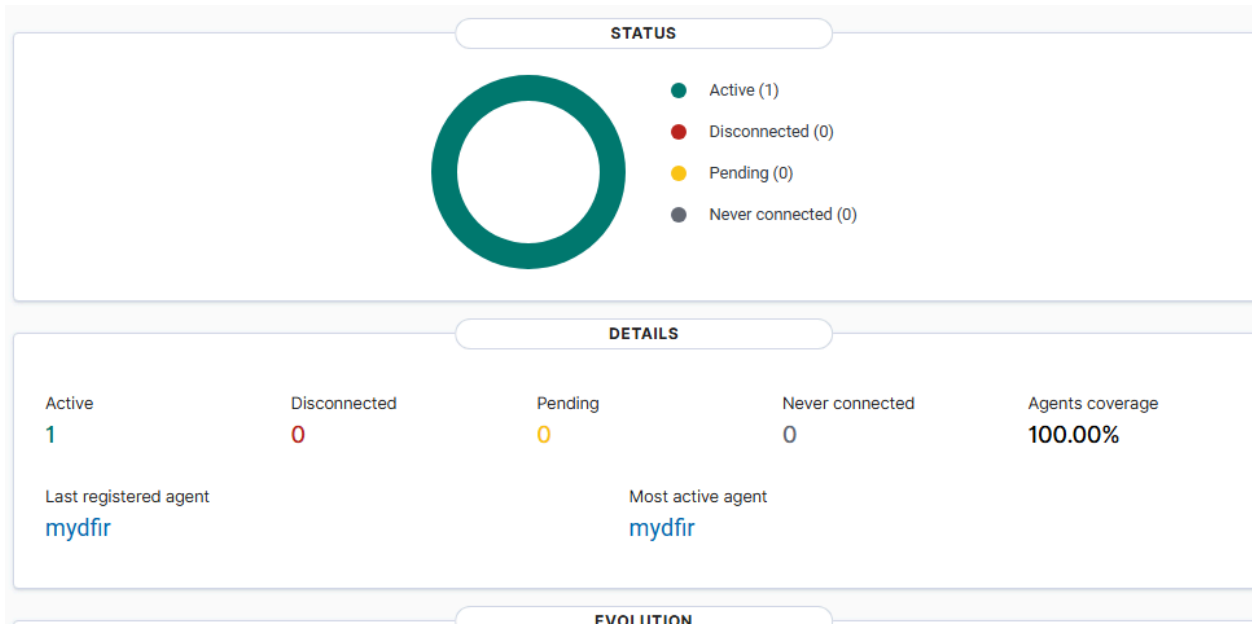


```
PS C:\> net start wazuhsvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\>
```

