SOC Automation Homelab

Savannah Carr - Rutgers Cybersecurity Bootcamp Final Project | 5/14/2025

SOC Automation Homelab

Overview & Purpose

To build out a home lab that will simulate a real world SOC Analyst environment with case management and active response capabilities.

*Using integrations of multiple softwares and platforms to streamline alerts of Mimikatz usage.

Software Integrations used

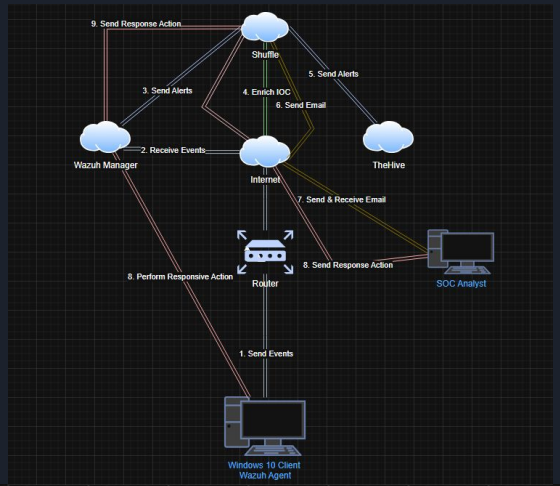
- Digital Ocean
- Wazuh
- The Hive
- VirtualBox
- Shuffle

SHUFFLE

DigitalOcean

TheHive

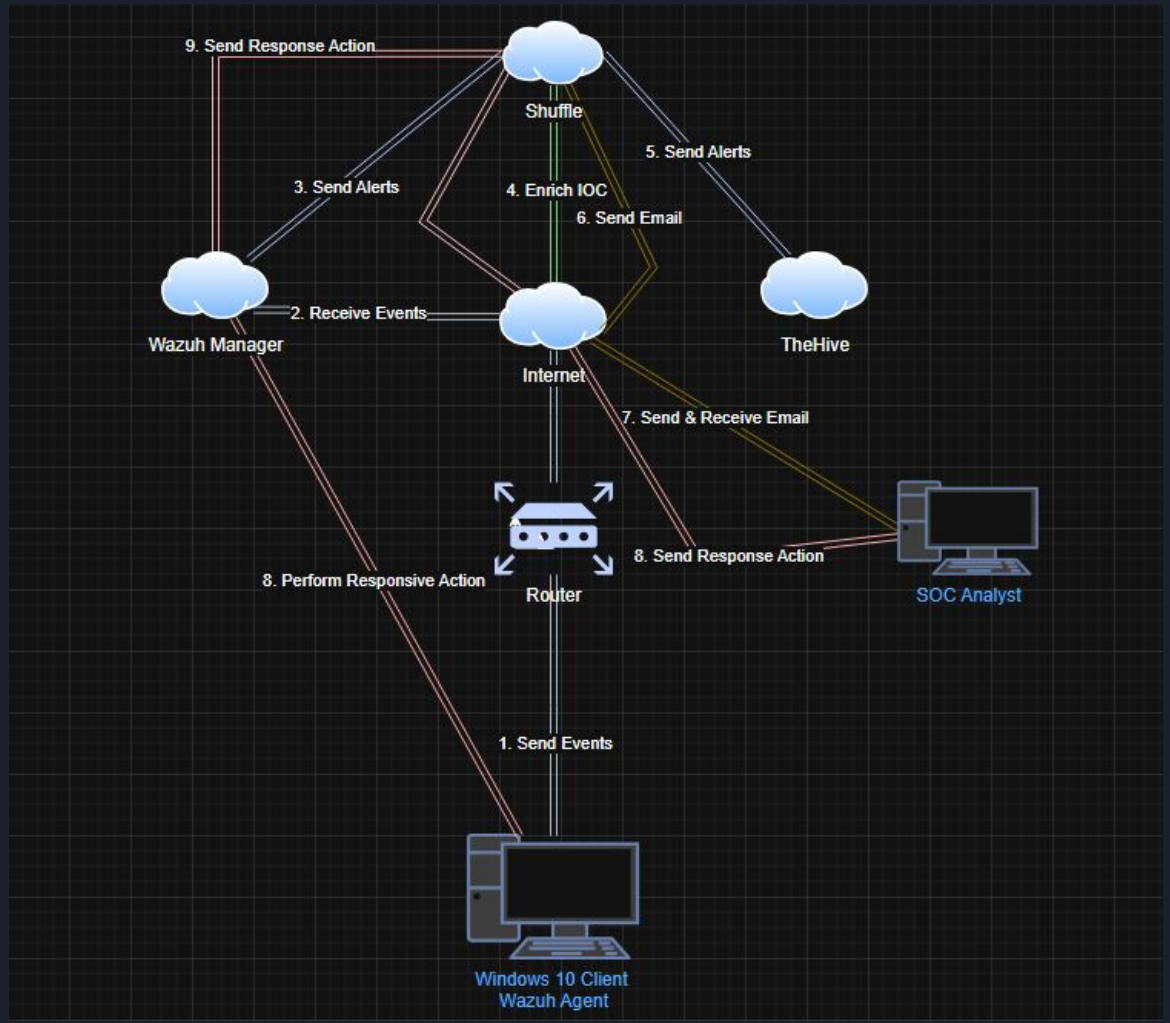
wazuh.



