# Bijlagen

## BIJLAGE 1: OSSEC.CONF

```
<!--
  Wazuh - Manager - Default configuration for ubuntu 24.04
  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>no</logall>
    <logall_json>no</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>
    <update_check>yes</update_check>
  </global>

  <alerts>
    <log_alert_level>8</log_alert_level>
    <email_alert_level>12</email_alert_level>
  </alerts>

  <integration>
    <name>custom-shuffle</name>
    <hook_url>https://172.17.0.226:3443/api/v1/hooks/webhook_ebd9e0e1-c840-49af-b05d-384c8e5015be </hook_url> <!-- Replace with your Shuffle hook URL -->
    <level>12</level>
    <alert_format>json</alert_format>
  </integration>

  <!-- Choose between "plain", "json", or "plain,json" for the format of internal logs -->
  <logging>
    <log_format>json</log_format>
  </logging>
```

```
  <remote>
    <connection>secure</connection>
    <port>1514</port>
    <protocol>tcp</protocol>
    <queue_size>131072</queue_size>
  </remote>

  <!-- Policy monitoring -->
  <rootcheck>
    <disabled>no</disabled>
    <check_files>yes</check_files>
    <check_trojans>yes</check_trojans>
    <check_dev>yes</check_dev>
    <check_sys>yes</check_sys>
    <check_pids>yes</check_pids>
    <check_ports>yes</check_ports>
    <check_if>yes</check_if>

    <!-- Frequency that rootcheck is executed - every 12 hours -->
    <frequency>43200</frequency>

    <rootkit_files>etc/rootcheck/rootkit_files.txt</rootkit_files>
    <rootkit_trojans>etc/rootcheck/rootkit_trojans.txt</rootkit_trojans>

    <skip_nfs>yes</skip_nfs>

    <ignore>/var/lib/containerd</ignore>
    <ignore>/var/lib/docker/overlay2</ignore>
  </rootcheck>

  <wodle name="cis-cat">
    <disabled>yes</disabled>
    <timeout>1800</timeout>
    <interval>1d</interval>
    <scan-on-start>yes</scan-on-start>

    <java_path>wodles/java</java_path>
    <ciscat_path>wodles/ciscat</ciscat_path>
  </wodle>
```

```
<!-- Osquery integration -->
<wodle name="osquery">
  <disabled>yes</disabled>
  <run_daemon>yes</run_daemon>
  <log_path>/var/log/osquery/osqueryd.results.log</log_path>
  <config_path>/etc/osquery/osquery.conf</config_path>
  <add_labels>yes</add_labels>
</wodle>

<!-- System inventory -->
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <scan_on_start>yes</scan_on_start>
  <hardware>yes</hardware>
  <os>yes</os>
  <network>yes</network>
  <packages>yes</packages>
  <ports all="no">yes</ports>
  <processes>yes</processes>

  <!-- Database synchronization settings -->
  <synchronization>
    <max_eps>10</max_eps>
  </synchronization>
</wodle>

<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<vulnerability-detection>
  <enabled>yes</enabled>
  <index-status>yes</index-status>
  <feed-update-interval>60m</feed-update-interval>
</vulnerability-detection>
```

```
<indexer>
  <enabled>yes</enabled>
  <hosts>
    <host>https://172.17.0.232:9200</host>
  </hosts>
  <ssl>
    <certificate_authorities>
      <ca>/etc/filebeat/certs/root-ca.pem</ca>
    </certificate_authorities>
    <certificate>/etc/filebeat/certs/filebeat.pem</certificate>
    <key>/etc/filebeat/certs/filebeat-key.pem</key>
  </ssl>
</indexer>

<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <scan_on_start>yes</scan_on_start>

  <!-- Generate alert when new file detected -->
  <alert_new_files>yes</alert_new_files>

  <!-- Don't ignore files that change more than 'frequency' times -->
  <auto_ignore frequency="10" timeframe="3600">no</auto_ignore>

  <!-- Directories to check  (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>

  <!-- Files/directories to ignore -->
  <ignore>/etc/mtab</ignore>
  <ignore>/etc/hosts.deny</ignore>
  <ignore>/etc/mail/statistics</ignore>
  <ignore>/etc/random-seed</ignore>
  <ignore>/etc/random.seed</ignore>
  <ignore>/etc/adjtime</ignore>
  <ignore>/etc/httpd/logs</ignore>
  <ignore>/etc/utmpx</ignore>
  <ignore>/etc/wtmpx</ignore>
```

```
  <ignore>/etc/cups/certs</ignore>
  <ignore>/etc/dumpdates</ignore>
  <ignore>/etc/svc/volatile</ignore>

  <!-- File types to ignore -->
  <ignore type="sregex">.log$|.swp$</ignore>

  <!-- Check the file, but never compute the diff -->
  <nodiff>/etc/ssl/private.key</nodiff>

  <skip_nfs>yes</skip_nfs>
  <skip_dev>yes</skip_dev>
  <skip_proc>yes</skip_proc>
  <skip_sys>yes</skip_sys>

  <!-- Nice value for Syscheck process -->
  <process_priority>10</process_priority>

  <!-- Maximum output throughput -->
  <max_eps>50</max_eps>

  <!-- Database synchronization settings -->
  <synchronization>
    <enabled>yes</enabled>
    <interval>5m</interval>
    <max_eps>10</max_eps>
  </synchronization>
</syscheck>

<!-- Active response -->
<global>
  <white_list>127.0.0.1</white_list>
  <white_list>^localhost.localdomain$</white_list>
  <white_list>127.0.0.53</white_list>
</global>

<command>
  <name>disable-account</name>
  <executable>disable-account</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>
```

```
  <command>
    <name>restart-wazuh</name>
    <executable>restart-wazuh</executable>
  </command>

  <command>
    <name>firewall-drop</name>
    <executable>firewall-drop</executable>
    <timeout_allowed>yes</timeout_allowed>
  </command>

  <command>
    <name>host-deny</name>
    <executable>host-deny</executable>
    <timeout_allowed>yes</timeout_allowed>
  </command>

  <command>
    <name>route-null</name>
    <executable>route-null</executable>
    <timeout_allowed>yes</timeout_allowed>
  </command>

  <command>
    <name>win_route-null</name>
    <executable>route-null.exe</executable>
    <timeout_allowed>yes</timeout_allowed>
  </command>

  <command>
    <name>netsh</name>
    <executable>netsh.exe</executable>
    <timeout_allowed>yes</timeout_allowed>
  </command>

  <!--
  <active-response>
    active-response options here
  </active-response>
  -->
```

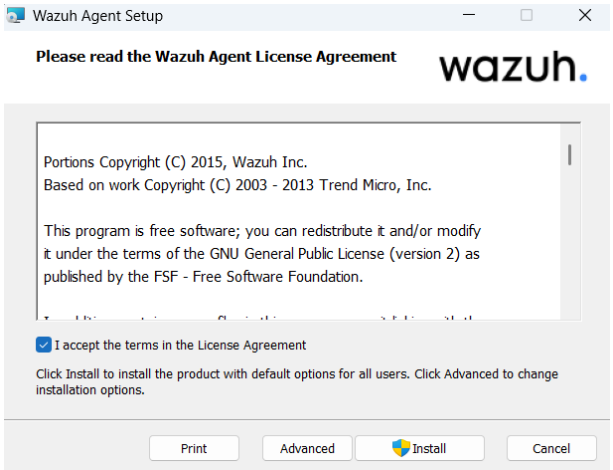
```
  <!-- Log analysis -->
  <localfile>
    <log_format>command</log_format>
    <command>df -P</command>
    <frequency>360</frequency>
  </localfile>

  <localfile>
    <log_format>full_command</log_format>
    <command>netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:digit:]]\+\ \+[[:digit:]]\+\ \+\(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:\*]\+\).\+\ \([[:digit:]]*
    <alias>netstat listening ports</alias>
    <frequency>360</frequency>
  </localfile>

  <localfile>
    <log_format>full_command</log_format>
    <command>last -n 20</command>
    <frequency>360</frequency>
  </localfile>

  <ruleset>
    <!-- Default ruleset -->
    <decoder_dir>ruleset/decoders</decoder_dir>
    <rule_dir>ruleset/rules</rule_dir>
    <rule_exclude>0215-policy_rules.xml</rule_exclude>
    <list>etc/lists/audit-keys</list>
    <list>etc/lists/amazon/aws-eventnames</list>
    <list>etc/lists/security-eventchannel</list>

    <!-- User-defined ruleset -->
    <decoder_dir>etc/decoders</decoder_dir>
    <rule_dir>etc/rules</rule_dir>
  </ruleset>

  <rule_test>
    <enabled>yes</enabled>
    <threads>1</threads>
    <max_sessions>64</max_sessions>
    <session_timeout>15m</session_timeout>
  </rule_test>
```

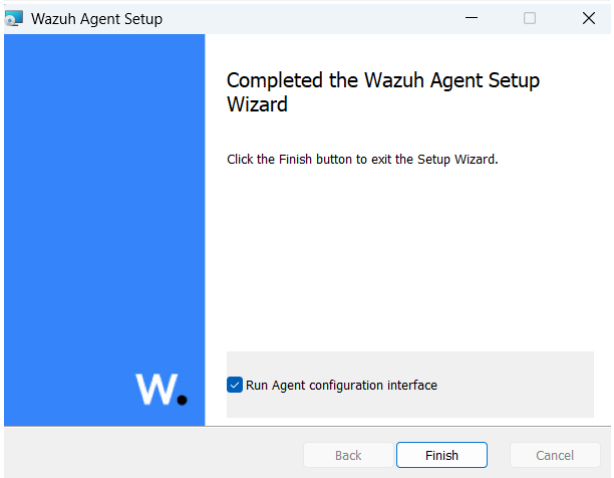
```
  <!-- Configuration for wazuh-authd -->
  <auth>
    <disabled>no</disabled>
    <port>1515</port>
    <use_source_ip>no</use_source_ip>
    <purge>yes</purge>
    <use_password>no</use_password>
    <ciphers>HIGH:!ADH:!EXP:!MD5:!RC4:!3DES:!CAMELLIA:@STRENGTH</ciphers>
    <!-- <ssl_agent_ca></ssl_agent_ca> -->
    <ssl_verify_host>no</ssl_verify_host>
    <ssl_manager_cert>etc/sslmanager.cert</ssl_manager_cert>
    <ssl_manager_key>etc/sslmanager.key</ssl_manager_key>
    <ssl_auto_negotiate>no</ssl_auto_negotiate>
  </auth>

  <cluster>
    <name>wazuh</name>
    <node_name>node01</node_name>
    <node_type>master</node_type>
    <key></key>
    <port>1516</port>
    <bind_addr>0.0.0.0</bind_addr>
    <nodes>
        <node>NODE_IP</node>
    </nodes>
    <hidden>no</hidden>
    <disabled>yes</disabled>
  </cluster>

</ossec_config>
```

### BIJLAGE 2: HANDLEIDING WAZUH AGENT INSTALLEREN

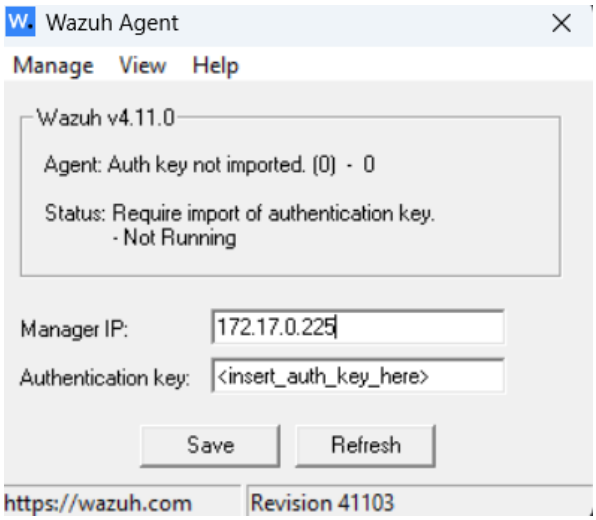
# Agent configuration

1. Download de Wazuh Agent via https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.0-1.msi en run de installer.
2. Volg de installatiestappen zoals hieronder. **Belangrijk** om **Run Agent configuration interface** aan te vinken. Als je vergeten bent aan te vinken of Wazuh Agent opent niet, zie Troubleshooting of Wazuh manager IP aanpassen.

