
• <b>VCResearch-Linux</b>	104.248.120.94		+ 🥪	+0	Upsize	•••
• 💧 thehive	165.227.197.170		+ 🥪	+0	Upsize	•••
• 💧 Wazuh	137.184.97.114		+ 😔	+0	Upsize	

On the left-hand side, click on "**Networking**". Scroll down to find the "**Firewalls**" section and click on the "**Edit**" button.

Then click on the "**Create Firewall**" button.

Domains	Reserved IPs	Load Balancers	VPC	Multi-cloud	integrations	Firewalls	PTR records	
								Create Firewall
Name		ſ	Droplets		Rules	Cre	ated	
wa	azuh-Firewall	:	2		5	4 da	ays ago	More ∨

I named this firewall "VCResearch-Linux-Firewall". It is separate from the other servers because I will be exposing it to the internet once everything is up and running.

Just like the first firewall we created, we want to set two rules to allow all inbound TCP and UDP traffic to be allowed from our actual IP address.

# In addition to our real IP, add the IP address for the Wazuh Server.

Create Firewall		Learn 🛃
Name	_	
Name VCResearch-Linux-Firewall	~	
	•	

## Inbound Rules

Set the Firewall rules for incoming traffic. Only the specified ports will accept inbound connections. All other traffic will be dropped.

Туре		Protocol	Port Range	Sources	
SSH	~	ТСР	22	All IPv4 All IPv6	Delete
New rule	~				

Once you have created the two rules, you can scroll down and apply the firewall to the Droplet we created. Once done with that, click on "**Create Firewall**".

All TCP	✓ TCP	All ports	All IPv4 All IPv6	Delete
All UDP	∨ UDP	All ports	All IPv4 All IPv6	Delete
New rule	~			
Apply to D	roplots			

Apply to Droplets

Select Droplets to apply your Firewall rules to.

<ul> <li>VCResearch-Linux</li> <li>Search for a Droplet or a tag</li> </ul>		
	Create Firewall	

#### Subsection - Agent Deployment

After creating and applying the new firewall, we need to log into the Wazuh Dashboard to get started on setting up the agent on the new Linux host. You will have to use the credentials that were given to you when you finished installing Wazuh.

 $\equiv$  $\triangle$ wazuh. 🗸 Modules а ? Total agents Active agents Disconnected Pending agents Never connected agents agents 0 0 0 0 Add agent ▲ No agents were added to this manager SECURITY INFORMATION MANAGEMENT AUDITING AND POLICY MONITORING Ϋ́ System auditing m Security events ⊨ Integrity Policy monitoring monitoring Browse through your Verify that your systems Audit users behavior, are configured security alerts. monitoring command Alerts related to file identifying issues and according to your execution and alerting changes, including threats in your security policies on access to critical permissions, content, baseline environment. files. ownership and attributes. Security configuration assessment Scan your assets as part of a configuration assessment audit.

Once logged in and on the dashboard, click on "Add agent".

Under Linux, select "DEB amd64".

For the Server address, input the Wazuh Public IP address.

I did not add an Agent name as the hostname is fine.

Step 4 will contain the commands you need to run to set up the agent. So, let us connect to the Linux machine via SSH and do that.

👌 LINUX		🗰 macOS
RPM amd64     RPM aarch64       DEB amd64     DEB aarch64	O MSI 32/64 bits	Intel Apple silicon
③ For additional systems and archite	ctures, please check our document	ation @.
Server address:		
This is the address the agent uses to cor name (FDQN).	nmunicate with the server. Enter an	IP address or a fully qualified do
This is the address the agent uses to cor name (FDQN). Assign a server address: ⑦	nmunicate with the server. Enter an	IP address or a fully qualified do
This is the address the agent uses to cor name (FDQN). Assign a server address: ⑦ 137.184.97.114	nmunicate with the server. Enter an	IP address or a fully qualified do
This is the address the agent uses to cor name (FDQN). Assign a server address: ⑦ 137.184.97.114	nmunicate with the server. Enter an	IP address or a fully qualified do
This is the address the agent uses to cor name (FDQN). Assign a server address: 137.184.97.114 Optional settings:	nmunicate with the server. Enter an	IP address or a fully qualified do
This is the address the agent uses to cor name (FDQN). Assign a server address: ③ 137.184.97.114 Optional settings: By default, the deployment uses the host the field below.	nmunicate with the server. Enter an	IP address or a fully qualified do
This is the address the agent uses to cor name (FDQN). Assign a server address: ⑦ 137.184.97.114 Optional settings: By default, the deployment uses the host the field below. Assign an agent name: ⑦	nmunicate with the server. Enter an	IP address or a fully qualified do y, you can use a different agent r

On the Linux machine, once logged in for the first time. Run an **"apt-get update && apt-get upgrade"**. Click **"ENTER**" on any red screens.

The output after running the agent deployment commands should look like the output below.



On the "**deploy new agent**" page on Wazuh, it will allow you to copy the commands, but I recommend running them one by one manually. Running them all at once can lead to issues.

#### # Commands are:

Systemctl daemon-reload Systemctl enable wazuh-agent Systemctl start wazuh-agent

# # Confirm agent is running with:

Systemctl status wazuh-agent

We will need to allow Wazuh to be able to communicate with the agent. We need to change the firewall rules that are applied to Wazuh.

On DigitalOcean, click on your Wazuh Droplet.



On the left-hand side, click on "networking". Then scroll down to the firewall section.

Click on "Wazuh-Firewall".



Once you are in the "**Rules**" page for the firewall, on the far-right side of the inbound rules, there will be a "**More**" dropdown. Click on it and select "**Edit**". Type in the Agent IP address and click "**ENTER**". Do this for the TCP and UDP rules.

Once you save those changes and check back in your Wazuh dashboard, you should be able to see an active agent.

$\equiv$ $\triangle$ wazuh. $\vee$ Modules				a 0
Total agents Active agents	Disconnected agents	Pending agents	Never connected agents	
SECURITY INFORMATION MANAGEMENT		AUDITING AN	D POLICY MONITORING	
Security events Browse through your security alerts, identifying issues and threats in your environment. Integrity Monitoring Alerts related to file changes, including permissions, content, ownership and attributes.	Ϋ́Ϋ́Ϋ́	Policy monitoring Verify that your systems are configured according to your security policies baseline.	System audit Audit users behav monitoring comme execution and alle on access to critic files.	ing rior, and rting :al
	Ģ	Security configuration assessment Scan your assets as part of a configuration assessment audit.		

## Section 5 - Wazuh XDR Server Configurations

After deploying our agent, we need to do some additional configurations on the Wazuh Server.

