A comprehensive approach to Detecting and Monitoring of Threats

Name: Mihir Shukla

IT IMS & Cyber Security

Semester: 6

Index

Introduction

In today's interconnected digital landscape, the need for robust threat detection and monitoring mechanisms has never been greater. Effective threat detection and monitoring are critical components of any robust cybersecurity strategy, enabling organizations to identify, assess, and mitigate potential risks proactively.

This project aims to introduce a comprehensive approach to identifying and overseeing potential threats in various digital environments. Leveraging open-source tools, we propose a multifaceted strategy that integrates advanced detection algorithms, real-time monitoring systems, and proactive threat intelligence analysis.

Security Information and Event Management: Wazuh

- SIEM, which stands for Security Information and Event Management, is a comprehensive approach to security management that integrates the capabilities of Security Information Management (SIM) and Security Event Management (SEM) into a unified platform.

- Wazuh is an open-source security monitoring platform that provides comprehensive threat detection, incident response, and compliance management capabilities. It is designed to enhance the security posture of organizations by offering real-time visibility into security events and threats across their IT infrastructure.

Virus Total

- Virus Total is an online service that analyzes files and URLs to detect malicious content and potential security threats.

- We highlight the following ones relevant to our purpose:

  - ✓ Virus Total stores all the analyses it performs, allowing users to search for file hashes. By sending the hash to the Virus Total engine, you can know if Virus Total has already scanned that specific file, and you can analyze its report.

  - ✓ Virus Total also provides an API that allows access to the information generated by Virus Total without needing to utilize the HTML website interface. This API is subject to its Terms of Service, which we briefly discuss in the following section.

Shuffle

- Shuffle is a general-purpose security automation platform. It is a cutting-edge software solution designed to streamline and optimize business processes through automation.

- Shuffle Automation emerges as a pivotal tool to fortify defenses, streamline operations, and mitigate threats effectively. By integrating Shuffle Automation into cybersecurity workflows, organizations can automate routine security tasks, enhance threat detection and response capabilities, and improve overall security posture.

The Hive

- The Hive is a robust security incident response platform that plays a pivotal role in orchestrating and optimizing cybersecurity operations. At its core, The Hive serves as a centralized hub for managing security incidents, offering functionalities such as incident creation, tracking, and assignment.

- The Hive enhances organizational governance, strengthens risk management practices, and ensures compliance with regulatory requirements and industry standards.

MISP (Malware Information Sharing Platform and Threat Sharing

- MISP (Malware Information Sharing Platform & Threat Sharing) stands as a pivotal tool in the cybersecurity landscape, facilitating collaboration and intelligence sharing among organizations. Designed to streamline threat intelligence sharing, MISP enables organizations to aggregate, share, and analyze cybersecurity threats in real-time.

- MISP facilitates the aggregation, sharing, and analysis of IOCs from various sources, enabling organizations to enhance their threat intelligence capabilities. This automation is greatly beneficial to our SOC team as they do not have to manually search alerts and MISP for Ios.

Literature Review

Paper / Article	Description
Comparative analysis of IBM Qradar and Wazuh for security information and event management. Research Paper by: Dario Suskalo, Zlatan Moric, Jasmin Redzepagic and Damir Regvart [December 2023]	The aim was to evaluate their performance in addressing security challenges, especially after updates or in community-driven environments. QRadar excels in comprehensive security features and scalability, suitable for large enterprises, while Wazuh provides a cost-effective open-source option, recommended for smaller companies with limited budgets.
Intrusion Detection using Open Source Tools Research Paper by: Jack TIMOFTE [January – 2008]	In this paper, they have discussed the benefits and challenges of open-source intrusion detection systems (IDS) like OS-SEC, Prelude, and Snort, and explore their relationship with commercial support. They examines how organizations, both large and small, can effectively leverage open-source and commercial IDS solutions to enhance their network security posture.

Literature Review

Paper / Article	Description
A Review of Wazuh Capabilities for Detecting Attacks Based on Log Analysis Research Paper by: Stefan Stanković, Slavko Gajin, and Ranko Petrović [June -2022]	The aim of the paper is to demonstrate Wazuh's effectiveness in detecting various attack. The paper suggests integrating Wazuh with Suricata, a Network Intrusion Detection System capable of generating JSON logs, for enhanced security insights.
Analysis of attacks and prevention methods in cybersecurity Research Paper by: Prof. Francesco Gringoli [October, 2022]	The thesis aims to evaluate Wazuh's effectiveness as an open-source tool for IT infrastructure protection, with a focus on threat detection, vulnerability management, and prevention.

Literature Review

Paper / Article	Description
Information And Security Event Management System Research Paper by: Information And Security Event Management System	This Paper focuses on proposing, analyzing, and evaluating cybersecurity solutions based on the Elastic Stack (ELK), which is widely used as an enterprise-grade logging suite and search engine. It discusses the importance of efficient log analysis, the impact of GDPR compliance within the ELK environment, and the role of Elasticsearch as a search engine.
A Survey on Network Security Monitoring: Tools and Functionalities Research Paper by: Z. S. Younus, M. Alanezi	This paper explores the growing prevalence of cybersecurity breaches and their impact on network infrastructure. It highlights various protective measures such as antivirus software, firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) are employed to secure network devices.

Research Gap

- Small startup companies often face financial constraints, limiting their access to commercial cybersecurity solutions. This creates a significant gap in providing affordable and effective security measures tailored to their needs.

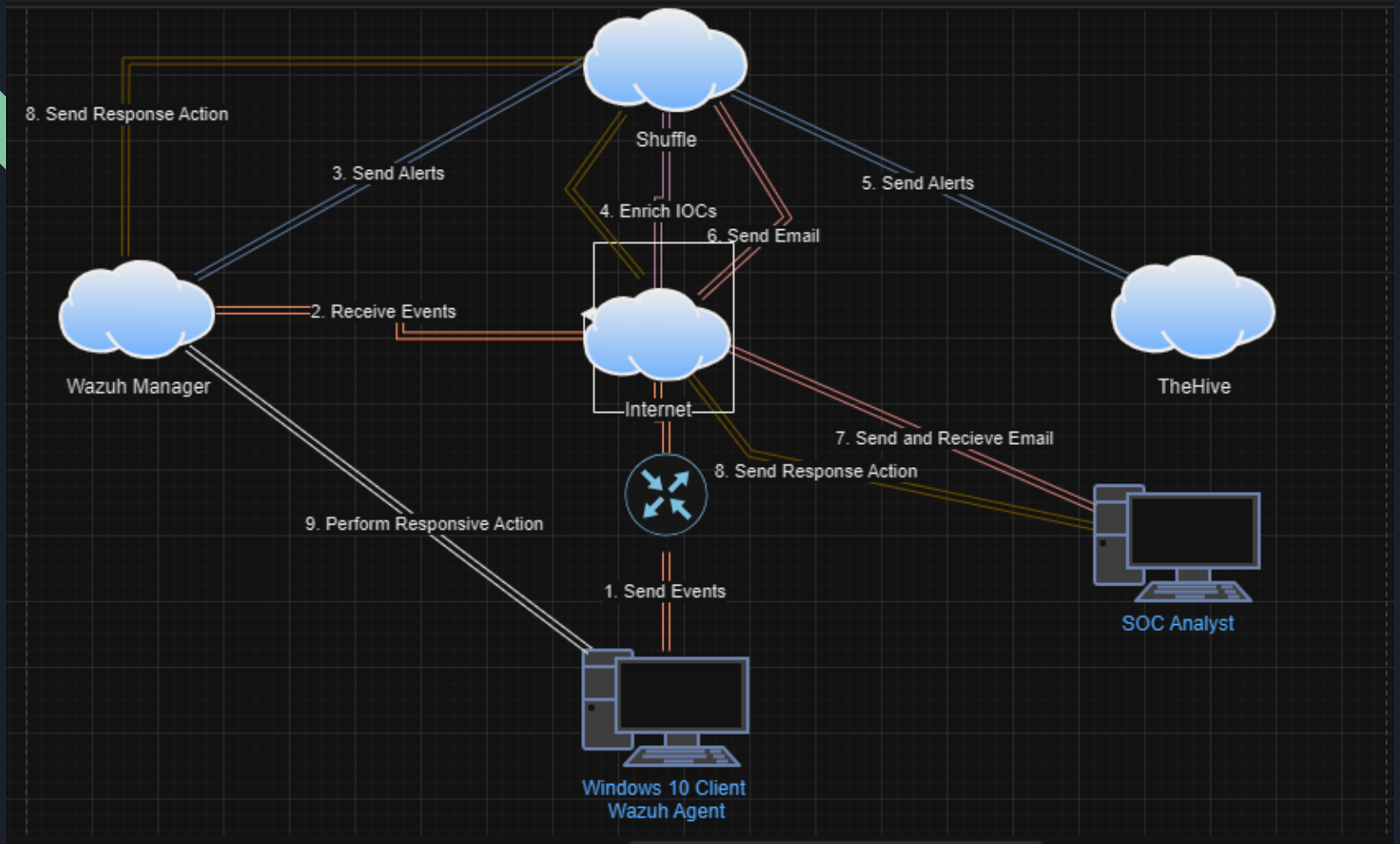
- To address this challenge, our research focuses on leveraging various automation techniques and integrating open-source tools to develop a comprehensive cybersecurity solution specifically designed for small businesses. By combining these technologies, we aim to offer a cost-effective alternative to traditional cybersecurity approaches, empowering startups to enhance their security posture without incurring significant expenses.

