

Configuration Manual

MSc Research Project
Masters in Cyber Security

Thirupathi Reddy Baswada
Student ID: x22208071

School of Computing
National College of Ireland

Supervisor: Niall Heffernan

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: THIRUPATHI REDDY BASWADA

Student ID: X22208071

Programme: Masters in Cyber Security

Year: 2023-24

Module: Practicum

Supervisor: Niall Heffernan

Submission

Due Date: 12/08/2024

Project Title: Configuration Manual

Word Count: 2557

Page Count: 32

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Thirupathi Reddy Baswada

Date: 12/08/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

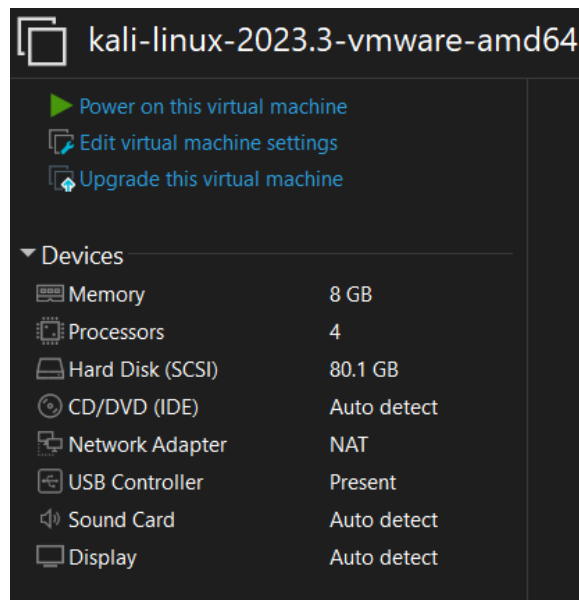
Configuration Manual

Thirupathi Reddy Baswada
x22208071

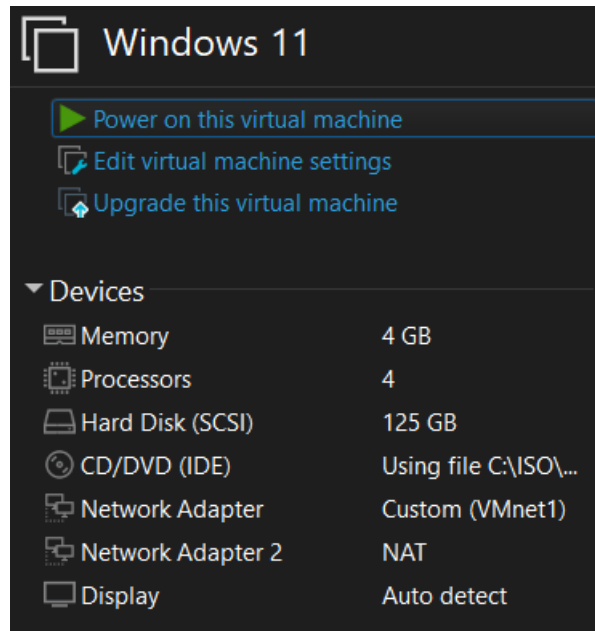
This is a manual for setting up, integrating and working with ransomware detection systems on the corporate network. It is intended for IT administrators and security professionals responsible for protecting organizational assets against ransomware threats.

1. Lab Setup

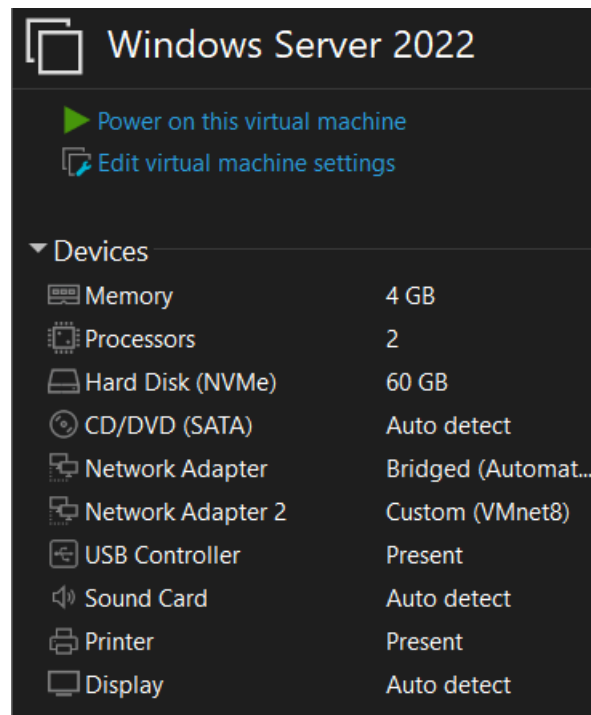
- This research is conducted under proper sandboxing environment, as this may involve testing few ransomware samples.
- Install VMware Workstation Pro from <https://access.broadcom.com/>
- After installation download Kali Linux 2023 from <https://www.kali.org/get-kali/#kali-installer-images>
- Now import the Kali image downloaded in VMware and make necessary changes (Memory = 8 GB, storage = 80 GB, processors = 4, Network adapter = NAT, etc)



- Now in similar pattern download and import windows 11 enterprise edition image from <https://www.microsoft.com/software-download/windows11> and make necessary changes (Memory = 4 GB, storage = 125 GB, processors = 4, Network adapter = NAT, etc)



- Now download and import windows server 2022 datacenter from <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022> and make necessary changes (Memory = 4 GB, storage = 60 GB, processors = 2, Network adapter = Bridged, etc)



- Now we are ready to use 3 Virtual machines setup and ready.

2. WAZUH Installation

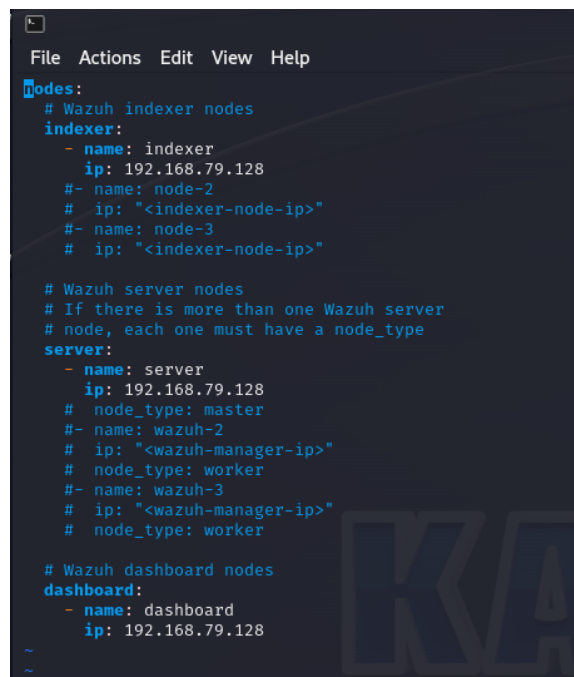
2.1 Wazuh Indexer Installation (Wazuh, 2024)

- Download the wazuh-certs-tool.sh script and the config.yml configuration file. This generates the certificates that encrypt communications between the central components of Wazuh.

```
# curl -sO https://packages.wazuh.com/4.8/wazuh-certs-tool.sh
```

```
# curl -sO https://packages.wazuh.com/4.8/config.yml
```

- Edit. /config.yml and replace node names with actual node name, IP of corresponding nodes too. Repeat these steps for all Wazuh server, the indexer Wazuh and dashboard nodes. You can add any number of node fields.



```
File Actions Edit View Help
nodes:
# Wazuh indexer nodes
indexer:
- name: indexer
  ip: 192.168.79.128
#- name: node-2
  ip: "<indexer-node-ip>"
#- name: node-3
  ip: "<indexer-node-ip>"

# Wazuh server nodes
# If there is more than one Wazuh server
# node, each one must have a node_type
server:
- name: server
  ip: 192.168.79.128
  node_type: master
#- name: wazuh-2
  ip: "<wazuh-manager-ip>"
  node_type: worker
#- name: wazuh-3
  ip: "<wazuh-manager-ip>"
  node_type: worker

# Wazuh dashboard nodes
dashboard:
- name: dashboard
  ip: 192.168.79.128
```

- Run. /wazuh-certs-tool.sh to actually generate the keys. For a multi-node cluster this needs to be deployed at all the Wazuh instances in your cluster later on.

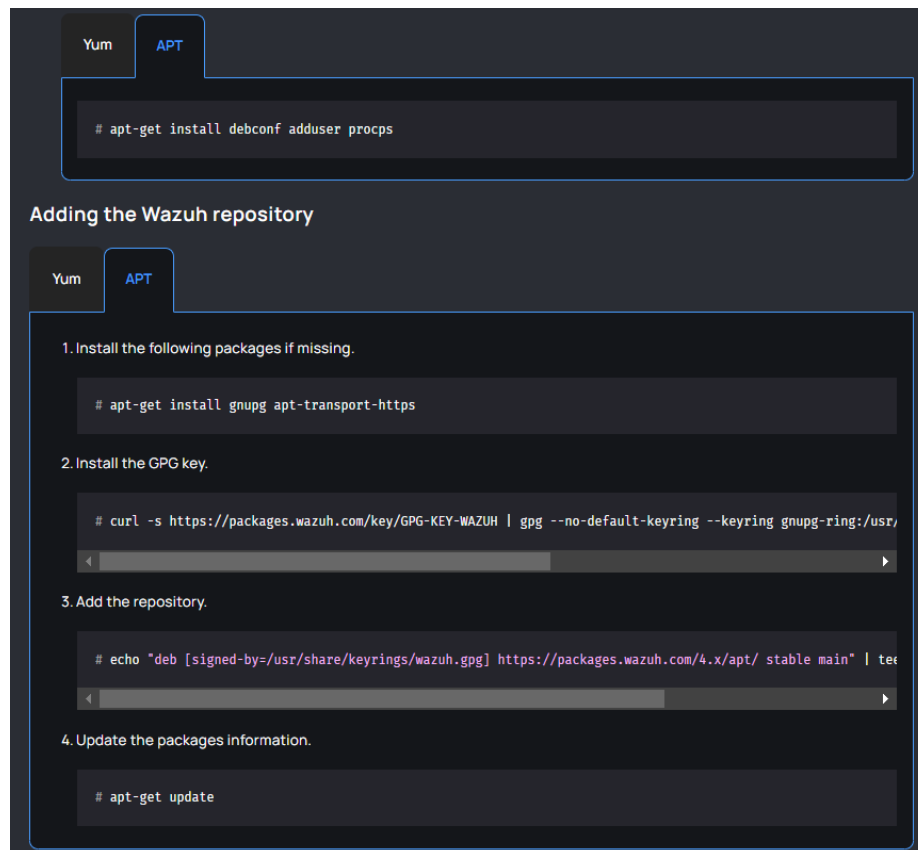
```
# bash ./wazuh-certs-tool.sh -A
```

- Zip everything needed.

```
# tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .
```

```
# rm -rf ./wazuh-certificates
```

