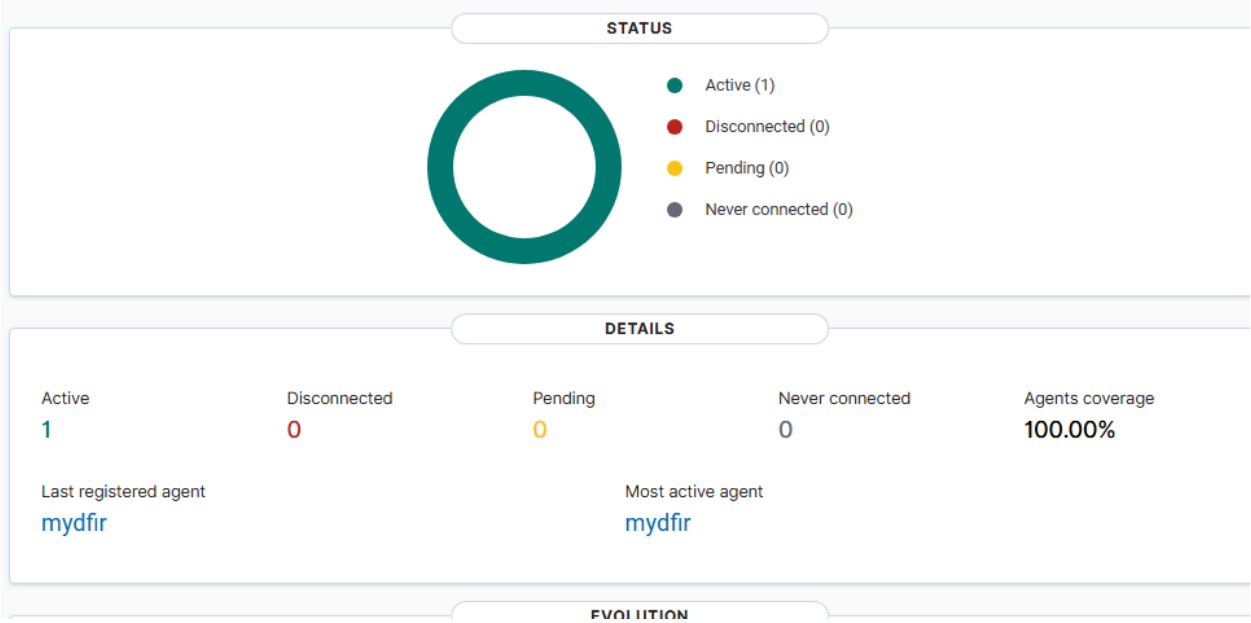
Next, start the service

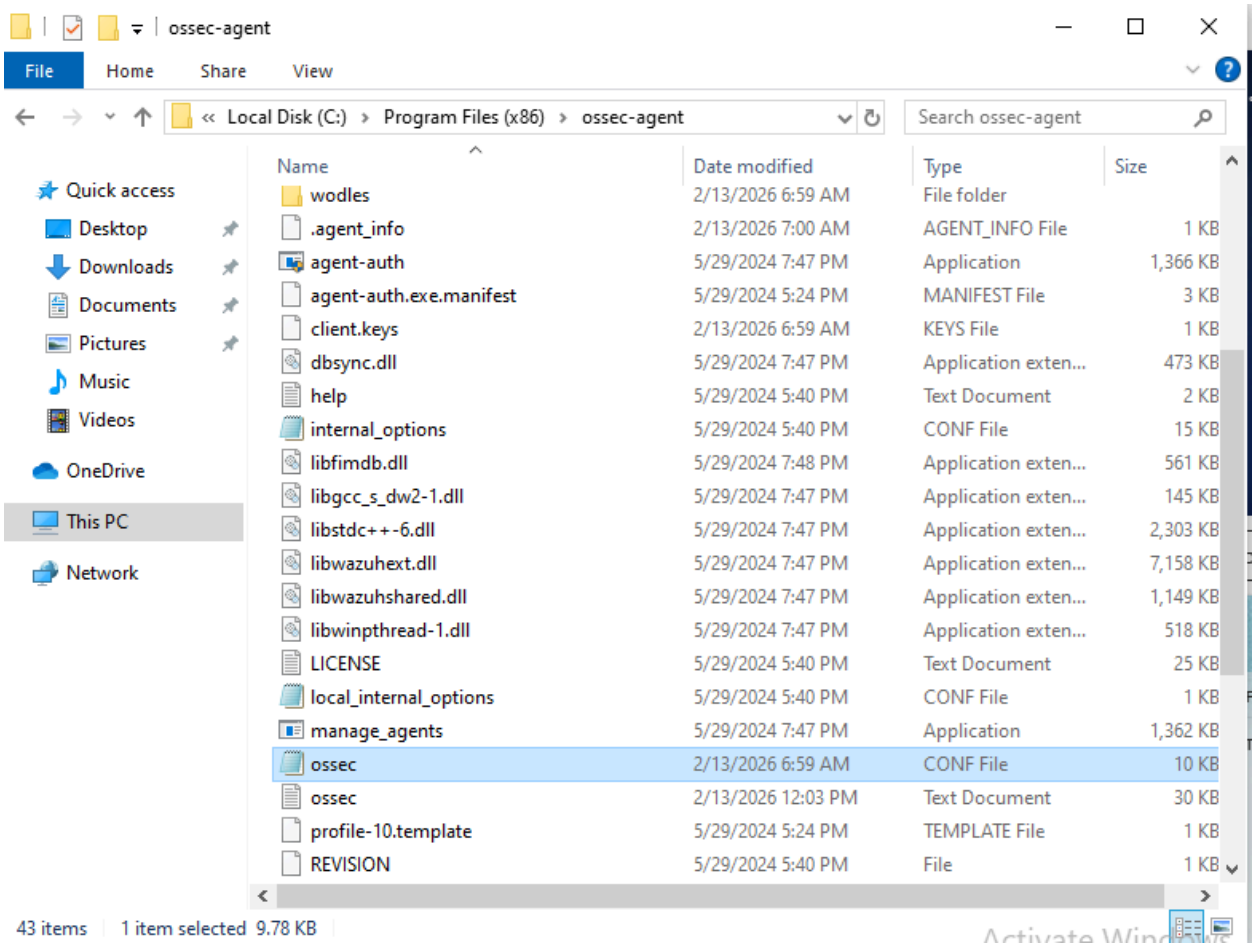
```
PS C:\> net start wazuhsvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\>
```