#### # On the Wazuh Server, create a backup for ossec.conf in case of any mistakes

cp /var/ossec/etc/ossec.conf ~/ossec-backup.conf

# nano into the ossec file on the Wazuh server

nano /var/ossec/etc/ossec.conf

### # In the file, change these

Logall from "no" to "yes" Logall\_json "no" to "yes"

#### # ctrl+x and Y to save, and ENTER to exit

Systemctl restart wazuh-manager.service

👞 root@Wazuh: ~	
GNU nano 6.2	<pre>/var/ossec/etc/ossec.conf *</pre>
<br Wazuh - Manager - Default com More info at: https://documen Mailing list: https://groups. >	figuration for ubuntu 22.04 tation.wazuh.com google.com/forum/#!forum/wazuh
<pre><ossec_config>     <global>     <jsonout_output>yes<td>t_output&gt; on&gt; ii_notification&gt; azuh.com azuh.com .wazuh.com _maxperhour&gt; g 10m _time&gt;0</td></jsonout_output></global></ossec_config></pre>	t_output> on> ii_notification> azuh.com azuh.com .wazuh.com _maxperhour> g 10m _time>0
<alerts> <log_alert_level>3<email_alert_level>12</email_alert_level></log_alert_level></alerts>	rt_level> l_alert_level>
Choose between "plain",<br <logging></logging>	"json", or "plain,json" for the format of interr

Subsection - Wazuh Logs, Archives, and Filebeat

## # Just a note that Wazuh logs can be found at "/var/ossec/logs/archives"

## # To start ingesting these logs, we need to modify the filebeat file.

nano /etc/filebeat/filebeat.yml

## # Scroll down until you find filebeat modules, archives will be on "false", swap to "true"

🖭 root@Wazuh: ~				
GNU nano 6.2			/etc/filebe	at/filebeat.yml
<pre># Wazuh - Filebea output.elasticsea</pre>	t configurati rch.hosts: .1:9200 icsearch_ip_r icsearch_ip_r	ion file node_2>:9200 node_3>:9200		
<pre>output.elasticsea protocol: https username: \${use password: \${pas ssl.certificate - /etc/filebe ssl.certificate ssl.key: "/etc/ setup.template.js setup.template.js setup.ilm.overwri setup.ilm.enabled</pre>	<pre>rch: rname} sword} _authorities: at/certs/root : "/etc/fileb filebeat/cert on.enabled: t on.path: '/et on.name: 'waz te: true : false</pre>	: t-ca.pem beat/certs/wazuh ts/wazuh-server- true tc/filebeat/wazu zuh'	-server.pem" key.pem" h-template.jso	n'
<pre>filebeat.modules:     - module: wazuh     alerts:         enabled: te         archives:_         enabled: tr logging.level: in logging.to_files: logging.files:     path: /var/log/</pre>	ue ue fo true filebeat			
^G Help ^ ^X Exit ^	O Write Out R Read File	^₩ Where Is ^\ Replace	<mark>^K</mark> Cut ^U Paste	<pre>^T Execute ^J Justify</pre>

## # ctrl+x and Y to save, and ENTER to exit

Systemctl restart filebeat

## # After that, go to the Wazuh dashboard, and click on the hamburger in the top left corner.

# Select "Stack Management" near the bottom.

= 🗅 🛛 wazuh. 🗸	Modules			
Recently viewed No recently viewed items	<ul> <li>Active agents</li> <li>1</li> </ul>			Never con agen
W. Wazuh	~	0		
Wazuh	NAGEMENT		AUDITING ANI	POLICY
OpenSearch Dashboards Discover Dashboard Visualize	<ul> <li>Integrity monitoring</li> <li>Alerts related to file changes, including permissions, content, ownership and attributes.</li> </ul>	ļļļ	Policy monitoring Verify that your systems are configured according to your security policies baseline.	C
OpenSearch Plugins Reporting Alerting Maps Notifications Index Management	× _	Ð	Security configuration assessment Scan your assets as part of a configuration assessment audit.	
Snapshot Management				
Security	TESPONSE		REGULAT	ORY COMP
Dev Tools Stack Management	MITRE ATT&CK Security events from the knowledge base of adversary tactics and techniques based on		PCI DSS Global security standard for entities that process, store or transmit payment cardholder	5

Then click on "**Index pattern**", after that click on the "**create index**" button. Name it "**wazuh-archives-\***", and then click on "Next Step".

Create index pattern	
An index pattern can match a single source, for example, filebeat-4-3-22, or <b>multiple</b> dation filebeat-*.	ata sources,
Read documentation 🖄	
Step 1 of 2: Define an index pattern	
Index pattern name	
wazuh-archives-**	Next step >
Use an asterisk (*) to match multiple indices. Spaces and the characters  /, ?, ", <, >,   are not allowed.	
○ × Include system and hidden indices	
<ul> <li>✓ Your index pattern matches 1 source.</li> </ul>	
wazuh-archives-4.x-2025.05.27	x
Rows per page: 10 $$	

For "Time field" select "timestamp". Then click on the "Create Index Pattern" button.

Click on the top left hamburger, then click on Discover.

You will see "wazuh-alerts" with a drop-down arrow. Click on it and select the index we just made.

This is where we will be keeping an eye out for our events

## Section 6 - Wazuh Detection Rule Creation

We are going to create a custom rule to detect SSH brute-force attacks.

Let us navigate back to the Wazuh dashboard.

Click on the home icon in the top left  $\rightarrow$  Click on the down Arrow to the right of "**Wazuh**"  $\rightarrow$  Click on "**Management**"  $\rightarrow$  "**Rules**"  $\rightarrow$  "**Manage rule file**"  $\rightarrow$  "**Custom Rules**" button on the right  $\rightarrow$  Click on the pencil for Local\_rules.

You should see the file shown below.

```
< local_rules.xml</pre>
                                                                                                  Ruleset Test
   1 <!-- Local rules -->
   2
   3 <!-- Modify it at your will. -->
  4 <!-- Copyright (C) 2015, Wazuh Inc. -->
  6 <!-- Example -->
  7 - <group name="local,syslog,sshd,">
  8
  9 -
      <!--
      Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
 10
 11
       -->
 12 - <rule id="100001" level="5">
       <if_sid>5716</if_sid>
<srcip>1.1.1.1</srcip>
 13
 14
        <description>sshd: authentication failed from IP 1.1.1.1.</description>
 15
 16
         <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
 17 </rule>
 18
  19 </group>
 20
```

Subsection - SSH Bruteforce Rule

The rule there will be the one that inspires our own rule. This is the one I will be using.

#### Template for SSH Bruteforce and secondary critical rule for successful logins # Be advised: If you copy and paste, the wrong variant of quotation marks may be used. # Swap them out in the XML file.

```
<rule id="100003" level="13" frequency="3" timeframe="30">
	<if_matched_sid>5710</if_matched_sid>
	<same_source_ip />
	<description>multiple SSH authentication failures from same IP</description>
	<group>authentication_failed</group>
	<mitre>
	<id>T1110</id>
	</mitre>
	</rule>
```

```
<rule id="100005" level="15">
<if_sid>5715</if_sid>
<match>^Accepted|authenticated.$</match>
<description>sshd: authentication success.</description>
<group>authentication_success</group>
</rule>
```

#### ####

#### Once done inputting the rule, click "Save" on the upper right.

After saving, it will want you to restart the manager.



Section 7 - MISP Threat Intelligence Platform Solution initial setup

It is time to launch MISP. Just like the other droplets...

In the main dashboard on DigitalOcean, click on "Create", then "Droplets."

Select the region closest to you. I selected "New York".

For the OS: Ubuntu, Version: 22.04 (LTS) x64

Droplet Type: Basic CPU options: Premium Intel \$48 option for 8GB of memory

Authentication Method: Password (Input a strong password)

Hostname: misp

**# The link below is the official MISP GitHub in case you run into any issues I do not cover.** Helpful Link: Source: https://misp.github.io/MISP/xINSTALL.ubuntu2204

Once you have created the VM, click on "**misp**". On the left-hand side, click on "**networking**". Scroll down to the firewall section and click "**Edit**".