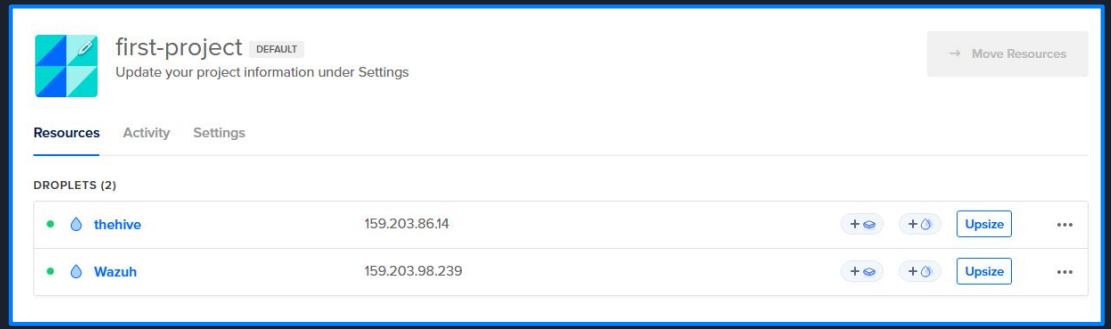
OSINT
Enrich IOCS

Windows 10
Send Events → Wazuh Manager
Trigger alerts & Perform responsive actions → Shuffle
Receive Wazuh alerts & Send responsive actions → Email
Send Email & responsive Actions

The Hive
Create alert in case management


9. Send Response Action
Shuffle
5. Send Alerts
3. Send Alerts
4. Enrich IOC
6. Send Email
2. Receive Events
Wazuh Manager
Internet
TheHive
7. Send & Receive Email
8. Send Response Action
8. Perform Responsive Action
Router
SOC Analyst
1. Send Events
Windows 10 Client
Wazuh Agent

DigitalOcean



A cloud for your entire journey

DigitalOcean's suite of products is designed to be with you on every step of your journey, whether you want to do it yourself or get help from the experts.

See all products →

Virtual machines

DigitalOcean Droplets are simple, scalable virtual machines for all your web hosting and VPS hosting needs.

Learn more →

Kubernetes

DigitalOcean Kubernetes is a managed solution that is easy to scale and includes a 99.95% SLA and free control plane.

Learn more →

AI / ML

Build, train, and deploy AI apps, and create AI agents with a suite of simple-to-use tools and GPU compute.

Learn more →

App Platform

App Platform is our fully-managed PaaS solution to get your app to market fast that's super simple to set up and cost-effective.

Learn more →

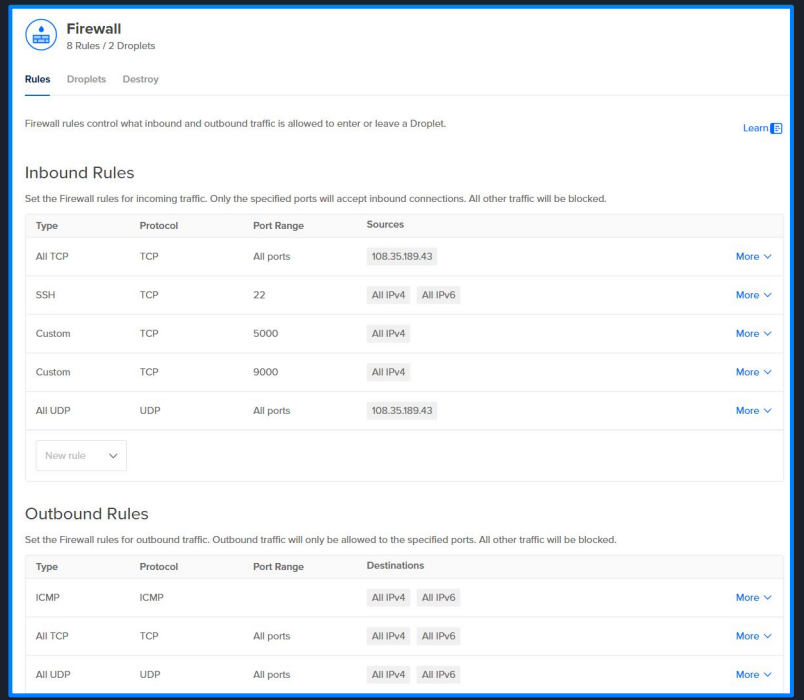
Managed databases

Managed MongoDB, Kafka, MySQL, PostgreSQL, and Caching let you focus on your apps while we update and scale your databases.