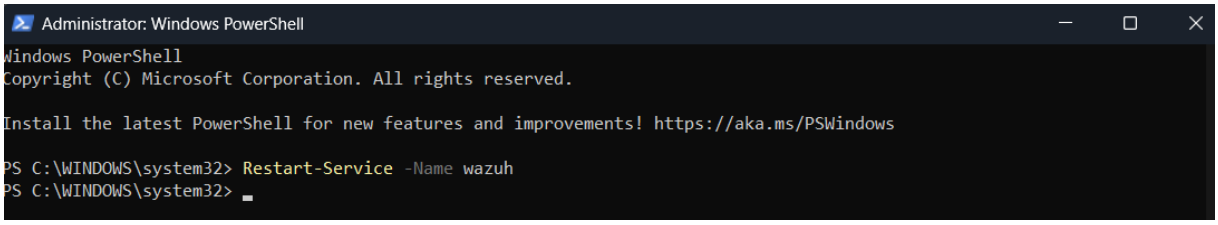


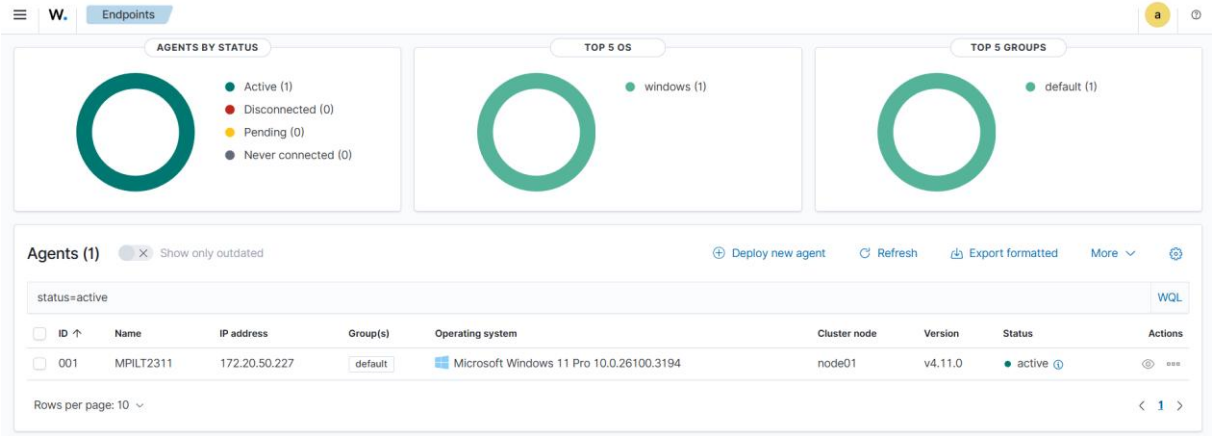

3. Vul het IP-adres van de Wazuh-manager in: 172.17.0.225. Laat de rest op default settings.



4. Herstart de Wazuh service in Powershell met Administrator rechten met het volgende commando: **Restart-Service -Name wazuh.**

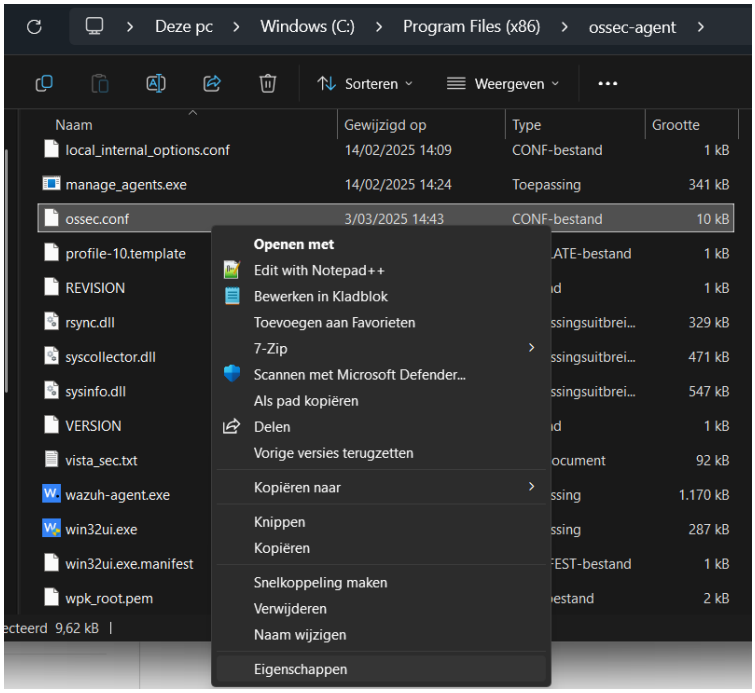



5. Controleer op Wazuh manager of de nieuwe agent toegevoegd is.

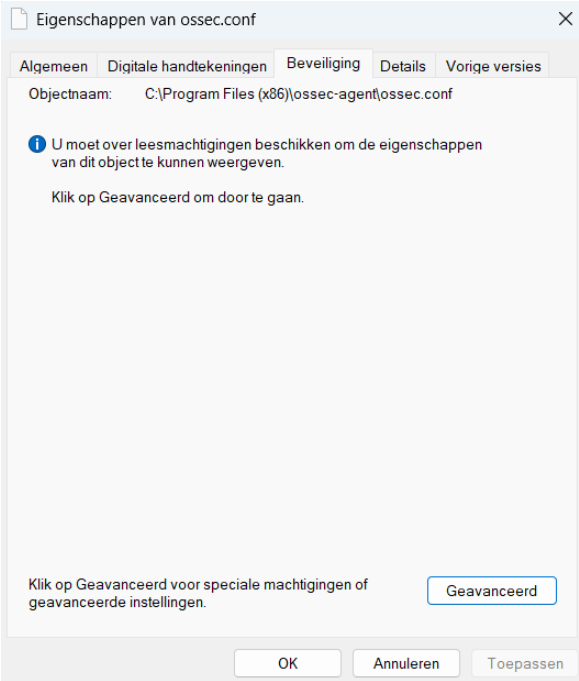


# Troubleshooting of Wazuh manager IP aanpassen

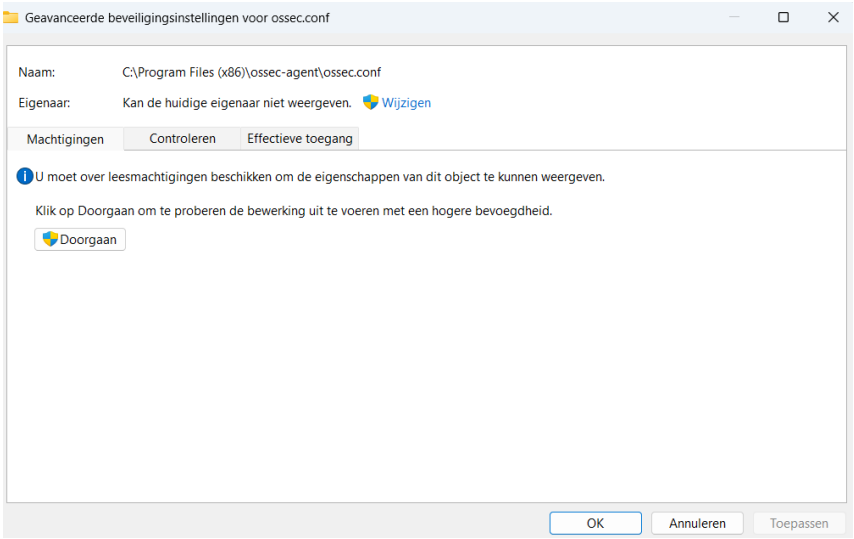
1. Er is standaard geen toegang tot het **ossec.conf** bestand. Rechtermuisklik op **ossec.conf** en selecteer **Eigenschappen**.



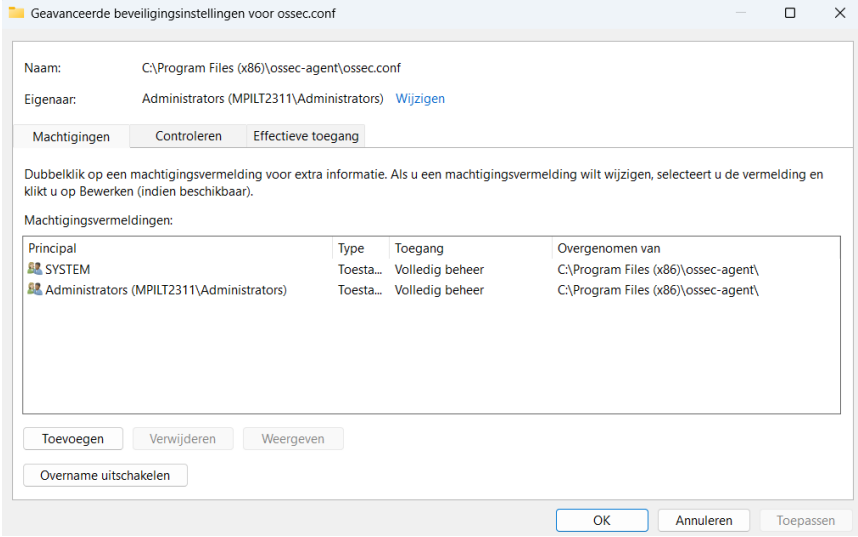

2. We gaan naar de tab **Beveiliging** en klikken op **Geavanceerd.**



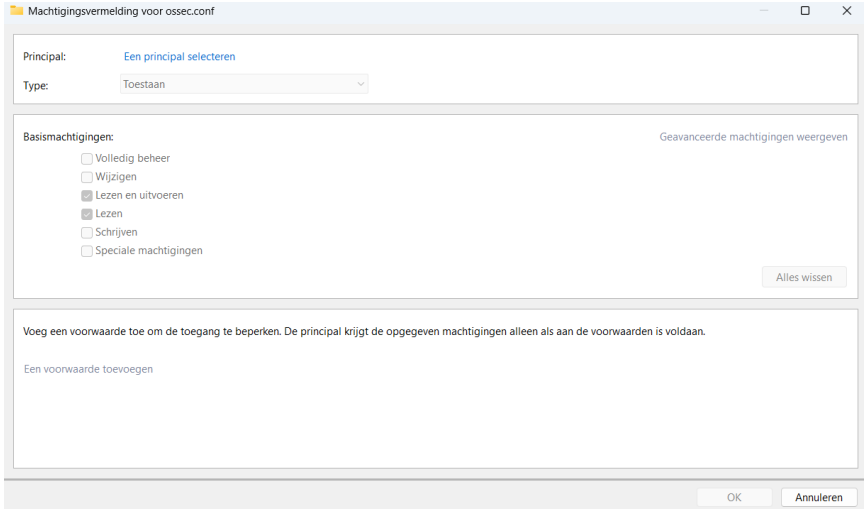
3. Klik op **Doorgaan** om de nodige rechten te krijgen aanpassingen te mogen maken.