We now have an agent running



Generate Telemetry & Ingest Into Wazuh

First, we need to configure the Windows 10 Wazauh client agent



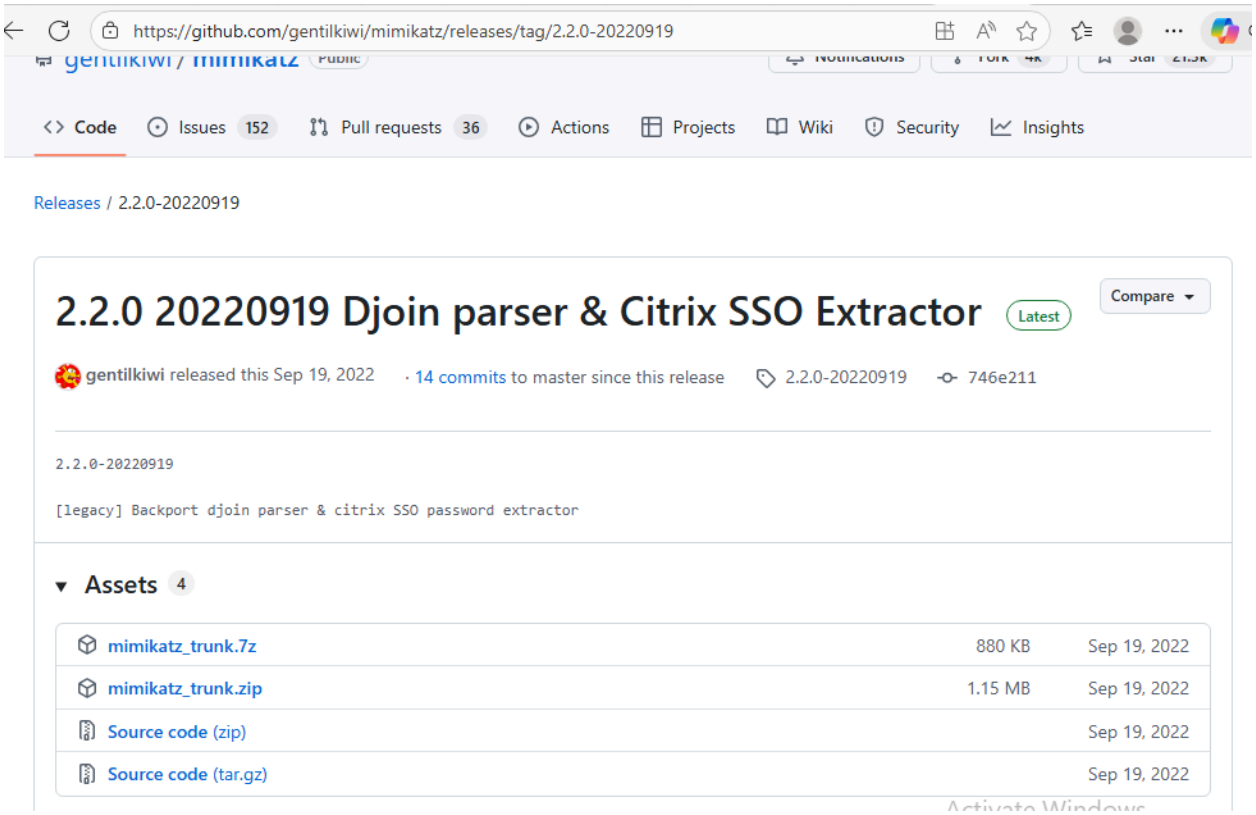
In the Log analysis section, replace application with the sysmon location, then restart Wazuh

```
<localfile>
  <location>active-response\active-responses.log</location>
  <log_format>syslog</log_format>
</localfile>

<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <windows_apps>./shared/win_applications_rcl.txt</windows_apps>
  <windows_malware>./shared/win_malware_rcl.txt</windows_malware>
</rootcheck>

<!-- Security Configuration Assessment -->
<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<!-- File integrity monitoring -->
<syscheck>
```