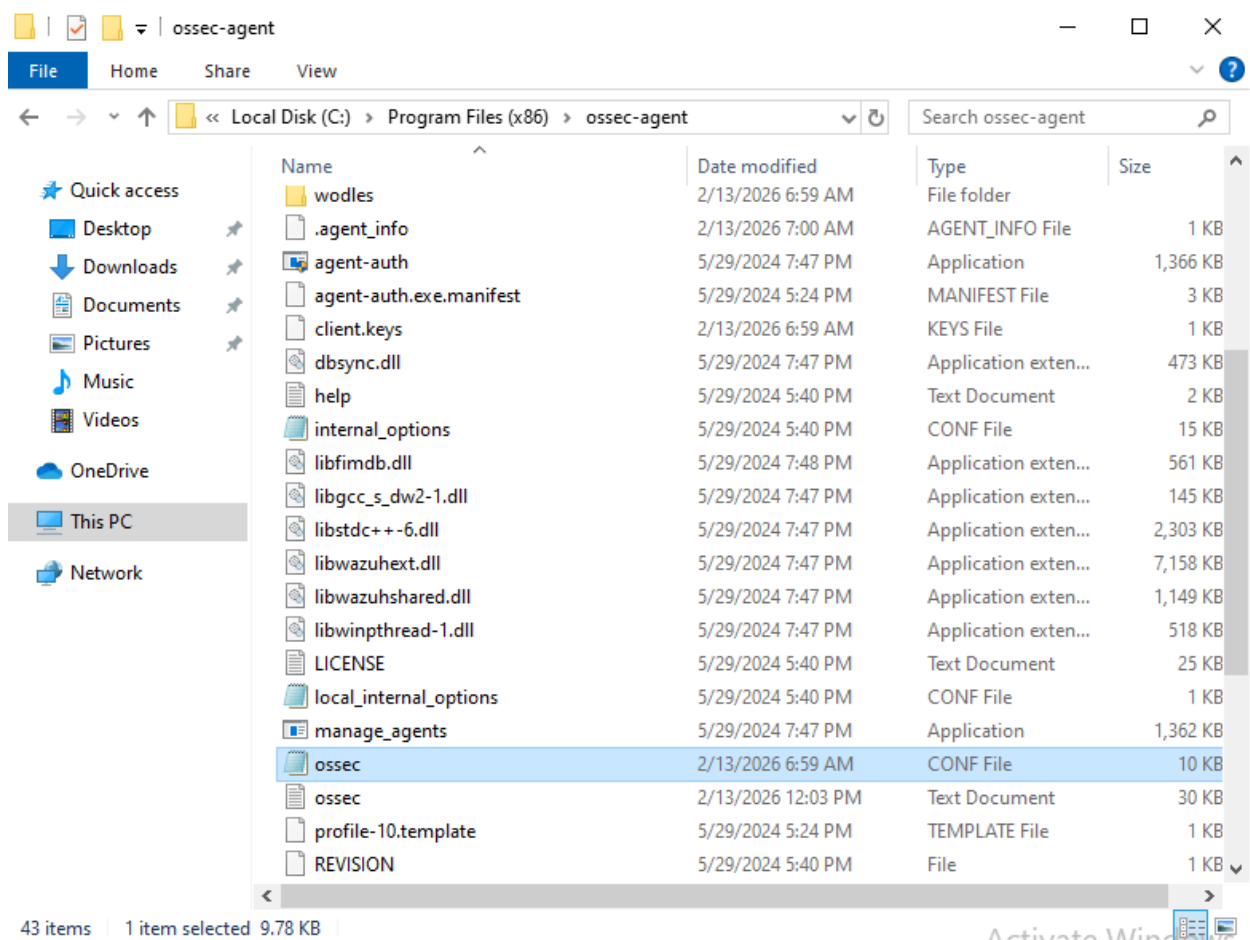
Next, start the service

We now have an agent running



Generate Telemetry & Ingest Into Wazuh

First, we need to configure the Windows 10 Wazuh 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>