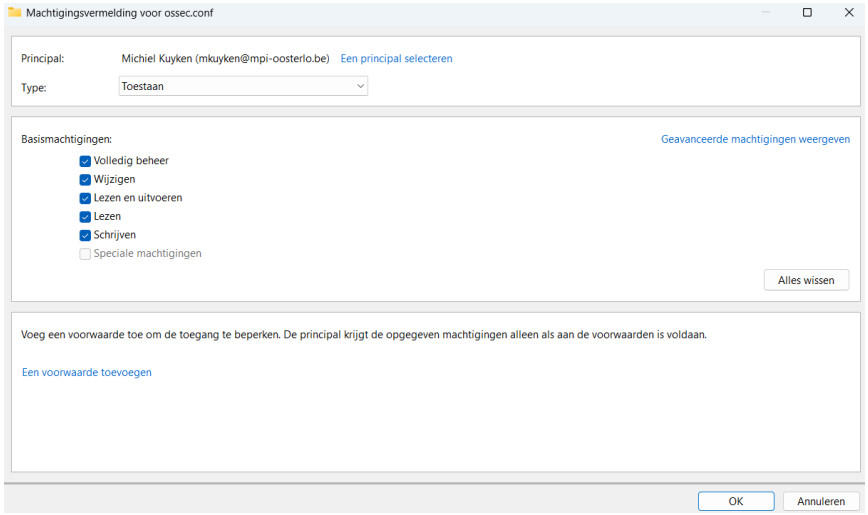

4. Klik op **Toevoegen** om een nieuwe machtiging te maken.



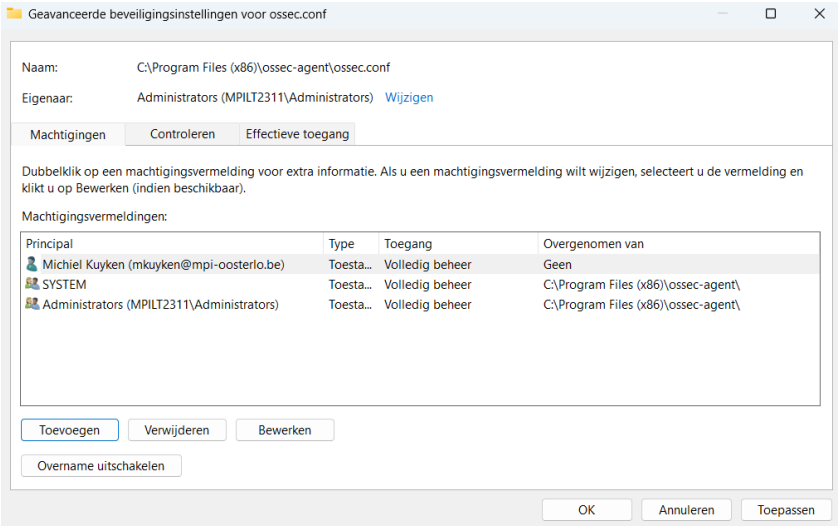
5. Klik op **Een principal selecteren** en vul je eigen gebruikersnaam in. Klik op **Namen controleren** om te kijken of het juiste e-mailadres gebruikt word. Geef **Volledig beheer**.



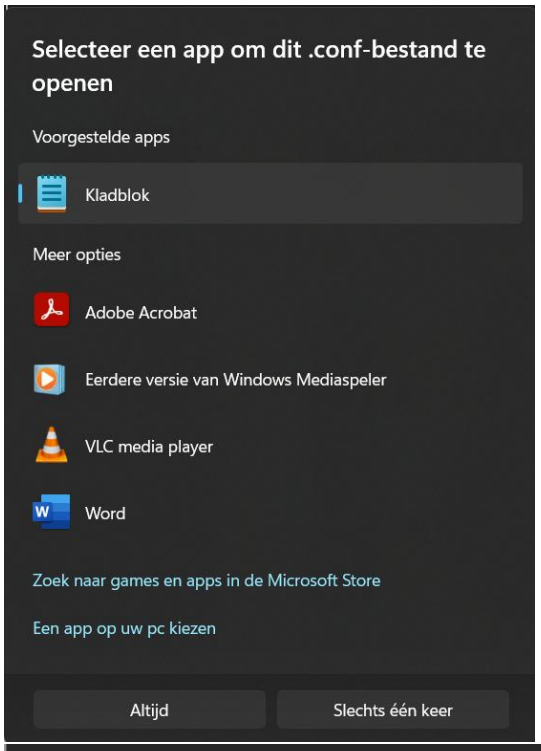




6. De nieuwe machtiging is nu zichtbaar. Klik eerst op **Toepassen** en daarna op **Ok**.




7. We kunnen nu **ossec.conf** openen en zien **<address>172.17.0.225</address>** staan. Als dit niet aanwezig is, geef je het IP handmatig in.




```
<ossec_config>

  <client>
    <server>
      <address>172.17.0.225</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>windows, windows10</config-profile>
    <crypto_method>aes</crypto_method>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
  </client>
```

## BIJLAGE 3: CUSTOM SHUFFLE BESTANDEN

custom-shuffle

```
#!/bin/sh
# Created by Shuffle, AS. <frikky@shuffler.io>.

WPYTHON_BIN="framework/python/bin/python3"

SCRIPT_PATH_NAME="$0"

DIR_NAME="$(cd $(dirname ${SCRIPT_PATH_NAME}); pwd -P)"
SCRIPT_NAME="$(basename ${SCRIPT_PATH_NAME})"

case ${DIR_NAME} in
    */active-response/bin | */wodles*)
        if [ -z "${WAZUH_PATH}" ]; then
            WAZUH_PATH="$(cd ${DIR_NAME}/../..; pwd)"
        fi

        PYTHON_SCRIPT="${DIR_NAME}/${SCRIPT_NAME}.py"
    ;;
    */bin)
        if [ -z "${WAZUH_PATH}" ]; then
            WAZUH_PATH="$(cd ${DIR_NAME}/..; pwd)"
        fi

        PYTHON_SCRIPT="${WAZUH_PATH}/framework/scripts/${SCRIPT_NAME}.py"
    ;;
     */integrations)
        if [ -z "${WAZUH_PATH}" ]; then
            WAZUH_PATH="$(cd ${DIR_NAME}/..; pwd)"
        fi

        PYTHON_SCRIPT="${DIR_NAME}/${SCRIPT_NAME}.py"
    ;;
esac


${WAZUH_PATH}/${WPYTHON_BIN} ${PYTHON_SCRIPT} "$@"
```

**custom-shuffle.py**

```
#!/usr/bin/env python3
# Created by Shuffle, AS. <frikky@shuffler.io>.
# Based on the Slack integration using Webhooks

import json
import sys
import time
import os

try:
    import requests
    from requests.auth import HTTPBasicAuth
except Exception as e:
    print("No module 'requests' found. Install: pip install requests")
    sys.exit(1)

# ADD THIS TO ossec.conf configuration:
#  <integration>
#      <name>custom-shuffle</name>
#      <hook_url>http://<IP>:3001/api/v1/hooks/<HOOK_ID></hook_url>
#      <level>3</level>
#      <alert_format>json</alert_format>
#  </integration>

# Global vars
debug_enabled = False
pwd = os.path.dirname(os.path.dirname(os.path.realpath(__file__)))
json_alert = {}
now = time.strftime("%a %b %d %H:%M:%S %Z %Y")

# Set paths
log_file = '{0}/logs/integrations.log'.format(pwd)

try:
    with open("/tmp/shuffle_start.txt", "w+") as tmp:
        tmp.write("Script started")
except:
    pass
```

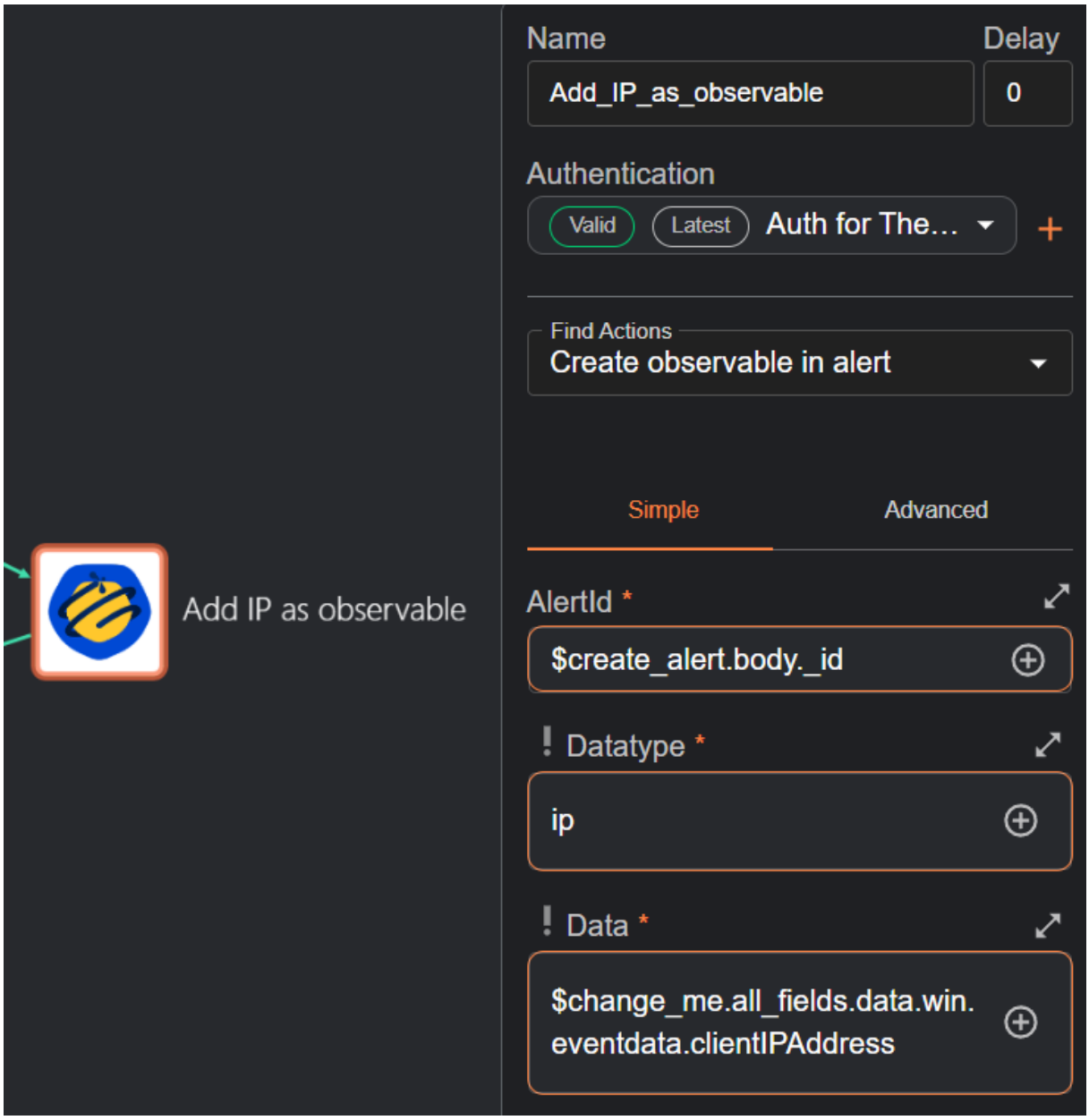
```
def main(args):
    debug("# Starting")

    # Read args
    alert_file_location = args[1]
    webhook = args[3]

    debug("# Webhook")
    debug(webhook)

    debug("# File location")
    debug(alert_file_location)

    # Load alert. Parse JSON object.
    try:
        with open(alert_file_location) as alert_file:
            json_alert = json.load(alert_file)
    except:
        debug("# Alert file %s doesn't exist" % alert_file_location)

    debug("# Processing alert")
    try:
        debug(json_alert)
    except Exception as e:
        debug("Failed getting json_alert %s" % e)
        sys.exit(1)

    debug("# Generating message")
    msg = generate_msg(json_alert)
    if isinstance(msg, str):
        if len(msg) == 0:
            return
    debug(msg)

    debug("# Sending message")

    try:
        with open("/tmp/shuffle_end.txt", "w+") as tmp:
            tmp.write("Script done pre-msg sending")
    except:
        pass

    send_msg(msg, webhook)
```