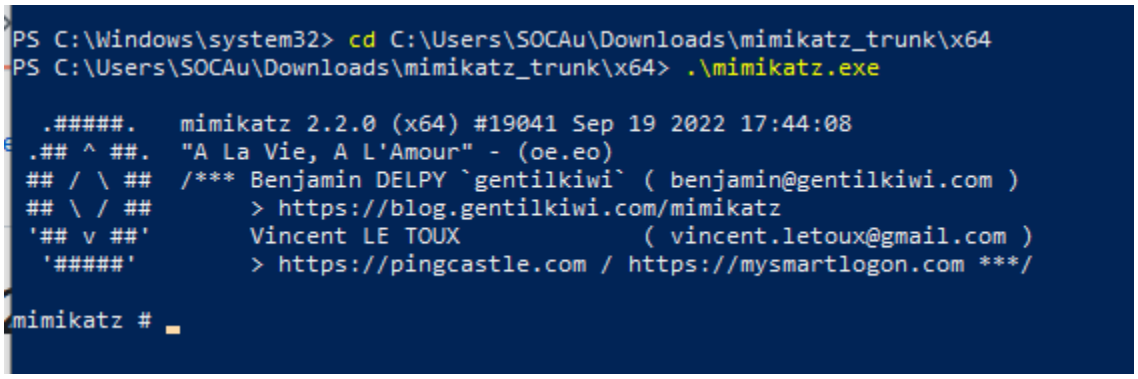

Next, we download Mimikatz

Disable Windows Security for the downloads folder

Download and extract Mimikatz

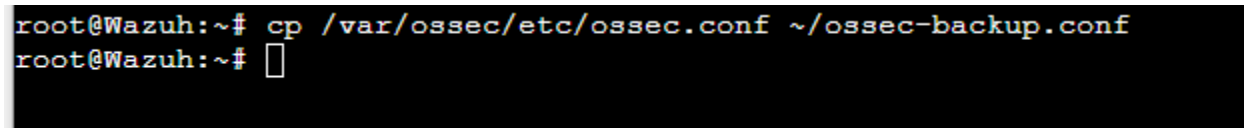


Open with PowerShell



Configure Wazuh to detect Mimikatz

Create a backup of ossec conf file,



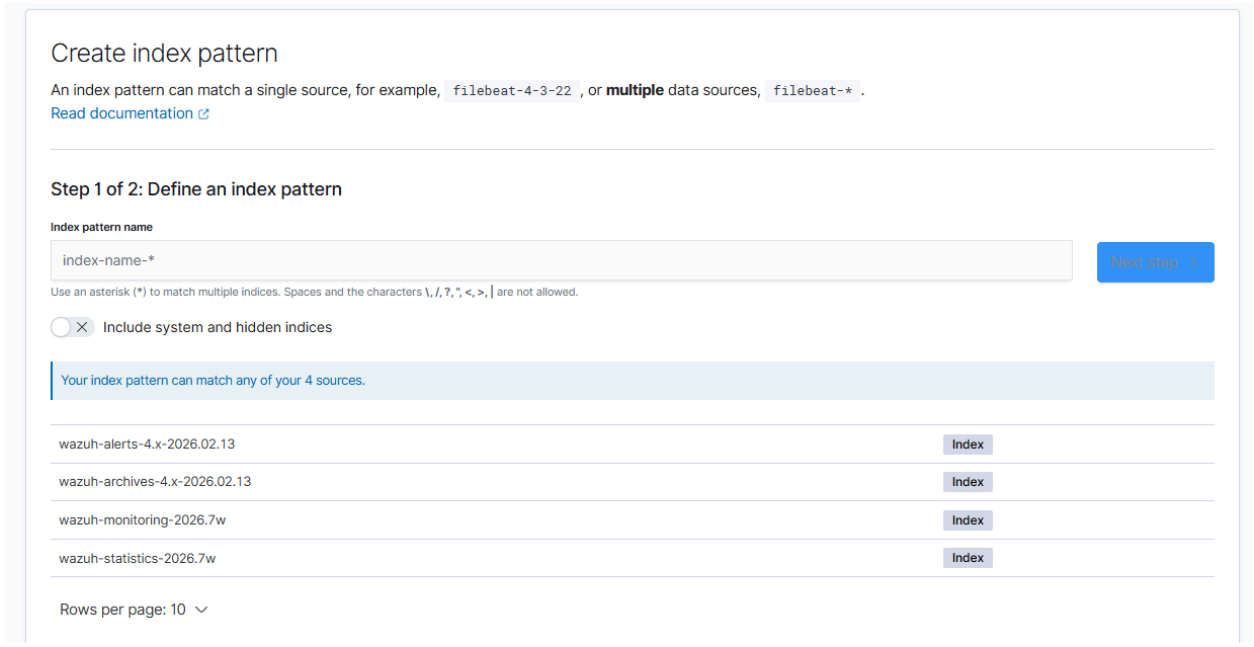
Edit the file, change logall to yes

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>yes</logall>
    <logall_json>yes</logall_json>
```

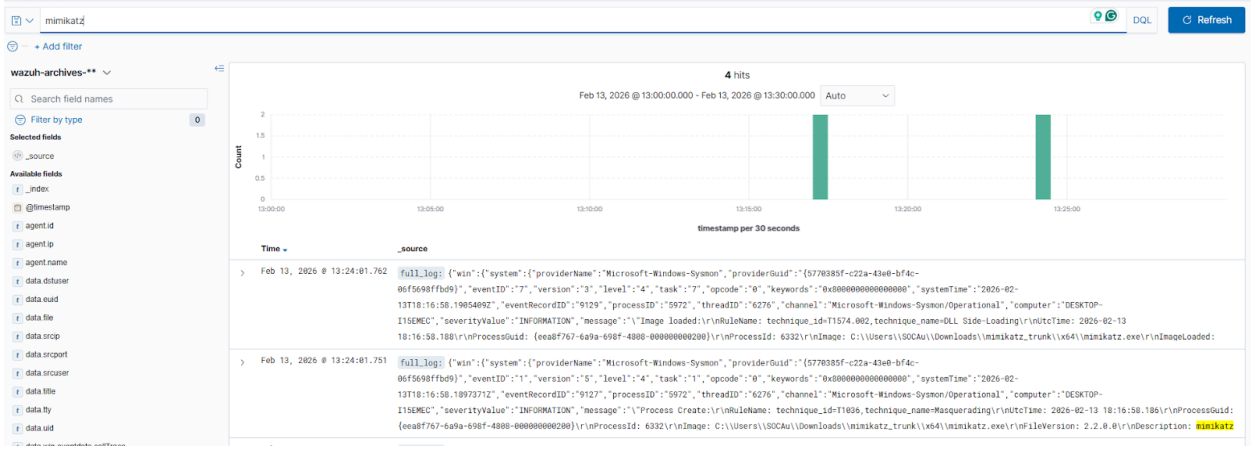
Next we need to edit filebeat, archives: enabled: true

```
  username: ${username}
  password: ${password}
  ssl.certificate_authorities:
    - /etc/filebeat/certs/root-ca.pem
  ssl.certificate: "/etc/filebeat/certs/wazuh-serv
  ssl.key: "/etc/filebeat/certs/wazuh-server-key.p
setup.template.json.enabled: true
setup.template.json.path: '/etc/filebeat/wazuh-tem
setup.template.json.name: 'wazuh'
setup.ilm.overwrite: true
setup.ilm.enabled: false

filebeat.modules:
  - module: wazuh
    alerts:
      enabled: true
    archives:
      enabled: true

logging.level: info
logging.to_files: true
logging.files:
  path: /var/log/filebeat
  name: filebeat
  keepfiles: 7
  permissions: 0644

logging.metrics.enabled: false

seccomp:
  default_action: allow
  syscalls:
  - action: allow
    names:
    - rseq
```

Now we need to create a new index on our wazuh dashboard



We can view Mimikatz logs in our archives index



Custom rules can be created in the rules management section

```
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

  <rule id="100002" level="15">
    <if_group>sysmon_event1</if_group>
    <field name="win.eventdata.originalFileName" type="pcre2">(?i)mimikatz\.exe</field>
    <description>Mimikatz usage detected</description>
    <mitre>
      <id>T1003</id>
    </mitre>
  </rule>