Objective

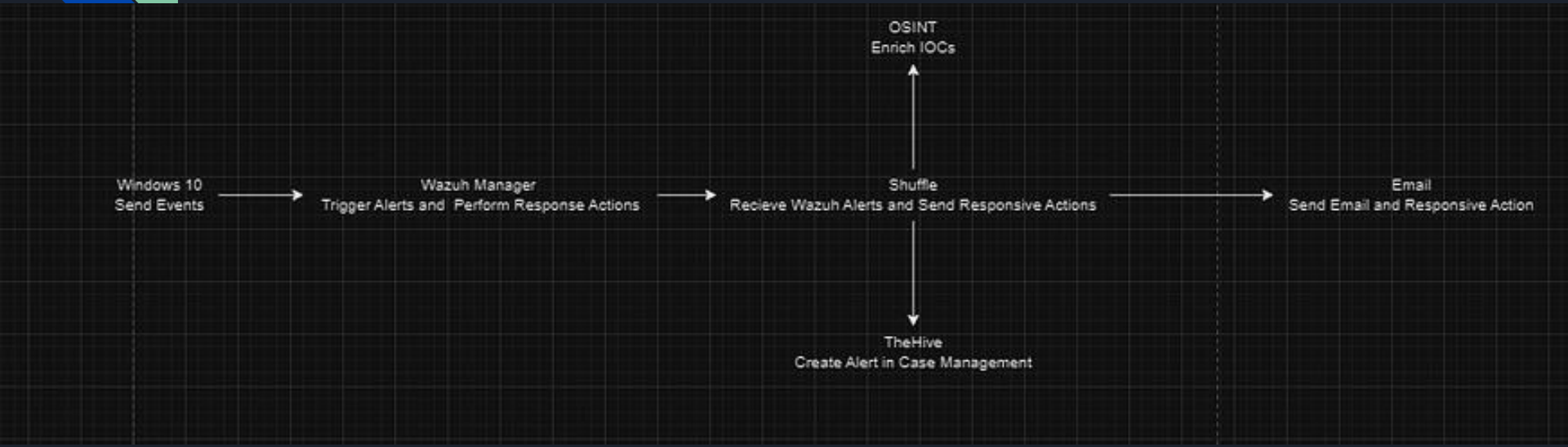
The objective of our research is to:

- Enhance IT security using open-source technologies, prioritizing Linux and Windows environments.
- Develop robust mechanisms for detecting and monitoring USB devices to prevent unauthorized data transfers.
- Implement solutions for SSH detection and blocking to prevent unauthorized access attempts and strengthen network security.
- Strengthen malware detection capabilities to identify and mitigate potential threats, safeguarding systems and data integrity.
- Conduct comprehensive vulnerability scanning to identify security weaknesses and prioritize remediation efforts.
- Establish File Integrity Monitoring (FIM) systems to detect unauthorized changes to critical system files, ensuring system integrity.
- Deploy Intrusion Detection Systems (IDS) to monitor network traffic and detect suspicious activities or potential security breaches.

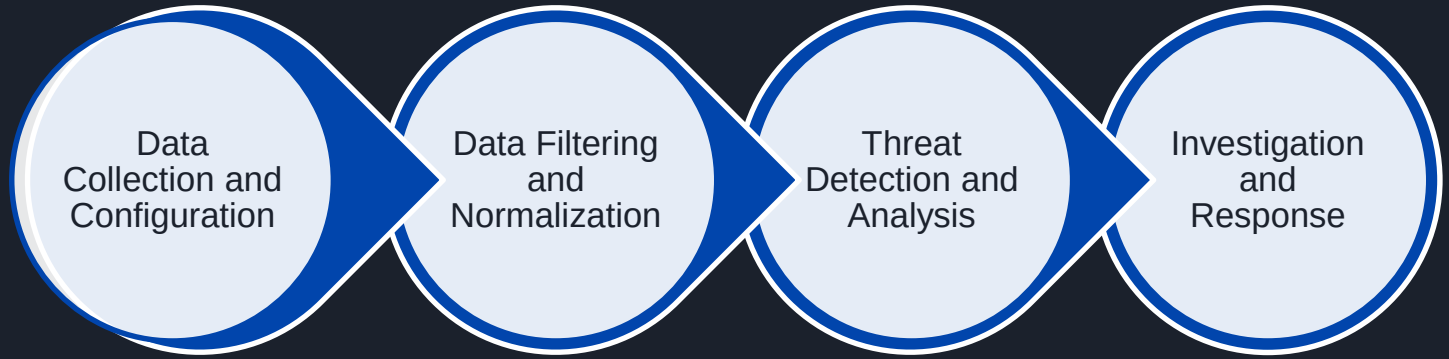
Flow Chart


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

Flow chart (Text Base)



Methodology

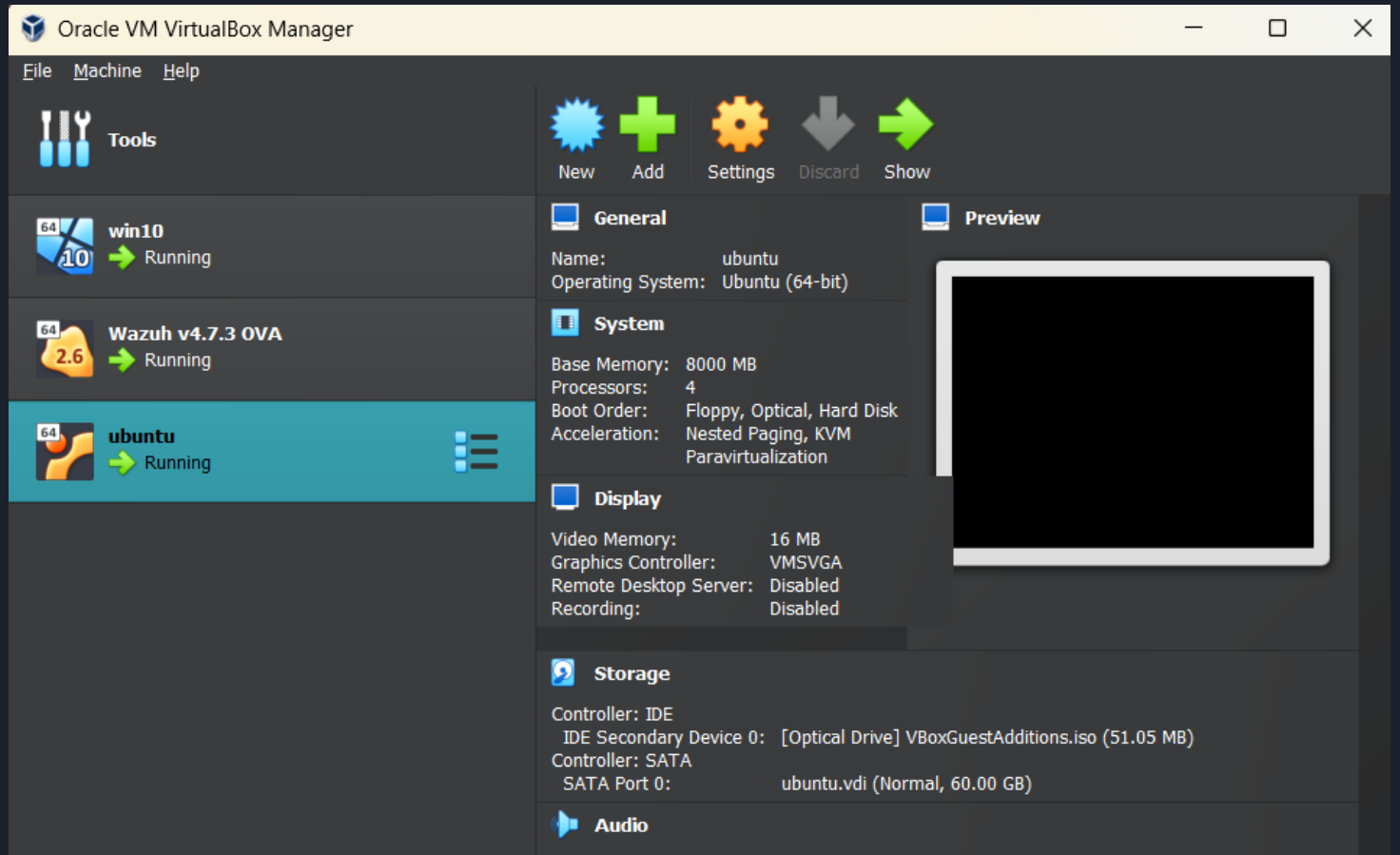


Implementation(Uses Case)

- The implementation of the SIEM tool Wazuh on both Windows and Linux platforms enables the demonstration of various use cases aimed at illustrating the enhancement of security measures and the centralization of SIEM detection and mitigation processes. Through this deployment, we showcase the efficacy of Wazuh in addressing security concerns across heterogeneous environments, empowering organizations to streamline threat detection, response, and remediation efforts effectively.

1. **Cross-Platform Integration**: Wazuh seamlessly integrates with both Windows and Linux environments, enabling organizations to establish a unified security monitoring infrastructure across heterogeneous IT landscapes.
2. **Use Case Demonstration**: By leveraging Wazuh's capabilities on both platforms, organizations can effectively demonstrate various security use cases, showcasing the tool's efficacy in detecting and mitigating threats in real-time.
3. **Centralized Security Management**: Wazuh facilitates centralized SIEM detection and mitigation, allowing for streamlined management and analysis of security events and incidents, thereby enhancing overall security posture and response capabilities.