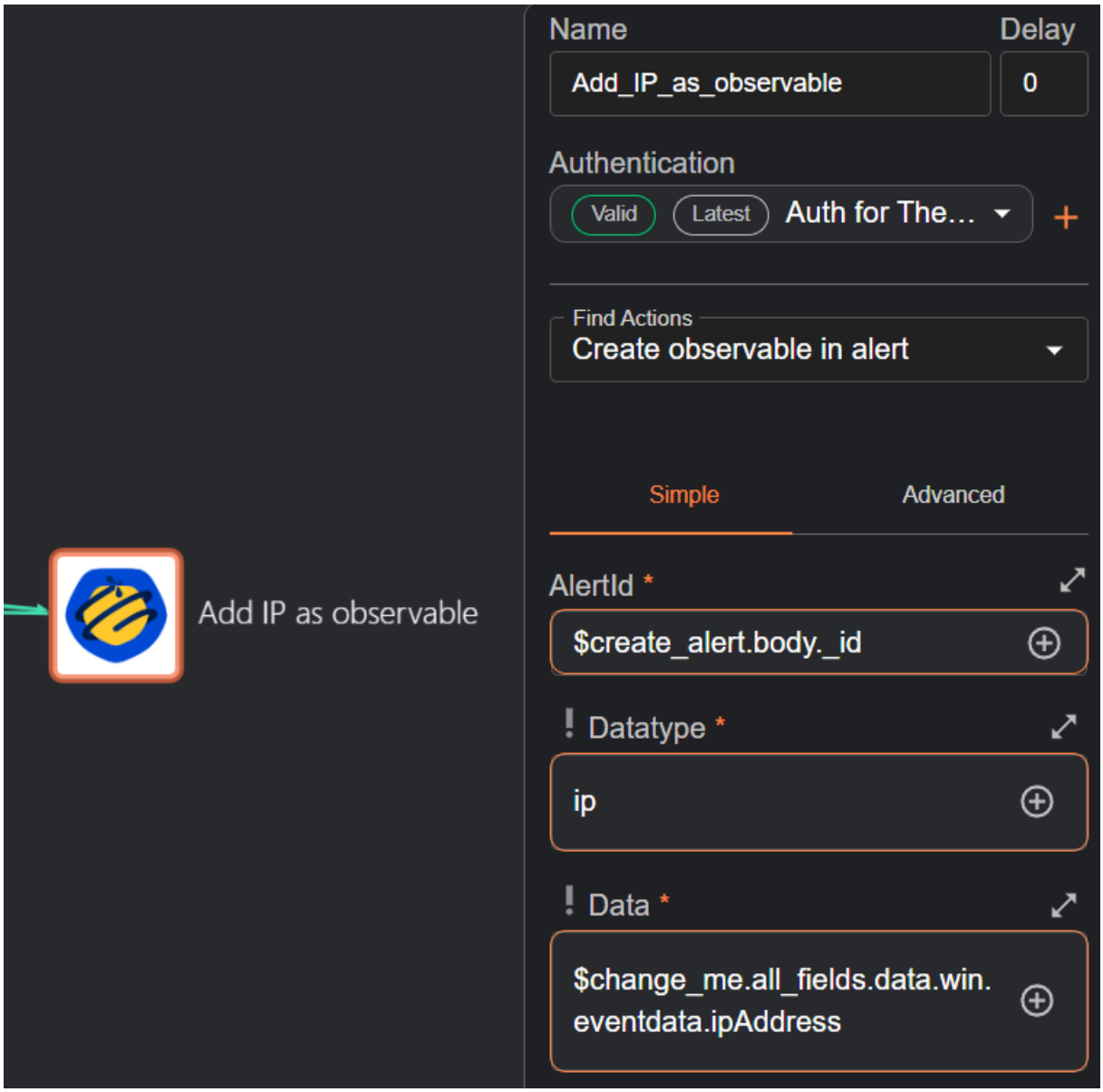
```
def debug(msg):
    if debug_enabled:
        msg = "{0}: {1}\n".format(now, msg)
        print(msg)
        f = open(log_file, "a")
        f.write(msg)
        f.close()

# Skips container kills to stop self-recursion
def filter_msg(alert):
    # These are things that recursively happen because Shuffle starts Docker containers
    skip = ["87924", "87900", "87901", "87902", "87903", "87904", "86001", "86002", "86003", "87932", "80710", "87929", "87928", "5710"]
    if alert["rule"]["id"] in skip:
        return False

    #try:
    #    if "docker" in alert["rule"]["description"].lower() and "
    #msg['text'] = alert.get('full_log')
    #except:
    #    pass
    #msg['title'] = alert['rule']['description'] if 'description' in alert['rule'] else "N/A"

    return True
```

```
def generate_msg(alert):
    if not filter_msg(alert):
        print("Skipping rule %s" % alert["rule"]["id"])
        return ""

    level = alert['rule']['level']

    if (level <= 4):
        severity = 1
    elif (level >= 5 and level <= 7):
        severity = 2
    else:
        severity = 3

    msg = {}
    msg['severity'] = severity
    msg['pretext'] = "WAZUH Alert"
    msg['title'] = alert['rule']['description'] if 'description' in alert['rule'] else "N/A"
    msg['text'] = alert.get('full_log')
    msg['rule_id'] = alert["rule"]["id"]
    msg['timestamp'] = alert["timestamp"]
    msg['id'] = alert['id']
    msg["all_fields"] = alert

    #msg['fields'] = []
    #    msg['fields'].append({
    #        "title": "Agent",
    #        "value": "({0}) - {1}".format(
    #            alert['agent']['id'],
    #            alert['agent']['name']
    #        ),
    #    })
    #if 'agentless' in alert:
    #    msg['fields'].append({
    #        "title": "Agentless Host",
    #        "value": alert['agentless']['host'],
    #    })

    #msg['fields'].append({"title": "Location", "value": alert['location']})
    #msg['fields'].append({
    #    "title": "Rule ID",
    #    "value": "{0} _(Level {1})_".format(alert['rule']['id'], level),
    #})

    #attach = {'attachments': [msg]}

    return json.dumps(msg)
```

```python
def send_msg(msg, url):
    debug("# In send msg")
    headers = {'content-type': 'application/json', 'Accept-Charset': 'UTF-8'}
    res = requests.post(url, data=msg, headers=headers, verify=False)
    debug("# After send msg: %s" % res)


if __name__ == "__main__":
    try:
        # Read arguments
        bad_arguments = False
        if len(sys.argv) >= 4:
            msg = '{0} {1} {2} {3} {4}'.format(
                now,
                sys.argv[1],
                sys.argv[2],
                sys.argv[3],
                sys.argv[4] if len(sys.argv) > 4 else '',
            )
            #debug_enabled = (len(sys.argv) > 4 and sys.argv[4] == 'debug')
            debug_enabled = True
        else:
            msg = '{0} Wrong arguments'.format(now)
            bad_arguments = True

        # Logging the call
        try:
            f = open(log_file, 'a')
        except:
            f = open(log_file, 'w+')
            f.write("")
            f.close()

        f = open(log_file, 'a')
        f.write(msg + '\n')
        f.close()

        if bad_arguments:
            debug("# Exiting: Bad arguments. Inputted: %s" % sys.argv)
            sys.exit(1)

        # Main function
        main(sys.argv)

    except Exception as e:
        debug(str(e))
        raise
```

**BIJLAGE 4: ADD IP AS OBSERVABLE**

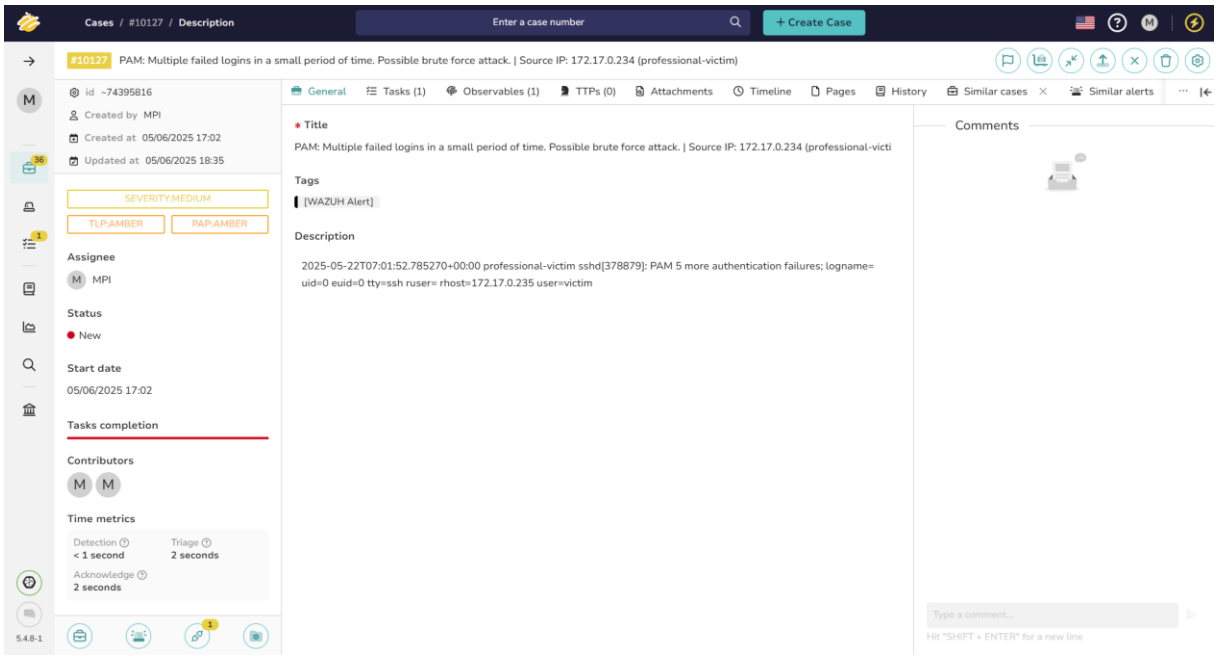



Name
Delay
Add_IP_as_observable
0
Authentication
Valid
Latest
Auth for The...
Find Actions
Create observable in alert
Simple
Advanced
Add IP as observable
AlertId *
$create_alert.body._id
Datatype *
ip
Data *
$change_me.all_fields.data.win.
eventdata.ipAddress

## BIJLAGE 5: MELDING IN TEAMS JSON-STRUCTUUR

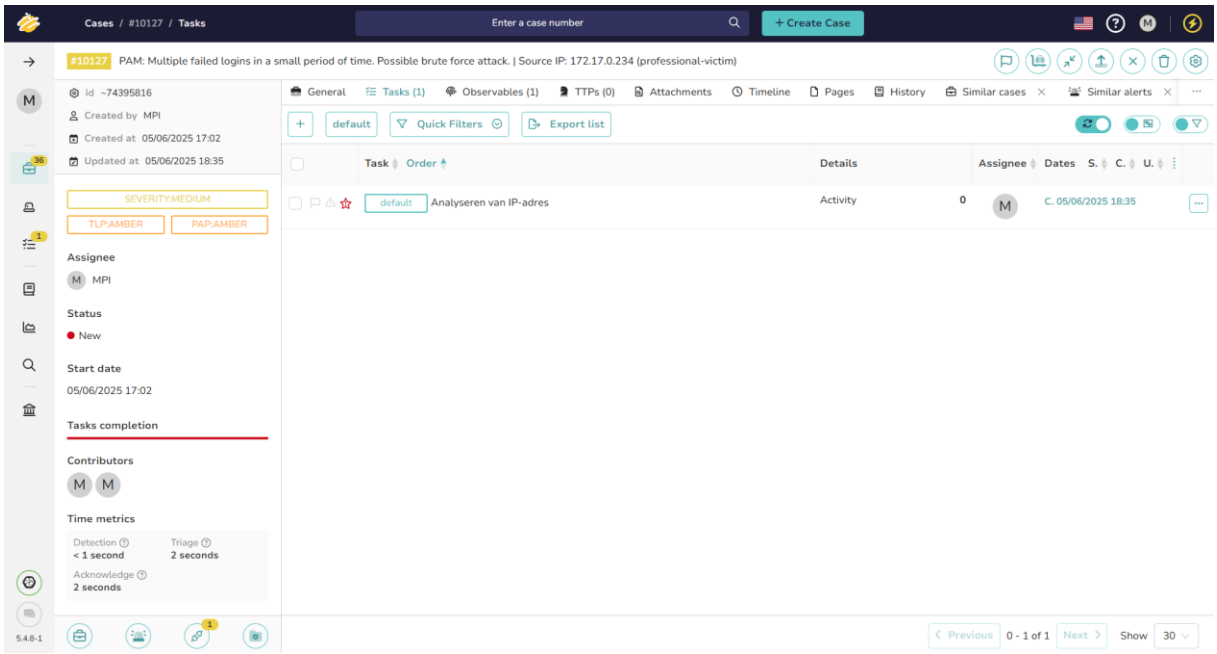
```
1  {
2    "type": "message",
3    "attachments": [
4      {
5        "contentType": "application/vnd.microsoft.card.adaptive",
6        "content": {
7          "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
8          "type": "AdaptiveCard",
9          "version": "1.0",
10         "body": [
11           {
12             "type": "TextBlock",
13             "text": "$get_alert.body.title",
14             "size": "large",
15             "wrap": true
16           },
17           {
18             "type": "TextBlock",
19             "text": "$change_me.all_fields.data.vulnerability.reference",
20             "wrap": true,
21             "spacing": "small"
22           }
23         ]
24       }
25     }
26   ]
27 }
```