- Install necessary packages and add wazuh repository



- Install wazuh indexer

```
# apt-get -y install wazuh-indexer
```

- Configure wazuh indexer (/etc/wazuh-indexer/opensearch.yml) as per requirement

```

network.host: 192.168.79.128
node.name: indexer
cluster.initial_master_nodes:
- indexer
#- "node-2"
#- "node-3"
cluster.name: "wazuh-cluster"
#discovery.seed_hosts:
# - "node-1-ip"
# - "node-2-ip"
# - "node-3-ip"
node.max_local_storage_nodes: "3"
path.data: /var/lib/wazuh-indexer
path.logs: /var/log/wazuh-indexer

plugins.security.ssl.http.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
plugins.security.ssl.http.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
plugins.security.ssl.http.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.transport.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
plugins.security.ssl.transport.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
plugins.security.ssl.transport.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.http.enabled: true
plugins.security.ssl.transport.enforce_hostname_verification: false
plugins.security.ssl.transport.resolve_hostname: false

plugins.security.authcz.admin_dn:
- "CN=admin,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.check_snapshot_restore_write_privileges: true
plugins.security.enable_snapshot_restore_privilege: true
plugins.security.nodes_dn:
- "CN=indexer,OU=Wazuh,O=Wazuh,L=California,C=US"
#- "CN=node-2,OU=Wazuh,O=Wazuh,L=California,C=US"
#- "CN=node-3,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.restapi.roles_enabled:
- "all_access"
- "security_rest_api_access"

```

- Deploy SSL certificates for Wazuh indexer

```
# NODE_NAME=<indexer-node-name>
```

```
#mkdir /etc/wazuh-indexer/certs
```

```
#tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/ ./${NODE_NAME}.pem
```

```
./${NODE_NAME}-key.pem ./admin.pem ./admin-key.pem ./root-ca.pem
```

```
#mv -n /etc/wazuh-indexer/certs/${NODE_NAME}.pem /etc/wazuh-indexer/certs/indexer.pem
```

```
#mv -n /etc/wazuh-indexer/certs/${NODE_NAME}-key.pem /etc/wazuh-indexer/certs/indexer-
key.pem
```

```
#chmod 500 /etc/wazuh-indexer/certs
```

```
#chmod 400 /etc/wazuh-indexer/certs/*
```

```
#chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs
```

- Start Wazuh indexer service

```
# systemctl daemon-reload
```

```
# systemctl enable wazuh-indexer
```

```
# systemctl start wazuh-indexer
```

2.2 Wazuh Server installation (Wazuh, no date e)

- Install the following packages if missing and run the following commands.

```
# apt-get install gnupg apt-transport-https
```

```
# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

```
# echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

```
# apt-get update
```

- Install Wazuh Manager

```
# apt-get -y install wazuh-manager
```

- Install Filebeat

```
# apt-get -y install filebeat
```

- Configure the filebeat as shown below in picture
- Edit configuration file and add hosts, create keystore, add username and password and download wazuh module for filebeat.

1. Download the preconfigured Filebeat configuration file.

```
# curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.8/tpl/wazuh/filebeat/filebeat.yml
```
2. Edit the `/etc/filebeat/filebeat.yml` configuration file and replace the following value:
 - a. `hosts` :The list of Wazuh indexer nodes to connect to. You can use either IP addresses or hostnames. By default, the host is set to localhost `hosts: ["127.0.0.1:9200"]` . Replace it with your Wazuh indexer address accordingly.

If you have more than one Wazuh indexer node, you can separate the addresses using commas. For example, `hosts: ["10.0.0.1:9200", "10.0.0.2:9200", "10.0.0.3:9200"]`

```
# Wazuh - Filebeat configuration file
output.elasticsearch:
  hosts: ["10.0.0.1:9200"]
  protocol: https
  username: ${username}
  password: ${password}
```
3. Create a Filebeat keystore to securely store authentication credentials.

```
# filebeat keystore create
```
4. Add the default username and password `admin : admin` to the secrets keystore.

```
# echo admin | filebeat keystore add username --stdin --force
# echo admin | filebeat keystore add password --stdin --force
```
5. Download the alerts template for the Wazuh indexer.

```
# curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/v4.8.1/extensions/alerts-template.json
# chmod go+r /etc/filebeat/wazuh-template.json
```
6. Install the Wazuh module for Filebeat.

```
# curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.4.tar.gz | tar -xvz -C /usr/share/filebeat/mc
```

- Deploy filebeat certificates

```
# NODE_NAME=<SERVER_NODE_NAME>

# mkdir /etc/filebeat/certs
# tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./${NODE_NAME}.pem ./${NODE_NAME}-key.pem ./root-ca.pem
# mv -n /etc/filebeat/certs/${NODE_NAME}.pem /etc/filebeat/certs/filebeat.pem
# mv -n /etc/filebeat/certs/${NODE_NAME}-key.pem /etc/filebeat/certs/filebeat-key.pem
# chmod 500 /etc/filebeat/certs
# chmod 400 /etc/filebeat/certs/*
# chown -R root:root /etc/filebeat/certs
```

- Configure indexer connection by editing `/var/ossec/etc/ossec.conf`

```
<indexer>
  <enabled>yes</enabled>
  <hosts>
    <host>https://192.168.79.128:9200</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>
```

- Start Wazuh manager and filebeat service and check their status

Starting the Wazuh manager

1. Enable and start the Wazuh manager service.

Systemd

SysV init

```
# systemctl daemon-reload
# systemctl enable wazuh-manager
# systemctl start wazuh-manager
```

2. Run the following command to verify the Wazuh manager status.

Systemd

SysV init

```
# systemctl status wazuh-manager
```

Starting the Filebeat service

1. Enable and start the Filebeat service.

Systemd

SysV init

```
# systemctl daemon-reload
# systemctl enable filebeat
# systemctl start filebeat
```

2. Run the following command to verify that Filebeat is successfully installed.

```
# filebeat test output
```

2.3 Wazuh Dashboard Installation (Wazuh, no date c)

- Install wazuh dashboard module

```
# apt-get -y install wazuh-dashboard
```

- Configure wazuh dashboard by editing /etc/wazuh-dashboard/opensearch_dashboards.yml, add hosts on which dashboard is hosted.

```
Server.host: 0.0.0.0
server.port: 443
opensearch.hosts: https://192.168.79.128:9200
opensearch.ssl.verificationMode: certificate
#opensearch.username:
#opensearch.password:
opensearch.requestHeadersAllowlist: ["securitytenant","authorization"]
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ["kibana_read_only"]
server.ssl.enabled: true
server.ssl.key: "/etc/wazuh-dashboard/certs/dashboard-key.pem"
server.ssl.certificate: "/etc/wazuh-dashboard/certs/dashboard.pem"
opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
uiSettings.overrides.defaultRoute: /app/wz-home
```

- Deploy dashboard certificates

```
# NODE_NAME=<DASHBOARD_NODE_NAME>

# mkdir /etc/wazuh-dashboard/certs
# tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/ ./${NODE_NAME}.pem ./${NODE_NAME}-key.pem ./root-c
# mv -n /etc/wazuh-dashboard/certs/${NODE_NAME}.pem /etc/wazuh-dashboard/certs/dashboard.pem
# mv -n /etc/wazuh-dashboard/certs/${NODE_NAME}-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem
# chmod 500 /etc/wazuh-dashboard/certs
# chmod 400 /etc/wazuh-dashboard/certs/*
# chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
```

- Edit /usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml and replace url with wazuh server master node IP address.

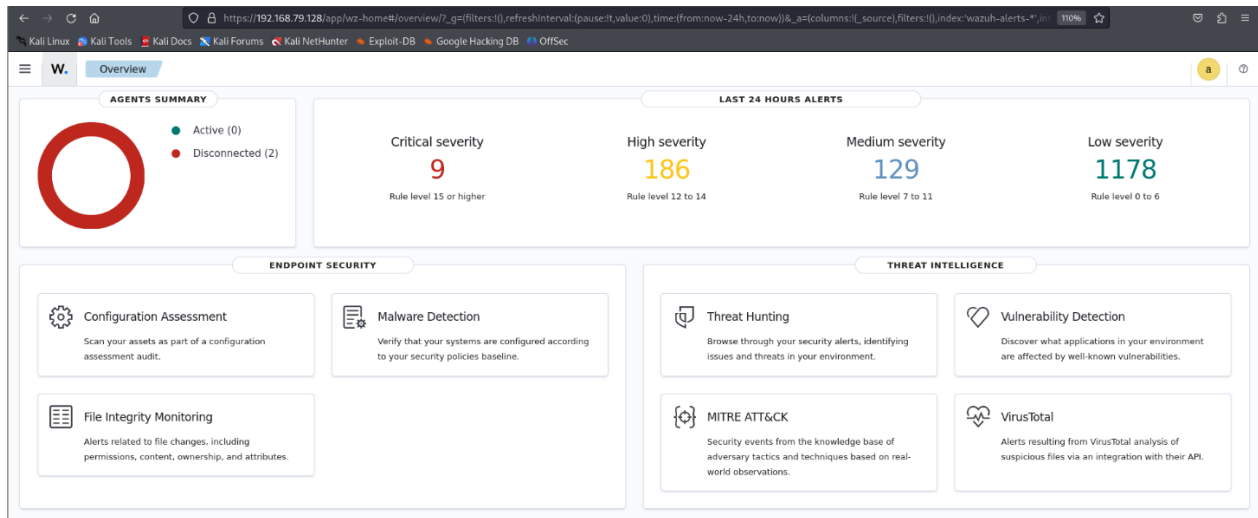
```
hosts:
  - default:
      url: https://192.168.79.128
      port: 55000
      username: wazuh-wui
      password: wazuh-wui
      run_as: false
```

- Access the Wazuh web interface with your credentials.