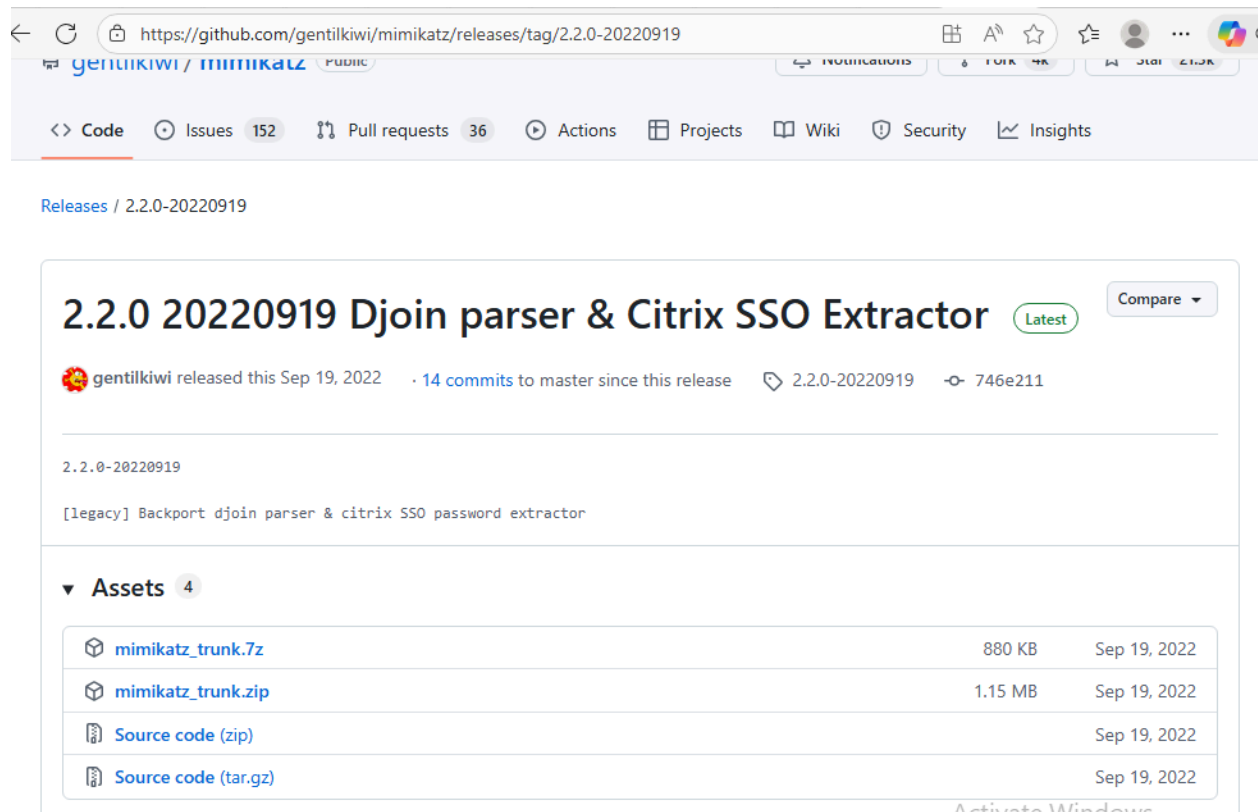
<!-- File integrity monitoring -->
<syscheck>
```

Activate Windows
Go to Settings to activate Windows.

Next, we download Mimikatz

Disable Windows Security for the downloads folder

Download and extract Mimikatz



The screenshot shows the GitHub release page for the repository `gentilkiwi/mimikatz`. The release is titled "2.2.0 20220919 Djoin parser & Citrix SSO Extractor" and is marked as the "Latest" version. It was released on September 19, 2022, and includes 14 commits to the master branch. The release description indicates it is a "[legacy] Backport djoin parser & citrix SSO password extractor".

Under the "Assets" section, there are four files available for download:

Asset Name	Size	Release Date
mimikatz_trunk.7z	880 KB	Sep 19, 2022
mimikatz_trunk.zip	1.15 MB	Sep 19, 2022
Source code (zip)		Sep 19, 2022
Source code (tar.gz)		Sep 19, 2022

Open with PowerShell

```
PS C:\Windows\system32> cd C:\Users\SOCau\Downloads\mimikatz_trunk\x64
PS C:\Users\SOCau\Downloads\mimikatz_trunk\x64> .\mimikatz.exe

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

mimikatz #
```

Configure Wazuh to detect Mimikatz

Create a backup of ossec conf file,

```
root@Wazuh:~# cp /var/ossec/etc/ossec.conf ~/ossec-backup.conf
root@Wazuh:~#
```

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

Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22`, or **multiple** data sources, `filebeat-*`.
[Read documentation](#)

Step 1 of 2: Define an index pattern

Index pattern name

[Next step](#)

Use an asterisk (*) to match multiple indices. Spaces and the characters `\, /, ?, *, <, >, |` are not allowed.

Include system and hidden indices

Your index pattern can match any of your 4 sources.

wazuh-alerts-4.x-2026.02.13	Index
wazuh-archives-4.x-2026.02.13	Index
wazuh-monitoring-2026.7w	Index
wazuh-statistics-2026.7w	Index

Rows per page: 10

wazuh-archives-4.x-2026.02.13 227 hits

Feb 13, 2026 @ 13:12:53.131

```
predecoder.hostname: Wazuh predecoder.program_name: sshd predecoder.timestamp: Feb 13 18:12:52 agent.name: Wazuh agent.id: 000 manager.name: Wazuh decoder.parent: sshd decoder.name: sshd full_log: Feb 13 18:12:52 Wazuh sshd[76396]: Received disconnect from 91.224.92.108 port 38972:111 [preauth] input.type: log @timestamp: Feb 13, 2026 @ 13:12:53.131 location: /var/log/auth.log id: 1771966373.5414637 timestamp: Feb 13, 2026 @ 13:12:53.131 index: wazuh-archives-4.x-2026.02.13
```

Feb 13, 2026 @ 13:12:53.131