## BIJLAGE 6: TABBLAD ‘GENERAL’ IN CASE THEHIVE

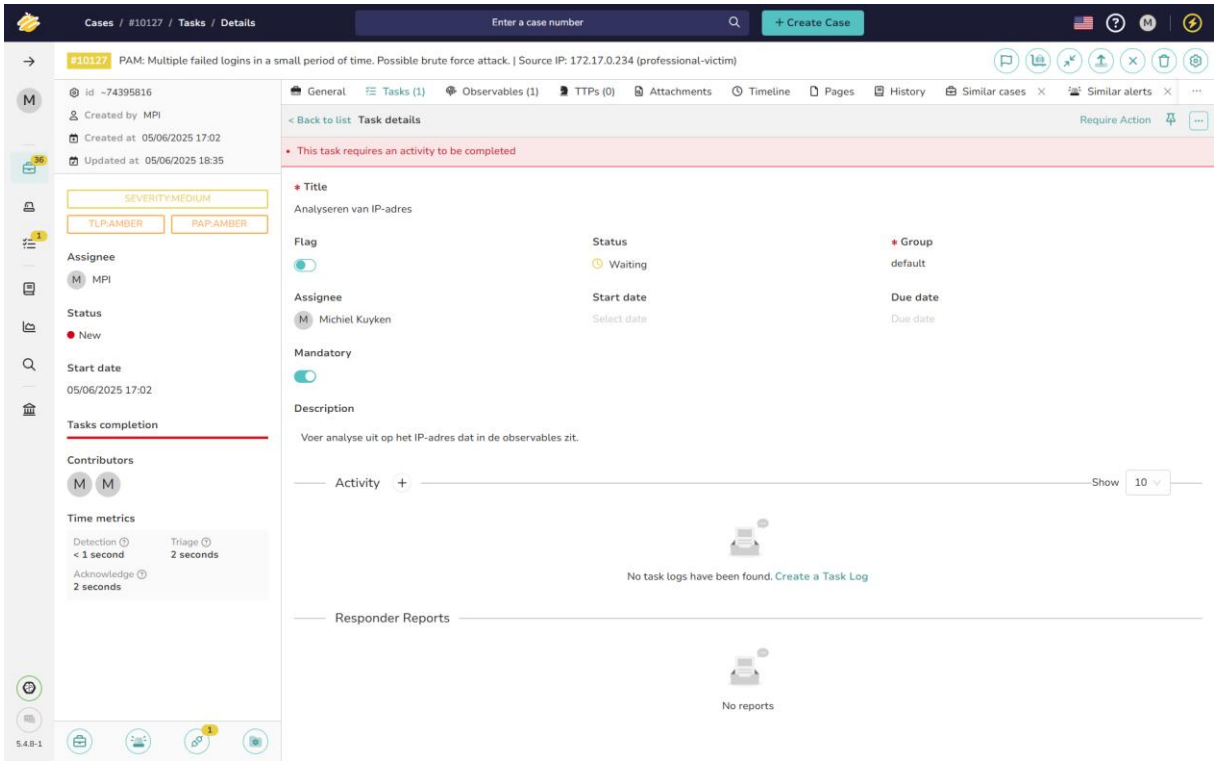


## BIJLAGE 7: TABBLAD ‘TASKS’ IN CASE THEHIVE

### Tabblad ‘tasks’ in case

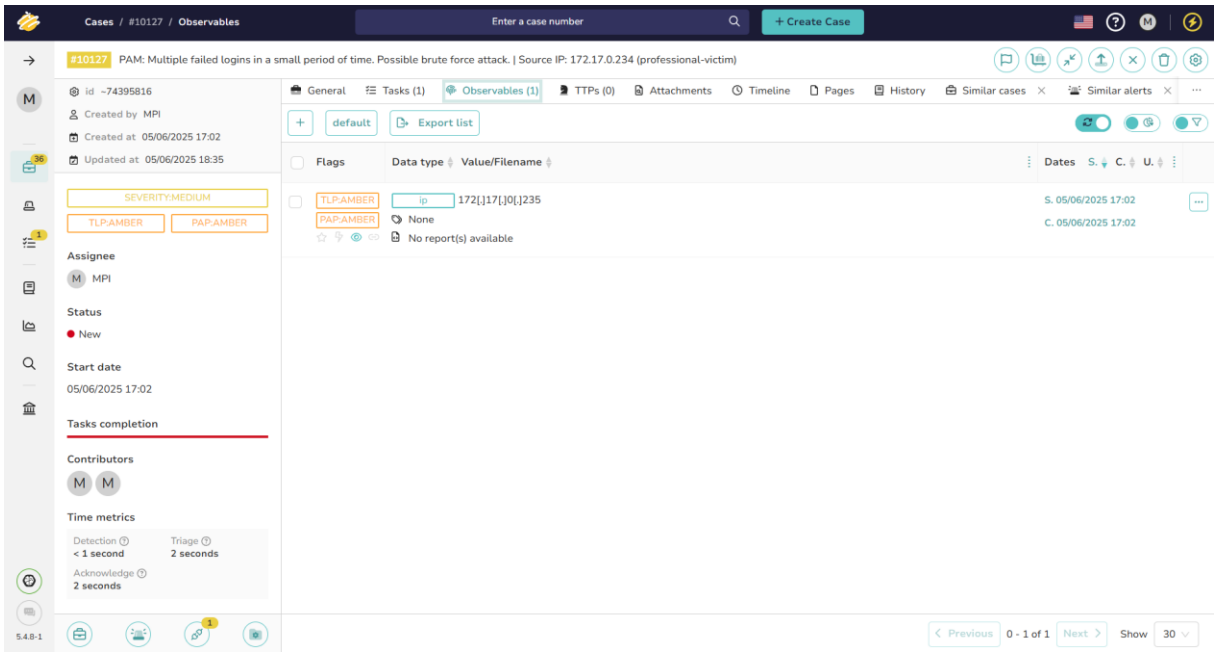



### De taak in tabblad ‘tasks’

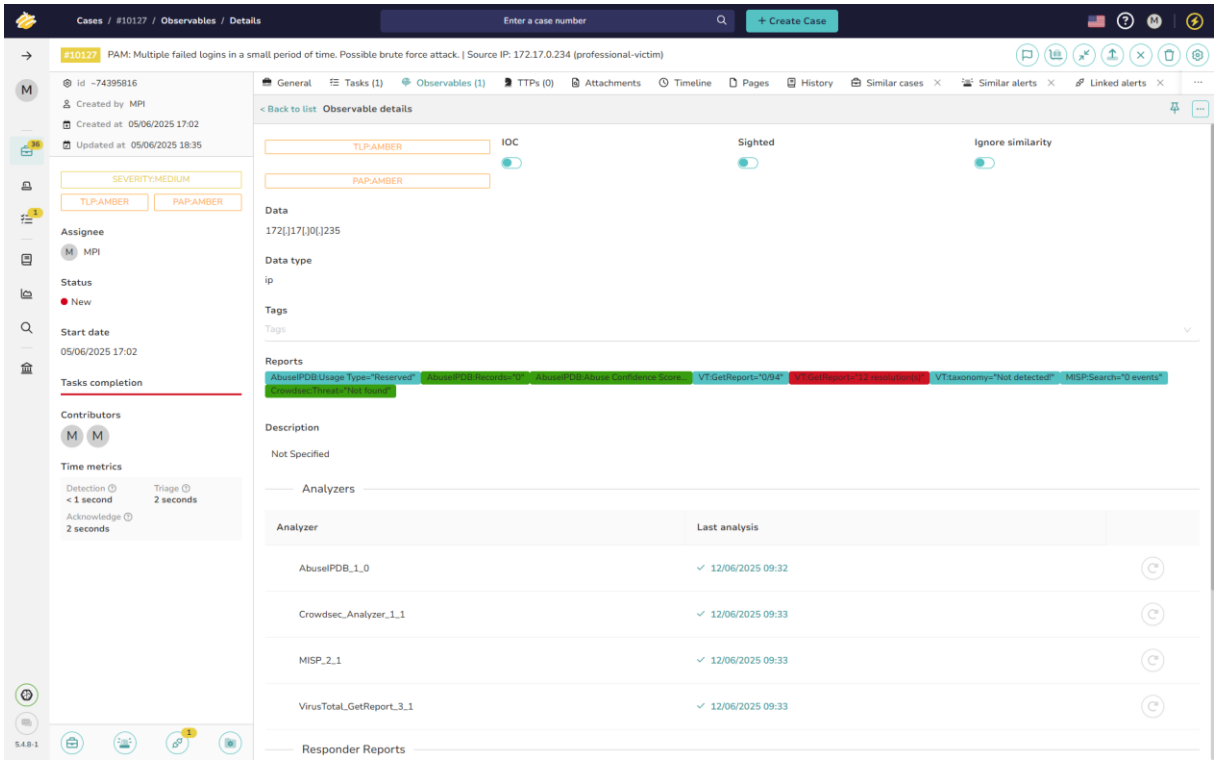


## BIJLAGE 8: TABBLAD ‘OBSERVABLES’ IN CASE THEHIVE

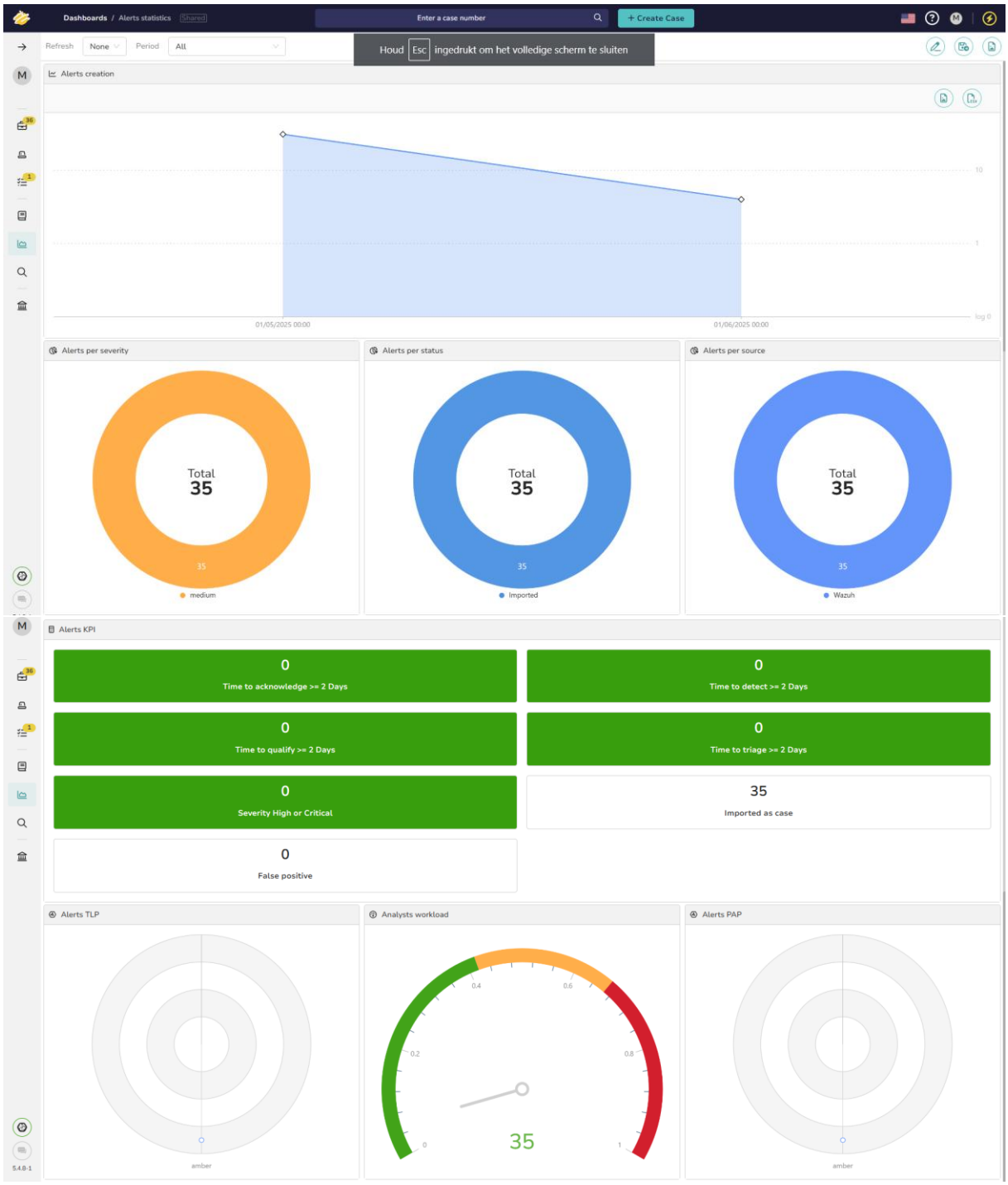
### Tabblad ‘Obeservables’ in case



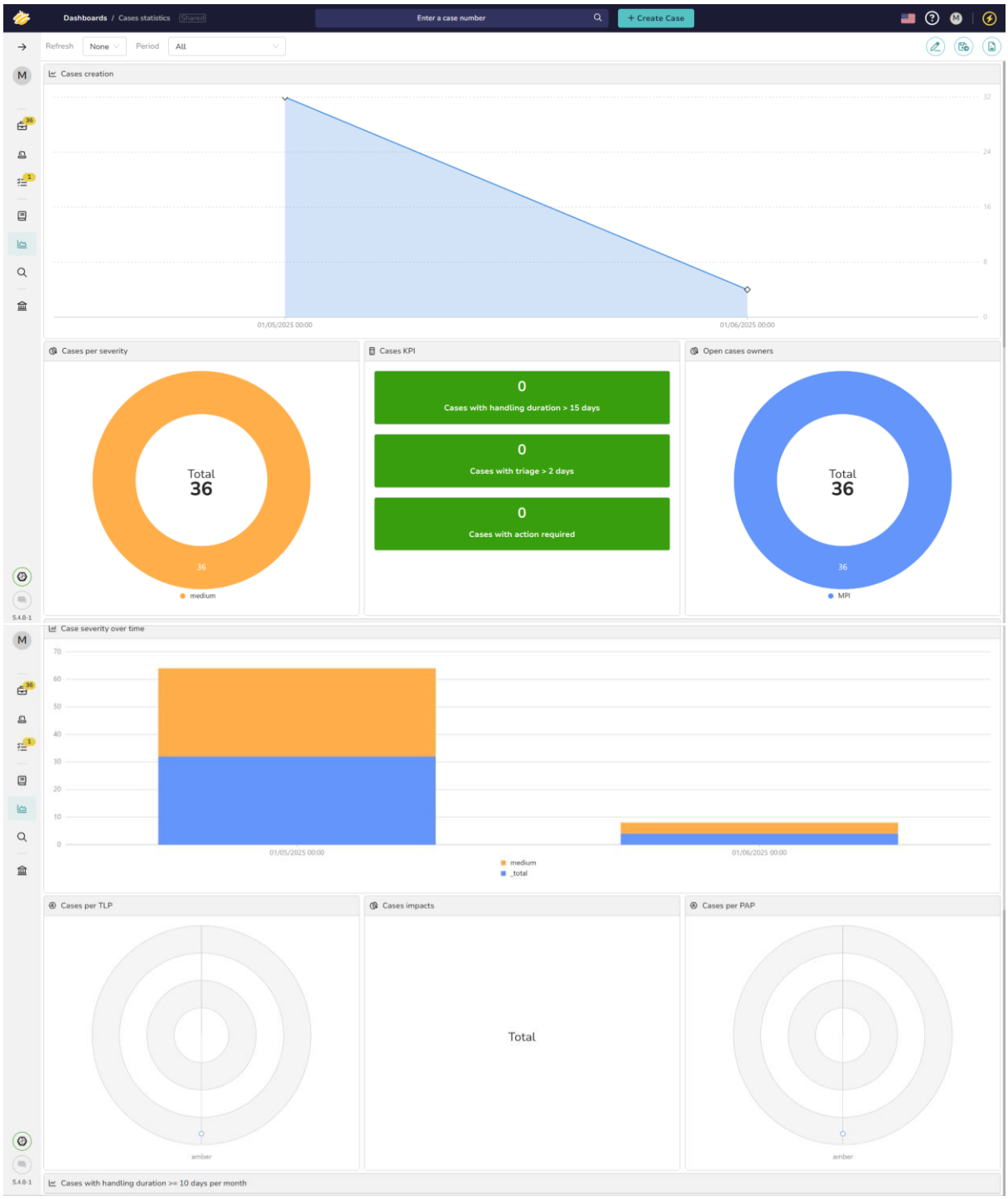