Learn more →

Storage

DigitalOcean Spaces object storage and Volumes block storage are business-ready storage solutions.



wazuh.

Used for the SIEM capabilities in this scenario.

Endpoint and Cloud **Workload Protection**

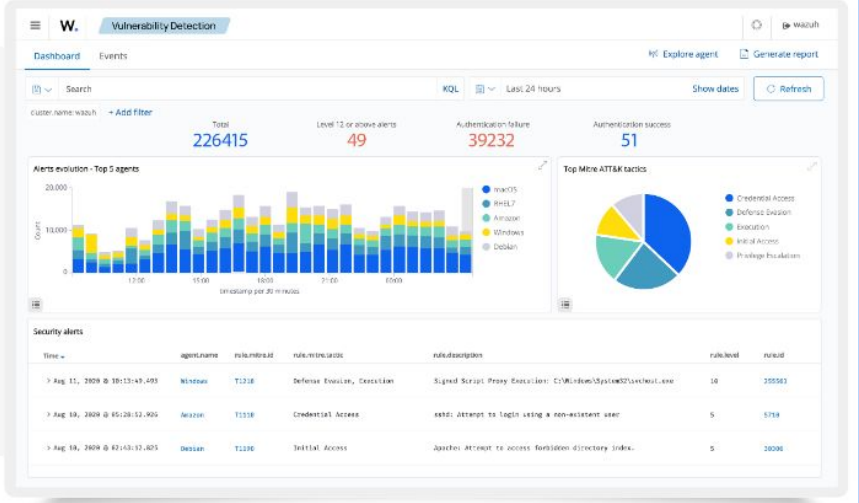
Wazuh unifies historically separate functions into a single agent and platform architecture.
Protection is provided for public clouds, private clouds, and on-premise data centers.

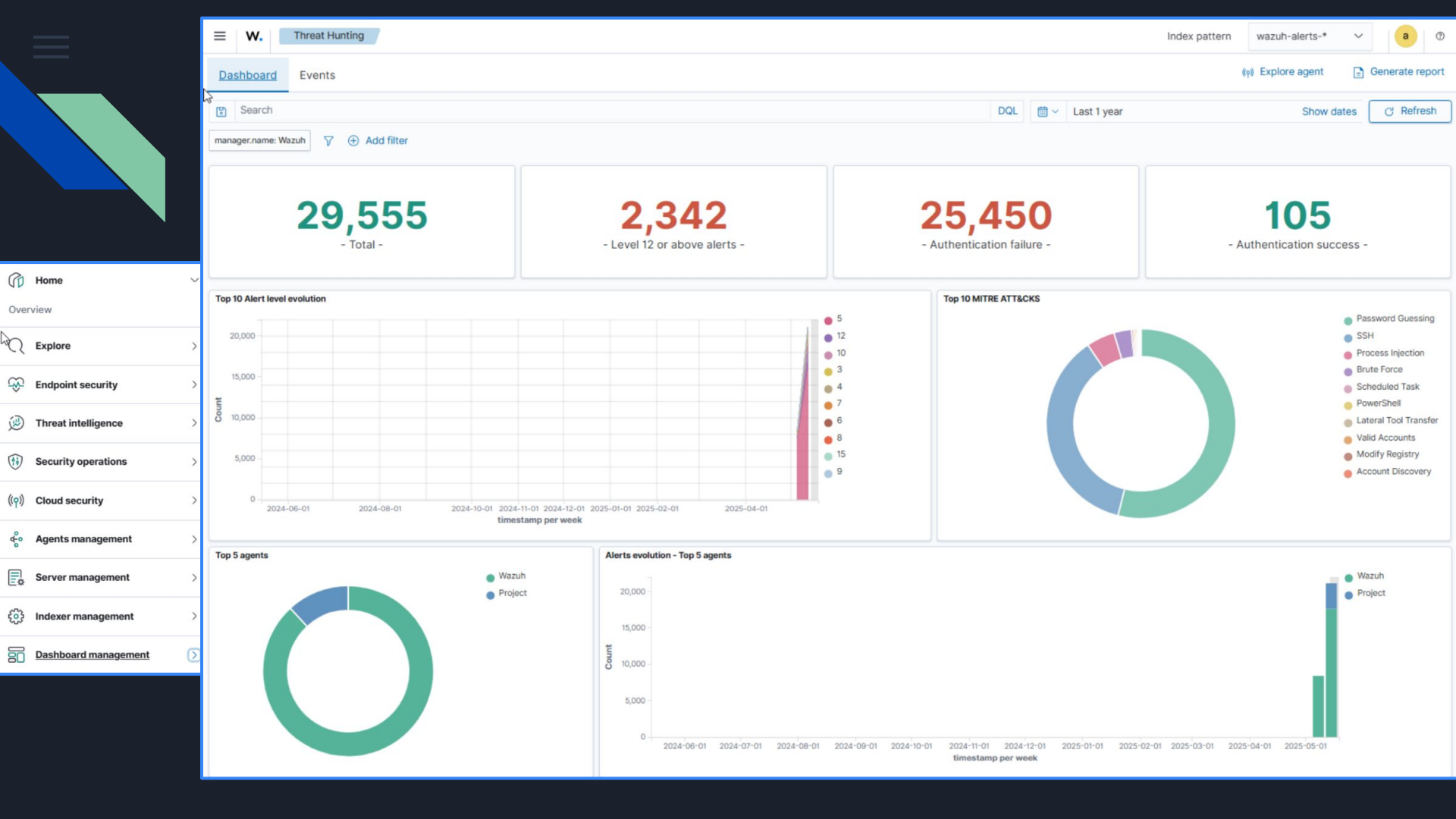
Endpoint Security	Threat Intelligence	Security Operations	Cloud Security
Configuration Assessment	Threat Hunting	Incident Response	Container Security
Malware Detection	Log Data Analysis	Regulatory Compliance	Posture Management
File Integrity Monitoring	Vulnerability Detection	IT Hygiene	Workload Protection