Create a New Firewall for MISP.

I named mine "**misp-Firewall**". For the inbound rules, allow all TCP and UDP from your IP address and TheHive's IP address.

Once done creating the rules, scroll down and apply the firewall to the "misp" droplet.

## Create Firewall

Name



## Inbound Rules

Set the Firewall rules for incoming traffic. Only the specified ports will accept inbound connections. All other traffic will be dropped

Туре		Protocol	Port Range	Sources	
All TCP	~	ТСР	All ports	165.227.197.170	
All UDP	~	UDP	All ports	165.227.197.170	
New rule	~				

## Once the MISP VM is running, connect to it via SSH as root.

first-project DEFAUL Update your project informa	т tion under Settings		$\rightarrow$ M	Nove Resources
Resources Activity Settings				
DROPLETS (4)				
• 💧 misp	137.184.134.84	+0	+0	Upsize •••
O VCResearch-Linux	104.248.120.94	+0	+0	Upsize ····
• 💧 thehive	165.227.197.170	+0	+0	Upsize ····
• 💧 Wazuh	137.184.97.114	+0	+0	Upsize ····

# Once connected, run the commands below.

# These commands are to add the misp user, put them into the sudo group, then switch to that user.

adduser misp Usermod -aG sudo misp Su - misp

**# Once you are the misp user, do a ...** Sudo apt-get update

# The command below will install everything needed for misp, no sudo needed

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

# Run without sudo (Takes a while)
bash /tmp/INSTALL.sh -A

# Click "ENTER" on any red screens

# If asked to input the baseURL, put the public IP of the MISP cloud # instance. Ex. "https://<InstanceIP>" then hit enter

# In the case that it is needed,# Manual URL setup can be done here:# nano /var/www/MISP/app/Config/config.php# Change Base URL

# After the "install.sh" script is done. Run the following commands # Activate an interactive sudo shell.

Sudo -i

**# The below command will activate the virtual environment** Source /var/www/MISP/venv/bin/activate

**# The command below will install all MISP modules** pip install misp-modules[all]

# # The below is not needed but can be done to confirm that it is working.# Then you should be able to run "misp-modules" as a command

#### Subsection - Creating a persistent service

**# Run the below commands to get a service running** sudo vim /etc/systemd/system/misp-modules.service

[Unit] Description=MISP modules

[Service] Type=simple User=root ExecStart=/bin/bash -c 'source /var/www/MISP/venv/bin/activate && misp-modules' Restart=always RestartSec=10

[Install] WantedBy=multi-user.target

#### 

#### # Once done, do a ":wq!" to save and exit Vim



### # Enable and start the service

sudo systemctl daemon-reexec sudo systemctl enable misp-modules sudo systemctl start misp-modules

#### # Confirm

sudo systemctl status misp-modules

# If the service shows that it is not running, try to exit out to the root user again and run the "reboot" # command. Log in again as the user misp and rerun the status command.

#### Subsection - MISP login, Organization and User Creation

## # Log in with the default Email/Pass and change it

admin@admin.test

admin



Let us edit the default organization name. Click on "ORGNAME"

Edit My Profile Change Password

## User admin@admin.test

	ID	1
My Profile	Email	admin@admin.test
My Settings	Organisation	ORGNAME
Periodic summary settings	Role	admin
Set Setting	TOTO	
List Organisations	IOIP	No Generate
Role Permissions	Email notifications	Event published notification No
List Sharing Groups		Daily notifications No
Add Sharing Group		Weekly notifications No
List Sharing Group Blueprints		Monthly notifications No
Add Sharing Group Blueprint	Contact alert enabled	No
Categories & Types	Invited By	N/A
Terms & Conditions	NIDS Start SID	4000000
Statistics	PGP key	No
	Created	N/A
	Last password change	2025-05-28 01:01:14
	Download user profile f	for data portability Review user logs Review user logins
	Auth keys 🗹	
	Benchmarks 🛃	
	Events 🗹	

## Click on "Edit Organization"

Add User List Users	Organisatio	n orgname					
Pending registrations	ID	1					
User settings	UUID	15a14830-c3e0-43c3-	ba85-c6bb65	bf65bc			
Set Setting	Local or remote	Local					
Contact Users	Description	Automatically generate	ed admin org	anisation			
Add Organisation	Created by	Unknown					
Edit Organisation	Creation time	2025-05-28 00:16:20					
Merge Organisation	Last modified	2025-05-28 00:16:20					
View Organisation	Organisation type	ADMIN					
Delete Organisation List Organisations	Members Events Sha	ring Groups					
Add Role List Roles	Users index	[					
Server Settings & Maintenance	« previous next »						
Update Progress	ID Org Rol	e Email	181	0 👂	NIDS SID	*	Last Login
	1 ORGNAME adm	nin admin@admin.test )	< ×	×	4000000	×	2025-05-28 01:00
Jobs							

Change the name, I went with VC Research. Once done, scroll down and click on "Submit".

1100 0001							
List Users							
Pending registrations	Mandatory Fields						
User settings	✓ Local organisation						
Set Setting	$^-$ If the organisation should have access to this instance, make sure that the Local organisation setting						
Contact Users	is checked. If you would only like to add a known external organisation for inclusion in sharing groups, uncheck the Local organisation setting.						
Add Organisation	Organisation Identifier						
Edit Organisation	VC Research						
Merge Organisation	UUID						
View Organisation	15a14830-c3e0-43c3-ba85-c6bb65bf65bc Generate UUID						
Delete Organisation							
List Organisations	Optional Fields						
Add Role	A brief description of the organisation						
List Roles	Automatically generated admin organisation						
Server Settings &							
Maintenance							
Update Progress							
Jobs	Bind user accounts to domains (line separated)						
	Enter a (list of) domain name(s) to enforce when creating users.						
Scheduled Tasks							
Event Block Rules							
Blocklists Event							
Manage Event Blocklists							
	Logo (48×48 PNG)						
Blocklists Organisation	Choose File No file chosen						
Manage Org Blocklists	Nationality Sector						
Diockliste Giabtinas	Not specified   For example "financial".						

🥶 Wazuh - Wazuh	× 🚽 🗟 Users - MISP	× (+)				— C
← → C ⋒ ⊗ N	lot secure <u>https</u> ://137.184	.134.84/users/view/1	\$	Тр 👵	··· 6	រាន
믬 🛛 🔀 Titan 👌 MySite	🕂 JobSheet 🕂 WCS	🕆 Index in Ln 👖 JFNG 🕰 THM 😢 XIN	TRA LABS 👩 Ai 👩 CTF-notes	Nishang	宿 Discord - S	ichool 👿 D2I
Home Event Actions	Dashboard Galaxies	Input Filters Global Actions Sync Actions	Administration Logs API		Bookmarks <del>-</del>	★ MISP Ad
Password Changed.			List Users			
			List Auth Keys			
Edit My Profile	llser admin@	admin test	Set User Settings			
Change Password	User adminie	gaanninitest	Add User			
Mu Drofile	ID	1	Contact Users			
My Profile My Settings	Email	admin@admin.test	User Registrations			
Periodic summary settings	Organisation ORGNAME					
Set Setting	Role	admin	Add Organisations			
List Organisations	ТОТР	No Generate	-			
Role Permissions	Email notifications	Event published notification No	List Roles			
List Sharing Groups		Daily notifications No	Add Roles			
Add Sharing Group		Weekly notifications No	Server Settings & Maintenance			
Add Sharing Group Blueprints		Monthly notifications No				
	Contact alert enabled	No	Jobs			
Categories & Types	Invited By	N/A	Scheduled Tasks			
Terms & Conditions	NIDS Start SID	4000000	WORNOWS			
Statistics	PGP key	No	Event Block Rules	_		
	Created	N/A	Event Blocklists			
	Last password change	2025-05-28 01:01:14	Org Blocklists			
	Download user profile	for data portability Review user logs R	Top Correlations			
			Correlation rules			
	Auth keys 🛃		Over-correlating values			
	Benchmarks 🗹					

## Navigate to "Server Settings & Maintenance"

This is where you can see the overall health of the instance, plugins, and issues that may show up. In a production environment, I highly recommend going through all of it. But as I am just using this to test certain things out, I will not be worrying much about it.