### De observable in tabblad ‘observables’



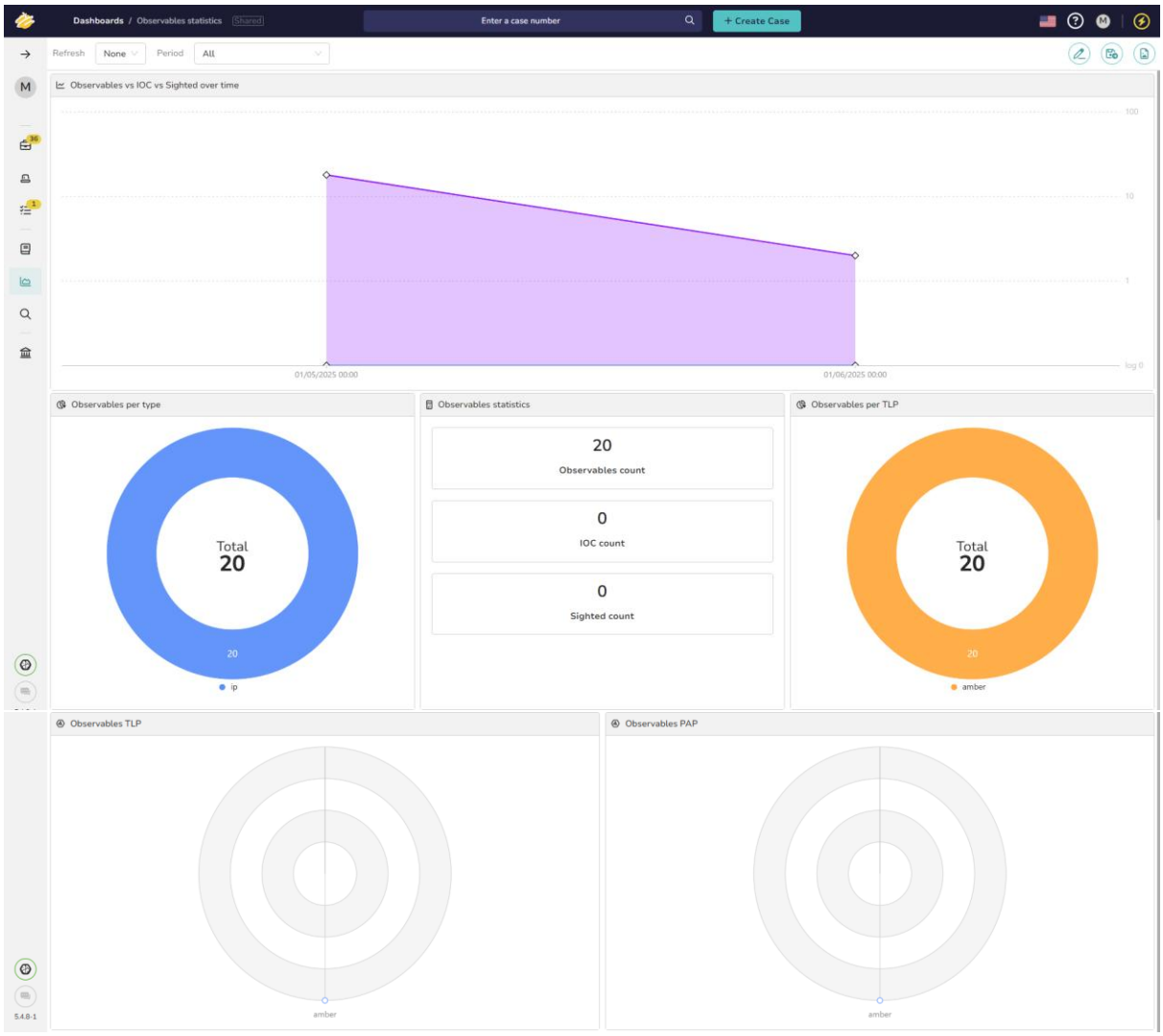
## BIJLAGE 9: THEHIVE DASHBOARD ALERTS



## BIJLAGE 10: THEHIVE DASHBOARD CASES

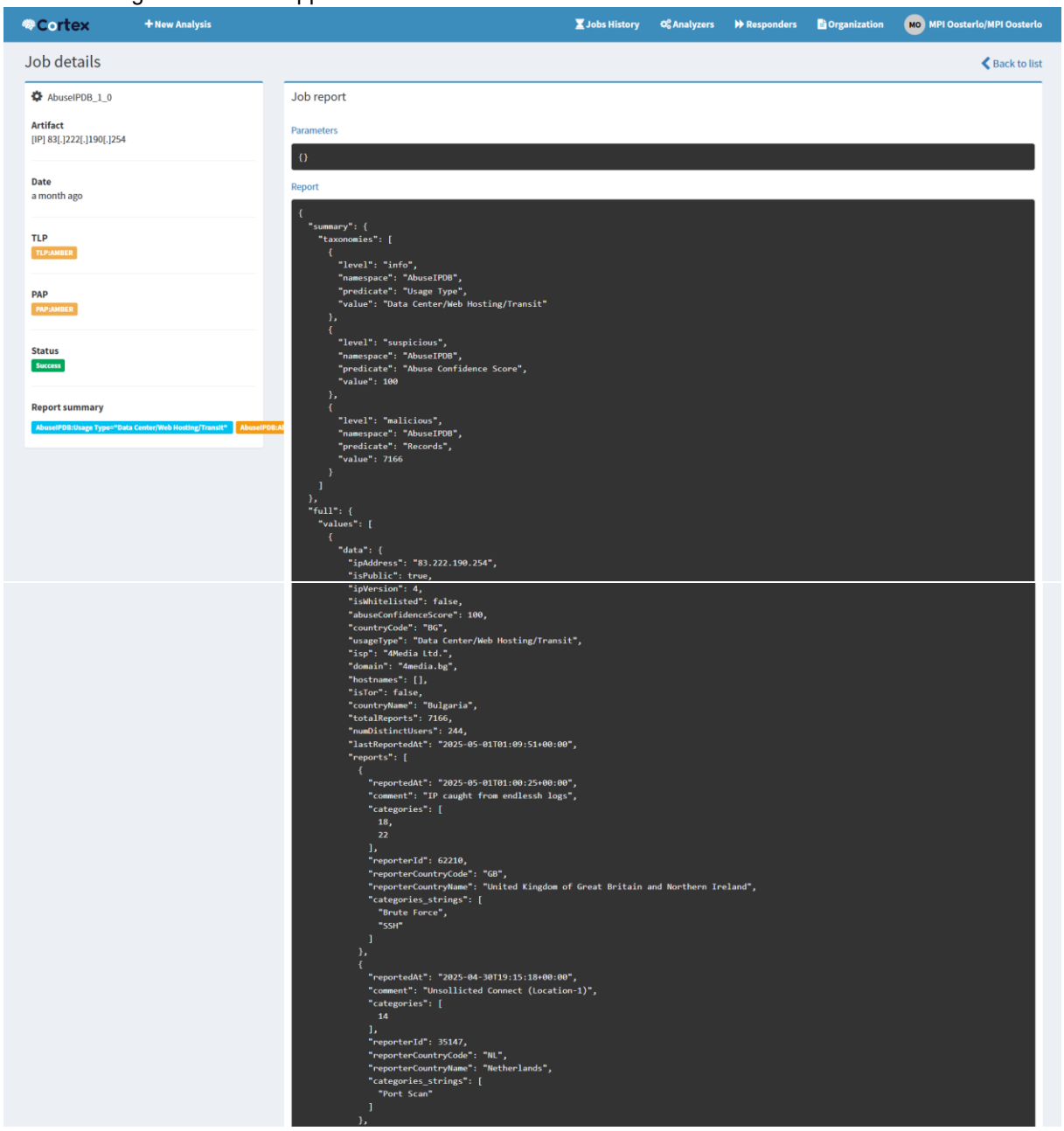


## BIJLAGE 11: THEHIVE DASHBOARD OBSERVABLES



## BIJLAGE 12: RAPPORT ABUSEIPDB

Het ganse rapport hiervan is enkele tientalle pagina’s lang, daarom staan er slecht enkele screenshots om een beeld te geven van het rapport.