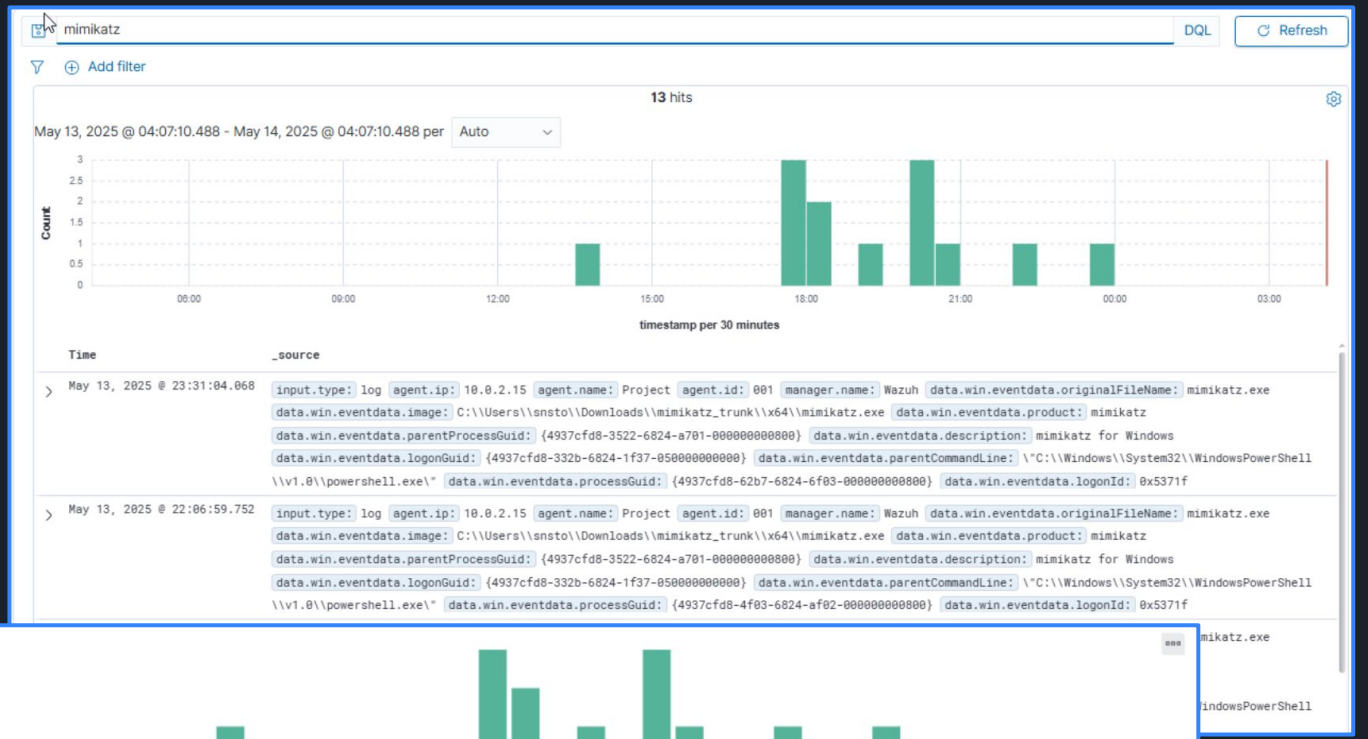
A comprehensive **SIEM solution**

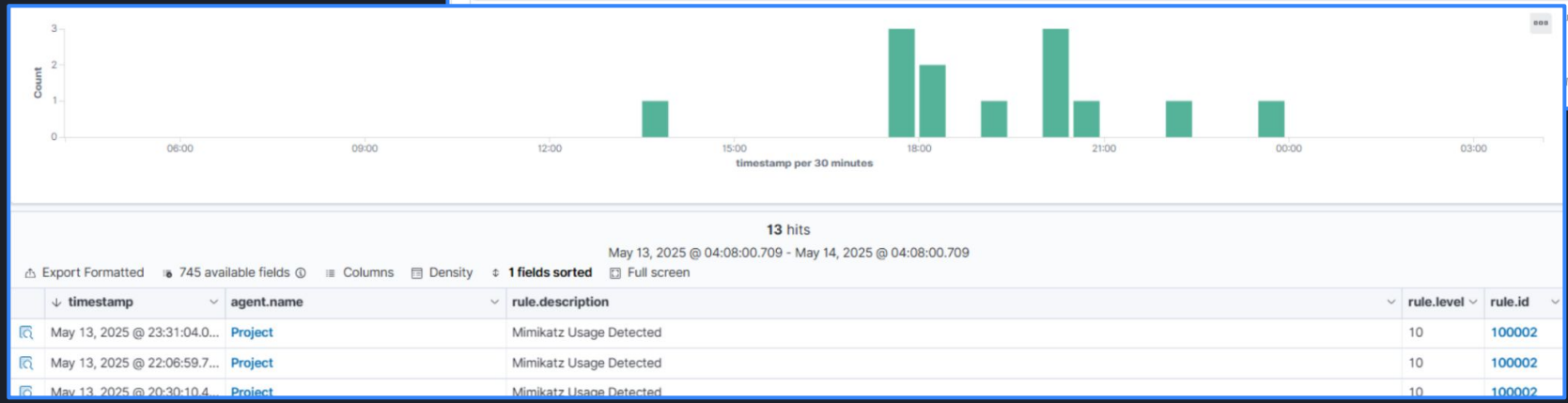
The Wazuh Security Information and Event Management (SIEM) solution provides monitoring, detection, and alerting of security events and incidents.

Learn more about SIEM >




Threat Hunting
Index pattern
wazuh-alerts-*
Dashboard
Events
Explore agent
Generate report
Search
DQL
Last 1 year
Show dates
Refresh
manager.name: Wazuh
Add filter
29,555
- Total -
2,342
- Level 12 or above alerts -
25,450
- Authentication failure -
105
- Authentication success -
Top 10 Alert level evolution
Count
timestamp per week
5
12
10
3
4
7
6
8
15
9
Top 10 MITRE ATT&CKS
Password Guessing
SSH
Process Injection
Brute Force
Scheduled Task
PowerShell
Lateral Tool Transfer
Valid Accounts
Modify Registry
Account Discovery
Top 5 agents
Wazuh
Project
Alerts evolution - Top 5 agents
Home
Overview
Explore
Endpoint security
Threat intelligence
Security operations
Cloud security
Agents management
Server management
Indexer management
Dashboard management


mimikatz
DQL
Refresh
Add filter
13 hits
May 13, 2025 @ 04:07:10.488 - May 14, 2025 @ 04:07:10.488 per Auto
Count
timestamp per 30 minutes
Time
_source
May 13, 2025 @ 23:31:04.068
input.type: log agent.ip: 10.0.2.15 agent.name: Project agent.id: 001 manager.name: Wazuh data.win.eventdata.originalFileName: mimikatz.exe
data.win.eventdata.image: C:\\Users\\snsto\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe data.win.eventdata.product: mimikatz
data.win.eventdata.parentProcessGuid: {4937cfd8-3522-6824-a701-000000000800} data.win.eventdata.description: mimikatz for Windows