URL: <https://192.168.79.128/>

Username: *admin*

Password: *admin*



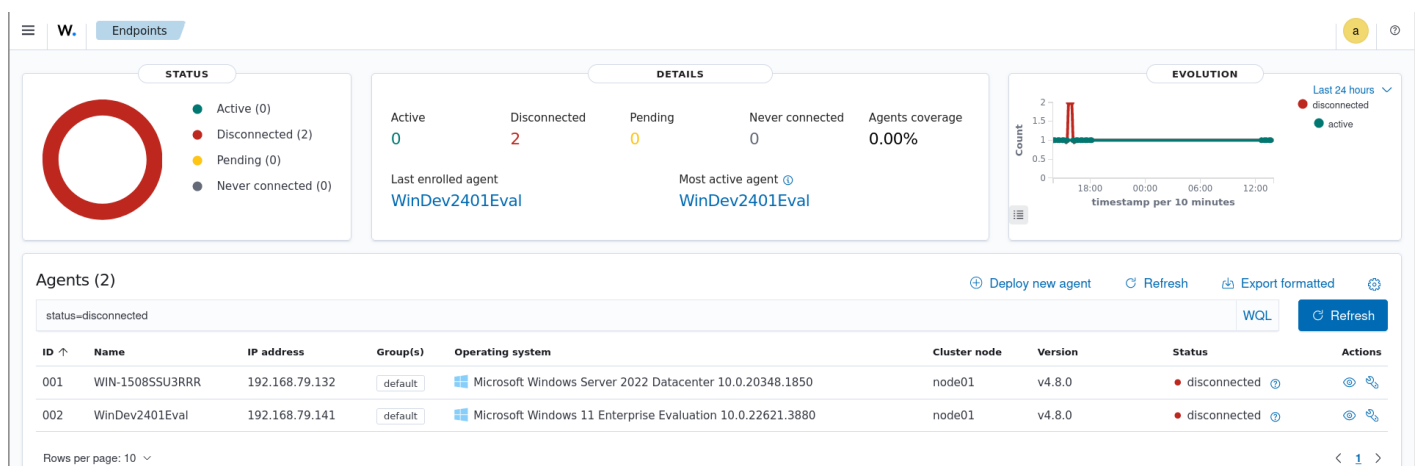
2.4 Wazuh Agent Installation (Wazuh, no date f)

- I have both Windows agents as mentioned (Windows 11, Windows server 2022 datacenter)
- Download Wazuh agent installer from <https://packages.wazuh.com/4.x/windows/wazuh-agent-4.8.1-1.msi>
- Run command prompt as administrator and execute following command to add wazuh manager address to communicate with manager and start the service

```
# wazuh-agent-4.8.1-1.msi /q WAZUH_MANAGER="192.168.79.128"
```

```
# NET START Wazuh
```

- Now we can see the agents in Wazuh Dashboard



3. Wazuh FIM module activation (Wazuh, no date b)

- Now edit ossec.conf on Wazuh Agents to configure which directories to monitor

```
<!-- Frequency that syscheck is executed default every 12 hours (now it's 5 sec) -->
<frequency>43200</frequency>

<!-- Default files to be monitored. -->
<directories recursion_level="0" restrict="regedit.exe|system.ini|win.ini">%WINDIR%</directories>

<directories recursion_level="0" restrict="at.exe|attrib.exe|cacls.exe|cmd.exe|eventcreate.exe|ftp.exe|lsass.exe|net.exe|net1.exe
|netsh.exe|reg.exe|regedt32.exe|regsvr32.exe|runas.exe|sc.exe|schtasks.exe|sethc.exe|subst.exe">%WINDIR%\SysNative</directories>
<directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe">%WINDIR%\SysNative\wbem</directories>
<directories recursion_level="0" restrict="powershell.exe">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>
<directories recursion_level="0" restrict="winrm.vbs">%WINDIR%\SysNative</directories>
<directories whodata="yes" report_changes="yes">C:\Users\User\Desktop</directories>
<directories whodata="yes" report_changes="yes">C:\Users\Public\Desktop</directories>
<directories whodata="yes" report_changes="yes">C:\Users\test\Desktop</directories>

<!-- 32-bit programs. -->
<directories recursion_level="0" restrict="at.exe|attrib.exe|cacls.exe|cmd.exe|eventcreate.exe|ftp.exe|lsass.exe|net.exe|net1.exe
|netsh.exe|reg.exe|regedt32.exe|regsvr32.exe|runas.exe|sc.exe|schtasks.exe|sethc.exe|subst.exe">%WINDIR%
\System32</directories>
<directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe">%WINDIR%\System32\wbem</directories>
<directories recursion_level="0" restrict="powershell.exe">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
<directories recursion_level="0" restrict="winrm.vbs">%WINDIR%\System32</directories>
```

- “whodata” is a module which is used to maintain Realtime monitoring and specifically indicate the user made any modifications, creations, deletions and what changes appended.
- “report_changes” module always actively searches for any changes made to report to wazuh manager
- <frequency> indicates the time taken by Wazuh agents to send all other logs to Wazuh manager in seconds (here 43200 seconds = 12 hours).
- In windows 11, I have only setup ‘Desktop’ folder of all user accounts for Realtime monitoring and on Windows server 2022, I have setup both ‘Desktop’ and ‘Downloads folder’ of all user accounts for Real time Monitoring.
- Now monitor the changes on Wazuh dashboard, by just creating a test file.

>	Aug 9, 2024 @ 13:39:53.500	c:\users\administrator\desktop\new text document.txt	deleted	File deleted.	7	553
>	Aug 9, 2024 @ 13:39:53.437	c:\users\administrator\desktop\test.txt	added	File added to the system.	5	554
>	Aug 9, 2024 @ 13:39:51.429	c:\users\administrator\desktop\new text document.txt	added	File added to the system.	5	554

4. Custom Detection Rules Development

- By default, Wazuh Architecture is not secure, we need to configure some custom detection rules, whenever these rules are triggered wazuh will show alerts and take necessary action as specified.

- I have configured a few custom detection rules to detect some general Ransomware behavior patterns. These rules should be embedded in touch `/var/ossec/etc/rules/local_rules.xml`
- Every time we update the rules or configurations, we need to restart the wazuh manager service by following command

```
# systemctl restart wazuh-manager
```

```

21 <group name="custom,ransomware">
22   <!-- Detect multiple failed login attempts -->
23   <rule id="100001" level="10">
24     <decoded_as>json</decoded_as>
25     <field name="full_log">.*failed login.*</field>
26     <description>Possible ransomware activity: Multiple failed login attempts</description>
27     <group>authentication_failed</group>
28   </rule>
29
30   <!-- Detect unauthorized access attempts -->
31   <rule id="100002" level="10">
32     <decoded_as>json</decoded_as>
33     <field name="full_log">.*unauthorized access.*</field>
34     <description>Possible ransomware activity: Unauthorized access attempt</description>
35     <group>unauthorized_access</group>
36   </rule>
37
38   <!-- Detect execution of suspicious commands -->
39   <rule id="100003" level="10">
40     <decoded_as>json</decoded_as>
41     <field name="full_log">.*execution of suspicious command.*</field>
42     <description>Possible ransomware activity: Execution of suspicious command</description>
43     <group>suspicious_command</group>
44   </rule>
45
46   <!-- Detect unusual file modifications -->
47   <rule id="100004" level="10">
48     <decoded_as>json</decoded_as>
49     <field name="full_log">.*unusual file modifications.*</field>
50     <description>Possible ransomware activity: Unusual file modifications detected</description>
51     <group>file_modification</group>
52   </rule>
53
54   <!-- Detect file encryption activity -->
55   <rule id="100005" level="10">
56     <decoded_as>json</decoded_as>
57     <field name="full_log">.*file encryption activity detected.*</field>
58     <description>Possible ransomware activity: File encryption detected</description>
59     <group>encryption_activity</group>
60   </rule>
61
62   <!-- Detect data exfiltration -->
63   <rule id="100006" level="10">
64     <decoded_as>json</decoded_as>
65     <field name="full_log">.*data exfiltration.*</field>
66     <description>Possible ransomware activity: Data exfiltration detected</description>
67     <group>data_exfiltration</group>
68   </rule>

```

```

70 <!-- Detect use of multiple file extensions -->
71 <rule id="100007" level="10">
72   <decoded_as>json</decoded_as>
73   <field name="full_log">.*multiple file extensions.*</field>
74   <description>Possible ransomware activity: Use of multiple file extensions</description>
75   <group>file_extension_anomaly</group>
76 </rule>
77
78 <!-- Detect high volume of file changes -->
79 <rule id="100008" level="10">
80   <decoded_as>json</decoded_as>
81   <field name="full_log">.*high volume of file changes.*</field>
82   <description>Possible ransomware activity: High volume of file changes detected</description>
83   <group>file_change_volume</group>
84 </rule>
85
86 <!-- Detect unusual network traffic -->
87 <rule id="100009" level="10">
88   <decoded_as>json</decoded_as>
89   <field name="full_log">.*unusual network traffic.*</field>
90   <description>Possible ransomware activity: Unusual network traffic detected</description>
91   <group>network_anomaly</group>
92 </rule>
93 </group>
94
95
96 <group name="windows,rootcheck,malware">
97   <!-- Ginwui Backdoor Detection -->
98   <rule id="100100" level="10">
99     <decoded_as>rootcheck</decoded_as>
100     <description>Ginwui Backdoor detection</description>
101     <group>pci_dss_11.4</group>
102     <match>zsyhide.dll</match>
103     <match>zsydll.dll</match>
104     <match>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\zsydll</match>
105     <match>AppInit_DLLs</match>
106   </rule>
107
108   <!-- Wargbot Backdoor Detection -->
109   <rule id="100101" level="10">
110     <decoded_as>rootcheck</decoded_as>
111     <description>Wargbot Backdoor detection</description>
112     <group>pci_dss_11.4</group>
113     <match>wgareg.exe</match>
114     <match>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\wgareg</match>
115   </rule>
116