Installation (Environment Setup)



1. File integrity

1. **Essential Security Layer**: File Integrity Monitoring (FIM) is a critical security process that safeguards system and application files, forming an integral defense layer for organizations protecting sensitive assets.
2. **Continuous Monitoring**: Wazuh's FIM module constantly monitors files and directories, promptly alerting administrators when changes like creation, modification, or deletion occur, ensuring the ongoing integrity of critical files.
3. **Baseline Comparison**: By establishing a baseline scan and storing cryptographic checksums and file attributes, Wazuh compares any alterations against this baseline, promptly flagging any discrepancies for immediate attention.
4. **Enhanced Security Posture**: The FIM capability not only aids in detecting unauthorized changes but also strengthens threat detection and response capabilities, reducing the risk of data theft or compromise.
5. **Compliance and Cost Savings**: Wazuh's FIM not only helps organizations meet regulatory compliance requirements but also saves time and money by mitigating the potential impact of security incidents, such as lost productivity, revenue, reputation damage, and legal penalties.

Wazuh - Wazuh

https://192.168.253.147/app/wazuh#/overview/?tab=fim&agentId=001&_g=(filters:!(),refreshInterval:(pause:!t,v 70%

wazuh. Modules Ubuntu Integrity monitoring

Inventory Dashboard Events

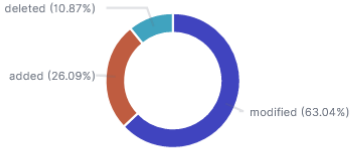
Ubuntu (001) Generate report

Search DQL Last 24 hours Show dates Refresh

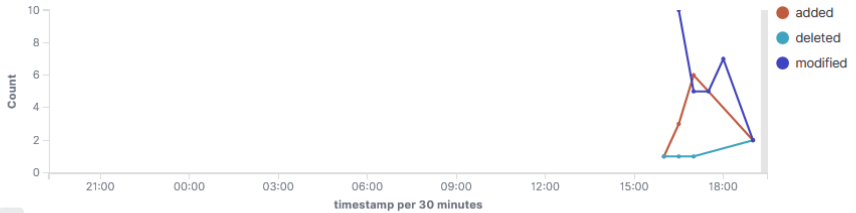
manager.name: wazuh-server rule.groups: syscheck agent.id: 001 + Add filter

Most active users

Actions



Events



Files added

Files modified

Files deleted

34°C Partly cloudy

ENG IN 19:16 31-03-2024

Wazuh - Wazuh

https://192.168.253.147/app/wazuh#/overview/?tab=fim&agentId=001&_g=(filters:!(),refreshInterval:(pause:!t,v

70%

wazuh.

Modules | Ubuntu | Integrity monitoring

Search

DQL

Last 24 hours

Show dates

Refresh

manager.name: wazuh-server | rule.groups: syscheck | agent.id: 001 | + Add filter

wazuh-alerts-*

Search field names

Filter by type 0

Selected fields

- rule.description
- rule.id
- rule.level
- syscheck.event
- syscheck.path

Available fields

- agent.id
- agent.ip
- agent.name
- decoder.name
- full_log
- id
- input.type
- location
- manager.name
- rule.firedtimes
- rule.gdpr
- rule.gpg13
- rule.groups
- rule.hipaa
- rule.mail

46 hits

Mar 30, 2024 @ 19:16:56.571 - Mar 31, 2024 @ 19:16:56.571 Auto

Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Mar 31, 2024 @ 19:09:37.001	/home/disha/Downloads/58c48e2b1d3d26ac96cebf8c114750582d4cdeef46a05bbf706c4b4630c541ff.exe	deleted	File deleted.	7	553
Mar 31, 2024 @ 19:09:32.252	/home/disha/Downloads/58c48e2b1d3d26ac96cebf8c114750582d4cdeef46a05bbf706c4b4630c541ff.exe	modified	File modified in /home/disha/Downloads directory.	7	100200
Mar 31, 2024 @ 19:09:32.209	/home/disha/Downloads/58c48e2b1d3d26ac96cebf8c114750582d4cdeef46a05bbf706c4b4630c541ff.exe	added	File added to /home/disha/Downloads directory.	7	100201
Mar 31, 2024 @ 19:09:14.217	/home/disha/Downloads/58c48e2b1d3d26ac96cebf8c114750582d4cdeef46a05bbf706c4b4630c541ff.exe	deleted	File deleted.	7	553
Mar 31, 2024 @ 19:09:09.125	/home/disha/Downloads/58c48e2b1d3d26ac96cebf8c114750582d4cdeef46a05bbf706c4b4630c541ff.exe	modified	File modified in /home/disha/Downloads directory.	7	100200
Mar 31, 2024 @ 19:09:09.084	/home/disha/Downloads/58c48e2b1d3d26ac96cebf8c114750582d4cdeef46a05bbf706c4b4630c541ff.exe	added	File added to /home/disha/Downloads directory.	7	100201
Mar 31, 2024 @ 18:09:35.107	/root/.lesshst	modified	Integrity checksum changed.	7	550
Mar 31, 2024 @ 18:03:23.157	/root/.viminfo	modified	Integrity checksum changed.	7	550

34°C Partly cloudy

ENG IN

19:17 31-03-2024

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

  <!-- File integrity monitoring -->
  <syscheck>
        <directories realtime="yes" check_all="yes" check_sum="yes" check_owner="yes" check_attrs="yes" check_mtime="yes" check-
inode="yes" report_change="yes" whodata="yes">/home/disha/Downloads</directories>
        <directories realtime="yes" check_all="yes" check_sum="yes" check_owner="yes" check_attrs="yes" check_mtime="yes" check-
inode="yes" report_change="yes" whodata="yes">/home/disha/Documents</directories>
        <nodiff>/home/disha/Documents/private.txt</nodiff>
  </syscheck>



  <syscheck>


    <disabled>no</disabled>
    <directories realtime="yes">/root</directories>
    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>43200</frequency>

    <scan_on_start>yes</scan_on_start>

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

2. Malware Detection and Prevention

- Wazuh uses the integrator module to connect to external APIs and alerting tools such as Virus Total.
- In this use case, you use the Wazuh File Integrity Monitoring (FIM) module to monitor a directory for changes and the Virus Total API to scan the files in the directory. Then, configure Wazuh to trigger an active response script and remove files that Virus Total detects as malicious. We test this use case on Ubuntu and Windows endpoints.
- You need a Virus Total API key in this use case to authenticate Wazuh to the Virus Total API.

Codeing

```
481
482 <ossec_config>
483   <integration>
484     <name>virustotal</name>
485     <api_key>d9a756b3a18225aa04ae33b9537ccd42cee75f3c92f34f9d0b402704d4ab530e</api_key> <!-- Replace with your VirusTotal API key -->
486     <rule_id>100200,100201</rule_id>
487     <alert_format>json</alert_format>
488   </integration>
489 </ossec_config>
490
491 <ossec_config>
492   <command>
493     <name>remove-threat</name>
494     <executable>remove-threat.sh</executable>
495     <timeout_allowed>no</timeout_allowed>
496   </command>
497
498   <active-response>
499     <disabled>no</disabled>
500     <command>remove-threat</command>
501     <location>local</location>
502     <rules_id>87105</rules_id>
503   </active-response>
504 </ossec_config>
505
```

local_rules.xml

```
<group name="syscheck,pci_dss_11.5,nist_800_53_SI.7,">
    <!-- Rules for Linux systems -->
    <rule id="100200" level="7">
        <if_sid>550</if_sid>
    <field name="file">/home/ubuntu/Downloads</field>
        <description>File modified in /home/ubuntu/Downloads directory.</description>
    </rule>
    <rule id="100201" level="7">
        <if_sid>554</if_sid>
        <field name="file">/home/ubuntu/Downloads</field>
        <description>File added to /home/ubuntu/Downloads directory.</description>
    </rule>
</group>
<group name="virustotal,">
  <rule id="100092" 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="100093" 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>
```