data.win.eventdata.logonGuid: {4937cfd8-332b-6824-1f37-050000000000} data.win.eventdata.parentCommandLine: \"C:\\Windows\\System32\\WindowsPowerShell
\\v1.0\\powershell.exe\" data.win.eventdata.processGuid: {4937cfd8-62b7-6824-6f03-000000000800} data.win.eventdata.logonId: 0x5371f
May 13, 2025 @ 22:06:59.752
input.type: log agent.ip: 10.0.2.15 agent.name: Project agent.id: 001 manager.name: Wazuh data.win.eventdata.originalFileName: mimikatz.exe
data.win.eventdata.image: C:\\Users\\snsto\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe data.win.eventdata.product: mimikatz
data.win.eventdata.parentProcessGuid: {4937cfd8-3522-6824-a701-000000000800} data.win.eventdata.description: mimikatz for Windows
data.win.eventdata.logonGuid: {4937cfd8-332b-6824-1f37-050000000000} data.win.eventdata.parentCommandLine: \"C:\\Windows\\System32\\WindowsPowerShell
\\v1.0\\powershell.exe\" data.win.eventdata.processGuid: {4937cfd8-4f03-6824-af02-000000000800} data.win.eventdata.logonId: 0x5371f


Count
timestamp per 30 minutes
13 hits
May 13, 2025 @ 04:08:00.709 - May 14, 2025 @ 04:08:00.709
Export Formatted
745 available fields
Columns
Density
1 fields sorted
Full screen
timestamp
agent.name
rule.description
rule.level
rule.id
May 13, 2025 @ 23:31:04.0...
Project
Mimikatz Usage Detected
10
100002
May 13, 2025 @ 22:06:59.7...
Project
Mimikatz Usage Detected
10
100002
May 13, 2025 @ 20:30:10.4...
Project
Mimikatz Usage Detected
10
100002

TheHive

Enriched case management

Create security cases using a simple yet powerful template engine. Customize them as you like, and work together with other analysts to thoroughly investigate alerts.