Overview	MISP (16 🔥)	Encryption (4)	Proxy (5)	Security	Plugin (555 🔥)	SimpleBackgroundJobs	Correlations	new	Diagnostics	Manage files	-
Test		Value				Description					
Overall health		Critica attenti	l, your MISP i on.	nstance req	uires immediate	The overall health of your i	nstance depen	ds on the	e most severe u	Inresolved issue	S.
Critical setting	s incorrectly or n	ot set 3 inco	rect settings.			MISP will not operate corre	ectly or will be u	insecure	until these issu	ies are resolved.	
Recommende not set	d settings incorre	ctly or 542 in	correct setting	JS.		Some of the features of MI	SP cannot be u	utilised ur	ntil these issue	s are resolved.	
Optional settin	igs incorrectly or	not set 35 inc	orrect settings	i.		There are some optional tw instance.	veaks that coul	d be don	e to improve th	e looks of your N	<b>/</b> ISP
Critical issues diagnostics	revealed by the	0 issue	es detected.			Issues revealed here can b dependencies.	e due to incorr	ect direc	tory permissior	is or not correctly	y insta

## Server Settings & Maintenance

To edit a setting, simply double click it.

I recommend you go through the plugins to see all the enrichment modules available to use!

Since this project is based on taking in SSH brute-force IPs, in this project, I used the APIs mentioned below.

Some enrichment modules to consider. I used these 2 alongside the VirusTotal API.

#### # Ip2location.io

Create an account with them to get a 7-day trial. Once you confirm your email and go past the quickstart, you" be able to see your API key

#### # AbuseIPDB

Create an account and confirm your email. Then in the API tab, you will have an option to create an API key.



To enable the enrichment modules that we want, we need to go into the plugins tab.

Add User **Server Settings & Maintenance** List Users Overview MISP (16 A) Encryption (4) Proxy (5) Security Plugin (555 A) SimpleBackgroundJobs Pending registrations Correlatio Diagnostics Manage files User settings Filter the table(s) below Enrichment Set Setting Critical Plugin.Enrichment\_services\_enable true Enable/disable the enrichment services Contact Users Critical Plugin.Enrichment\_hover\_enable Enable/disable the hover over information retrieved from the false Add Organisation enrichment modules List Organisations Critical Plugin.Enrichment\_hover\_popover\_only false When enabled, users have to click on the magnifier icon to show the enrichment Add Role Recommended Plugin.Enrichment timeout 300 Set a timeout for the enrichment services List Roles Recommended Plugin.Enrichment\_hover\_timeout 150 Set a timeout for the hover services Recommended Plugin.Enrichment\_services\_url http://127.0.0.1 The url used to access the enrichment services. By default, it is accessible at http://127.0.0.1:6666 Maintenance Recommended Plugin.Enrichment\_services\_port 6666 The port used to access the enrichment services. By default, it is Update Progress accessible at 127.0.0.1:6666 Recommended Plugin.Enrichment\_ipqs\_fraud\_and\_risk\_scoring\_enabled [Enable or disable the ipqs\_fraud\_and\_risk\_scoring module.] Value Jobs false IPQualityScore MISP Expansion Module for IP reputation, Email not Validation, Phone Number Validation, Malicious Domain and set. Scheduled Tasks Malicious URL Scanner. Event Block Rules Recommended Plugin.Enrichment\_ipqs\_fraud\_and\_risk\_scoring\_restrict No organisation Restrict the ipgs fraud and risk scoring module to the given Value selected. organisation. not Blocklists Event set. Manage Event Blocklists nded. Diugin Enrichment inge fraud and rick cooring anikor Set this required module specific setting

In the top right, we can search for the plugins.

For Ip2location, we will need to enable the plug-in by switching it from false to true. We can leave the second line as it is. Then, we will enter our API key on the third line.

You can change the false by double-clicking on it and then clicking the checkmark.

Overview N	IISP (16 🛕)	Encryption	(4) Proxy (5	5) Security	Plugin (555 🛕)	SimpleBackgroundJobs	Correlations	new	Diagnostics	Manage	files 🛛 📥 W
Inrichment									ip2loca		
Recommende	d Plugin.Enric	chment_ip2l	ocationio_enabl	led false	[Enable IP2Loca	or disable the ip2location tion.io to gather more info	nio module.] Ar mation on a give	expar	ision module to q ddress.	uery	Value not set.
Recommende	d Plugin.Enric	chment_ip2l	ocationio_restri	ct No organis selected.	sation Restrict	the ip2locationio module to	o the given organ	nisatior	l.		Value not set.
Recommende	d Plugin.Enric	chment_ip2l	ocationio_key		Set this	required module specific s	etting.				Value not set.

For AbuseIPDB, you will have to

- 1 Activate it
- 2. Input API key
- 3. Put a max age in days, I put 90
- 4. Abuse Threshold 60

Subsection - Manual Enrichment

After putting in the two APIs, I went out and grabbed an IP that was linked to Mimikatz.

I created an event and added that IP as an attribute to it. Then clicked "Enrich Event". AbuseIPDB and IP2Location then managed to get 11 other attributes connected to that IP.

Home Event Actions	Dashboard Galaxies	Input Filters Global Actions Sync Actions Administration Logs API	Bookmarks
View Event	IP linked to M	/imikatz	
View Correlation Graph			
View Event History	Event ID	1	
dia Francia	UUID	cb7107b3-36c5-40ea-8a0d-43df06afdf09 📭 🛨 🧱	
	Creator org	VC Research	
dd Attribute	Owner org	VC Research	
dd Object	Creator user	admin@admin.test	
dd Attachment	Protected Event	Event is in unprotected mode.	
dd Event Report	(experimental) 🚯	Switch to protected mode	
opulate from	Tags	(♂+) ≗+	
nrich Event	Date	2025-05-28	
erge attributes from	Threat Level	<b>☆</b> High	
	Analysis	Ongoing	
ublish Event	Distribution	This community only	
uplish (no email)	Mana in an		
ontact Reporter	warnings	Contextualisation:	
ownload as		Your event has neither tags nor galaxy clusters attached - generally adding context to an event allows for quicker decision making and more accurate	
		filtering, it is highly recommended that you label your events to the best of your	
dd Event to Collection		ability.	
st Events	Published	No	
ld Event	#Attributes	12 (2 Objects)	
	First recorded change	2025-05-28 01:46:15	
	Last change	2025-05-28 01:59:47	
	Modification map		
	Sightings	0 (0) - restricted to own organisation only. 🌽	

$\leftarrow \rightarrow$	C 🛱 😣 Not secure	https://137.184.134.84/servers/serverSettings/Plugin
88   🞽 1	Titan 🗮 MySite 🚹 JobS	Sheet 干 WCS 干 Index in Ln 👖 JFNG 🔩 THM 🔞 X
Home	Event Actions Dashboa	ard Galaxies Input Filters Global Actions Sync Actions
	List Events	
Add User	Add Event	er Settings & Maintenance
List Users	List Attributes	<b>3</b>
Pending regi	Search Attributes	iew MISP (16 \Lambda) Encryption (4) Proxy (5) Security Plu
User settings		ment
Set Setting	List Collections	
Contact User		
	List Event Reports	
Add Organis		
List Organisa	List Analyst Data	

After this, I activated the MalwareBazzar plugin as it does not require an API.