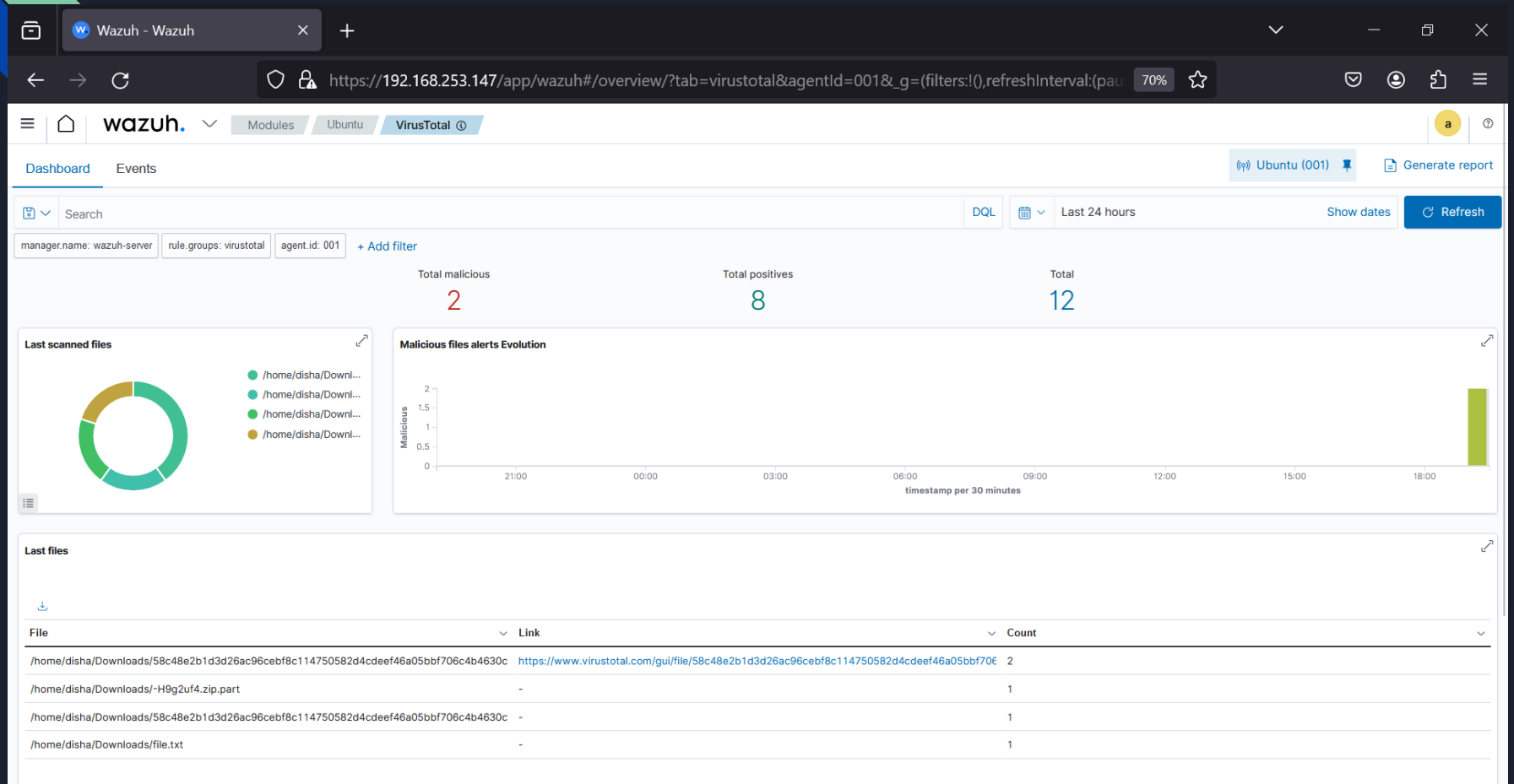
Open

*remove-threat.sh
/var/ossec/active-response/bin

```
SS#!/bin/bash

LOCAL=`dirname $0`;
cd $LOCAL
cd ../

PWD=`pwd`

read INPUT_JSON
FILENAME=$(echo $INPUT_JSON | jq -r .parameters.alert.data.virustotal.source.file)
COMMAND=$(echo $INPUT_JSON | jq -r .command)
LOG_FILE="${PWD}/../logs/active-responses.log"

#------------------------ Analyze command -------------------------#
if [ ${COMMAND} = "add" ]
then
 # Send control message to execd
 printf '{"version":1,"origin":{"name":"remove-threat","module":"active-response"},"command":"check_keys", "parameters":{"keys":[]}}\n'

 read RESPONSE
 COMMAND2=$(echo $RESPONSE | jq -r .command)
 if [ ${COMMAND2} != "continue" ]
 then
  echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Remove threat active response aborted" >> ${LOG_FILE}
  exit 0;
 fi
fi

# Removing file
rm -f $FILENAME
if [ $? -eq 0 ]; then
 echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Successfully removed threat" >> ${LOG_FILE}
else
 echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Error removing threat" >> ${LOG_FILE}
fi

exit 0;
```

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

  <!-- File integrity monitoring -->
  <syscheck>
        <directories realtime="yes" check_all="yes" check_sum="yes" check_owner="yes" check_attrs="yes" check_mtime="yes" check-
inode="yes" report_change="yes" whodata="yes">/home/disha/Downloads</directories>
        <directories realtime="yes" check_all="yes" check_sum="yes" check_owner="yes" check_attrs="yes" check_mtime="yes" check-
inode="yes" report_change="yes" whodata="yes">/home/disha/Documents</directories>
        <nodiff>/home/disha/Documents/private.txt</nodiff>
  </syscheck>



  <syscheck>


    <disabled>no</disabled>
    <directories realtime="yes">/root</directories>
    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>43200</frequency>

    <scan_on_start>yes</scan_on_start>

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

Dashboard


Wazuh - Wazuh
https://192.168.253.147/app/wazuh#/overview/?tab=virustotal&agentId=001&_g=(filters:!(),refreshInterval:(pau
70%
wazuh.
Modules
Ubuntu
VirusTotal
Dashboard
Events
Ubuntu (001)
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
rule.groups: virustotal
agent.id: 001
+ Add filter
Total malicious
2
Total positives
8
Total
12
Last scanned files
/home/disha/Downl...
/home/disha/Downl...
/home/disha/Downl...
/home/disha/Downl...
Malicious files alerts Evolution
Malicious
2
1.5
1
0.5
0
21:00
00:00
03:00
06:00
09:00
12:00
15:00
18:00
timestamp per 30 minutes
Last files
File
Link
Count
/home/disha/Downloads/58c48e2b1d3d26ac96cebf8c114750582d4cdeef46a05bbf706c4b4630c
https://www.virustotal.com/gui/file/58c48e2b1d3d26ac96cebf8c114750582d4cdeef46a05bbf706
2
/home/disha/Downloads/-H9g2uf4.zip.part
-
1
/home/disha/Downloads/58c48e2b1d3d26ac96cebf8c114750582d4cdeef46a05bbf706c4b4630c
-
1
/home/disha/Downloads/file.txt
-
1

Wazuh - Wazuh | VirusTotal - File - 58c48e2b1d3c

https://www.virustotal.com/gui/file/58c48e2b1d3d26ac96cebf8c114750582d4cdeef46a05bbf706c4b4630c541ff/detecti

58c48e2b1d3d26ac96cebf8c114750582d4cdeef46a05bbf706c4b4630c541ff

Sign in | Sign up

25 / 72

Community Score

25/72 security vendors and 2 sandboxes flagged this file as malicious

Reanalyze | Similar | More

58c48e2b1d3d26ac96cebf8c114750582d4cdeef46a05bbf706c4b4630c541ff

CMSTP.EXE

Size 234.63 KB

Last Modification Date 42 minutes ago

EXE

peexe | signed | checks-user-input | calls-wmi | persistence | overlay | long-sleeps | assembly | detect-debug-environment | invalid-signature | spreader | checks-cpu-name

DETECTION | DETAILS | RELATIONS | BEHAVIOR | TELEMETRY | COMMUNITY 7

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.msil/risepro | Threat categories trojan | Family labels msil | risepro | pwsx

Security vendors' analysis

Do you want to automate checks?

Alibaba	Trojan:MSIL/GenKryptik.9d4e0a62	Avast	Win32:PWSX-gen [Trj]
AVG	Win32:PWSX-gen [Trj]	BitDefenderTheta	Gen:NN.ZemsilCO.36802.om2@aul9wKhi

34°C Partly cloudy

ENG IN

19:12 31-03-2024

Access level	⚠ **Limited**, standard free public API Upgrade to premium
Usage	**Must not be used in business workflows, commercial products or services.**
Request rate	4 lookups / min
Daily quota	500 lookups / day
Monthly quota	15.5 K lookups / month

Want to learn more about how VirusTotal can supercharge your security operations? check our 360 overview brief.

Want to upgrade your access? Please do not hesitate to contact us, we'll go the extra mile to make you successful.