</group>

```

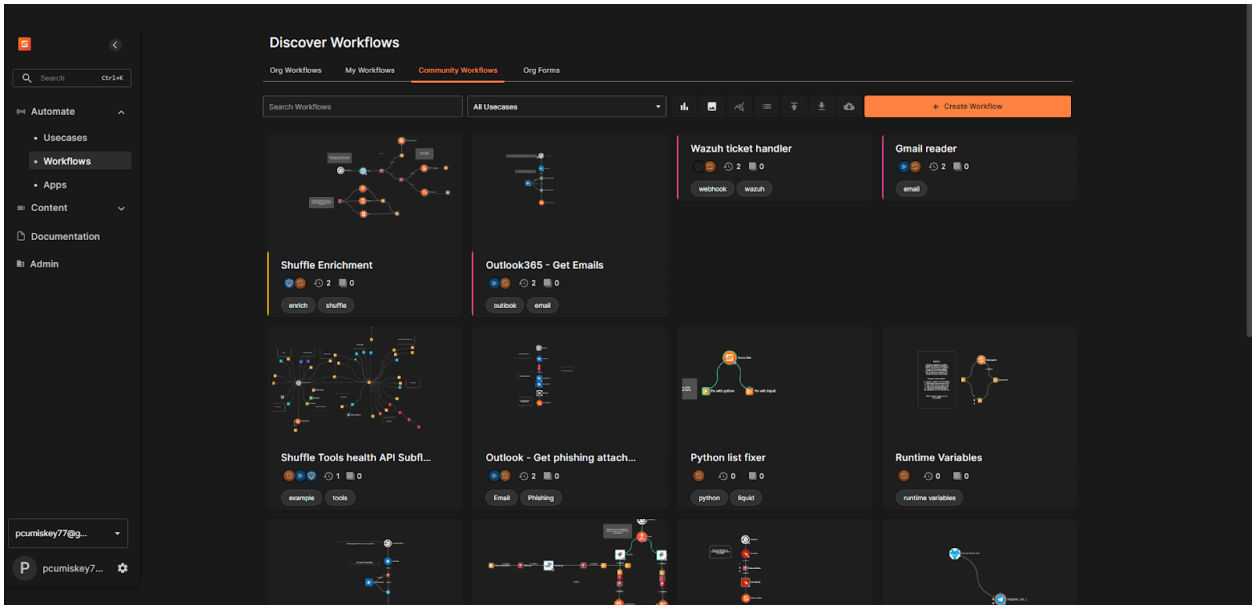
We can now detect the mimikatz usage

13:38:35.781				Movement			
Feb 13, 2026 @ 13:38:34.158	001	mydfir	T1003	Credential Access	Mimikatz usage detected	15	100002
Feb 13, 2026 @	000	Wazuh	T1110.001 T1021.004	Credential Access, Lateral	sshd: Attempt to login using a non-existent user	5	5710

Automation with Shuffle and TheHive

Shuffle

Shuffle is a soar that will assist with SOC automation



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 *

Soc Automation Project

Description

Usecases

Email management, Inter...