On the far right of the event, you will see an eye that allows you to see the event.

			Enter value to search	Event info 🗸 Filter
r user	Date	Info		Distribution Actions
⊇admin.test	2025-05-28	IP lin	iked to Mimikatz	Community < 12

Click on Enrich Event and select the plugins you want to use.

from Event motory	LYGHTID	
	UUID	cb7107b3-36c5-40ea-8a0d-43df06afdf09 🗭 📑
	Creator org	VC Research
	Owner org	VC Research
	Creator user	admin@admin.test
Add Attachment	Protected Event (experimental)	Event is in unprotected mode.     Switch to protected mode
	Tags	<b>⊗</b> + <b>≜</b> +
Enrich Event	Date	2025-05-28
Merge attributes from	Threat Level	<b>☆</b> High
	Analysis	
	Distribution	This commun Select the enrichments yeu wish to run
Run Ad-Hoc Workflow Contact Reporter Download as Add Event to Collection	Warnings	Contextua       Imalwarebazaar         Your eve       abuseipdb         context ti       ip2locationio         filtering, 1       Enrich         ability.       Cancel
	Published	No
	#Attributes	12 (2 Objects)

No new events were added, as this is usually used on malware hashes. But I just wanted to go through and show the process of enriching.

I suspect that if the VirusTotal API is used in MISP, it will help form those connections. But this should show the importance and crazy potential that MISP offers.

2025-05-28*	aeffe7 具	Object name: geolocation [] References: 1 [] []		countrycode :: text US				184.27.218.9/ enriched via the
				2 Hid	e / Attributes			ip2locationio module.
2025-05-28*	a6138c 📕	Other	countrycode: text		US	(♂+) ▲+	⊗+ ≛+	
2025-05-28*	099cca 📕	Other	country: text		United States of America	(♂+ ≜+	⊗+ ≗+	
2025-05-28*	377eeb 📭	Other	region: text		Washington	(♂+) ≗+	()+ 2+	
2025-05-28*	2e44d3 📭	Other	city: text		Seattle	(♂+) ≗+	<b>⊗</b> + <b>≗</b> +	
2025-05-28*	2748ba 📭	Other	zipcode: text		98164	<b>⊗</b> + <b>≜</b> +	⊗+ ≗+	
2025-05-28*	b5db70 📭	Other	latitude: float		47.60431	<b>⊗</b> + <b>≜</b> +	⊗+ ≗+	
2025-05-28*	c4b2c0 📕	Other	longitude: float		-122.32985	(♂+) ≗+	()+ 2+	
2025-05-28*	29bdc7 📑	Object name: abuseipdb []		is-malicious :: boolean 0 & Hide 4 Attributes				184.27.218.92
	References: 1 🖸 🕂		20					enriched via the abuseipdt
2025-05-28*	d000b2 📭	Other	is-malicious: boolean		0	<ul> <li>ioc:artifact-state="not-malicious"  x</li> <li>x</li> <li>x</li> </ul>	()+ ≗+	module.
2025-05-28*	fd8386 📭	Other	is-tor: boolean		0	<b>⊗</b> + <b>≜</b> +	(⊗+ 💄+	
2025-05-28*	16069f 📭	Other	is-public: boolean		1	<b>⊗</b> + <b>≜</b> +	()+ ≗+	
2025-05-28*	49ad29 📭	Other	abuse-confidence-s	core:	0	(♂+] ≜+	⊗+ ≛+	
2025-05-28*	5702ca 🗖	Network activity	ip-src		184.27.218.92	<b>⊗</b> + <b>≗</b> +	⊗+ ≗+	IP linked to Mimikatz
# Section 8 - Shuffle SOAR solution deployment

You must log in first to see your workflows	
Welcome Back!	
Find new ways to automate by discovering usecases Shufflers	
Email	
username@example.com	OR
Password	
at least 10 characters 🛛 🔤 🕸	
Password must be at least 9 characters long	
Forgot password?	_
Continue	
Don't have an account yet? Register here	

For our SOAR solution, we will be using shuffle. Go on over to their website and make an account.

Once your account is all set, navigate your way to your workflows and click on the "Create Workflow" button.

5	<	arkflows My Workflows Discover Workflows Ora Forms
Q Search	Ctrl+K	
(*) Automate	^	Norkflows All Categories - K 😑 🖬 🛨 + Create Workflow
Usecases		
Workflows		SUC Automation Project ·
• Apps		
≕ Content	~	
	n	
🗈 Admin		

You can name it however you want; I chose "IP-SOC-Automation".

As for the use cases, I selected the following down below. After that, we can select "Save changes."

- EDR to ticket
- Internal Enrichment
- External historical Enrichment
- Honeypot access
- Block an IP

New	Workflow

Workflows can be built from scratch, or from templates. Usecases can help you discover next steps, and you can search for them directly. Learn more

Name \*

**IP-SOC-Automation** 

- Usecases

Internal Enrichment, Ext... -

Tags

After saving changes, we will be introduced to our workspace as shown below.

The left-hand side will have the widgets that we will be using. I have run through this project before, so you may not have some of the apps there, but you can search for them in the top left search bar.

Q Search apps, triggers	✓ IP-SOC-Automation
Popular Actions	Runtime Location
🕗 🔽 🐼 🚺	
😫 🛃 🚬	
Triggers	
🙈 🕙 🖻 🛞	
Your Apps	
Email	
Http	Change Me
Shuffle Tools	
Virustotal v3	
🧭 TheHive	
W. Wazuh	
MISP	
Webhook	
Apps need to be activated before	
they can be used. Search from our 2500+ apps to activate them for	
your organisation.	

Below is what our workflow will be.

Webhook (Activates when Rule is Triggered)  $\rightarrow$  HTTP (Gets Wazuh API)  $\rightarrow$  VirusTotal (Enriches gathered IP)  $\rightarrow$  Makes a case in TheHive AND sends an email to the Analyst for response approval  $\rightarrow$  Response on Wazuh



The following sections will explain how to set up each widget.

### Subsection - Webhook

Clicking on the Webhook Widget will display a parameter that provides the Webhook URI, which we need to place in the Wazuh server. Click on it to copy it to your clipboard.

PIP-SOC-Automation		[
Runtime Location		Webhook: stopped
Default Cloud -		What are webhooks?
		Name
		Webhook_1
		Associated App (optional)
-		Parameters
Webbook m		Webhook URI
	Virustotal v3 2	https://shuffler.io/api/v1/hooks/web
		Start Stop
	TheHive 1	Authentication headers
		AUTH_HEADER=AUTH_VALUE1
		ОК

#### # On the Wazuh server, nano into the ossec.conf file

nano /var/ossec/etc/ossec.conf

# Scroll down a bit, and right below the first "Global" block, add in the code below. Make sure the # block aligns with the other blocks' spacing. Input your Webhook URI in the hook\_url section.