API reference

Python client

Golang library

Command-line interface

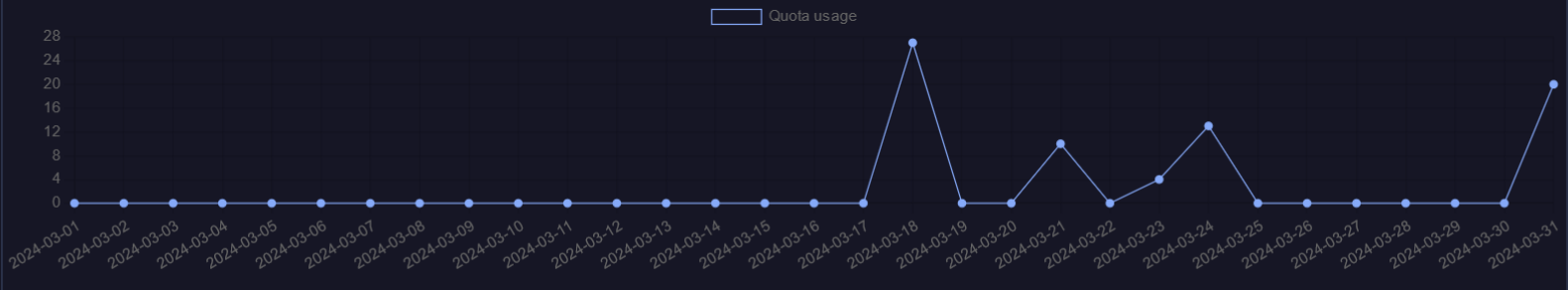
Go premium

Use in browser

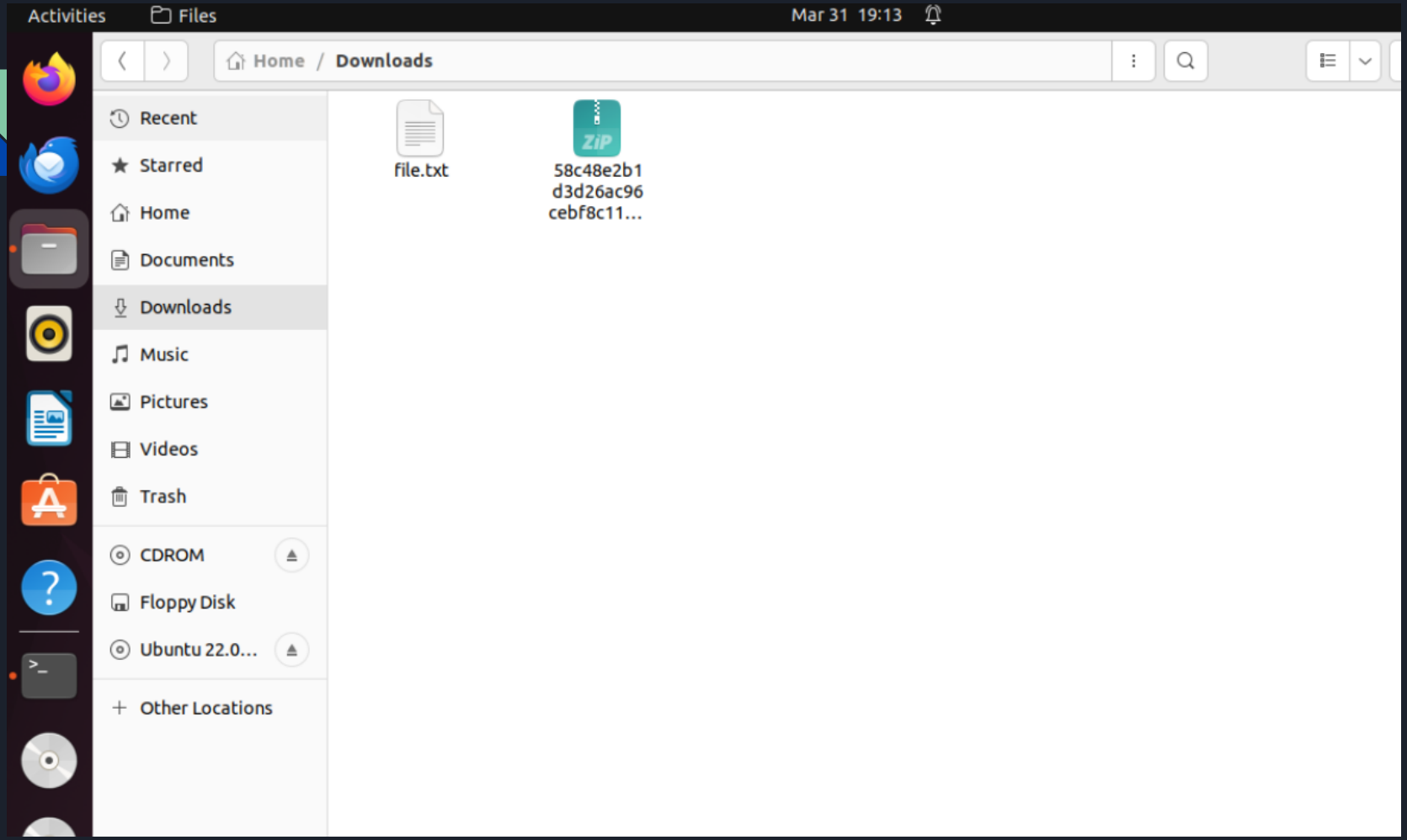
Discover feeds

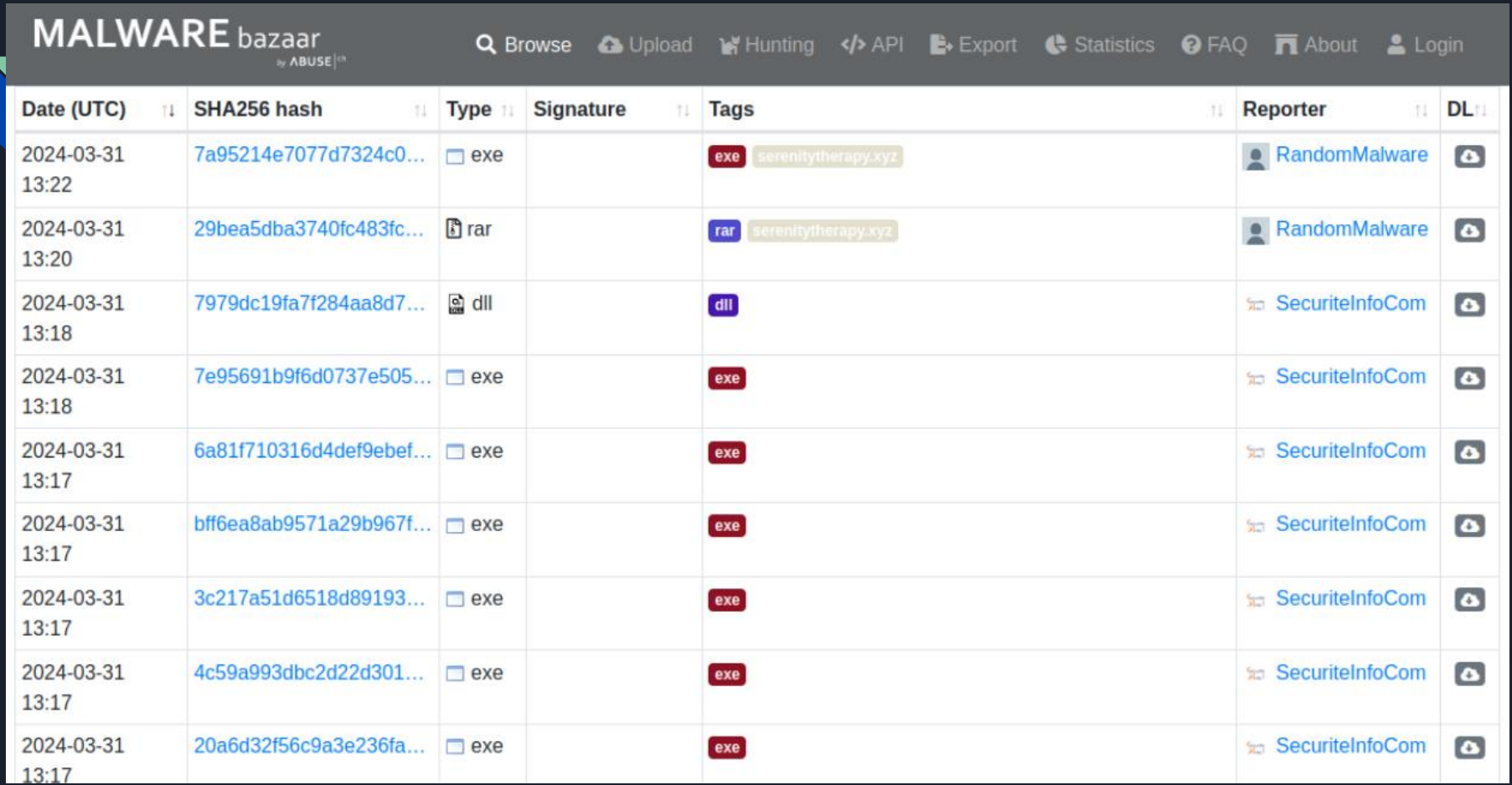
Other services

Consumption last 30 days



PROTIP: You can programmatically retrieve quota details making use of the APIv3 groups endpoint, "quotas" is the property you should be looking at.


Activities
Files
Mar 31 19:13
Home / Downloads
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
CDROM
Floppy Disk
Ubuntu 22.0...
Other Locations
file.txt
58c48e2b1
d3d26ac96
cebf8c11...



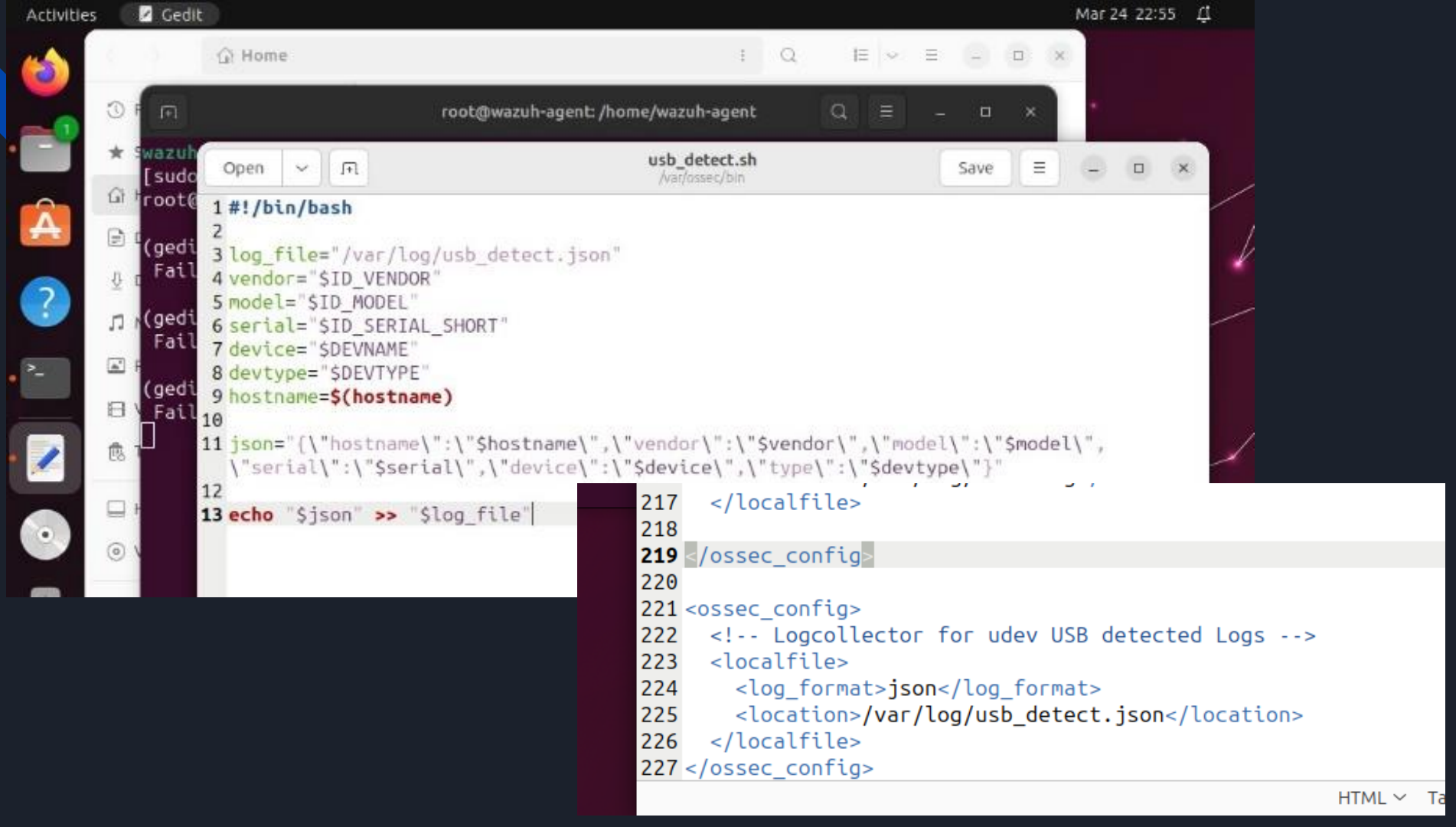
Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2024-03-31 13:22	7a95214e7077d7324c0...	exe		exe serenitytherapy.xyz	RandomMalware	
2024-03-31 13:20	29bea5dba3740fc483fc...	rar		rar serenitytherapy.xyz	RandomMalware	
2024-03-31 13:18	7979dc19fa7f284aa8d7...	dll		dll	SecuriteInfoCom	
2024-03-31 13:18	7e95691b9f6d0737e505...	exe		exe	SecuriteInfoCom	
2024-03-31 13:17	6a81f710316d4def9ebef...	exe		exe	SecuriteInfoCom	
2024-03-31 13:17	bff6ea8ab9571a29b967f...	exe		exe	SecuriteInfoCom	
2024-03-31 13:17	3c217a51d6518d89193...	exe		exe	SecuriteInfoCom	
2024-03-31 13:17	4c59a993dbc2d22d301...	exe		exe	SecuriteInfoCom	
2024-03-31 13:17	20a6d32f56c9a3e236fa...	exe		exe	SecuriteInfoCom	