```

```

117 <!-- Sober Worm Detection -->
118 <rule id="100102" level="10">
119   <decoded_as>rootcheck</decoded_as>
120   <description>Sober Worm detection</description>
121   <group>pci_dss_11.4</group>
122   <match>nonzipsr.noz</match>
123   <match>clonzipr.ssc</match>
124   <match>clsobrn.isc</match>
125   <match>sb2run.dii</match>
126   <match>winsend32.dal</match>
127   <match>winroot64.dal</match>
128   <match>zippedsr.piz</match>
129   <match>winexerun.dal</match>
130   <match>winprot.dal</match>
131   <match>dgssxy.yoi</match>
132   <match>cvqalkxt.apk</match>
133   <match>sysmms32.lla</match>
134   <match>Odin-Anon.Ger</match>
135 </rule>
136
137 <!-- Hotword Trojan Detection -->
138 <rule id="100103" level="10">
139   <decoded_as>rootcheck</decoded_as>
140   <description>Hotword Trojan detection</description>
141   <group>pci_dss_11.4</group>
142   <match>explore.exe</match>
143   <match>svchost.exe</match>
144   <match>mmsystem.dlx</match>
145   <match>WINDLL-ObjectsWin*.DLX</match>
146   <match>CFXP.DRV</match>
147   <match>CHJO.DRV</match>
148   <match>MMSYSTEM.DLX</match>
149   <match>OLECLI.DL</match>
150 </rule>
151
152 <!-- Beagle Worm Detection -->
153 <rule id="100104" level="10">
154   <decoded_as>rootcheck</decoded_as>
155   <description>Beagle Worm detection</description>
156   <group>pci_dss_11.4</group>
157   <match>winxp.exe</match>
158   <match>winxp.exeopen</match>
159   <match>winxp.exeopenopen</match>
160   <match>winxp.exeopenopenopen</match>
161   <match>winxp.exeopenopenopenopenopen</match>
162 </rule>
163
164 <!-- Gpcoder Trojan Detection -->
165 <rule id="100105" level="10">
166   <decoded_as>rootcheck</decoded_as>
167   <description>Gpcoder Trojan detection</description>
168   <group>pci_dss_11.4</group>
169   <match>ntos.exe</match>
170   <match>wsnpoem</match>
171   <match>audio.dll</match>
172   <match>video.dll</match>
173   <match>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run -> userinit -> ntos.exe</match>
174 </rule>

```



```

176 <!-- Looked.BK Worm Detection -->
177 <rule id="100106" level="10">
178   <decoded_as>rootcheck</decoded_as>
179   <description>Looked.BK Worm detection</description>
180   <group>pci_dss_11.4</group>
181   <match>rundl132.exe</match>
182   <match>Logo1_.exe</match>
183   <match>RichD11.d11</match>
184   <match>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run -> load -> rundl132.exe</match>
185 </rule>
186
187 <!-- Possible Malware - Svchost running outside system32 -->
188 <rule id="100107" level="10">
189   <decoded_as>rootcheck</decoded_as>
190   <description>Possible Malware - Svchost running outside system32</description>
191   <group>pci_dss_11.4</group>
192   <match>svchost.exe</match>
193   <match>!%WINDIR%\System32\svchost.exe</match>
194   <match>!%WINDIR%\SysWow64</match>
195 </rule>
196
197 <!-- Possible Malware - Inetinfo running outside system32\inetrv -->
198 <rule id="100108" level="10">
199   <decoded_as>rootcheck</decoded_as>
200   <description>Possible Malware - Inetinfo running outside system32\inetrv</description>
201   <group>pci_dss_11.4</group>
202   <match>inetinfo.exe</match>
203   <match>!%WINDIR%\System32\inetrv\inetinfo.exe</match>
204   <match>!%WINDIR%\SysWow64</match>
205 </rule>
206
207 <!-- Possible Malware - Rbot/Sdbot detected -->
208 <rule id="100109" level="10">
209   <decoded_as>rootcheck</decoded_as>
210   <description>Possible Malware - Rbot/Sdbot detected</description>
211   <group>pci_dss_11.4</group>
212   <match>rdriv.sys</match>
213   <match>lsass.exe</match>
214 </rule>
215
216 <!-- Possible Malware File -->
217 <rule id="100110" level="10">
218   <decoded_as>rootcheck</decoded_as>
219   <description>Possible Malware File</description>
220   <group>pci_dss_11.4</group>
221   <match>utorrent.exe</match>
222   <match>Files32.vxd</match>
223 </rule>
224

```

```

225 <!-- Anti-virus site on the hosts file -->
226 <rule id="100111" level="10">
227   <decoded_as>rootcheck</decoded_as>
228   <description>Anti-virus site on the hosts file</description>
229   <group>pci_dss_11.4</group>
230   <match>avp.ch</match>
231   <match>avp.ru</match>
232   <match>nai.com</match>
233   <match>awaps.net</match>
234   <match>ca.com</match>
235   <match>mcafee.com</match>
236   <match>microsoft.com</match>
237   <match>f-secure.com</match>
238   <match>sophos.com</match>
239   <match>symantec.com</match>
240   <match>my-etrust.com</match>
241   <match>viruslist.ru</match>
242   <match>networkassociates.com</match>
243   <match>kaspersky</match>
244   <match>grisoft.com</match>
245   <match>symantecliveupdate.com</match>
246   <match>clamav.net</match>
247   <match>bitdefender.com</match>
248   <match>antivirus.com</match>
249   <match>sans.org</match>
250 </rule>
251 </group>
252
253 <group name="win_evt_channel, windows">
254   <rule id="92650" level="12">
255     <if_sid>61138</if_sid>
256     <field name="win.eventdata.imagePath">%Systemroot%\...exe</field>
257     <options>no_full_log</options>
258     <description>New Windows Service Created to start from windows root path. Suspicious event as the binary may have been dropped using Windows Admin Shares.</description>
259     <mitre>
260       <id>T1021.002</id>
261       <id>T1569.002</id>
262     </mitre>
263   </rule>
264
265   <rule id="92651" level="0">
266     <if_sid>60106</if_sid>
267     <field name="win.eventdata.ipAddress" type="pcre2">(?[0-9]{1,3}\.){3}[0-9]{1,3}</field>
268     <field name="win.eventdata.ipAddress" type="pcre2" negate="yes">127.0.0.1</field>
269     <description>Successful Remote Logon by user:$(win.eventdata.targetDomainName)\$(win.eventdata.targetUserName) from $(win.eventdata.ipAddress).</description>
270     <mitre>
271       <id>T1078</id>
272     </mitre>
273     <group>authentication_success,gdpr_IV_32.2,pgp13_7.1,pgp13_7.2,hipaa_164.312.b,nist_800_53_AC.7,nist_800_53_AU.14,pci_dss_10.2.5,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3</group>
274   </rule>
275

```

```

276 <rule id="92652" level="6">
277   <if_sid>92651</if_sid>
278   <field name="win.eventdata.authenticationPackage" type="pcrc2">NTLM</field>
279   <description>Successful Remote Logon Detected - User:${win.eventdata.subjectDomainName}\${win.eventdata.targetUserName} - NTLM authentication, possible pass-the-hash attack.</description>
280   <mitre>
281     <id>T1550.002</id>
282     <id>T1078.002</id>
283   </mitre>
284   <group>authentication_success,gdpr_IV_32.2,ggp13_7.1,ggp13_7.2,hlpaa_164.312.b,nist_800_53_AC.7,nist_800_53_AU.14,pci_dss_10.2.5,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3</group>
285 </rule>
286
287 <rule id="92653" level="3">
288   <if_sid>92651</if_sid>
289   <field name="win.eventdata.logonType" type="pcrc2">10</field>
290   <description>User: ${win.eventdata.subjectDomainName}\${win.eventdata.targetUserName} logged using Remote Desktop Connection (RDP) from ip:${win.eventdata.ipAddress}.</description>
291   <mitre>
292     <id>T1021.001</id>
293     <id>T1078.002</id>
294   </mitre>
295 </rule>
296
297 <rule id="92654" level="6">
298   <if_sid>60018</if_sid>
299   <field name="win.system.eventID">*5857</field>
300   <field name="win.operation_StartedOperational.providerName">^CIMWin32</field>
301   <description>WMI query for System Information Discovery.</description>
302   <mitre>
303     <id>T1082</id>
304     <id>T1047</id>
305   </mitre>
306 </rule>
307
308 <rule id="92655" level="15">
309   <if_sid>60011</if_sid>
310   <field name="win.system.eventID">*8065</field>
311   <description>Printer driver failed to load, possible remote code execution using PrinterNightmare exploit: CVE-2021-34527.</description>
312   <mitre>
313     <id>T1210</id>
314     <id>T1547.012</id>
315   </mitre>
316 </rule>
317
318 <rule id="92656" level="15">
319   <if_sid>60106</if_sid>
320   <field name="win.eventdata.logonType" type="pcrc2">*105</field>
321   <field name="win.eventdata.ipAddress" type="pcrc2">::1|127\.\0\.\0\1</field>
322   <description>User: ${win.eventdata.subjectDomainName}\${win.eventdata.targetUserName} logged using Remote Desktop Connection (RDP) from loopback address, possible exploit over reverse tunneling using stolen credentials.
323   <mitre>
324     <id>T1021.001</id>
325     <id>T1078.002</id>
326   </mitre>
327 </rule>
328
329 <rule id="92657" level="6">
330   <if_sid>92652</if_sid>
331   <field name="win.eventdata.workstationName" type="pcrc2">. </field>
332   <description>Successful Remote Logon Detected - User:${win.eventdata.subjectDomainName}\${win.eventdata.targetUserName} - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that $(w
333   <mitre>
334     <id>T1550.002</id>
335     <id>T1078.002</id>
336     <id>T1021.001</id>
337   </mitre>
338   <group>authentication_success,pci_dss_10.2.5,ggp13_7.1,ggp13_7.2,gdpr_IV_32.2,hlpaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3</group>
339 </rule>
340 </group>
341

```

Rule 100001: Exactly when there were too many failed logins, which is a common sign of ransomware presence.