```
predecoder.hostname: Wazuh predecoder.program_name: sshd predecoder.timestamp: Feb 13 18:12:51 agent.name: Wazuh agent.id: 000 manager.name: Wazuh rule.mail: false rule.level: 5 rule.hipaa: 164.312.b rule.pci_dss: 10.2.4, 10.2.5 rule.tsc: C06.1, C06.8, C07.2, C07.3 rule.description: ssh: authentication failed. rule.groups: syslog, sshd, authentication_failed rule.mitre: 888.S3; AU.14, AC.7 rule.gdpr: IV.35.7.4, IV.32.2 rule.firedtimes: 0 rule.mitre.technique: Password Guessing, SSH rule.mitre.id: 11116.081, T1021.004 rule.mitre.tactic: Credential Access, Lateral Movement rule.id: 5769 rule.gpg13: 7.1 decoder.name: sshd full_log: Feb 13 18:12:51 Wazuh sshd[76396]: message repeated 2 times: [ Failed password for root from 91.224.92.108 port 38972 ssh2] input.type: log @timestamp: Feb 13, 2026 @ 13:12:53.131 location: /var/log/auth.log
```

Feb 13, 2026 @ 13:12:53.131

```
predecoder.hostname: Wazuh predecoder.program_name: sshd predecoder.timestamp: Feb 13 18:12:52 agent.name: Wazuh agent.id: 000 manager.name: Wazuh decoder.name: sshd full_log: Feb 13 18:12:52 Wazuh sshd[76396]: Disconnected from authenticating user root 91.224.92.108 port 38972 [preauth] input.type: log @timestamp: Feb 13, 2026 @ 13:12:53.131 location: /var/log/auth.log id: 1771966373.5414637 timestamp: Feb 13, 2026 @ 13:12:53.131 index: wazuh-archives-4.x-2026.02.13
```

Feb 13, 2026 @ 13:12:53.131

```
agent.name: Wazuh agent.id: 000 data.scrip: 91.224.92.108 data.dtsuser: root rule.mail: false rule.level: 10 rule.pci_dss: 10.2.4, 10.2.5 rule.hipaa: 164.312.b rule.tsc: C06.1, C06.8, C07.2, C07.3 rule.description: syslog: User missed the password more than one time rule.groups: syslog, access_control, authentication_failed
```

We can view Mimikatz logs in our archives index

mimikatz 4 hits

Feb 13, 2026 @ 13:24:01.762

```
full_log: ("win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":{"5778385f-c22a-43e8-bf4c-06f5698fbd9"},"eventId":7,"version":3,"level":4,"task":7,"opcode":0,"keywords":"0x0000000000000000","systemTime":"2026-02-13T18:16:58.1985489Z"},"eventRecordID":"9129","processID":"5972","threadID":"6276","channel":"Microsoft-Windows-Sysmon/Operational","computer":"DESKTOP-I15EMEC","severityValue":"INFORMATION","message":"\\Image Loaded:\\r\\nRuleName: technique_id=T1574.002,technique_name=DLL Side-Loading\\r\\nTime: 2026-02-13 18:16:58.188\\r\\nProcessId: (ea8f767-6a9a-698f-4888-000000000208)\\r\\nProcessId: 6332\\r\\nImage: C:\\Users\\S0CAU\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe\\r\\nImageLoaded:
```

Feb 13, 2026 @ 13:24:01.751