3. USB detection

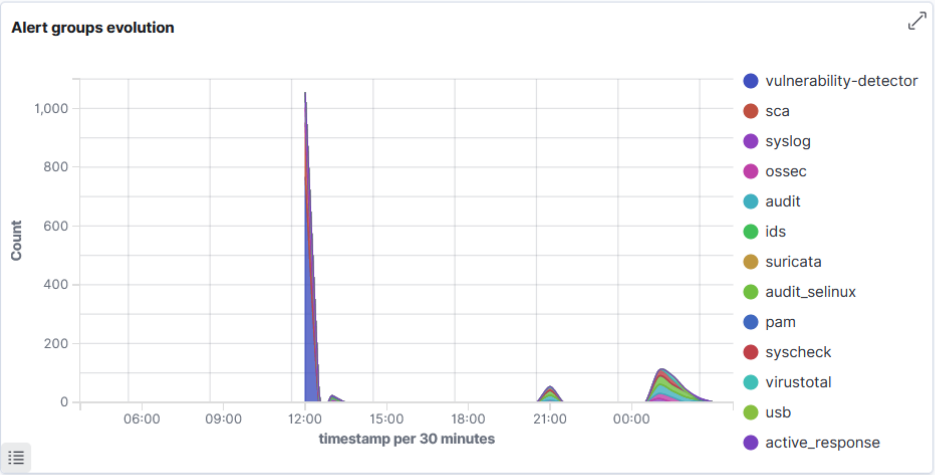
1. **Security Importance**: Monitoring USB drives on Linux endpoints is crucial for system security as they pose potential entry points for malware and unauthorized data access, making it imperative to detect and prevent such threats.
2. **Threat Prevention**: By actively monitoring USB drives, administrators can proactively detect and block the introduction of malicious software or unauthorized data transfers, thereby reducing the risk of system compromise.
3. **Compliance and Data Protection**: USB drive monitoring ensures compliance with security policies and regulations, safeguarding sensitive data and mitigating the risk of data breaches, thus maintaining organizational integrity.
4. **Proactive Security Measure**: Monitoring USB drives is a proactive security measure that enhances overall system security by identifying and mitigating potential threats posed by external storage devices before they can cause harm.
5. **Enhanced Logging with udev Rules**: While Wazuh offers basic USB device monitoring, utilizing udev rules enhances logging capabilities, providing richer information about USB events, which is essential for comprehensive threat detection and response.

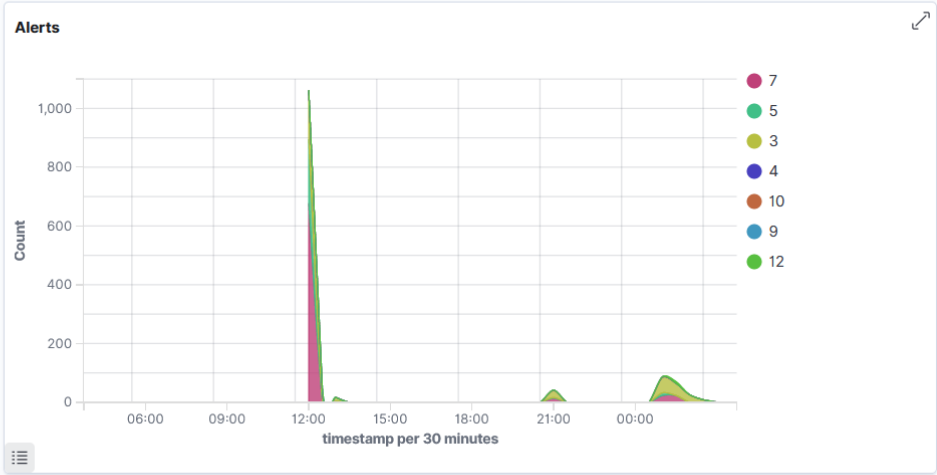
```
374
375     <!-- User-defined ruleset -->
376     <decoder_dir>etc/decoders</decoder_dir>
377     <rule_dir>etc/rules</rule_dir>
378     <list>etc/lists/usb-drives</list>
379   </ruleset>
```

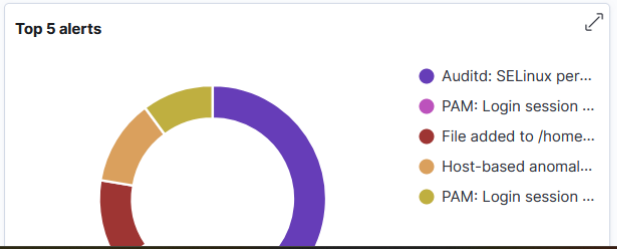
```
47
48  <!-- Rule for USB monitoring in Linux-->
49  <group name="Linux, usb,">
50    <rule id="111010" level="7">
51      <field name="serial">\w+</field>
52      <field name="type">usb_device</field>
53      <description>A PNP device $(vendor) $(model) was connected to $(hostname).</description>
54    </rule>
55
56    <rule id="111011" level="8">
57      <if_sid>111010</if_sid>
58      <list field="serial" lookup="not_match_key">etc/lists/usb-drives</list>
59    <description>Unauthorized PNP device $(vendor) $(model) was connected to $(hostname).</description>
60    </rule>
61  </group>
```

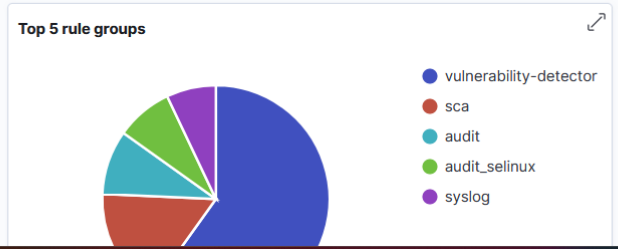

Activities
Gedit
Mar 24 22:55
Home
root@wazuh-agent: /home/wazuh-agent
Open
usb_detect.sh
/var/ossec/bin
Save
#!/bin/bash
log_file="/var/log/usb_detect.json"
vendor="$ID_VENDOR"
model="$ID_MODEL"
serial="$ID_SERIAL_SHORT"
device="$DEVNAME"
devtype="$DEVTYPE"
hostname=$(hostname)
json="{\"hostname\":\"$hostname\",\"vendor\":\"$vendor\",\"model\":\"$model\",
\"serial\":\"$serial\",\"device\":\"$device\",\"type\":\"$devtype\"}"
echo "$json" >> "$log_file"
</localfile>
</ossec_config>
<ossec_config>
<!-- Logcollector for udev USB detected Logs -->
<localfile>
<log_format>json</log_format>
<location>/var/log/usb_detect.json</location>
</localfile>
</ossec_config>
HTML

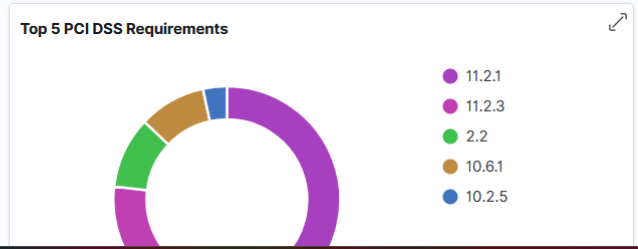
Total	Level 12 or above alerts	Authentication failure	Authentication success
1368	8	9	22