Rule 100002: Detects unauthorized access attempts which may indicate ransomware activity.

Rule 100003: Identifies the execution of suspicious commands that could be ransomware-related

Rule 100004: Ransomware or others using unusual file modifications as an indicator of a ransom.

Rule 100005: Looks for evidence of ransomware by monitoring file encryption behavior

Rule 100006: Data Exfiltration potential sign of Ransomware

Rule 100007: Detects generic multiple file extension use, a clue that the ransomware used is low-end.

Rule 100008: High volume of file changes (susceptible to false positives)

Rule 100009: Monitors network traffic for anything out of the ordinary, especially data patterns and other signs which could point to a ransomware activity.

Rule 100100: Detects Ginwui Backdoor, possible malware

Rule 100101; Detects Wargbot Backdoor, possible malware

Rule 100102: Detects Sober Worm, possible malware

Rule 100103: Detects Hotword Trojan, possible malware

Rule 100104: Detects Beagle Worm, malware activity

Rule 100105: Detects Gpcoder Trojan, possible malware

Rule 100106: Detects Looked.BK Worm, possible malware

Rule 100107: Detects svchost running outside system32, possible malware

Rule 100108: Detects inetinfo running outside system32\inetsrv, possible malware

Rule 100109: Detects Rbot/Sdbot malware possible infection

Rule 100110: Detects malware files

Rule 100111: Detects anti-virus sites at hosts file, antivirus tampering

Rule 92650: A new Windows service was created in root path, possibly dropped via admin shares

Rule 92651: A successful remote logon type 3, could be authorized or intrusion

Rule 92652: A successful remote logon had logon type 10, NTLM authentication was present, possible pass-the-hash attack

Rule 92653: RD was used to logon by user, from IP address, possible unauthorized access

Rule 92654: WMI was used to query system information

Rule 92655: A printer driver was failed to load

Rule 92656: User was used to log into RDP from loopback address, possible reverse tunneling with stolen credentials

Rule 92657: NTLM authentication was used, most likely RDP, check if workstation is allowed RDP access

5. Integrations and Custom detection rules for known Ransomwares

5.1 VirusTotal Integration (Wazuh, 2024)

- Add below integration code to /var/ossec/etc/ossec.conf to get files scan by VirusTotal.
- Now we need to register on VirusTotal and get the API key from <https://www.virustotal.com/gui/my-apikey>

```
<ossec_config>
<integration>
  <name>virustotal</name>
  <api_key>42fbc0f64b84757d423fbd69e75360c7898f5e0bbde173f394345e8b5e01f9ad</api_key>
  <alert_format>json</alert_format>
</integration>
</ossec_config>
```

5.2 Phobos Ransomware Detection (Wazuh and Okelola, 2024)

- Download Sysmon from <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon> on all agents
- Extract the file, then download Sysmon configuration file by this command

```
# wget -Uri https://wazuh.com/resources/blog/emulation-of-attack-techniques-and-detection-
with-wazuh/sysmonconfig.xml -OutFile
```

```
<SYSMON_EXECUTABLE_PATH>\sysmonconfig.xml
```

- Run following command to install and start Sysmon

```
# .\Sysmon64.exe -accepteula -i sysmonconfig.xml
```

- Add following code block to C:\Program Files (x86)\ossec-agent\ossec.conf in all agents

```
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

- Restart Wazuh agent
- Now add the following rules to /var/ossec/etc/rules/local_rules.xml

```

342 <!-- Phobos Ransomware -->
343 <group name="phobos, ransomware,">
344
345 <!-- Suspicious file creation -->
346 <rule id="100201" level="12">
347   <if_sid>61613</if_sid>
348   <field name="win.eventdata.image" type="pcre2">\\.exe</field>
349   <field name="win.eventdata.targetFilename" type="pcre2">(?!)[c-z]:\\\\Users\\\\.*\\\\AppData\\\\Local\\\\.*\\.exe</field>
350   <description>The executable $(win.eventdata.image) created a copy of itself $(win.eventdata.targetFilename) in a system folder.</description>
351   <mitre>
352     <id>T1059</id>
353   </mitre>
354 </rule>
355
356 <!-- Persistence detection -->
357 <rule id="100202" level="15">
358   <if_sid>92300</if_sid>
359   <field name="win.eventdata.image" type="pcre2">(?!).exe</field>
360   <field name="win.eventdata.eventType" type="pcre2">(?!)SetValue</field>
361   <field name="win.eventdata.targetObject" type="pcre2">(?!)HKLM\\\\SOFTWARE\\\\Microsoft\\\\Windows\\\\CurrentVersion\\\\Run\\\\[A-Za-z0-9]+</field>
362   <description>New run key added to registry by $(win.eventdata.image).</description>
363   <mitre>
364     <id>T1547.001</id>
365   </mitre>
366 </rule>
367
368 <rule id="100203" level="12">
369   <if_sid>61613</if_sid>
370   <field name="win.eventdata.image" type="pcre2">\\.exe</field>
371   <field name="win.eventdata.targetFilename" type="pcre2">(?!)ProgramData\\\\Microsoft\\\\Windows\\\\Start Menu\\\\Programs\\\\Startup\\\\.*\\.exe</field>
372   <description>$(win.eventdata.targetFilename) added to Startup programs by $(win.eventdata.image).</description>
373   <mitre>
374     <id>T1547.001</id>
375   </mitre>
376 </rule>
377
378 <!-- Impair defenses -->
379 <rule id="100204" level="12">
380   <if_sid>92042</if_sid>
381   <field name="win.eventdata.CommandLine" type="pcre2">netsh advfirewall set currentprofile state off</field>
382   <description>Windows firewall disabled.</description>
383   <mitre>
384     <id>T1562</id>
385   </mitre>
386 </rule>
387
388 <!-- System recovery inhibition -->
389 <rule id="100205" level="12">
390   <if_sid>61603</if_sid>
391   <field name="win.eventdata.CommandLine" type="pcre2">(?!)vssadmin\\s\\delete\\sshadows\\s\\all\\s\\quiet</field>
392   <description>Volume shadow copy deleted using $(win.eventdata.originalFileName). Potential ransomware activity detected.</description>
393   <mitre>
394     <id>T1490</id>
395     <id>T1059.003</id>
396   </mitre>
397 </rule>

```

```

399 <rule id="100206" level="12">
400   <if_sid>61603</if_sid>
401   <field name="win.eventdata.CommandLine" type="pcre2">wmic shadowcopy delete</field>
402   <description>$(win.eventdata.originalFileName) invoked to delete shadow copies. Potential ransomware activity detected.</description>
403   <mitre>
404     <id>T1490</id>
405     <id>T1059.003</id>
406   </mitre>
407 </rule>
408
409 <rule id="100207" level="12">
410   <if_sid>61603</if_sid>
411   <field name="win.eventdata.CommandLine" type="pcre2">(?!)bcdedit\\s\\set\\s\\(default)\\s\\bootstatuspolicy\\signoreallfailures</field>
412   <description>Boot configuration data edited.</description>
413   <mitre>
414     <id>T1059</id>
415   </mitre>
416 </rule>
417
418 <rule id="100208" level="12">
419   <if_sid>61603</if_sid>
420   <field name="win.eventdata.CommandLine" type="pcre2">(?!)bcdedit\\s\\set\\s\\(default)\\s\\recoveryenabled\\s\\No</field>
421   <description>System recovery disabled. Possible ransomware activity detected.</description>
422   <mitre>
423     <id>T1059</id>
424   </mitre>
425 </rule>
426
427 <rule id="100209" level="12">
428   <if_sid>61603</if_sid>
429   <field name="win.eventdata.CommandLine" type="pcre2">(?!)wbadmin\\s\\delete\\s\\catalog\\s\\quiet</field>
430   <description>System catalog deleted. Possible ransomware activity detected.</description>
431   <mitre>
432     <id>T1059</id>
433   </mitre>
434 </rule>
435
436 <!-- Ransom note file creation -->
437 <rule id="100210" level="12" timeframe="100" frequency="2">
438   <if_sid>61613</if_sid>
439   <field name="win.eventdata.image" type="pcre2">\\.exe</field>
440   <field name="win.eventdata.targetFilename" type="pcre2">(?!)[c-z]:\\\\.*\\8base</field>
441   <description>The file $(win.eventdata.targetFilename) has been created in multiple directories. Phobos ransomware activity detected.</description>
442   <mitre>
443     <id>T1059</id>
444   </mitre>
445 </rule>
446
447 </group>
448

```

Rule 100201: The rule detects the creation of executable copies by other executables in system folders.

Rule 100202: The rule identifies that another executable added new run keys in the registry to achieve persistence.

Rule 100203: The rule monitors the folder, where executables are added to the Startup programs by other executables.

Rule 100204: The rule detects if the Windows firewall is disabled via the command line.

Rule 100205: Another executable deletes volume shadow copies using the command vssadmin, which implies that ransomware deleted the files.

Rule 100206: The use of WMIC by another executable to delete shadow copies, which implies that the ransomware used WMIC to delete files.

Rule 100207: Another executable edits the boot configuration data, which might prevent system recovery.

Rule 100208: Another executable disables system recovery via the command bcdedit, which implies that ransomware disabled the functionality.

Rule 100209: The analyzes the deletion of the system catalog via the command wbadmin.

Rule 100210: The rule detects that another executable created files in multiple directories with ‘8base’, which implies that they were created by Phobos ransomware.

- Download the latest Python from <https://www.python.org/downloads/> and install on agents.
- Install PyInstaller by running following command in command prompt

```
# pip install -U pyinstaller
```

- Now save the following code as remove_threat.py extension on all endpoints