## BIJLAGE 13: RAPPORT CROWDSEC

Cortex | + New Analysis | Jobs History | Analyzers | Responders | Organization | MO MPI Oosterlo/MPI Oosterlo

Job details

Houd Esc ingedrukt om het volledige scherm te sluiten

Back to list

Crowdsec_Analyzer_1_1

**Artifact**
[IP] 83[.]222[.]190[.]254

**Date**
a month ago

**TLP**
TLP:AMBER

**PAP**
PAP:AMBER

**Status**
Success

**Report summary**
Crowdsec:Reputation="malicious" | Crowdsec:ASN="SS-Net" | Crowdsec

Job report

Parameters

```
{}
```

Report


```
{
  "summary": {
    "taxonomies": [
      {
        "level": "malicious",
        "namespace": "Crowdsec",
        "predicate": "Reputation",
        "value": "malicious"
      },
      {
        "level": "info",
        "namespace": "Crowdsec",
        "predicate": "ASN",
        "value": "SS-Net"
      },
      {
        "level": "info",
        "namespace": "Crowdsec",
        "predicate": "Score",
        "value": 5
      },
      {
        "level": "info",
        "namespace": "Crowdsec",
        "predicate": "LastSeen",
        "value": "2025-04-30T18:15:00+00:00"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Attack",
        "value": "crowdsecurity/suricata-major-severity"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Attack",
        "value": "crowdsecurity/endlessh-bf"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Attack",
        "value": "crowdsecurity/ssh-bf"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Attack",
        "value": "crowdsecurity/suricata-high-medium-severity"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Attack",
        "value": "crowdsecurity/iptables-scan-multi_ports"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Attack",
        "value": "crowdsecurity/ssh-slow-bf"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Attack",
        "value": "firewallservices/pf-scan-multi_ports"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Attack",
        "value": "crowdsecurity/ssh-bf_user-enum"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Behavior",
        "value": "generic:exploit"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Behavior",
        "value": "ssh:bruteforce"
      },
```

```
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Behavior",
        "value": "tcp:scan"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Mitre",
        "value": "T1190"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Mitre",
        "value": "T1595"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Mitre",
        "value": "T1110"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Mitre",
        "value": "T1018"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Mitre",
        "value": "T1046"
      },
      {
        "level": "suspicious",
        "namespace": "Crowdsec",
        "predicate": "Mitre",
        "value": "T1589"
      }
    ]
  },
  "full": {
    "ip": "83.222.190.254",
    "reputation": "malicious",
    "ip_range": "83.222.190.0/23",
    "background_noise": "high",
    "confidence": "high",
    "background_noise_score": 10,
    "ip_range_score": 5,
    "as_name": "SS-Net",
    "as_num": 204428,
    "ip_range_24": "83.222.190.0/24",
    "ip_range_24_reputation": "unknown",
    "ip_range_24_score": 0,
    "location": {
      "country": "RO",
      "city": null,
      "latitude": 45.9968,
      "longitude": 24.997
    },
    "reverse_dns": null,
    "behaviors": [
      {
        "name": "generic:exploit",
        "label": "Exploitation attempt",
        "description": "IP has been reported trying to exploit known vulnerability/CVE on unspecified protocols.",
        "references": []
      },
      {
        "name": "ssh:bruteforce",
        "label": "SSH Bruteforce",
        "description": "IP has been reported for performing brute force on ssh services.",
        "references": []
      },
      {
        "name": "tcp:scan",
        "label": "TCP Scan",
        "description": "IP has been reported for performing TCP port scanning.",
        "references": []
      }
    ],
    "history": {
      "first_seen": "2024-10-07T19:00:00+00:00",
      "last_seen": "2025-04-30T18:15:00+00:00",
      "full_age": 186,
      "days_age": 185
    },
    "classifications": {
      "false_positives": [],
      "classifications": [
        {
          "name": "community-blocklist",
          "label": "CrowdSec Community Blocklist",
          "description": "IP belongs to the CrowdSec Community Blocklist"
        }
      ]
    },
    "attack_details": [
      {
        "name": "crowdsecurity/suricata-major-severity",
        "label": "Suricata Severity 1 Event"
```

```
      "label": "Suricata Severity 1 Event",
      "description": "Detect exploit attempts via emerging threat rules",
      "references": []
    },
    {
      "name": "crowdsecurity/endlessh-bf",
      "label": "Endlessh Bruteforce",
      "description": "Detect SSH bruteforce caught by Endlessh",
      "references": []
    },
    {
      "name": "crowdsecurity/ssh-bf",
      "label": "SSH Bruteforce",
      "description": "Detect ssh bruteforce",
      "references": []
    },
    {
      "name": "crowdsecurity/suricata-high-medium-severity",
      "label": "Suricata Severity 2 Event",
      "description": "Detect exploit attempts via emerging threat rules",
      "references": []
    },
    {
      "name": "crowdsecurity/iptables-scan-multi_ports",
      "label": "TCP Port Scan",
      "description": "Detect aggressive portscans",
      "references": []
    },
    {
      "name": "crowdsecurity/ssh-slow-bf",
      "label": "SSH Slow Bruteforce",
      "description": "Detect slow ssh bruteforce",
      "references": []
    },
    {
      "name": "firewallservices/pf-scan-multi_ports",
      "label": "PF Scan Multi Ports",
      "description": "Detect aggressive portscans (pf)",
      "references": []
    },
    {
      "name": "crowdsecurity/ssh-bf_user-enum",
      "label": "SSH User Enumeration",
      "description": "Detect ssh user enum bruteforce",
      "references": []
    }
  ],
  "target_countries": {
    "DE": 39,
    "US": 17,
    "FR": 13,
    "CA": 5,
    "AT": 4,
    "AU": 4,
    "RO": 4,
    "GB": 3,
    "CH": 3,
    "NL": 3
  },
  "mitre_techniques": [
    {
      "name": "T1190",
      "label": "Exploit Public-Facing Application",
      "description": "Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network.",
      "references": []
    },
    {
      "name": "T1595",
      "label": "Active Scanning",
      "description": "Adversaries may execute active reconnaissance scans to gather information that can be used during targeting.",
      "references": []
    },
    {
      "name": "T1110",
      "label": "Brute Force",
      "description": "Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are
      "references": []
    },
    {
      "name": "T1018",
      "label": "Remote System Discovery",
      "description": "Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network
      "references": []
    },
    {
      "name": "T1046",
      "label": "Network Service Discovery",
      "description": "Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, inclu
      "references": []
    },
    {
      "name": "T1589",
      "label": "Gather Victim Identity Information",
      "description": "Adversaries may gather information about the victim's identity that can be used during targeting.",
      "references": []
    }
  ],
  "cves": [],
  "scores": {
    "overall": {
      "aggressiveness": 5,
      "threat": 3,
      "trust": 5,
      "popularity": 1
```

```
      "trust": 5,
      "anomaly": 1,
      "total": 4
    },
    "last_day": {
      "aggressiveness": 0,
      "threat": 3,
      "trust": 2,
      "anomaly": 1,
      "total": 1
    },
    "last_week": {
      "aggressiveness": 5,
      "threat": 3,
      "trust": 5,
      "anomaly": 1,
      "total": 4
    },
    "last_month": {
      "aggressiveness": 5,
      "threat": 3,
      "trust": 5,
      "anomaly": 1,
      "total": 4
    }
  },
  "references": [
    {
      "name": "list:crowdsec_high_background_noise",
      "label": "High Background Noise",
      "description": "Contains IPs considered internet background noise, identified as malicious or potential threats. Blocking these IPs can redu
      "references": []
    },
    {
      "name": "list:crowdsec_mssp_blocklist",
      "label": "MSSP Attackers",
      "description": "Contains IPs identified as frequent attackers of MSSPs. Proactively blocking these IPs enhances threat mitigation capabiliti
      "references": []
    }
  ]
},
"success": true,
"artifacts": [],
"operations": []
}
```




Version: 3.1.8-1

## BIJLAGE 14: RAPPORT VIRUSTOTAL

Cortex | + New Analysis | Jobs History | Analyzers | Responders | Organization | MO MPI Oosterlo/MPI Oosterlo