Enrichment

- Assign tasks and add observables
- Merge similar cases
- Add tags and flag IOCs
- Attach evidence files, including password-protected ZIP archives
- Define the Permissible Actions Protocol level for each observable

Collaboration

- Define and edit user profiles capabilities
- Synchronize them via LDAP or AD
- Customize roles and permissions
- Isolate cases or make them accessible to more collaborators
- Contribute to dynamic timelines and dashboards together

The Case Management Platform that will make your security job easier

What was once a humble open-source project is now trusted by hundreds of SOC, CERT, CSIRT and other teams worldwide. The current version of the platform, TheHive 5, is our most advanced one ever, thanks to years of innovation, development, and invaluable real-world input from our users and community.

100% visibility

Get complete visibility of all incidents and reduce alert fatigue.

Automation

Automate incident response's tedious steps, saving time to concentrate on what matters.

Customization

Customize without limits: choose where to receive alerts, what to integrate with, how to filter criteria, and more.

Collaboration

Collaborate in real time, investigating incidents together with other teams and reaching resolutions faster.

TheHive's features

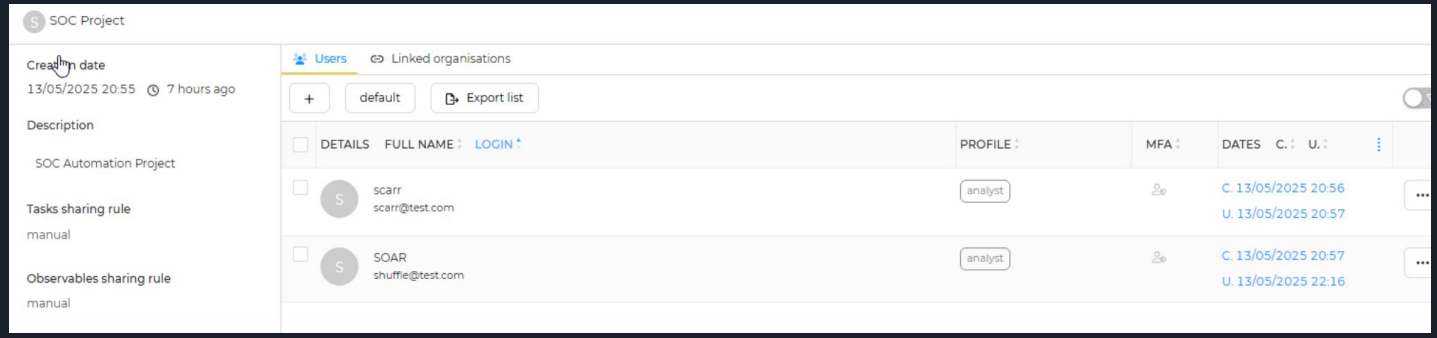
What makes our platform your best friend

- Alert management
- Case management
- Multi-tenant environments
- Advanced user management
- Notifications framework
- Metrics and dashboards
- Comprehensive APIs
- MISP integration
- MITRE ATT&CK integration
- Case reporting
- Knowledge base
- Timelines

Centralized alert management

Automatically collect and manage all security alerts on one dedicated and detailed page.

- Make comments
- Identify similar alerts
- Define custom statuses and fields
- Escalate alerts to investigations or incident response
- Import shared IOCs from MISP and framework TTPs from MITRE ATT&CK



New	Mimikatz Detected T1003 None	-	internal Wazuh Rule 100006	Observables TTPs	0 0	?	O. 14/05/2025 15:18 C. 14/05/2025 15:18	•••
New	Mimikatz Detected T1003 None	-	internal Wazuh Rule 100004	Observables TTPs	0 0	?	O. 14/05/2025 15:05 C. 14/05/2025 15:05	•••
New	Mimikatz Detected T1003 None	-	internal Wazuh Rule 100001	Observables TTPs	0 0	?	O. 14/05/2025 15:01 C. 14/05/2025 15:01	•••
New	Mimikatz Detected T1003 None	-	internal Wazuh Rule 100002	Observables TTPs	0 0	?	O. 13/05/2025 22:19 C. 13/05/2025 22:19	•••
New	Mimikatz Detected T1003 None	-	internal Wazuh Rule 100003	Observables TTPs	0 0	?	O. 13/05/2025 22:17 C. 13/05/2025 22:17	•••

The Hive configuration - Cassandra/Elasticsearch

```
Install Java
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"

Install Cassandra
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

Install ElasticSearch
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
```

```
Install TheHive
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
```

Cassandra and Elasticsearch are both used with the configuration of TheHive.