```

1  #!/usr/bin/python3
2  # Copyright (C) 2015-2022, Wazuh Inc.
3  # All rights reserved.
4
5  import os
6  import sys
7  import json
8  import datetime
9
10 if os.name == 'nt':
11     LOG_FILE = "C:\\Program Files (x86)\\ossec-agent\\active-response\\active-responses.log"
12 else:
13     LOG_FILE = "/var/ossec/logs/active-responses.log"
14
15 ADD_COMMAND = 0
16 DELETE_COMMAND = 1
17 CONTINUE_COMMAND = 2
18 ABORT_COMMAND = 3
19
20 OS_SUCCESS = 0
21 OS_INVALID = -1
22
23 class message:
24     def __init__(self):
25         self.alert = ""
26         self.command = 0
27
28     def write_debug_file(ar_name, msg):
29         with open(LOG_FILE, mode="a") as log_file:
30             log_file.write(str(datetime.datetime.now().strftime('%Y/%m/%d %H:%M:%S')) + " " + ar_name + ": " + msg + "\n")
31
32     def setup_and_check_message(argv):
33
34         # get alert from stdin
35         input_str = ""
36         for line in sys.stdin:
37             input_str = line
38             break
39
40         try:
41             data = json.loads(input_str)
42         except ValueError:
43             write_debug_file(argv[0], 'Decoding JSON has failed, invalid input format')
44             message.command = OS_INVALID
45             return message
46

```

```

48     message.alert = data
49
50     command = data.get("command")
51
52     if command == "add":
53         message.command = ADD_COMMAND
54     elif command == "delete":
55         message.command = DELETE_COMMAND
56     else:
57         message.command = OS_INVALID
58         write_debug_file(argv[0], 'Not valid command: ' + command)
59
60     return message
61
62
63 def send_keys_and_check_message(argv, keys):
64
65     # build and send message with keys
66     keys_msg = json.dumps({"version": 1, "origin": {"name": argv[0], "module": "active-response"}, "command": "check_keys", "parameters": {"keys": keys}})
67
68     write_debug_file(argv[0], keys_msg)
69
70     print(keys_msg)
71     sys.stdout.flush()
72
73     # read the response of previous message
74     input_str = ""
75     while True:
76         line = sys.stdin.readline()
77         if line:
78             input_str = line
79             break
80
81     # write_debug_file(argv[0], input_str)
82
83     try:
84         data = json.loads(input_str)
85     except ValueError:
86         write_debug_file(argv[0], 'Decoding JSON has failed, invalid input format')
87         return message
88

```

```

89     action = data.get("command")
90
91     if "continue" == action:
92         ret = CONTINUE_COMMAND
93     elif "abort" == action:
94         ret = ABORT_COMMAND
95     else:
96         ret = OS_INVALID
97         write_debug_file(argv[0], "Invalid value of 'command'")
98
99     return ret
100
101 def main(argv):
102     write_debug_file(argv[0], "Started")
103
104     # validate json and get command
105     msg = setup_and_check_message(argv)
106
107     if msg.command < 0:
108         sys.exit(OS_INVALID)
109
110     if msg.command == ADD_COMMAND:
111         alert = msg.alert["parameters"]["alert"]
112         keys = [alert["rule"]["id"]]
113         action = send_keys_and_check_message(argv, keys)
114
115         # if necessary, abort execution
116         if action != CONTINUE_COMMAND:
117             if action == ABORT_COMMAND:
118                 write_debug_file(argv[0], "Aborted")
119                 sys.exit(OS_SUCCESS)
120             else:
121                 write_debug_file(argv[0], "Invalid command")
122                 sys.exit(OS_INVALID)
123
124         try:
125             os.remove(msg.alert["parameters"]["alert"]["data"]["virustotal"]["source"]["file"])
126             write_debug_file(argv[0], json.dumps(msg.alert) + " Successfully removed threat")
127         except OSError as error:
128             write_debug_file(argv[0], json.dumps(msg.alert) + "Error removing threat")
129
130     else:
131         write_debug_file(argv[0], "Invalid command")
132
133     write_debug_file(argv[0], "Ended")
134
135     sys.exit(OS_SUCCESS)
136
137 if __name__ == "__main__":
138     main(sys.argv)

```

- The `os.remove()` function (line no. 127) handles removal of the malicious file
- Now convert this script to executable file by running following command

```
# pyinstaller -F remove-threat.py
```

- Now restart wazuh service in services app on all wazuh agents.
- Making the following changes to `/var/ossec/etc/ossec.conf` in Wazuh server will active the active-response module of Wazuh to take necessary actions when the set alert triggers.


```

<ossec_config>
  <command>
    <name>remove-threat</name>
    <executable>remove-threat.exe</executable>
    <timeout_allowed>no</timeout_allowed>
  </command>
  <active-response>
    <disabled>no</disabled>
    <command>remove-threat</command>
    <location>local</location>
    <rules_id>87105</rules_id>
  </active-response>
</ossec_config>

```

- Add following rules to /var/ossec/etc/rules/local_rules.xml to let Wazuh know the exactly on what behavior (log analysis) to trigger the alert

```

<group name="virustotal,">
  <!-- VirusTotal detection rules -->
  <rule id="200201" level="12">
    <if_sid>657</if_sid>
    <match>Successfully removed threat</match>
    <description>$(parameters.program) removed threat located at $(parameters.alert.data.virustotal.source.file)</description>
  </rule>
  <rule id="200202" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
    <description>Error removing threat located at $(parameters.alert.data.virustotal.source.file)</description>
  </rule>
</group>

```

- Now restart the Wazuh Manager.

5.3 Kuiper Ransomware Detection and YARA integration (Wazuh and Faruna, 2024)

- We need to follow the same procedure of installing Sysmon as discussed above. As we have already installed and configured it we can move to the next steps.
- Now add the following rules to /var/ossec/etc/rules/local_rules.xml and restart wazuh manager.

```

467 <!-- Kuiper Ransomware Detection rules -->
468
469 <group name="kuiper,ransomware,">
470 <!-- Ransom note file creation -->
471 <rule id="100011" level="15" timeframe="100" frequency="2">
472   <if_sid>61613</if_sid>
473   <field name="win.eventdata.image" type="pcr2">\.exe</field>
474   <field name="win.eventdata.targetFilename" type="pcr2">{?}[C-Z]:\.*\README_TO_DECRYPT.txt</field>
475   <description>The file $(win.eventdata.targetFilename) has been created in multiple directories. Kuiper ransomware detected.</description>
476   <mitre>
477     <id>T1059</id>
478   </mitre>
479 </rule>
480
481 <rule id="100012" level="12">
482   <if_sid>61603</if_sid>
483   <field name="win.eventdata.CommandLine" type="pcr2">{?}cmd.exe\s\c\s\ssadmin\sresize\shadowstorage\s\for=[C-Z]:\s\on=C:\s\maxsize=401MB|ssadmin\sdelete\sshadows\s\all\s\quiet</field>
484   <description>Shadow copies have been deleted. Possible ransomware detected.</description>
485   <mitre>
486     <id>T1087</id>
487     <id>T1059.003</id>
488   </mitre>
489 </rule>
490
491 <rule id="100013" level="12">
492   <if_sid>61603</if_sid>
493   <field name="win.eventdata.CommandLine" type="pcr2">{?}powershell.exe\s\s-ep\s\bypass\s-c\sSet-MpPreference\s-DisableRealtimeMonitoring 1\s-ErrorAction\sSilentlyContinue|powershell.exe\\s-ep\s\bypass\s-w\shidden
494   <description>Microsoft Defender Real-time Monitoring disabled. Possible ransomware activity.</description>
495   <mitre>
496     <id>T1087</id>
497     <id>T1059.003</id>
498   </mitre>
499 </rule>
500
501 <rule id="100014" level="12">
502   <if_sid>92032</if_sid>
503   <field name="win.eventdata.CommandLine" type="pcr2">{?}taskkill\s\s\f\s\im\sCETASvc.exe</field>
504   <description>Trend Micro process terminated. Possible ransomware activity detected.</description>
505   <mitre>
506     <id>T1087</id>
507     <id>T1059.003</id>
508   </mitre>
509 </rule>
510
511 <rule id="100015" level="12">
512   <if_sid>92032</if_sid>
513   <field name="win.eventdata.CommandLine" type="pcr2">{?}taskkill\s\s\f\s\im MortonSecurity.exe</field>
514   <description>Morton Security process terminated. Possible ransomware activity detected.</description>
515   <mitre>
516     <id>T1087</id>
517     <id>T1059.003</id>
518   </mitre>
519 </rule>
520

```