Job details | Back to list

VirusTotal_GetReport_3_1

**Artifact**
[IP] 83[.]222[.]190[.]254

**Date**
a month ago

**TLP**
TLP:AMBER

**PAP**
PAP:AMBER

**Status**
Success

**Report summary**
VT:GetReport="10/94" | VT:GetReport="0 resolution(s)" | VT:taxonomy=

Job report

Parameters


```
{}
```


Report


```
{
  "summary": {
    "taxonomies": [
      {
        "level": "malicious",
        "namespace": "VT",
        "predicate": "GetReport",
        "value": "10/94"
      },
      {
        "level": "safe",
        "namespace": "VT",
        "predicate": "GetReport",
        "value": "0 resolution(s)"
      },
      {
        "level": "info",
        "namespace": "VT",
        "predicate": "taxonomy",
        "value": "Not detected!"
      }
    ]
  },
  "full": {
    "type": "ip_address",
    "attributes": {
      "whois_date": 1743694590,
      "continent": "EU",
      "last_analysis_results": {
        "Acronis": {
          "method": "blacklist",
          "engine_name": "Acronis",
          "category": "harmless",
          "result": "clean"
        },
        "0xSI_f33d": {
          "method": "blacklist",
          "engine_name": "0xSI_f33d",
          "category": "undetected",
          "result": "unrated"
        },
        "Abusix": {
          "method": "blacklist",
          "engine_name": "Abusix",
          "category": "harmless",
          "result": "clean"
        },
        "ADMINUSLabs": {
          "method": "blacklist",
          "engine_name": "ADMINUSLabs",
          "category": "harmless",
          "result": "clean"
        },
        "Axur": {
          "method": "blacklist",
          "engine_name": "Axur",
          "category": "undetected",
          "result": "unrated"
        },
        "Criminal IP": {
          "method": "blacklist",
          "engine_name": "Criminal IP",
          "category": "malicious",
          "result": "malicious"
        },
        "AILabs (MONITORAPP)": {
          "method": "blacklist",
          "engine_name": "AILabs (MONITORAPP)",
          "category": "harmless",
          "result": "clean"
        },
        "AlienVault": {
          "method": "blacklist",
          "engine_name": "AlienVault",
          "category": "harmless",
          "result": "clean"
        },
        "alphaMountain.ai": {
          "method": "blacklist",
          "engine_name": "alphaMountain.ai",
          "category": "malicious",
          "result": "malicious"
        },
        "AlphaSOC": {
          "method": "blacklist",
          "engine_name": "AlphaSOC",
          "category": "suspicious",
          "result": "suspicious"
```

```
    },
    "Antiy-AVL": {
      "method": "blacklist",
      "engine_name": "Antiy-AVL",
      "category": "harmless",
      "result": "clean"
    },
    "ArcSight Threat Intelligence": {
      "method": "blacklist",
      "engine_name": "ArcSight Threat Intelligence",
      "category": "malicious",
      "result": "phishing"
    },
    "AutoShun": {
      "method": "blacklist",
      "engine_name": "AutoShun",
      "category": "undetected",
      "result": "unrated"
    },
    "benkow.cc": {
      "method": "blacklist",
      "engine_name": "benkow.cc",
      "category": "harmless",
      "result": "clean"
    },
    "Bfore.Ai PreCrime": {
      "method": "blacklist",
      "engine_name": "Bfore.Ai PreCrime",
      "category": "undetected",
      "result": "unrated"
    },
    "BitDefender": {
      "method": "blacklist",
      "engine_name": "BitDefender",
      "category": "harmless",
      "result": "clean"
    },
    "Bkav": {
      "method": "blacklist",
      "engine_name": "Bkav",
      "category": "undetected",
      "result": "unrated"
    },
    "Blueliv": {
      "method": "blacklist",
      "engine_name": "Blueliv",
      "category": "harmless",
      "result": "clean"
    },
    "Certego": {
      "method": "blacklist",
      "engine_name": "Certego",
      "category": "harmless",
      "result": "clean"
    },
    "Chong Lua Dao": {
      "method": "blacklist",
      "engine_name": "Chong Lua Dao",
      "category": "harmless",
      "result": "clean"
    },
    "CINS Army": {
      "method": "blacklist",
      "engine_name": "CINS Army",
      "category": "harmless",
      "result": "clean"
    },
    "Cluster25": {
      "method": "blacklist",
      "engine_name": "Cluster25",
      "category": "undetected",
      "result": "unrated"
    },
    "CRDF": {
      "method": "blacklist",
      "engine_name": "CRDF",
      "category": "harmless",
      "result": "clean"
    },
    "CSIS Security Group": {
      "method": "blacklist",
      "engine_name": "CSIS Security Group",
      "category": "undetected",
      "result": "unrated"
    },
    "Snort IP sample list": {
      "method": "blacklist",
      "engine_name": "Snort IP sample list",
      "category": "harmless",
      "result": "clean"
    },
    "CMC Threat Intelligence": {
      "method": "blacklist",
      "engine_name": "CMC Threat Intelligence",
      "category": "harmless",
      "result": "clean"
    },
    "Cyan": {
      "method": "blacklist",
      "engine_name": "Cyan",
      "category": "undetected",
      "result": "unrated"
    }
```

```
      "Cyble": {
        "method": "blacklist",
        "engine_name": "Cyble",
        "category": "malicious",
        "result": "malicious"
      },
      "CyRadar": {
        "method": "blacklist",
        "engine_name": "CyRadar",
        "category": "malicious",
        "result": "malicious"
      },
      "DNS8": {
        "method": "blacklist",
        "engine_name": "DNS8",
        "category": "harmless",
        "result": "clean"
      },
      "Dr.Web": {
        "method": "blacklist",
        "engine_name": "Dr.Web",
        "category": "harmless",
        "result": "clean"
      },
      "Ermes": {
        "method": "blacklist",
        "engine_name": "Ermes",
        "category": "undetected",
        "result": "unrated"
      },
      "ESET": {
        "method": "blacklist",
        "engine_name": "ESET",
        "category": "harmless",
        "result": "clean"
      },
      "ESTsecurity": {
        "method": "blacklist",
        "engine_name": "ESTsecurity",
        "category": "harmless",
        "result": "clean"
      },
      "EmergingThreats": {
        "method": "blacklist",
        "engine_name": "EmergingThreats",
        "category": "harmless",
        "result": "clean"
      },
      "Emsisoft": {
        "method": "blacklist",
        "engine_name": "Emsisoft",
        "category": "harmless",
```

```
        "result": "clean"
      },
      "Forcepoint ThreatSeeker": {
        "method": "blacklist",
        "engine_name": "Forcepoint ThreatSeeker",
        "category": "malicious",
        "result": "malicious"
      },
      "Fortinet": {
        "method": "blacklist",
        "engine_name": "Fortinet",
        "category": "malicious",
        "result": "malware"
      },
      "G-Data": {
        "method": "blacklist",
        "engine_name": "G-Data",
        "category": "harmless",
        "result": "clean"
      },
      "GCP Abuse Intelligence": {
        "method": "blacklist",
        "engine_name": "GCP Abuse Intelligence",
        "category": "undetected",
        "result": "unrated"
      },
      "Google Safebrowsing": {
        "method": "blacklist",
        "engine_name": "Google Safebrowsing",
        "category": "harmless",
        "result": "clean"
      },
      "GreenSnow": {
        "method": "blacklist",
        "engine_name": "GreenSnow",
        "category": "harmless",
        "result": "clean"
      },
      "Gridinsoft": {
        "method": "blacklist",
        "engine_name": "Gridinsoft",
        "category": "undetected",
        "result": "unrated"
      },
      "Heimdal Security": {
        "method": "blacklist",
        "engine_name": "Heimdal Security",
        "category": "harmless",
        "result": "clean"
      },
      "Hunt.io Intelligence": {
        "method": "blacklist",
```

```
      "engine_name": "Hunt.io Intelligence",
      "category": "undetected",
      "result": "unrated"
    },
    "IPsum": {
      "method": "blacklist",
      "engine_name": "IPsum",
      "category": "harmless",
      "result": "clean"
    },
    "Juniper Networks": {
      "method": "blacklist",
      "engine_name": "Juniper Networks",
      "category": "harmless",
      "result": "clean"
    },
    "Kaspersky": {
      "method": "blacklist",
      "engine_name": "Kaspersky",
      "category": "undetected",
      "result": "unrated"
    },
    "Lionic": {
      "method": "blacklist",
      "engine_name": "Lionic",
      "category": "malicious",
      "result": "malicious"
    },
    "Lumu": {
      "method": "blacklist",
      "engine_name": "Lumu",
      "category": "undetected",
      "result": "unrated"
    },
    "MalwarePatrol": {
      "method": "blacklist",
      "engine_name": "MalwarePatrol",
      "category": "harmless",
      "result": "clean"
    },
    "MalwareURL": {
      "method": "blacklist",
      "engine_name": "MalwareURL",
      "category": "undetected",
      "result": "unrated"
    },
    "Malwared": {
      "method": "blacklist",
      "engine_name": "Malwared",
      "category": "harmless",
      "result": "clean"
    },
    "Mimecast": {
      "method": "blacklist",
      "engine_name": "Mimecast",
      "category": "undetected",
      "result": "unrated"
    },
    "Netcraft": {
      "method": "blacklist",
      "engine_name": "Netcraft",
      "category": "undetected",
      "result": "unrated"
    },
    "OpenPhish": {
      "method": "blacklist",
      "engine_name": "OpenPhish",
      "category": "harmless",
      "result": "clean"
    },
    "Phishing Database": {
      "method": "blacklist",
      "engine_name": "Phishing Database",
      "category": "harmless",
      "result": "clean"
    },
    "PhishFort": {
      "method": "blacklist",
      "engine_name": "PhishFort",
      "category": "undetected",
      "result": "unrated"
    },
    "PhishLabs": {
      "method": "blacklist",
      "engine_name": "PhishLabs",
      "category": "undetected",
      "result": "unrated"
    },
    "Phishtank": {
      "method": "blacklist",
      "engine_name": "Phishtank",
      "category": "harmless",
      "result": "clean"
    },
    "PREBYTES": {
      "method": "blacklist",
      "engine_name": "PREBYTES",
      "category": "harmless",
      "result": "clean"
    },
    "PrecisionSec": {
      "method": "blacklist",
      "engine_name": "PrecisionSec",
      "category": "undetected",
```

```
      "result": "unrated"
    },
    "Quick Heal": {
      "method": "blacklist",
      "engine_name": "Quick Heal",
      "category": "harmless",
      "result": "clean"
    },
    "Quttera": {
      "method": "blacklist",
      "engine_name": "Quttera",
      "category": "harmless",
      "result": "clean"
    },
    "SafeToOpen": {
      "method": "blacklist",
      "engine_name": "SafeToOpen",
      "category": "undetected",
      "result": "unrated"
    },
    "Sansec eComscan": {
      "method": "blacklist",
      "engine_name": "Sansec eComscan",
      "category": "undetected",
      "result": "unrated"
    },
    "Scantitan": {
      "method": "blacklist",
      "engine_name": "Scantitan",
      "category": "harmless",
      "result": "clean"
    },
    "SCUMWARE.org": {
      "method": "blacklist",
      "engine_name": "SCUMWARE.org",
      "category": "harmless",
      "result": "clean"
    },
    "Seclookup": {
      "method": "blacklist",
      "engine_name": "Seclookup",
      "category": "harmless",
      "result": "clean"
    },
    "SecureBrain": {
      "method": "blacklist",
      "engine_name": "SecureBrain",
      "category": "undetected",
      "result": "unrated"
    },
    "SOCRadar": {
      "method": "blacklist",
      "engine_name": "SOCRadar",
      "category": "malicious",
      "result": "malware"
    },
    "Sophos": {
      "method": "blacklist",
      "engine_name": "Sophos",
      "category": "harmless",
      "result": "clean"
    },
    "Spam404": {
      "method": "blacklist",
      "engine_name": "Spam404",
      "category": "harmless",
      "result": "clean"
    },
    "StopForumSpam": {
      "method": "blacklist",
      "engine_name": "StopForumSpam",
      "category": "harmless",
      "result": "clean"
    },
    "Sucuri SiteCheck": {
      "method": "blacklist",
      "engine_name": "Sucuri SiteCheck",
      "category": "harmless",
      "result": "clean"
    },
    "ThreatHive": {
      "method": "blacklist",
      "engine_name": "ThreatHive",
      "category": "harmless",
      "result": "clean"
    },
    "Threatsourcing": {
      "method": "blacklist",
      "engine_name": "Threatsourcing",
      "category": "harmless",
      "result": "clean"
    },
    "Trustwave": {
      "method": "blacklist",
      "engine_name": "Trustwave",
      "category": "harmless",
      "result": "clean"
    },
    "Underworld": {
      "method": "blacklist",
      "engine_name": "Underworld",
      "category": "undetected",
      "result": "unrated"
```

```
      },
      "URLhaus": {
        "method": "blacklist",
        "engine_name": "URLhaus",
        "category": "harmless",
        "result": "clean"
      },
      "URLQuery": {
        "method": "blacklist",
        "engine_name": "URLQuery",
        "category": "undetected",
        "result": "unrated"
      },
      "Viettel Threat Intelligence": {
        "method": "blacklist",
        "engine_name": "Viettel Threat Intelligence",
        "category": "harmless",
        "result": "clean"
      },
      "VIPRE": {
        "method": "blacklist",
        "engine_name": "VIPRE",
        "category": "undetected",
        "result": "unrated"
      },
      "VX Vault": {
        "method": "blacklist",
        "engine_name": "VX Vault",
        "category": "harmless",
        "result": "clean"
      },
      "ViriBack": {
        "method": "blacklist",
        "engine_name": "ViriBack",
        "category": "harmless",
        "result": "clean"
      },
      "Webroot": {
        "method": "blacklist",
        "engine_name": "Webroot",
        "category": "harmless",
        "result": "clean"
      },
      "Yandex Safebrowsing": {
        "method": "blacklist",
        "engine_name": "Yandex Safebrowsing",
        "category": "harmless",
        "result": "clean"
      },
      "ZeroCERT": {
        "method": "blacklist",
        "engine_name": "ZeroCERT",
        "category": "harmless",
        "result": "clean"
      },
      "desenmascara.me": {
        "method": "blacklist",
        "engine_name": "desenmascara.me",
        "category": "harmless",
        "result": "clean"
      },
      "malwares.com URL checker": {
        "method": "blacklist",
        "engine_name": "malwares.com URL checker",
        "category": "harmless",
        "result": "clean"
      },
      "securolytics": {
        "method": "blacklist",
        "engine_name": "securolytics",
        "category": "harmless",
        "result": "clean"
      },
      "Xcitium Verdict Cloud": {
        "method": "blacklist",
        "engine_name": "Xcitium Verdict Cloud",
        "category": "undetected",
        "result": "unrated"
      },
      "zvelo": {
        "method": "blacklist",
        "engine_name": "zvelo",
        "category": "undetected",
        "result": "unrated"
      },
      "ZeroFox": {
        "method": "blacklist",
        "engine_name": "ZeroFox",
        "category": "undetected",
        "result": "unrated"
      }
    },
    "country": "RO",
    "total_votes": {
      "harmless": 0,
      "malicious": 3
    },
    "last_modification_date": 1746160560,
    "regional_internet_registry": "RIPE NCC",
    "as_owner": "SS-Net",
    "tags": [],
    "reputation": -3,
    "last_analysis_date": 1744493709,
```

```
      "asn": 204428,
      "network": "83.222.190.0/23",
      "last_analysis_stats": {
        "malicious": 9,
        "suspicious": 1,
        "undetected": 29,
        "harmless": 55,
        "timeout": 0
      },
      "whois": "inetnum: 83.222.190.0 - 83.222.191.255\nnetname: Net_4Media\norg: ORG-AA2048-RIPE\ncountry: BG\nadmin-c: PD8817-RIPE\ntech-c: PD8817
    },
    "id": "83.222.190.254",
    "iocs": {
      "ip": [],
      "domain": [],
      "url": [],
      "other": []
    }
  },
  "success": true,
  "artifacts": [],
  "operations": []
}
```