```
full_log: ("win":{"system":{"providerName":"Microsoft-Windows-Sysmon","providerGuid":{"5778385f-c22a-43e8-bf4c-06f5698fbd9"},"eventId":1,"version":5,"level":4,"task":1,"opcode":0,"keywords":"0x0000000000000000","systemTime":"2026-02-13T18:16:58.1897372Z"},"eventRecordID":"9127","processID":"5972","threadID":"6276","channel":"Microsoft-Windows-Sysmon/Operational","computer":"DESKTOP-I15EMEC","severityValue":"INFORMATION","message":"\\Process Create:\\r\\nRuleName: technique_id=T1036,technique_name=Masquerading\\r\\nTime: 2026-02-13 18:16:58.186\\r\\nProcessId: (ea8f767-6a9a-698f-4888-000000000208)\\r\\nProcessId: 6332\\r\\nImage: C:\\Users\\S0CAU\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe\\r\\nFileVersion: 2.2.0.0\\r\\nDescription: Mimikatz
```

Custom rules can be created in the rules management section

```
1 <!-- Local rules -->
2
3 <!-- Modify it at your will. -->
4 <!-- Copyright (C) 2015, Wazuh Inc. -->
5
6 <!-- Example -->
7 <group name="local,syslog,sshd,">
8
9 <!--
10 Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
11 -->
12 <rule id="100001" level="5">
13 <if_sid>5716</if_sid>
14 <srcip>1.1.1.1</srcip>
15 <description>sshd: authentication failed from IP 1.1.1.1.</description>
16 <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
17 </rule>
18
19 <rule id="100002" level="15">
20 <if_group>sysmon_event1</if_group>
21 <field name="win.eventdata.originalFileName" type="pcre2">(i)mimikatz\.exe</field>