```

521
522   <rule id="100016" level="12">
523     <if_sid>92032</if_sid>
524     <field name="win.eventdata.CommandLine" type="pcr2">{?}taskkill\s\s\f\s\im SophosSAU.exe</field>
525     <description>Sophos process terminated. Possible ransomware activity detected.</description>
526     <mitre>
527       <id>T1087</id>
528       <id>T1059.003</id>
529     </mitre>
530   </rule>
531
532   <rule id="100017" level="12">
533     <if_sid>92036</if_sid>
534     <field name="win.eventdata.CommandLine" type="pcr2">{?}net\s\sstop\sTrend\sMicro</field>
535     <description>Trend Micro service disabled. Possible ransomware activity detected.</description>
536     <mitre>
537       <id>T1087</id>
538       <id>T1059.003</id>
539     </mitre>
540   </rule>
541
542   <rule id="100018" level="12">
543     <if_sid>92036</if_sid>
544     <field name="win.eventdata.CommandLine" type="pcr2">{?}net\s\sstop\sNrtscan</field>
545     <description>Norton Security service disabled. Possible ransomware activity detected.</description>
546     <mitre>
547       <id>T1087</id>
548       <id>T1059.003</id>
549     </mitre>
550   </rule>
551
552   <rule id="100019" level="12">
553     <if_sid>92036</if_sid>
554     <field name="win.eventdata.CommandLine" type="pcr2">{?}net\s\sstop\sAvast\sAntivirus!</field>
555     <description>Avast Antivirus service detected. Possible ransomware disabled.</description>
556     <mitre>
557       <id>T1087</id>
558       <id>T1059.003</id>
559     </mitre>
560   </rule>
561
562   <rule id="100020" level="12">
563     <if_sid>92032</if_sid>
564     <field name="win.eventdata.CommandLine" type="pcr2">{?}wevtutil\s\scl\ssecurity</field>
565     <description>Windows security event logs deleted. Possible ransomware activity detected.</description>
566     <mitre>
567       <id>T1070.001</id>
568     </mitre>
569   </rule>
570
571   <rule id="100021" level="12">
572     <if_sid>92032</if_sid>
573     <field name="win.eventdata.CommandLine" type="pcr2">{?}wevtutil\s\scl\sapplication</field>
574     <description>Windows application event deleted. Possible ransomware activity detected.</description>
575     <mitre>
576       <id>T1070.001</id>
577     </mitre>
578   </rule>
579

```

Rule ID 100011: Creation of ransomware files in multiple directories. It shows that the Kuiper ransomware was detected.

Rule ID 100012: Shadow copies were deleted via the command line. In fact, I suppose it indicates possible ransomware activity.

Rule ID 100013: Microsoft defender real-time monitoring was disabled by using PowerShell. As for me, this step signified possible ransomware activity.

Rule ID 100014: Trend Micro process was terminated with taskkill. I think this step indicates possible ransomware activity.

Rule ID 100015: Norton Security process was terminated with taskkill. I suppose this step shows possible ransomware activity.

Rule ID 100016: Sophos process was terminated with taskkill. It was possible ransomware activity.

Rule ID 100017: “net stop” was used for disabling the Trend Micro service. In my opinion, it indicates possible ransomware activity.

Rule ID 100018: net stop was used for disabling the Norton Security service and for me, it implies possible ransomware activity.

Rule ID 100019: Avast Antivirus service was disabled with the help of net stop. I believe this step was ransomware activity.

Rule ID 100020: eventlogs were deleted using the “wevtutil” of windows security. It was possible ransomware activity.

Rule ID 100021: Deletion of Windows application event logs using wevtutil. Indicates possible ransomware activity.

- Download yara using following command

```
# Invoke-WebRequest -Uri https://github.com/VirusTotal/yara/releases/download/v4.3.2/yara-4.3.2-2150-win64.zip -OutFile v4.3.2-2150-win64.zip
```

- Expand YARA executable

```
# Expand-Archive v4.3.2-2150-win64.zip
```

- Create folder C:\Program Files (x86)\ossec-agent\active-response\bin\yara\ and copy yara binary into it using this command

```
# mkdir 'C:\Program Files (x86)\ossec-agent\active-response\bin\yara'
```

```
# cp .\v4.3.2-2150-win64\yara64.exe 'C:\Program Files (x86)\ossec-agent\active-response\bin\yara'
```

- Now create a new batch file yara.bat at C:\Program Files (x86)\ossec-agent\active-response\bin\ and copy below script into bat file.

```

1 @echo off
2 setlocal enableDelayedExpansion
3 reg Query "HKLM\Hardware\Description\System\CentralProcessor\0" | find /i "x86" > NUL && SET OS=32BIT || SET OS=64BIT
4 if %OS%==32BIT (
5     SET log_file_path="%programfiles%\ossec-agent\active-response\active-responses.log"
6 )
7 if %OS%==64BIT (
8     SET log_file_path="%programfiles(x86)\ossec-agent\active-response\active-responses.log"
9 )
10 set input=
11 for /f "delims=" %%a in ('PowerShell -command "$logInput = Read-Host; Write-Output $logInput"') do (
12     set input=%%a
13 )
14 set json_file_path="C:\Program Files (x86)\ossec-agent\active-response\stdin.txt"
15 set syscheck_file_path=
16 echo %input% > %json_file_path%
17 FOR /F "tokens=* USEBACKQ" %%F IN ("Powershell -Nop -C "(Get-Content 'C:\Program Files (x86)\ossec-agent\active-response\stdin.txt')[ConvertFrom-Json].parameters.alert.syscheck.path") DO (
18     SET syscheck_file_path=%%F
19 )
20 set yara_exe_path="C:\Program Files (x86)\ossec-agent\active-response\bin\yara\yara64.exe"
21 set yara_rules_path="C:\Program Files (x86)\ossec-agent\active-response\bin\yara\rules\yara_rules.yar"
22 echo %syscheck_file_path% >> %log_file_path%
23 for /f "delims=" %%a in ('powershell -command "& \"%yara_exe_path%\" \"%yara_rules_path%\" \"%syscheck_file_path%\""') do (
24     echo wazuh-yara: INFO - Scan result: %%a >> %log_file_path%
25     :: Deleting the scanned file.
26     del /f "%syscheck_file_path%" >nul 2>&1
27 if exist "%syscheck_file_path%" (
28     echo wazuh-yara: INFO - Error removing threat: %%a >> %log_file_path%
29 ) else (
30     echo wazuh-yara: INFO - Successfully deleted: %%a >> %log_file_path%
31 )
32 )
33 exit /b

```

- Restart wazuh service on all agents wherever changes were made.
- Now in wazuh server add these rules to /var/ossec/etc/rules/local_rules.xml to generate alerts

```

581 <group name= "syscheck,">
582     <rule id="100024" level="7">
583         <if_sid>550</if_sid>
584         <field name="file" type="pcre2">(?!i)C:\\Users.+Desktop</field>
585         <description>File modified in the Desktop folder.</description>
586     </rule>
587
588     <rule id="100025" level="7">
589         <if_sid>554</if_sid>
590         <field name="file" type="pcre2">(?!i)C:\\Users.+Desktop</field>
591         <description>File added to the Desktop folder.</description>
592     </rule>
593 </group>

```

- Add few configurations to /var/ossec/etc/ossec.conf in <ossec_config> block

```

231 <command>
232     <name>yara</name>
233     <executable>yara.bat</executable>
234     <timeout_allowed>no</timeout_allowed>
235 </command>
236
237 <active-response>
238     <command>yara</command>
239     <location>local</location>
240     <rules_id>100024,100025</rules_id>
241 </active-response>

```

- Add following decoders to /var/ossec/etc/decoders/local_decoder.xml to decode the logs generated

```

25
26 <decoder name="yara_decoder">
27 |   <prematch>wazuh-yara:</prematch>
28 </decoder>
29 <decoder name="yara_decoder1">
30 |   <parent>yara_decoder</parent>
31 |   <regex>wazuh-yara: (\S+) - Scan result: (\S+) (\S+)</regex>
32 |   <order>log_type, yara_rule, yara_scanned_file</order>
33 </decoder>
34
35 <decoder name="yara_decoder1">
36 |   <parent>yara_decoder</parent>
37 |   <regex>wazuh-yara: (\S+) - Successfully deleted: (\S+) (\S+)</regex>
38 |   <order>log_type, yara_rule, yara_scanned_file</order>
39 </decoder>
40
41 <decoder name="yara_decoder1">
42 |   <parent>yara_decoder</parent>
43 |   <regex>wazuh-yara: (\S+) - Error removing threat: (\S+) (\S+)</regex>
44 |   <order>log_type, yara_rule, yara_scanned_file</order>
45 </decoder>
46

```

- Create few custom rules for YARA and add them to /var/ossec/etc/rules/local_rules.xml and reload the wazuh manager