<integration> <name>shuffle</name> <hook\_url></hook\_url> <rule\_id>100003</rule\_id> <alert\_format>json</alert\_format>

</integration>

#### 疏 root@Wazuh: ~ GNU nano 6.2 /var/ossec/etc/ossec.conf I \_ \_ Wazuh - Manager - Default configuration for ubuntu 22.04 More info at: https://documentation.wazuh.com Mailing list: https://groups.google.com/forum/#!forum/wazuh ossec\_config> <global> <jsonout output>yes</jsonout output> <alerts log>yes</alerts log> <logall>yes</logall> <logall\_json>yes</logall\_json> <email notification>no</email notification> <smtp server>smtp.example.wazuh.com</smtp server> <email\_from>wazuh@example.wazuh.com</email\_from> <email to>recipient@example.wazuh.com</email to> <email\_maxperhour>12</email\_maxperhour> <email\_log\_source>alerts.log</email\_log\_source> <agents disconnection time>10m</agents disconnection time> <agents\_disconnection\_alert\_time>0</agents\_disconnection\_alert\_time> </global> <integration> name\chuffle//name <hook\_url>https://shuffler.io/api/v1/hooks bhook 7d6b79c7-6104-4f26-88 Inte Invionos/Lute Inv <alert\_format>json</alert\_format> </integration>

#### # ctrl+x and Y to save, and ENTER to exit

Systemctl restart wazuh-manager.service Systemctl status wazuh-manager.service

# On the Wazuh Agent / Linux Honeypot, we need to add a log analysis code block

# On the Agent, nano into the ossec.conf file

nano /var/ossec/etc/ossec.conf

#### # CTRL+W and search for "Log analysis", add the code. Make sure the spacing matches the other code.

<localfile> <log\_format>syslog</log\_format> <location>/var/log/auth.log</location> </localfile>



#### # ctrl+x and Y to save, and ENTER to exit

Systemctl restart wazuh-agent Systemctl status wazuh-agent

###### We can test this by triggering an SSH alert (we can lower the threshold or remove it)

Before you try and fail a SSH login, make sure you click on the Webhook widget, and click on "start". After that, try and trigger the rule.

You know it was successful if it shows up in the "Explore Runs" section.

		+ у ке	resh Runs		
	All	Finished	Executing	Aborte	ed
	29/05/	2025, 18:41:06	1 + 4 = 5	!	>
	29/05/	2025, 18:26:44	1 + 4 = 5	!	>
	29/05/	2025, 17:37:30	1 + 4 = 5	!	>
Webhook_1 💮 Http 1	29/05/	2025, 17:31:55	1 + 4 = 5	!	>
	29/05/	2025, 17:14:18	1 + 4 = 5	!	>
	29/05/	2025, 16:41:50	1 + 4 = 5	!	>
	29/05/	2025, 16:18:21	1 + 4 = 5	!	>
	29/05/	2025, 16:09:34	1 + 4 = 5	!	>

Subsection - HTTP widget

# On the Wazuh Firewall, make a rule to allow all inbound traffic on port 55000

# On DigitalOcean, click on your Wazuh Droplet, on the left-hand side, click "networking", # Scroll down to the Firewall section and click on the Firewall name.

# For the inbound rule, allow all TCP on port 55000 from any IPv4. Remember to save.

# Back on Shuffle, change the fields below for the HTTP widget

Rename to "Get-API"

Find action: Curl

# Replace the User and Password with the "Wazuh API" user credentials. As well as swapping the# localhost with the Wazuh public IP# The next page will explain on how to get the API credentials.

#### Statement:

curl -u <user>:<password> -k -X GET "https://localhost:55000/security/user/authenticate?raw=true"



# To extract the API user credentials, go to the directory where you downloaded Wazuh. And run...

tar -xvf wazuh-install-files.tar

# The output should be similar to the picture below.

root@Wazuh:~# ls
ossec-backup.conf snap wazuh-install-files.tar wazuh-install.sh
root@Wazuh:~# pwd
/root
root@Wazuh:~# tar -xvf wazuh-install-files.tar
wazuh-install-files/
wazuh-install-files/root-ca.pem
wazuh-install-files/wazuh-indexer.pem
wazuh-install-files/admin.pem
wazuh-install-files/wazuh-passwords.txt
wazuh-install-files/admin-key.pem
wazuh-install-files/config.yml
wazuh-install-files/wazuh-indexer-key.pem
wazuh-install-files/wazuh-dashboard-key.pem
wazuh-install-files/root-ca.key
wazuh-install-files/wazuh-dashboard.pem
wazuh-install-files/wazuh-server.pem
wazuh-install-files/wazuh-server-key.pem
"root@Wazuh:~# ls
ossec-backup.conf snap wazuh-install-files wazuh-install-files.tar wazuh-install.sh
froot@Wazuh:~#

Go into the "wazuh-install-files" directory and cat out the "wazuh-passwords.txt".

The credentials we need are the "wazuh API user". Use those to fill in the curl command on shuffle.

Friendly reminder to save your shuffle workflow at this point.

### Subsection - VirusTotal Widget

Get the API after making an account with VirusTotal. Once logged in, click on your name and then "**API key**" from the dropdown. It will be at the top of the page.

dress, domain or file hash			☆ ۞ ݨ	Sign in	Sign up
Analyse sus breact	<b>VIRUST</b> spicious files, domains, IPs and URLs to de hes, automatically share them with the ser	TOTAL tect malware and other curity community.			
FILE	URL	SEARCH	¢Þ		
By submitting data above Sample submission wit	choose file you are agreeing to our Terms of Service and Pri th the security community. Please do not submit responsible for the contents of your submission	ivacy Notice, and to the <b>sharing of you</b> t any personal information; we are not . Learn more.	<b>IF</b> :		

Back in shuffle, click on the VirusTotal Widget (make sure it is the square widget)

Rename to: VirusTotal Find Actions: Get an IP address report Click on the "+" sign to authenticate. Input API key Leave URL as is

The IP field should be "\$exec.all\_fields.data.srcip"

	<b>D</b> Get an ip address report	
	• 🖹 🎉 🕞 🕨	Rerun
	Name	Delay
	Virustotal	
	Valid Latest Auth for Viru	· +
	Find Actions Get an ip address report	•
Virustotal	Ž× lp *	~
	\$exec.all_fields.agent.ip	Ð
TheHive 1		
	Headers	~
	Secret. Replaced during app execution!	Ð
	Queries	2
	view=basic&redirect=test	Æ

Subsection - TheHive Widget

Let us log into TheHive Server using the default creds

admin@thehive.local secret



Create a new organization, and input this (You can name it something else)

- Name: VCResearch
- **Description:** SOC Automation project
- Task sharing rule: Manual
- **Observation sharing rule:** Manual

Click confirm at the bottom.