22 <description>Mimikatz usage detected</description>
23 <mitre>
24 <id>T1003</id>
25 </mitre>
26 </rule>
27
28 </group>
29
```

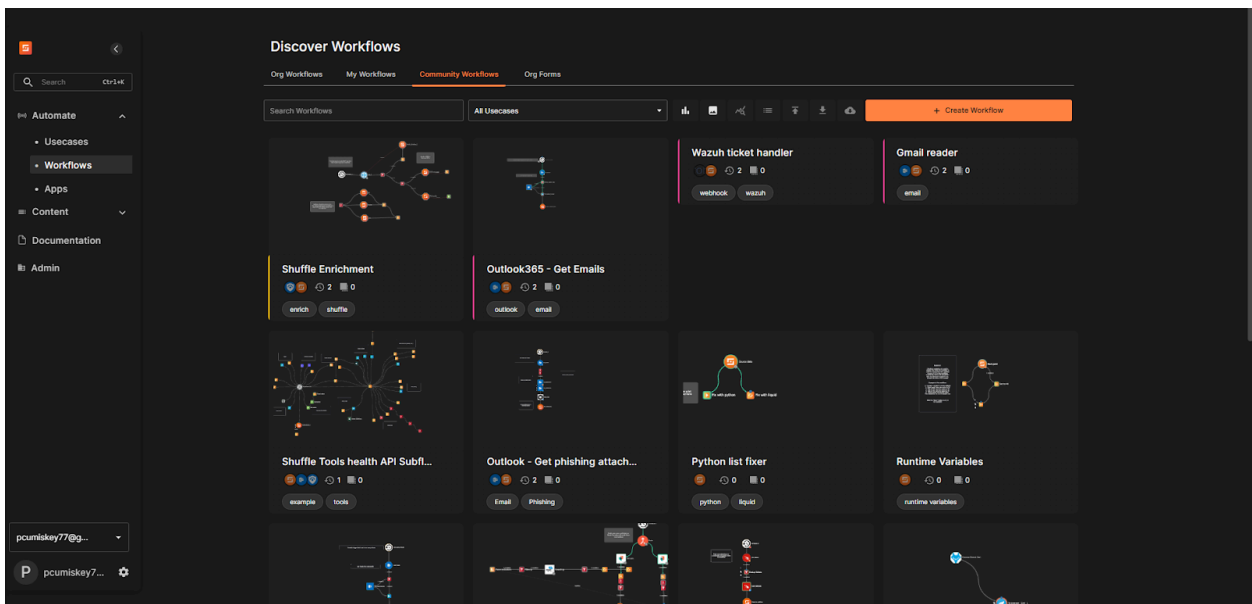
We can now detect the mimikatz usage

Time	Event ID	Source	Category	Severity	Score
Feb 13, 2020 @ 13:38:34.158	001	mydfir	T1003	Credential Access	Mimikatz usage detected

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)

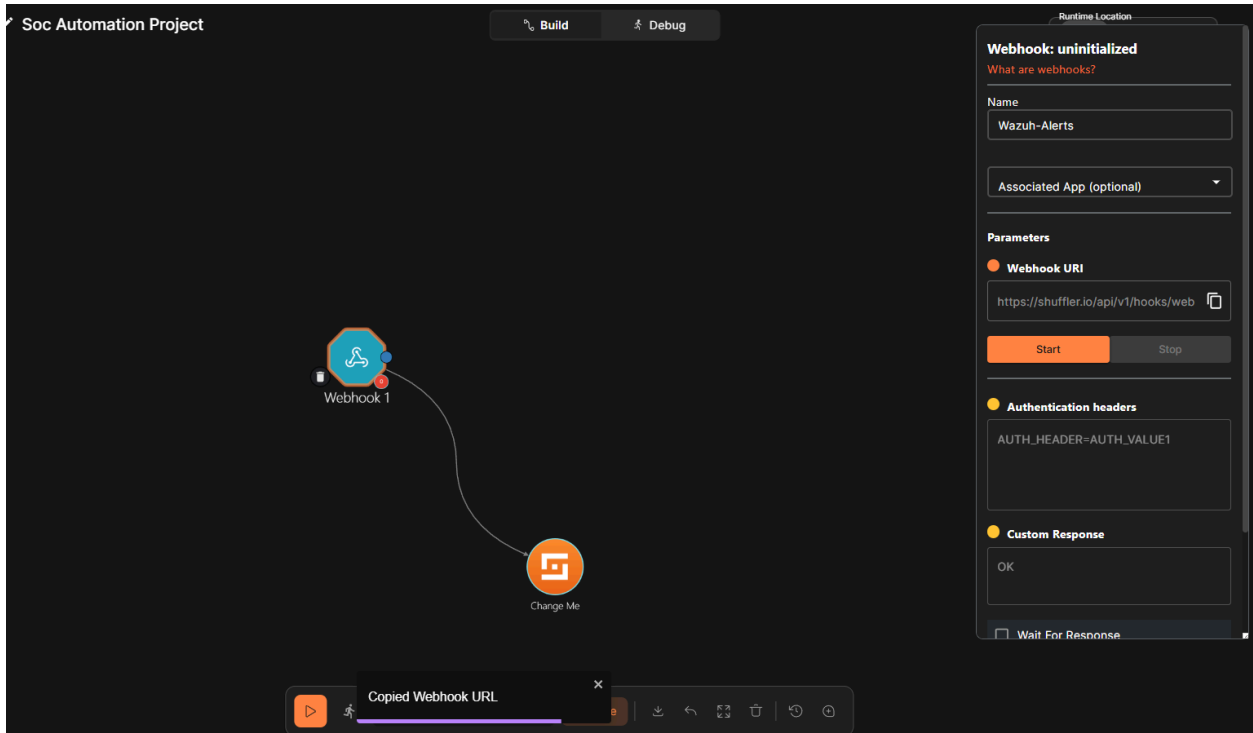
Click to upload your flowchart - Your LLM will convert it to a workflow

PNG, JPG, JPEG • Max 5MB

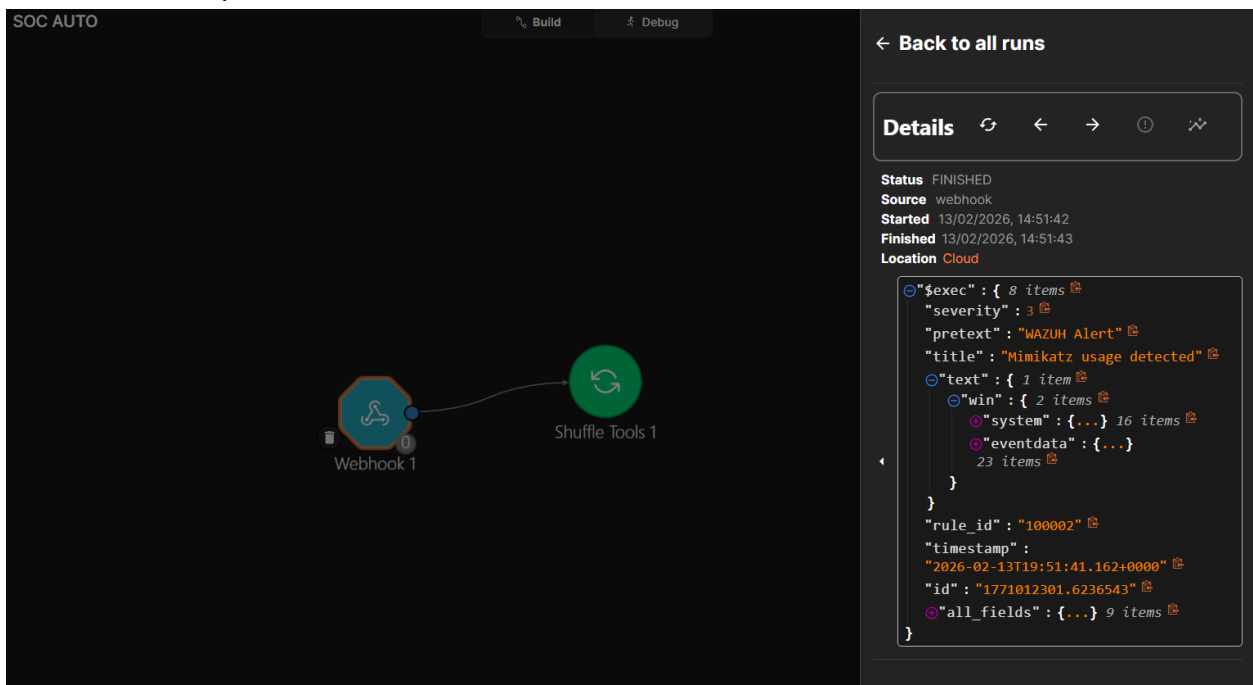
Create from scratch



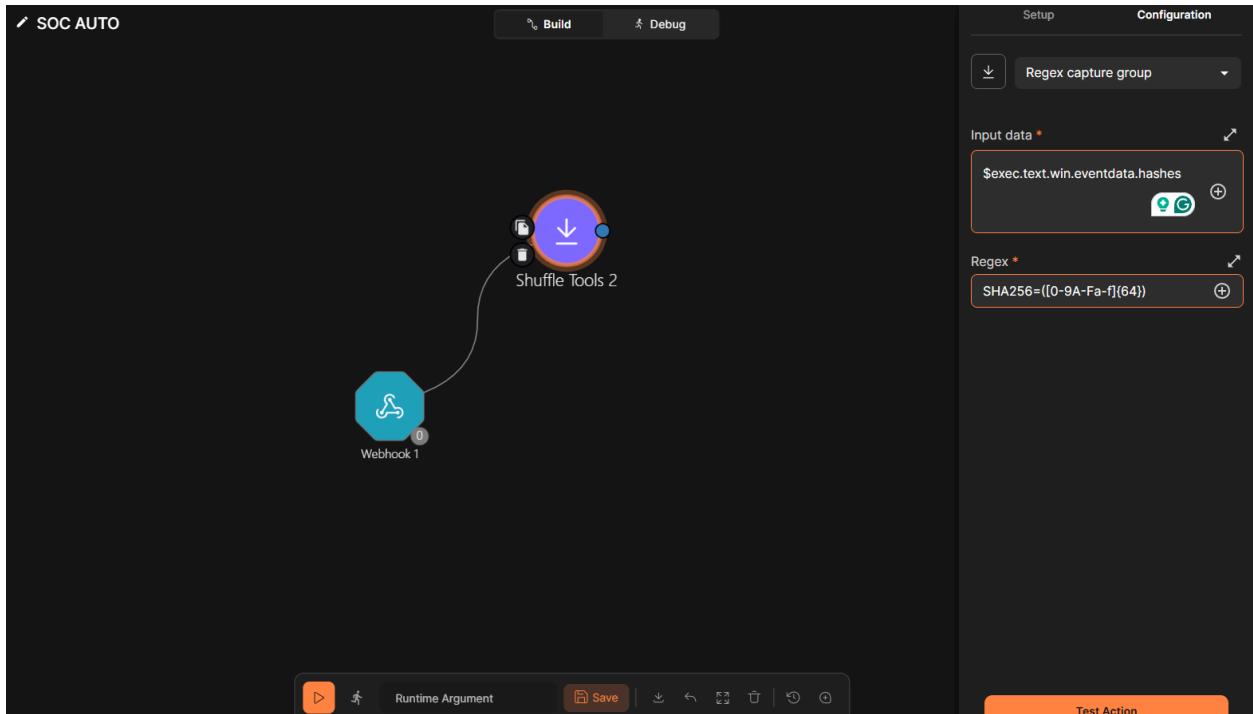
AI Generate (beta)



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