```

594
595 <!-- Rule for the decoder (yara_decoder) -->
596 <group name="yara,">
597 |   <rule id="100026" level="0">
598 |     <decoded_as>yara_decoder</decoded_as>
599 |     <description>Yara grouping rule</description>
600 |   </rule>
601
602 <!-- YARA scan detects a positive match -->
603 <rule id="100027" level="12">
604 |   <if_sid>100026</if_sid>
605 |   <match type="pcre2">wazuh-yara: INFO - Scan result: </match>
606 |   <description>File "$(yara_scanned_file)" is a positive match. Yara rule: $(yara_rule)</description>
607 | </rule>
608
609 <!-- Wazuh successfully deletes malware with a positive match -->
610 <rule id="100028" level="12">
611 |   <if_sid>100026</if_sid>
612 |   <match type="pcre2">wazuh-yara: INFO - Successfully deleted: </match>
613 |   <description>Successfully removed "$(yara_scanned_file)" by active response due to YARA rule $(yara_rule) positive match</description>
614 | </rule>
615
616 <!-- Wazuh encounters an error when deleting malware with a positive match -->
617 <rule id="100029" level="12">
618 |   <if_sid>100026</if_sid>
619 |   <match type="pcre2">wazuh-yara: INFO - Error removing threat: </match>
620 |   <description>Error removing "$(yara_scanned_file)". YARA rule: $(yara_rule)</description>
621 | </rule>
622 </group>
623

```

Rule 100026: A grouping rule for YARA alerts in Wazuh.

Rule 100027: Generated when a YARA scan finds a match in a file.

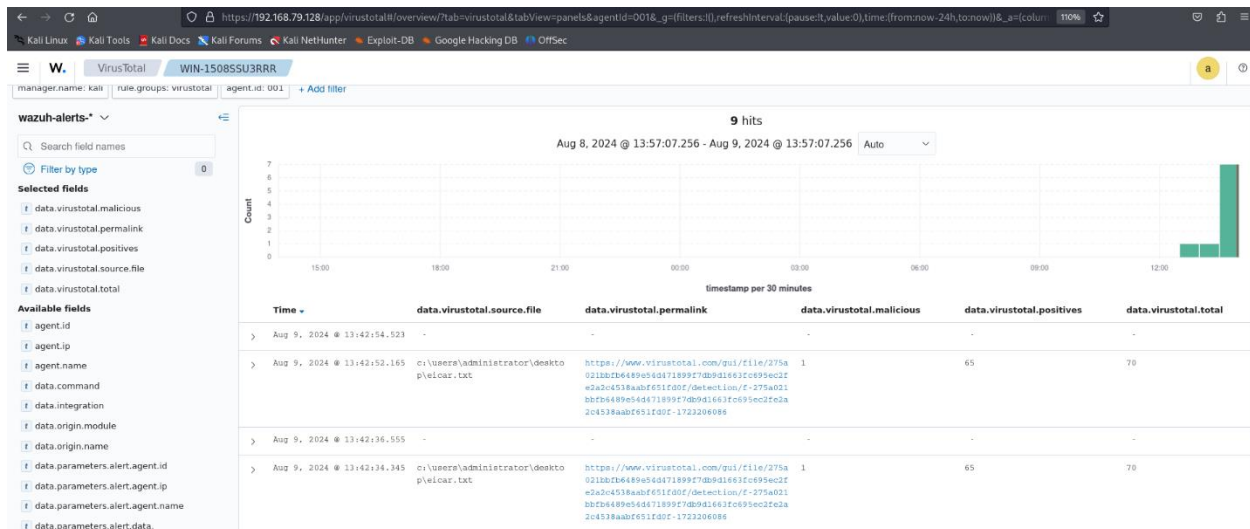
Rule 100028: Informational alert after malware is successfully deleted.

Rule 100029: Error logs when a threat attempted to be removed and the YARA rule was able to detect it.

6. Simulation, Testing and Results

- Downloaded few Ransomwares and tried to place them in directories on which Wazuh have been watching in Realtime, Wazuh has detected 90% of samples I have tested and few malicious activities like encryption, unauthorized access, Failed logon attempts have been detected by Wazuh. All Result data and snapshots have been presented below.

Malware	Malware data	Description
240387329dee4f03f98a89a2feff9bg4kk5sy0f614cdac24129da54442762.zip	10 engines detect malicious files	active response removes the threat located at C:\Users\User\Desktop\240387329dee4f03f98a89a2feff9bg4kk5sy0f614cdac24129da54442762.zip
WY4CB9TMALWARESAMPLE.rar	3 engines detected malicious files	active response removes the threat located at C:\Users\User\Desktop\WY4CB9TMALWARESAMPLE.rar
yitaly.exe.zip	2 engines detected malicious files	active response removes the threat located at C:\Users\User\Desktop\yitaly.exe.zip
942e275de833c7d0f8a5ebe519c621136cbf467d079d7890018aa84.zip	No record in VirusTotal Database	New File downloaded
Eicar.com	56 engines detected malicious files	active response removes the threat located at C:\Users\User\Desktop\eicar.com
.eh.exe.zip	10 engines detected malicious files	active response removes the threat located at C:\Users\User\Desktop\eh.exe.zip
340s.exe.zip	10 engines detected malicious files	active response removes the threat located at C:\Users\User\Desktop\340s.exe.zip
0.exe.zip	2 engines detected malicious files	active response removes the threat located at C:\Users\User\Desktop\0.exe.zip



VirusTotal Dashboard

VirusTotal: Alert - c:\users\user\desktop\test.txt - No positives found	3	87104
Powershell process created an executable file in Windows root folder	9	92205
Suspicious Windows cmd shell execution	3	92032
Suspicious Windows cmd shell execution	3	92032
Suspicious Windows cmd shell execution	3	92032
Windows command prompt started by an abnormal process	4	92052
Suspicious Windows cmd shell execution	3	92032
File modified in the Desktop folder.	7	100024

Encryption Logs

W. Threat Hunting WIN-1508SSU3RRR

> Aug 9, 2024 @ 13:42:59.524	2\python312.dll from the Temp directory.	-	-	-	-
> Aug 9, 2024 @ 13:42:59.524	Executable dropped in Windows root folder	-	-	6	92217
> Aug 9, 2024 @ 13:42:53.492	Executable dropped in Windows root folder	-	-	6	92217
> Aug 9, 2024 @ 13:42:53.354	Executable dropped in Windows root folder	-	-	6	92217
> Aug 9, 2024 @ 13:42:52.165	VirusTotal: Alert - c:\users\administrator\desktop\leicar.txt - 65 engines detected this file	-	-	12	87105
> Aug 9, 2024 @ 13:42:37.399	File deleted.	-	-	7	553
> Aug 9, 2024 @ 13:42:37.241	An executable - C:\Program Files (x86)\osec-agent\active-response\bin\remove-threat.exe - loaded C:\Windows\Temp\XBI5032 2\python312.dll from the Temp directory.	-	-	6	92157
> Aug 9, 2024 @ 13:42:37.238	An executable - C:\Program Files (x86)\osec-agent\active-response\bin\remove-threat.exe - loaded C:\Windows\Temp\XBI5032 2\python312.dll from the Temp directory.	-	-	6	92157
> Aug 9, 2024 @ 13:42:36.555	active-response/bin/remove-threat.exe removed threat located at c:\users\administrator\desktop\leicar.txt	-	-	12	200201
> Aug 9, 2024 @ 13:42:36.399	Executable dropped in Windows root folder	-	-	6	92217
> Aug 9, 2024 @ 13:42:36.385	Executable dropped in Windows root folder	-	-	6	92217
> Aug 9, 2024 @ 13:42:36.274	Executable dropped in Windows root folder	-	-	6	92217
> Aug 9, 2024 @ 13:42:36.345	VirusTotal: Alert - c:\users\administrator\desktop\leicar.txt - 65 engines detected this file	-	-	12	87105
> Aug 9, 2024 @ 13:42:30.413	File added to the system.	-	-	5	554

VirusTotal threat removal

> Aug 9, 2024 @ 15:35:40.642	Successfully removed "c:\users\user\desktop\leicar.com" by active response due to YARA rule SUSP_Just_EICAR_RID2C24 positive match	12	100028
> Aug 9, 2024 @ 15:35:40.640	File "c:\users\user\desktop\leicar.com" is a positive match. Yara rule: SUSP_Just_EICAR_RID2C24	12	100027

Yara threat removal

rule.description	rule.level	rule.id
Successfully removed "c:\users\wazuh\downloads\1d2db070008116a7a1992ed7dad7e7f26a0bfee3499338c3e603161e3f18db2f.exe" by active response due to YARA rule _Blackbit_ransomware positive match	12	100033
File "c:\users\wazuh\downloads\1d2db070008116a7a1992ed7dad7e7f26a0bfee3499338c3e603161e3f18db2f.exe" is a positive match. Yara rule: _Blackbit_ransomware	12	100032
File added to the Downloads folder.	7	100030

Blackbit Ransomware threat removal

rule.description	rule.level	rule.id
An executable - C:\Program Files (x86)\ossec-agent\active-response\bin\remove-threat.exe - loaded C:\Windows\Temp_MEI31802\VCRUNTIME140.dll from the Temp directory.	6	92157
An executable - C:\Program Files (x86)\ossec-agent\active-response\bin\remove-threat.exe - loaded C:\Windows\Temp_MEI31802\python311.dll from the Temp directory.	6	92157
VirusTotal: Alert - c:\users\Windows11\downloads\495fbfecbcbdb103389cc33828db139fa6d66bece479c7f70279834051412d72.exe - 55 engines detected this file	12	87105
active-response/bin/remove-threat.exe removed threat located at c:\users\tony\downloads\495fbfecbcbdb103389cc33828db139fa6d66bece479c7f70279834051412d72.exe	12	110006
An executable - C:\Program Files (x86)\ossec-agent\active-response\bin\remove-threat.exe - loaded C:\Windows\Temp_MEI45922\VCRUNTIME140.dll from the Temp directory.	6	92157
An executable - C:\Program Files (x86)\ossec-agent\active-response\bin\remove-threat.exe - loaded C:\Windows\Temp_MEI45922\python311.dll from the Temp directory.	6	92157
VirusTotal: Alert - c:\users\Windows11\downloads\495fbfecbcbdb103389cc33828db139fa6d66bece479c7f70279834051412d72.exe - 55 engines detected this file	12	87105
File added to the system.	5	554
Integrity checksum changed.	7	550

Crosslock Ransomware threat removal

7. Challenges

Setting up the policy and enforcement method of ransomware detection system is first to his at the volume of logs an enormous problematic As the network continuously monitors a variety of terminals, it will generate and store a large amount of log information This means that you need storage solutions which are able to go with the flow of ever-increasing data volumes, because ransomware is constantly changing, all rules have to remain updated accurately updated. This is achieved through strict regular routine updates and ongoing testing of rules to ensure that they also work satisfactorily in the face new and emerging strains of ransomware The conflict between demands for storage space and needs to swiftly adapt rule sets is a major headache in the development of systems that remain operational.

As in my case, I have embedded a automatic cronjob running in my manager to delete previous day logs. This cronjob is set to run every 30 minutes to save memory and time.

```
*/30 * * * * find /var/ossec/logs/alerts/ -type f -mtime +1 -exec rm -f {} \;
*/30 * * * * find /var/ossec/logs/archives/ -type f -mtime +1 -exec rm -f {} \;
```

8. References

Wazuh (2024) *Detecting and removing malware using VirusTotal integration*. Available at: <https://documentation.wazuh.com/current/proof-of-concept-guide/detect-remove-malware-virustotal.html> (Accessed: 11 August 2024).

Wazuh (2024) *File integrity monitoring - Proof of Concept guide*. Available at: <https://documentation.wazuh.com/current/proof-of-concept-guide/poc-file-integrity-monitoring.html> (Accessed: 12 August 2024).

Wazuh (2024) *Installing the Wazuh dashboard step by step - Wazuh dashboard*. Available at: <https://documentation.wazuh.com/current/installation-guide/wazuh-dashboard/step-by-step.html> (Accessed: 12 August 2024).

Wazuh (2024) *Installing the Wazuh indexer step by step - Wazuh indexer*. Available at: <https://documentation.wazuh.com/current/installation-guide/wazuh-indexer/step-by-step.html> (Accessed: 12 August 2024).

Wazuh (2024) *Installing the Wazuh server step by step - Wazuh server*. Available at: <https://documentation.wazuh.com/current/installation-guide/wazuh-server/step-by-step.html> (Accessed: 12 August 2024).

Wazuh (2024) *Installing Wazuh agents on Windows endpoints - Wazuh agent*. Available at: <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html> (Accessed: 12 August 2024).

Wazuh and Faruna, A. (2024) *Kuiper ransomware detection and response with Wazuh, Wazuh*. Available at: <https://wazuh.com/blog/kuiper-ransomware-detection-and-response/> (Accessed: 30 July 2024).

Wazuh and Okelola, A. (2024) *Detecting and responding to Phobos ransomware using Wazuh, Wazuh*. Available at: <https://wazuh.com/blog/detecting-and-responding-to-phobos-ransomware-using-wazuh/> (Accessed: 12 August 2024).