Tags

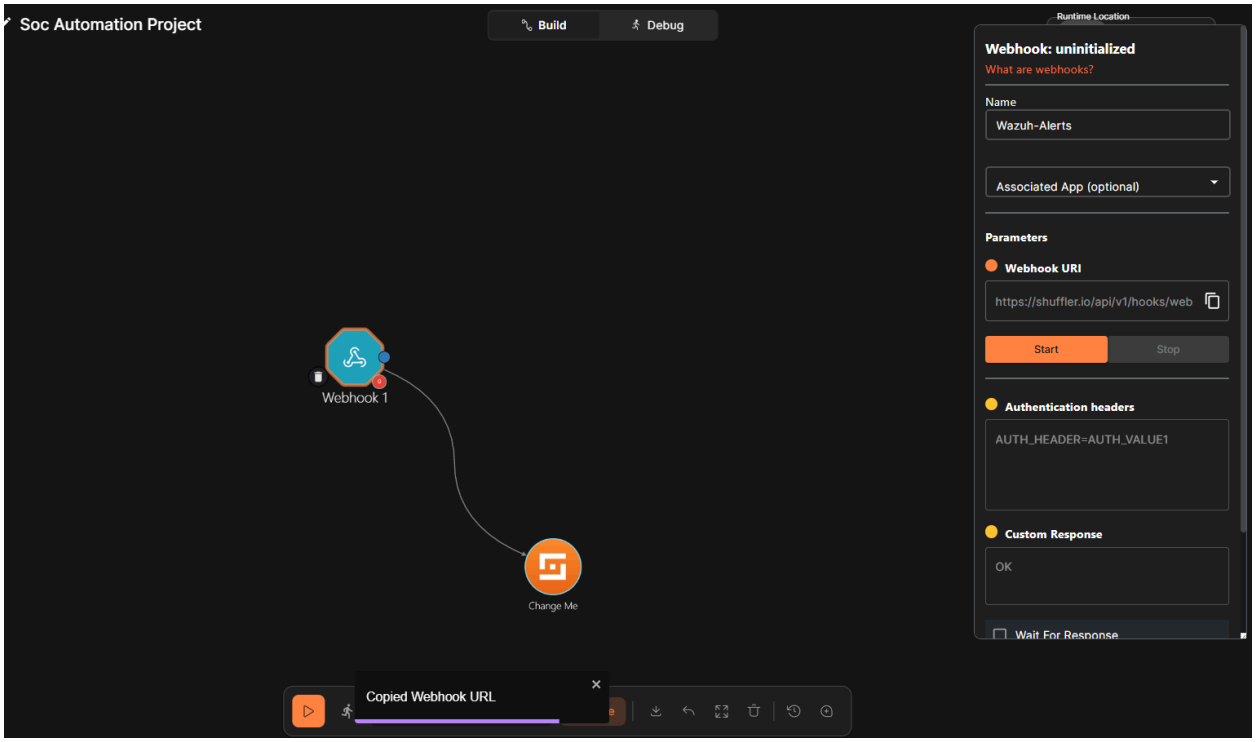
Generate Workflow from Flowchart (beta)

Click to upload your flowchart - Your LLM will convert it to a workflow

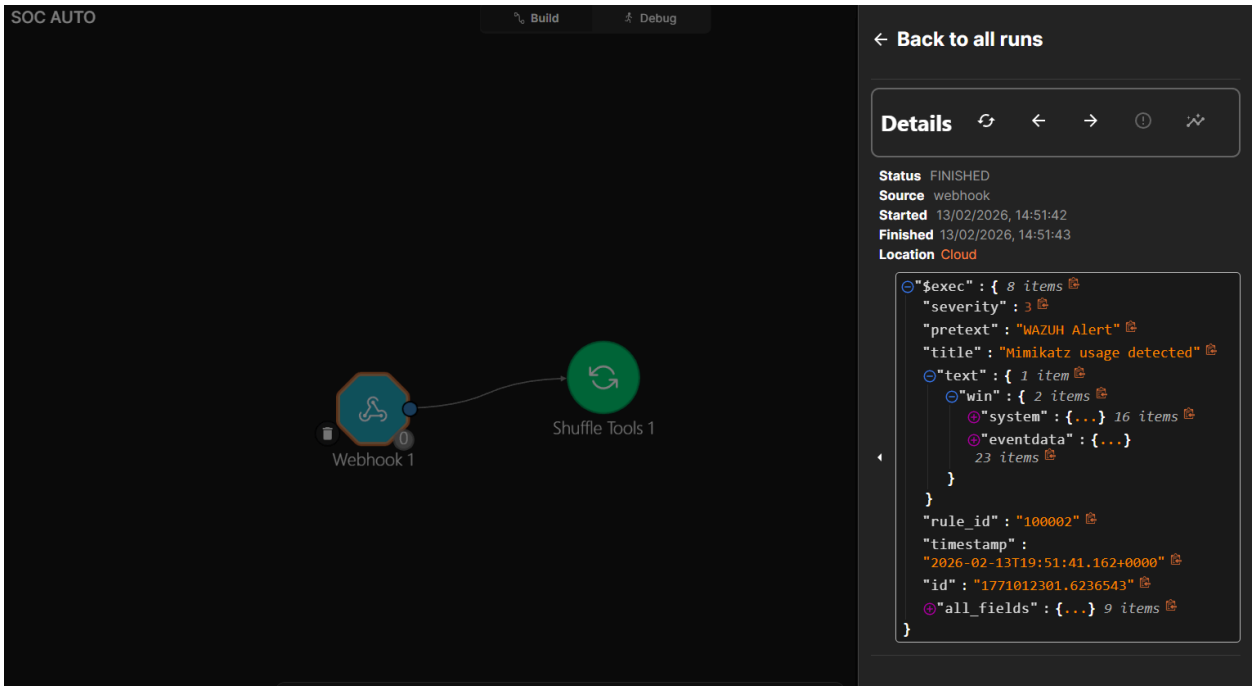
PNG, JPG, JPEG • Max 5MB

Create from scratch

AI Generate (beta)



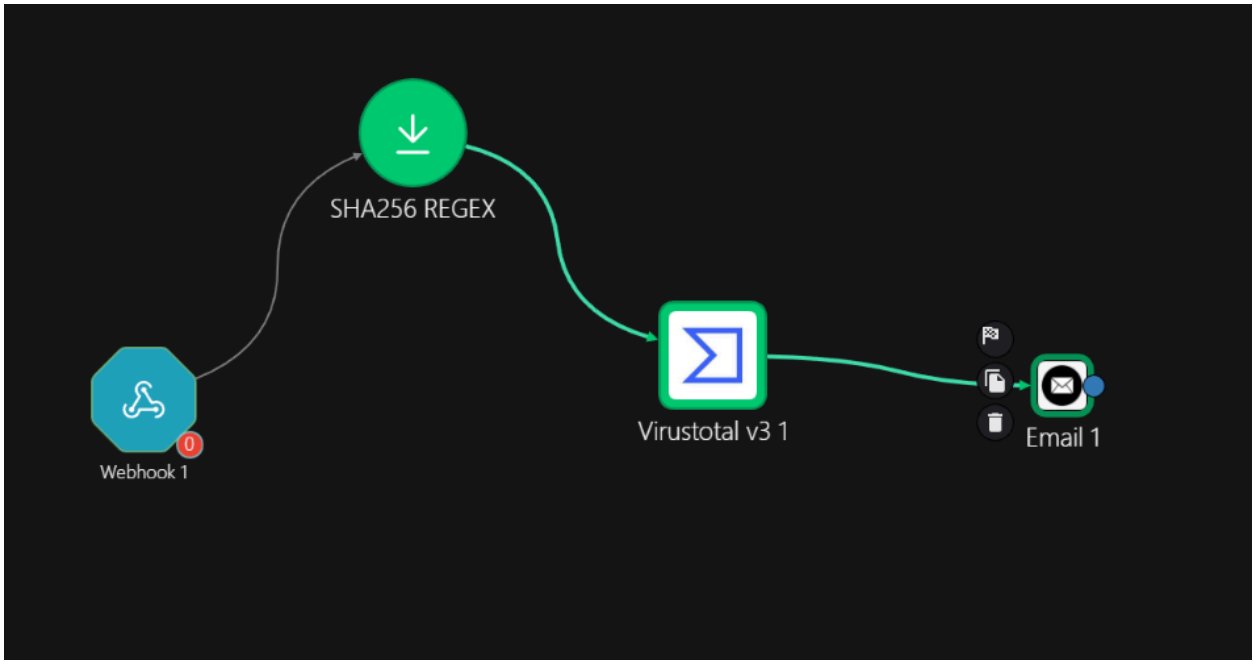
Next, we need to add an integration tag in the ossec configuration file and restart the service
We should end up with results like this

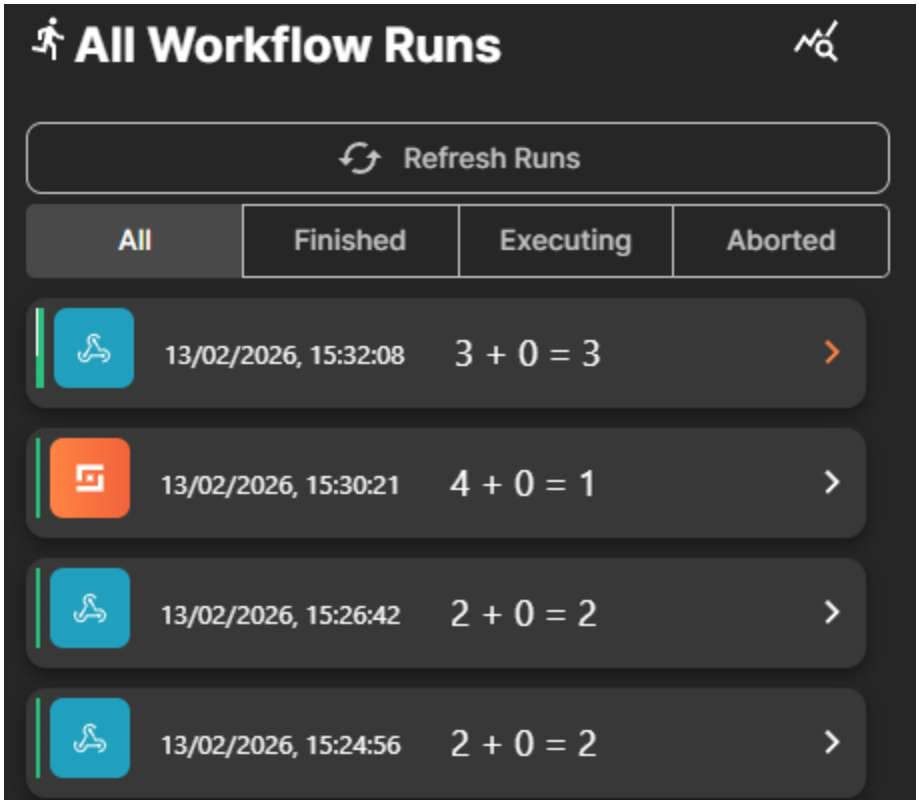


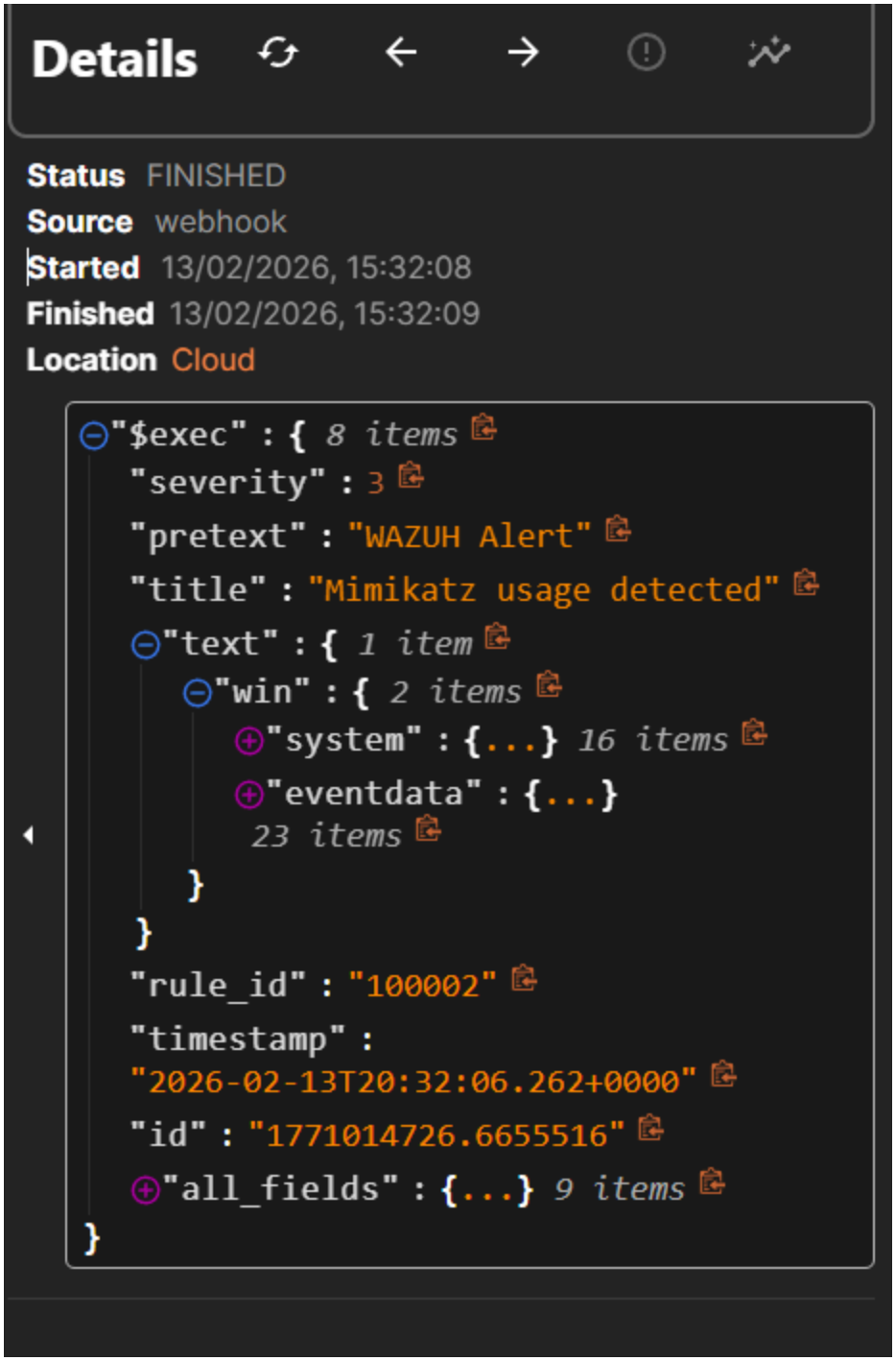
Next, we are gunna automatically extract a hash using REGEX to run through VirusTotal