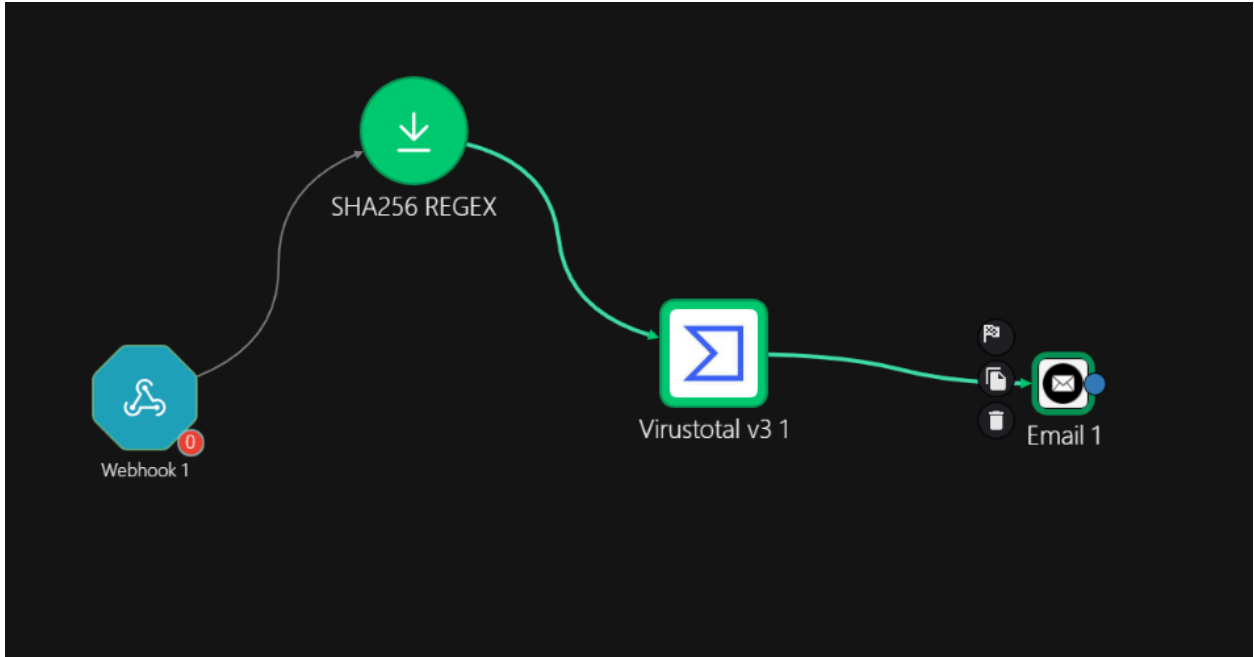
Next, we are gunna automatically extract a hash using REGEX to run through VirusTotal



After the virus total is added, make these configurations




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



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/api/v3/files/61c0810a23580cf492a6ba4f7654566" 📄  
          ...  
        }  
        ⊕ "attributes" : {...} 📄  
          41 items 📄  
      }  
    }  
    "url" :  
    "https://www.virustotal.com/api/v3/files/61c0810a23580cf492a6ba4f7654566" 📄  
    ...  
    ⊕ "headers" : {...} 9 items 📄  
    ⊕ "cookies" : {} 0 items 📄  
    "success" : true 📄  
  }  
]
```



I plan to add TheHive at a later date