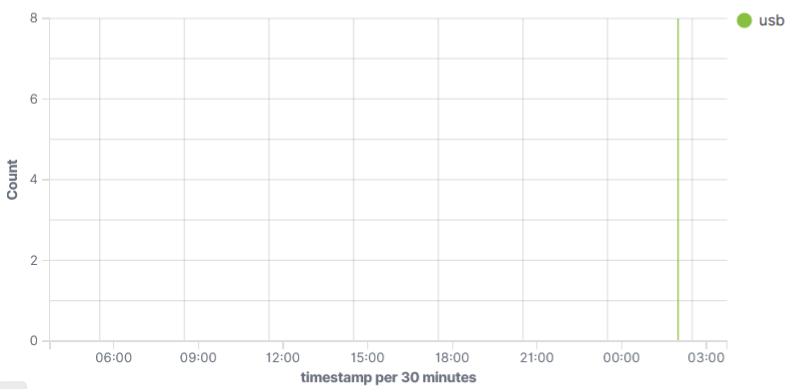




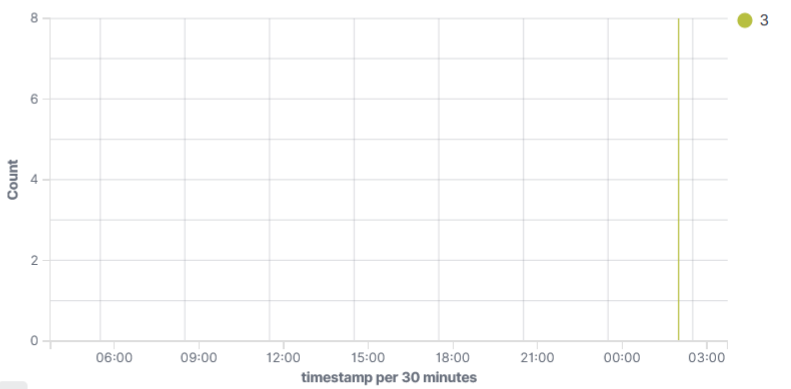


8 0 0 0

Alert groups evolution

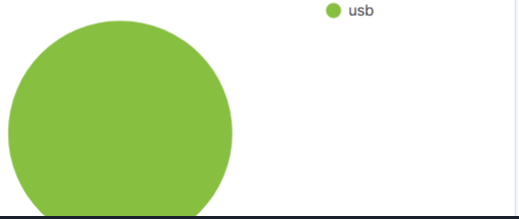


Alerts



Top 5 alerts

Top 5 rule groups



Top 5 PCI DSS Requirements

No results found

Security Alerts

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
Apr 1, 2024 @ 02:23:35.354			USB device disconnected	3	81102
Apr 1, 2024 @ 02:23:35.350			USB device disconnected	3	81102
Apr 1, 2024 @ 02:23:34.818			USB device disconnected	3	81102
Apr 1, 2024 @ 02:23:34.694			USB device disconnected	3	81102
Apr 1, 2024 @ 02:16:57.685			Attached USB Storage	3	81101
Apr 1, 2024 @ 02:16:57.656			Attached USB Storage	3	81101
Apr 1, 2024 @ 02:03:18.471			Attached USB Storage	3	81101
Apr 1, 2024 @ 02:03:18.441			Attached USB Storage	3	81101

Rows per page: 10

@timestamp	2024-03-31T20:53:35.354Z
_id	SFRKIo4BkCEaZL6kGOa0
agent.id	003
agent.ip	192.168.175.65
agent.name	linux
data.id	usb
decoder.name	kernel
decoder.parent	kernel
full_log	Apr 1 02:23:34 ubuntu kernel: [4859.397214] usb 2-2: USB disconnect, device number 3
id	1711918415.3254084
input.type	log
location	/var/log/kern.log
manager.name	wazuh-server
predecoder.hostname	ubuntu
predecoder.program_name	kernel
predecoder.timestamp	Apr 1 02:23:34
rule.description	USB device disconnected
rule.firedtimes	4

4. Vulnerability Scan

1. **Enable Vulnerability Detector Module**: The first step involves enabling the Vulnerability Detector module on the Wazuh server, as it is disabled by default upon installation.
2. **Check Agent Configuration**: Ensure that the Wazuh agent's Syscollector is enabled by default, which is necessary for collecting system information required for vulnerability scanning.
3. **Configuration Setup**: Configure the settings for the vulnerability scan, including specifying which assets or endpoints to scan and setting scan parameters such as frequency and depth.
4. **Customize Scan Parameters**: Tailor the vulnerability scan parameters to meet specific organizational needs, considering factors such as network size, criticality of assets, and compliance requirements.
5. **Execute Vulnerability Scans**: Once configured, initiate vulnerability scans using Wazuh to proactively identify and address security weaknesses across the network, enhancing overall security posture.

wazuh. Modules linux Vulnerabilities

Inventory Events

linux (003)

SEVERITY

- Critical (2)
- High (2)
- Medium (550)
- Low (218)

DETAILS

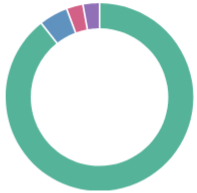
Critical	High	Medium	Low
2	2	550	218

Last full scan
Apr 1, 2024 @ 02:40:43.000

Last partial scan
Apr 1, 2024 @ 03:20:53.000

SUMMARY

Name



- libmozjs-91-0 (252)
- fonts-opensymbol (14)
- bsdutils (8)
- gir1.2-javascriptcoregtk-4.0 (8)

Vulnerabilities (772)

Refresh Export formatted

Search WQL

Name	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time
amd64-microcode	3.20191218.1ubuntu2.2	amd64	Medium	CVE-2021-26318	0	0	Mar 31, 2024 @ 12:04:41.000
apparmor	3.0.4-2ubuntu2.3	amd64	Critical	CVE-2016-1585	7.5	9.8	Mar 31, 2024 @ 12:04:34.000
apport	2.20.11-0ubuntu82.5	all	Low	CVE-2022-28653	0	0	Mar 31, 2024 @ 12:04:42.000
apport-gtk	2.20.11-0ubuntu82.5	all	Low	CVE-2022-28653	0	0	Mar 31, 2024 @ 12:04:42.000
bluez	5.64-0ubuntu1.1	amd64	Low	CVE-2022-24695	0	0	Mar 31, 2024 @ 12:04:31.000
bluez	5.64-0ubuntu1.1	amd64	Low	CVE-2020-9770	0	0	Mar 31, 2024 @ 12:04:43.000

Vulnerabilities (772)

Refresh | Export formatted

Search | WQL

Name	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time
amd64-microcode	3.20191218.1ubuntu2.2	amd64	Medium	CVE-2021-26318	0	0	Mar 31, 2024 @ 12:04:41.000
apparmor	3.0.4-2ubuntu2.3	amd64	Critical	CVE-2016-1585	7.5	9.8	Mar 31, 2024 @ 12:04:34.000
apport	2.20.11-0ubuntu82.5	all	Low	CVE-2022-28653	0	0	Mar 31, 2024 @ 12:04:42.000
apport-gtk	2.20.11-0ubuntu82.5	all	Low	CVE-2022-28653	0	0	Mar 31, 2024 @ 12:04:42.000
bluez	5.64-0ubuntu1.1	amd64	Low	CVE-2022-24695	0	0	Mar 31, 2024 @ 12:04:31.000
bluez	5.64-0ubuntu1.1	amd64	Low	CVE-2020-9770	0	0	Mar 31, 2024 @ 12:04:43.000
bluez	5.64-0ubuntu1.1	amd64	Medium	CVE-2020-10134	0	0	Mar 31, 2024 @ 12:04:44.000
bluez	5.64-0ubuntu1.1	amd64	Low	CVE-2022-3563	0	0	Mar 31, 2024 @ 12:04:48.000
bluez-cups	5.64-0ubuntu1.1	amd64	Low	CVE-2022-24695	0	0	Mar 31, 2024 @ 12:04:31.000
bluez-cups	5.64-0ubuntu1.1	amd64	Low	CVE-2020-9770	0	0	Mar 31, 2024 @ 12:04:43.000

Rows per page: 10

< 1 2 3 4 5 ... 78 >

CVE-2016-1585

Details

Title
CVE-2016-1585 affects apparmor

Name
apparmor

CVE
CVE-2016-1585

Version
3.0.4-2ubuntu2.3

Architecture
amd64

Condition
Package unfixed

Last full scan
Apr 1, 2024 @ 02:40:43.000

Last partial scan
Apr 1, 2024 @ 03:20:53.000

Published
Apr 22, 2019 @ 00:00:00.000

Updated
Nov 7, 2023 @ 00:00:00.000

References
View external references

Recent events

1 hit

Search DQL Last 24 hours Show dates Refresh

+ Add filter

Time ↓	Description	Level	Rule ID	Status
Mar 31, 2024 @ 12:04:34.302	CVE-2016-1585 affects apparmor	13	23506	Active

Manager configuration

Edit **ossec.conf** of **Manager**

```
130     <!-- RedHat OS vulnerabilities -->
131     <provider name="redhat">
132       <enabled>yes</enabled>
133       <os>5</os>
134       <os>6</os>
135       <os>7</os>
136       <os>8</os>
137       <os>9</os>
138       <update_interval>1h</update_interval>
139     </provider>
140
141     <!-- Amazon Linux OS vulnerabilities -->
142     <provider name="alas">
143       <enabled>yes</enabled>
144       <os>amazon-linux</os>
145       <os>amazon-linux-2</os>
146       <os>amazon-linux-2022</os>
147       <os>amazon-linux-2023</os>
148       <update_interval>1h</update_interval>
149     </provider>
150
151     <!-- SUSE OS vulnerabilities -->
152     <provider name="suse">
153       <enabled>yes</enabled>
154       <os>11-server</os>
155       <os>11-desktop</os>
156       <os>12-server</os>
```