×	Organisation List
$\rightarrow$	+ default Export list
鱼	
	Active A admin Linked organisations None
ဗိုမို	
×	

# Click into the organization

	+ default 🕒 Export list
t	NAME *
	Active A admin Linked organisations None
	Active VCResearch
þ	
÷	

And add a new user

- Type: Normal
- Login: VCresearcher@test.com
- Name: VCResearcher
- Profile: Analyst

#### Click on "Save and add another."

VCResearch
Creation date
29/05/2025 19:54 () a minute ago
Description
SOC Automation Project
Tasks sharing rule
manual
Observables sharing rule
manual

For the second user

- Type: Service
- Login: shuffle@test.com
- Name: SOAR
- Profile: Analyst

Click on "Confirm" at the bottom.

On the left-hand side, click on "Users", and select "Preview" next to the VCResearcher account (Or equivalent)

Scroll down and input a password for the account. Click on "Confirm" when done.

For the SOAR User, click on "Preview," but this time create an API key (Take note of this API)

#### # Change the Admin Password too.

After copying the API key and changing the passwords, log out of the admin account and log in to the VCResearcher account.

#### **#** Note: Use the Email for the account, not the name.

Back on shuffle, authenticate to TheHive just like with VirusTotal.

### Click on the "+" sign to authenticate

- API key
- URL is the public IP and port of TheHive

ne Location	🥝 Post create alert
	🔹 🖹 🧪 🕞 Rerun
	Name Delay
	TheHive_1
Get-API Virustotal	Authentication       Latest     Auth for TheHive     +
	- Find Actions
	Simple Advanced
🗈 🥟 TheHive 1	! Title *
	Value 🕀
	! Tags *
	Value
	! Summary *
	Value

Just like with Wazuh, we need to modify the DigitalOcean Firewalls.

You can make a separate firewall for TheHive and separate it or just allow the current firewall group to accept TCP Traffic on Port 9000 from all IPv4 addresses.

Back in shuffle, inside of TheHive Widget, click on the "**advanced**" tab and use the body template below, and fill in the title, tag, summary, and severity. Modify it as you see fit.

# IMPORTANT NOTE: This is after I completed and brought down the infrastructure.

# The payload below will have a "sourceRef" field.

# I recommend you add the timestamp from your webhook to that number.

# The reason is that TheHive will not make any more alerts if an alert with this sourceRef already # exists. The timestamp will make it unique.

#### ## Template for shuffle TheHive payload

#### **IP Trigger message**

### # Body

```
{
 "description": "{{ "'SSH Brute Force Detected'" | replace: '\n', '\\r\\n' }}",
 "externallink": "",
 "flag": "",
 "pap": "",
 "severity": "2",
 "source": "Wazuh",
 "sourceRef": "\"Rule:100003\"",
 "status": "",
 "summary": "SSH Brute Force Detected",
 "tags": ["T1110"],
 "title": "Shuffle response",
 "tlp": "2",
 "type": "Internal",
 "observables": [
  {
   "dataType": "ip",
   "data": "$exec.all_fields.data.srcip",
   "ioc": true
  }
 ]
}
```

```
*>* Title
Shuffle response
```

\*>\* - Tags ["T1110"]

```
*>* - Summary
RDP Brute Force Detected
```

```
*>* - Severity
2
```

**# NOTE: Severity is 0-3, Low to severe** 

We can rerun previous attempts at SSH login failures, and it should make a case in TheHive.

→	default	Quick Filters 🧿 🕒 Export list					<b>3</b> (k)
•	STATUS ‡	SEVERITY + TITLE +	# CASE	TYPE COURCE CREFERENCE	DETAILS	ASSIGNEE ‡	DATES 0. + C. + U. +
: <b>_</b> D	New	M Shuffle response		Internal Wazuh	Observables TTPs	。 ⑦	O. 29/05/2025 21:16 C. 29/05/2025 21:16
¥≡		se None		Rule:100003			
Q							
鱼							

Subsection - User Input Widget

To set up the Email widget that will be used for approving the active response. On the User Input Widget, fill out the fields with the information below.

Information: Would you like to block this source IP: {"srcip":"\$exec.all\_fields.data.srcip"}}

Contact Option: Email

Email: Your email

	What is the user input trigger?
	Name
	User_Input_1
	Information
	The information you want to show the user. Supports variables. Supports Markdown & HTML.
to. 🕒 🔐 User Input 1	Would you like to block this source IP: {"srcip":"\$exec.all_fields.data.srcip"}
	Input options Use subflows to connect to any app you want, or use the default email and sms options
	🗌 Subflow 🗹 Email 🗌 SMS
	Email *
	test@test.com
	Required Input-Questions No Input-Questions found. Click to add them!

The email to be received should be like the one below.

The top link will be to continue the workflow. The bottom will abort it.

😈 Archive   前 Delete 🄺 Star 🛛 Mark unread	🖨 Block 🛛 🔮 Label	😲 Spam \cdots	
Shuffle - User input required			
<b>Shuffle</b> <shuffle-support@shuffler.io> To: me</shuffle-support@shuffler.io>		12:02 pm 📘	· □ ◆ …
Action required! Would you like to block this source IP: {"srcip":			
If this is TRUE click this: <u>https://shuffler.io/workflow</u> authorization=10f49780-8ae1-4d48-ae1f-da89307 c35c4dc2475d&reference execution=3b376e82-b0	vs/179ad958-63e8-4e06 86aa0&start=c1e5791c 089-4d66-b74f-0af5309	5-8541-f9475a385a33/run? :-8465-43a7-8d61- )700e6&answer=true	
IF THIS IS FALSE, click this: <u>https://shuffler.io/workf</u> authorization=10f49780-8ae1-4d48-ae1f-da89307 c35c4dc2475d&reference_execution=3b376e82-b0	lows/179ad958-63e8-4 86aa0&start=c1e5791c 089-4d66-b74f-0af5309	e06-8541-f9475a385a33/ru :-8465-43a7-8d61- )700e6&answer=false	<u>n?</u>
Please contact us at shuffler.io/contact or support@	@shuffler.io if there is a	n issue with this message.	

Subsection - Wazuh Active Response Widget

Parameters to change Find Actions: Run command ApiKey: # Should be the output of "Get-API" URL: swap localhost to Wazuh public IP Command: firewall-drop0 Agent list: \$exec.all\_fields.agents.id Wait for complete: true

• 🗈 🎢	► Rerun
Name	Delay
Wazuh_1	O
+ Authenticate V	Vazuh
Find Actions Run command	•
🔒 Apikey *	~
Use "\\$" instead of "\$" if you want to Url *	to escape \$ (2)
https://137.184.97.114:5500	00 <b>(</b>
Simple	Advanced
Body *	2
{ "alert": "\${alert}", "arguments": "\${argumen "command": "\${command "custom": "\${custom}" }	nts}", ⊕ <sub>}}",</sub> ⊕
	<ul> <li>Name</li> <li>Wazuh_1</li> <li>→ Authenticate V</li> <li>Find Actions Run command</li> <li>Apikey *</li> <li>Out *</li> <li>Urt *</li> <li>https://137.184.97.114:5500</li> <li>Simple</li> <li>Body *</li> <li>{     "alert": "\${alert}",     "arguments": "\${argument "command": "\${command"} </li> </ul>

# In the Wazuh server
#Nano into the ossec.conf file
Nano /var/ossec/etc/ossec.conf

# Click on CTRL+W and search for "active response"

# Scroll down to the bottom of active response, uncomment and add in the block below to where it # says "active response commands here"

<active-response>

<command>firewall-drop</command> <location>local</location> <level>13</level> <timeout>no</timeout> </active-response>

<active-response> <command>firewall-drop</command> <location>local</location> <level>13</level> <timeout>no</timeout> </active-response>

```
<!-- Log analysis -->
<localfile>
<log_format>command</log_format>
<command>df -P</command>
<frequency>360</frequency>
</localfile>
```

#### # ctrl+x and Y to save, and ENTER to exit

Systemctl restart wazuh-manager

I tested this active response feature by allowing MISP to SSH to the Honeypot.