Cassandra - used as the primary database within TheHive.
Elasticsearch - Serves as the indexing engine.

```
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

# The name of the cluster. This is mainly used to prevent machines in
# one logical cluster from joining another.
cluster_name: 'Test Cluster'
```

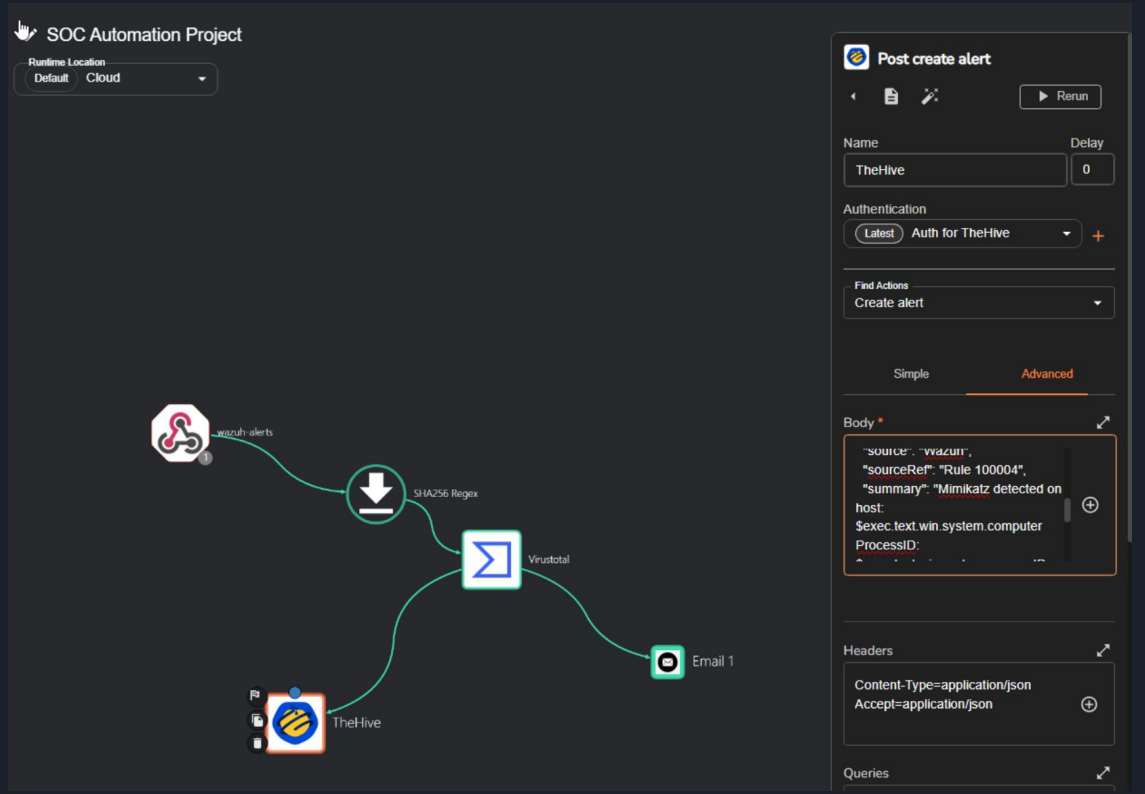
```
GNU nano 6.2                                /etc/elasticsearch/elasticsearch.yml
# ======================== Elasticsearch Configuration =========================
#
# NOTE: Elasticsearch comes with reasonable defaults for most settings.
#       Before you set out to tweak and tune the configuration, make sure you
#       understand what are you trying to accomplish and the consequences.
#
# The primary way of configuring a node is via this file. This template lists
# the most important settings you may want to configure for a production cluster.
#
# Please consult the documentation for further information on configuration options:
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html
#
# ---------------------------------- Cluster -----------------------------------
#
# Use a descriptive name for your cluster:
#
cluster.name: thehive
```

Elasticsearch and Cassandra have separate configuration files. The Public IP address of The Hive must be placed within these files. (Found within the Digital Ocean instance.)

```
GNU nano 6.2                                /etc/thehive/application.conf
# TheHive configuration - application.conf
#
#
# This is the default configuration file.
# This is prepared to run with all services locally:
# - Cassandra for the database
# - Elasticsearch for index engine
# - File storage is local in /opt/thp/thehive/files
```

SHUFFLE

Used for SOAR implementation.



What is SOAR?

Security

Protecting systems and data.

Orchestration

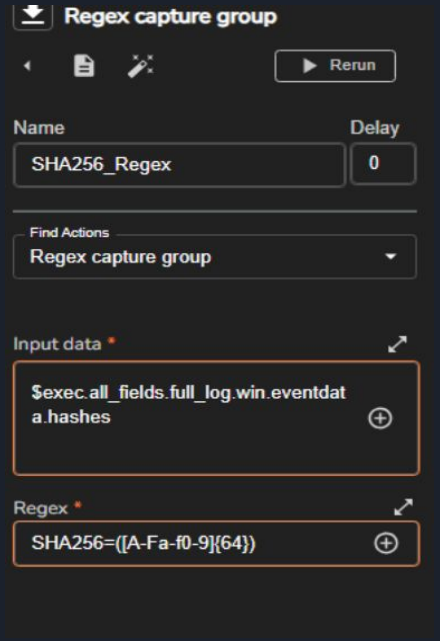
Coordinating and integrating security tools.