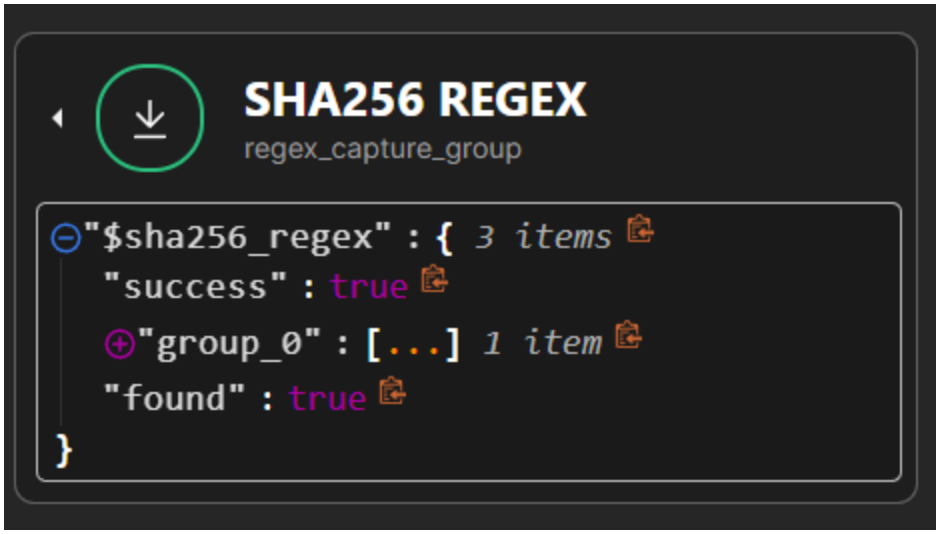
After the virus total is added, make these configurations

Lastly, by adding an email nod,e you can automatically send alerts to analysts.


SHA256 REGEX
Webhook 1
0
Virustotal v3 1
Email 1


All Workflow Runs
Refresh Runs
All
Finished
Executing
Aborted
13/02/2026, 15:32:08
3 + 0 = 3
13/02/2026, 15:30:21
4 + 0 = 1
13/02/2026, 15:26:42
2 + 0 = 2
13/02/2026, 15:24:56
2 + 0 = 2


Details
Status FINISHED
Source webhook
Started 13/02/2026, 15:32:08
Finished 13/02/2026, 15:32:09
Location Cloud
"$exec" : { 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" :
"2026-02-13T20:32:06.262+0000"
"id" : "1771014726.6655516"
"all_fields" : {...} 9 items
}


SHA256 REGEX
regex_capture_group
"$sha256_regex" : { 3 items
"success" : true
"group_0" : [...] 1 item
"found" : true
}


Virustotal v3 1
get_a_hash_report_
"$virustotal_v3_1" : [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
..."
}
"attributes" : {...}
41 items
}
}
"url" :
"https://www.virustotal.com/api/v3/fil
..."
"headers" : {...} 9 items
"cookies" : {} 0 items
"success" : true
}
]

I plan to add TheHive at a later date