When the workflow was triggered and I clicked on the link in the Email, I was directed to this page.

Would you like to block th {"srcip":"137.184.134.84"}	is source IP: }		
What do yo	ou want to do?		
Continue	or	Stop	

After clicking on "continue", the response begins.

We can verify through the shuffle logs or run an iptables command on the honeypot to see the blocked IP.

root@VCResearch-Linux:/var/ossec/bin# root@VCResearch-Linux:/var/ossec/bin# iptableslist Chain INPUT (policy ACCEPT)									
target	prot opt	source	destination						
DROP	all	137.184.134.84	anywhere						
Chain FORWA target	ARD (polic prot opt	cy ACCEPT) source	destination						

# Since this is the MISP IP, we would want to remove it.

**# If you are unfamiliar with iptables, run the command below to list blocked IPs and their line number.** Iptables -L –line-number

**# For the MISP IP, it was number 1, so I had to run these commands to unblock it...** Iptables -D INPUT 1 Iptables -D FORWARD 1

# The picture shows an empty iptables again.

```
root@VCResearch-Linux:/var/ossec/bin# iptables -D INPUT 1
root@VCResearch-Linux:/var/ossec/bin# iptables -D FORWARD 1
root@VCResearch-Linux:/var/ossec/bin# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num target
              prot opt source
                                            destination
Chain FORWARD (policy ACCEPT)
             prot opt source
                                            destination
num target
Chain OUTPUT (policy ACCEPT)
             prot opt source
num target
                                            destination
root@VCResearch-Linux:/var/ossec/bin# _
```

# Section 9 - Integrating TheHive into MISP

# Will need to make a firewall rule to allow communications between TheHive and MISP # The firewall rule can just be all IPv4 traffic between the two.

#### After changing those rules,

Log in to the admin account in TheHive, then click on "Platform management."

Organisation List		) 💥 English (UK) Dei
÷	+ default Export list	
🟛 Organisations		CREATE
🛓 Users	Active A admin Linked organisations None	Th m
🙀 Entities Management	Active VCResearch Linked organisations None	A ad
💥 Platform Management		

Fill out the information.

Interval: 1 minute

Server Name: MISP Server URL: MISP URL API: <Grab from MISP> Purpose: Import and Export Proxy disabled Check that the cert authority is disabled, just because this is a project. Everything else was left as default

To get the MISP API key, log in to MISP, select the administration tab, and list the Auth keys. You will have to create a new one.

Dashboard Galaxies	Input Filters	Global Actions	Sync Action:	s	Administration	Logs	API	
					List Users			
Authenticat	ion key l	ndex			List Auth Keys			
A list of API keys bound to	) a user.				List User Settin	gs		
					Set User Setting	g		
« previous next »					Add User			
					Contact Users			
+ Add authentication	key				User Registratio	ons		e to sear
# ↓ User	Auth Key		Expiration	La	List Organisatio	inc		Allowed
2 admin@admin.test	vjFq	tsy8	Indefinite	Ne	Add Organisatio	ons		
				-				
Page 1 of 1, showing 1 re	cords out of 1 total,	starting on record 1	, ending on 1		List Roles			
« previous next »					Add Roles			
					Server Settings	& Maintena	ance	
					Jobs			
					Scheduled Task	(S		
					Workflows			

Auth keys are used for API access. A user can have more than one authkey, so if you would like to use separate keys per tool that queries MISP, add additional keys. Use the comment field to make identifying your keys easier.

User	
admin@admin.test	~
Comment	
MISP to Hive Key	
	<b>Q (</b>
Allowed IPs	
165.227.197.170/	
	<b>?</b>
Expiration (keep empty for indefinite)	
YYYY-MM-DD	

Read only (it will unset all permissions. This should not be used for sync users)



At the bottom of the configurations, there will be a button to test the connection. Click on it, if it succeeds, then confirm it.

←	Platform Management		
	🛿 License 🔉 Status 💿 Branding Corte	ex MISP 🗟 Authentication	🚨 SMTP 🖁 Global Endpoints
Organisations	General settings		
Users	* Interval		
	1	minute	\[         \]     \[
Entities Management	Servers (+)		
	SERVER NAME	DATES	
Platform Management	MISP https://137.184.134.84		•••

# ## Can test it out by making a case with the Mimikatz IP and see if MISP enriches TheHive

STATUS ‡	SEVERITY 🗧 TITLE 🗧	# CASE		DETAILS	1	ASSIGNEE ‡	DATES 0.‡ C.‡ U.‡	
New	11 #1 IP linked to Mimikatz つ srcVC Research 幸 None		misp VC Research 1 🗗	Observables TTPs	10 0		O. 27/05/2025 19:00 C. 31/05/2025 18:06 U. 31/05/2025 18:32	•••
Imported () an hour	M Shuffle response ③ T1110 莽 None	#1	Internal Wazuh Rule:100003	Observables TTPs	2 0	V	O. 31/05/2025 17:13 C. 31/05/2025 17:13 U. 31/05/2025 18:32	•••

# Section 10 - Atomic Threat Intelligence Gathered

Because of other matters I had to take care of, I had to bring the infrastructure down fast. Which led to me not being able to troubleshoot the alert generation issue. I do plan to append the results when I run through this lab a third time.

As brought up before, the sourceRef parameter in shuffle was not unique, so I ran into the problem that new events were not being generated in the hive. But the emails and active response were still working.

The image below is just the first brute force attempt alert that was created, and a secondary alert is being created with the enriched observables.



The third was the enriched alert that was created when I tested the Mimikatz-linked IP.

In the alerts created, they have a link pointing back to MISP, which allows analysts to see the full list of observables and how they were correlated. The next two images show those MISP pages.



Home Event A	ctions D	ashboar	rd Galaxie	s Input Fill	ers	Global Ac	tions		c Actions	Administration		API	Bookmarks 👻 🔺	MISP A	dmin 🖂 🛛 L
List Events Add Event Import from REST client		eve « prev	nts												
List Attributes		Q   1	My Events	Org Events		Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Enter value to search	Event info	✓ Filter Actions
Search Attributes		0 × 0	VC Research	VC Research	- 4			13	2	admin@admin.test	2025-06-01	SSH	Bruteforce attempt Case 3	All <	16 i 0
View Proposals		<b>×</b>	VC Research	VC Research	- 3			13	2	admin@admin.test	2025-06-01	SSH	Bruteforce attempt Case 2	All <	1010
Events with proposals		<b>×</b>	VC Research	VC Research	- 2			13		admin@admin.test	2025-06-01	SSH	Bruteforce attempt Case 1	All <	10 i 0
View periodic summary	1.5	<b>×</b>	VC Research	VC Research	<b>☆</b> 1			12	2	admin@admin.test	2025-05-28	IP lir	nked to Mimikatz	All <	1° 10
Export Automation		Page 1 o « prev	of 1, showing 4	records out of 4	I total,	starting on r	ecord 1	i, endini	g on 4						

- End of project -