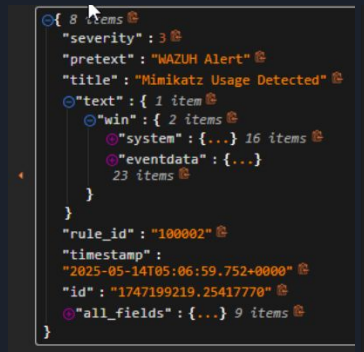
Automation

Automating repetitive tasks with software.

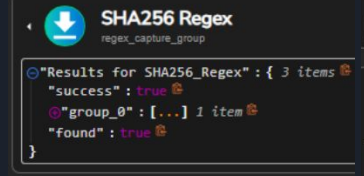
Response

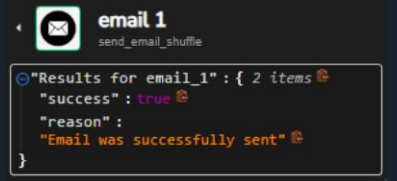
Executing predefined actions.

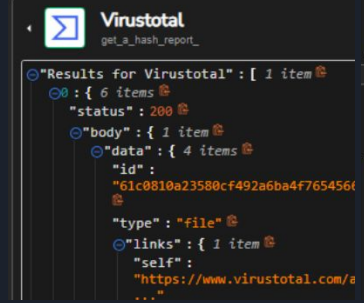

Regex capture group
Rerun
Name
Delay
SHA256_Regex
0
Find Actions
Regex capture group
Input data *
$exec.all_fields.full_log.win.eventdata.hashes
Regex *
SHA256=([A-Fa-f0-9]{64})

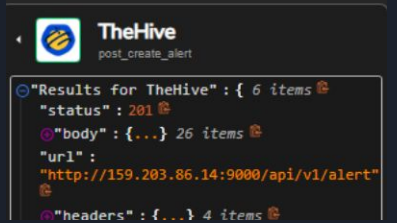

{ 8 items
"severity" : 3
"pretext" : "WAZUH Alert"
"title" : "Mimikatz Usage Detected"
"text" : { 1 item
"win" : { 2 items
"system" : {...} 16 items
"eventdata" : {...}
23 items
}
}
"rule_id" : "100002"
"timestamp" : "2025-05-14T05:06:59.752+0000"
"id" : "1747199219.25417770"
"all_fields" : {...} 9 items
}

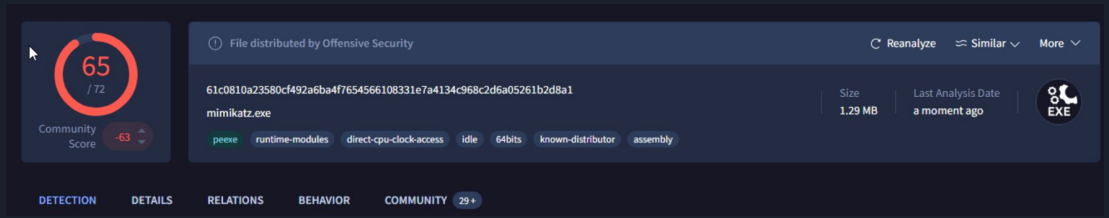

"type" : "file"
"links" : { 1 item
"self" : "https://www.virustotal.com/a..."
}
"attributes" : {...}
41 items
}
}
"url" : "https://www.virustotal.com/api/v3/fi..."
"headers" : {...} 9 items
"cookies" : {} 0 items
"success" : true
}
]


SHA256 Regex
regex_capture_group
"Results for SHA256_Regex" : { 3 items
"success" : true
"group_0" : [...] 1 item
"found" : true
}


email 1
send_email_shuffle
"Results for email_1" : { 2 items
"success" : true
"reason" : "Email was successfully sent"
}


Virustotal
get_a_hash_report_
"Results for Virustotal" : [1 item
0 : { 6 items
"status" : 200
"body" : { 1 item
"data" : { 4 items
"id" : "61c0810a23580cf492a6ba4f7654566
"type" : "file"
"links" : { 1 item
"self" : "https://www.virustotal.com/a...
}


TheHive
post_create_alert
"Results for TheHive" : { 6 items
"status" : 201
"body" : {...} 26 items
"url" : "http://159.203.86.14:9000/api/v1/alert"
"headers" : {...} 4 items


65
/ 72
Community Score
-63
File distributed by Offensive Security
Reanalyze
Similar
More
61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1
mimikatz.exe
Size
1.29 MB
Last Analysis Date
a moment ago
EXE
peexe
runtime-modules
direct-cpu-clock-access
idle
64bits
known-distributor
assembly
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 29+