Manager configuration

Edit **ossec.conf** of **Manager**

```
104  <vulnerability-detector>
105    <enabled>yes</enabled>
106    <interval>5m</interval>
107    <min_full_scan_interval>1h</min_full_scan_interval>
108    <run_on_start>yes</run_on_start>
109
110    <!-- Ubuntu OS vulnerabilities -->
111    <provider name="canonical">
112      <enabled>yes</enabled>
113      <os>trusty</os>
114      <os>xenial</os>
115      <os>bionic</os>
116      <os>focal</os>
117      <os>jammy</os>
118      <update_interval>1h</update_interval>
119    </provider>
120
121    <!-- Debian OS vulnerabilities -->
122    <provider name="debian">
123      <enabled>yes</enabled>
124      <os>buster</os>
125      <os>bullseye</os>
126      <os>bookworm</os>
127      <update_interval>1h</update_interval>
128    </provider>
129
```

5. SSH Detection and blocking

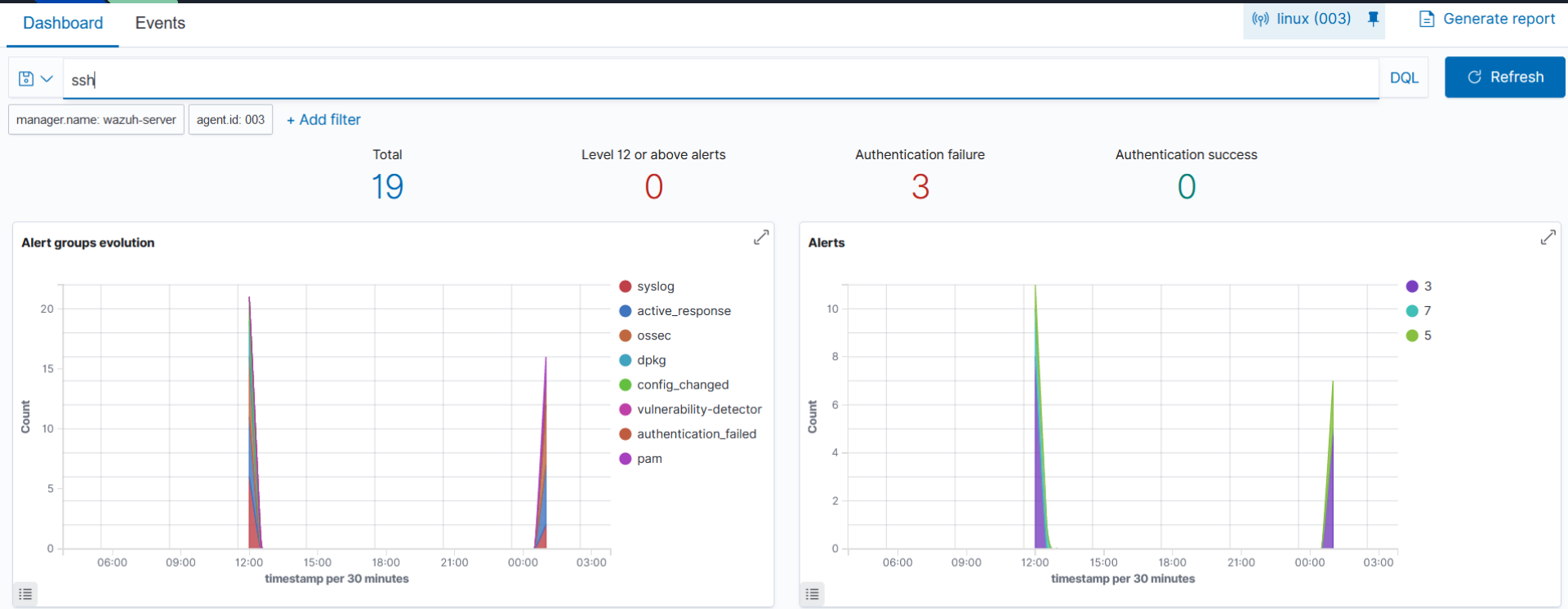
1. **Active Response Module**: Wazuh employs its active response module to execute scripts or executables on monitored endpoints, enabling automated actions in response to specific triggers.
2. **Use Case Objective**: The objective is to thwart SSH brute-force attacks on a Red Hat Enterprise Linux (RHEL) endpoint by configuring the active response module to block the IP address of the attacker.
3. **Simulation of Brute-Force Attack**: A simulated SSH brute-force attack is initiated against the RHEL endpoint to simulate unauthorized attempts to gain access to the system.
4. **Triggering Response Action**: When rule 5763, indicating an SSHD brute force attempt, is triggered, the active response module executes a predefined script to block the IP address associated with the attacker, effectively preventing further unauthorized access attempts.
5. **Prevention of Brute-Force Attacks**: By leveraging the active response module in this manner, Wazuh enhances security posture by automatically responding to detected threats, mitigating the risk of successful SSH brute-force attacks on the monitored endpoint.

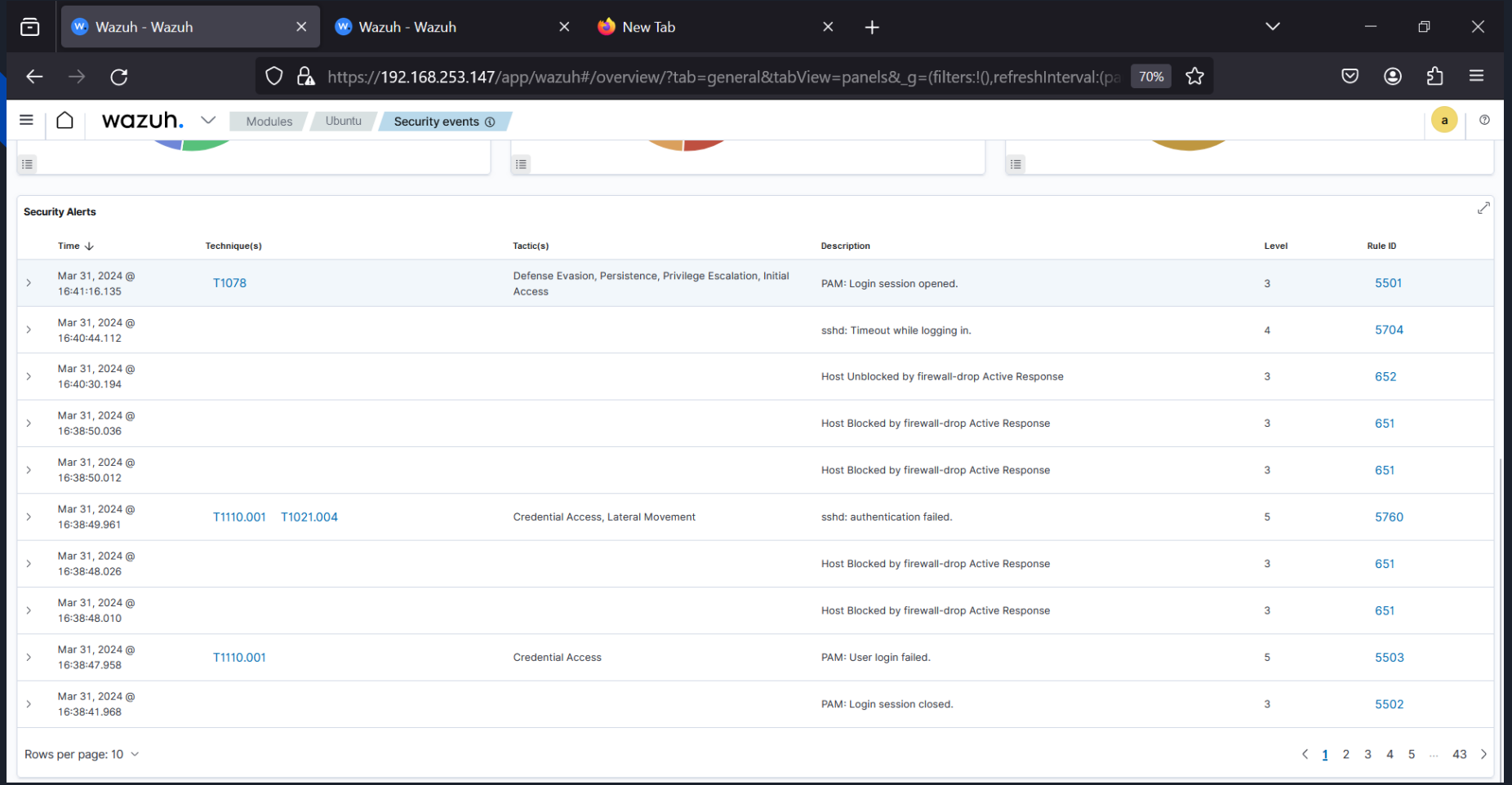
Detection

```
C:\Users\pdish>ssh disha@192.168.253.136
ssh: connect to host 192.168.253.136 port 22: Connection refused

C:\Users\pdish>ssh disha@192.168.253.136
The authenticity of host '192.168.253.136 (192.168.253.136)' can't be established.
ED25519 key fingerprint is SHA256:Efwaa2GTN698tSp/OUUhpLtWuLWEuok9t+v6kyBl8Dc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.253.136' (ED25519) to the list of known hosts.
disha@192.168.253.136's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 6.5.0-26-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

223 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable

*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

disha@disha-virtual-machine:~$ exit
```

```
296
297 <active-response>
298   <command>firewall-drop</command>
299   <location>local</location>
300   <agent_id>002</agent_id>
301   <rules_id>5710,5762,5760,5503</rules_id
302   <timeout>100</timeout>
303 </active-response>
304
```

Dashboards


Dashboard
Events
linux (003)
Generate report
ssh
DQL
Refresh
manager.name: wazuh-server
agent.id: 003
+ Add filter
Total
19
Level 12 or above alerts
0
Authentication failure
3
Authentication success
0
Alert groups evolution
Count
timestamp per 30 minutes
syslog
active_response
ossec
dpkg
config_changed
vulnerability-detector
authentication_failed
pam
Alerts
3
7
5

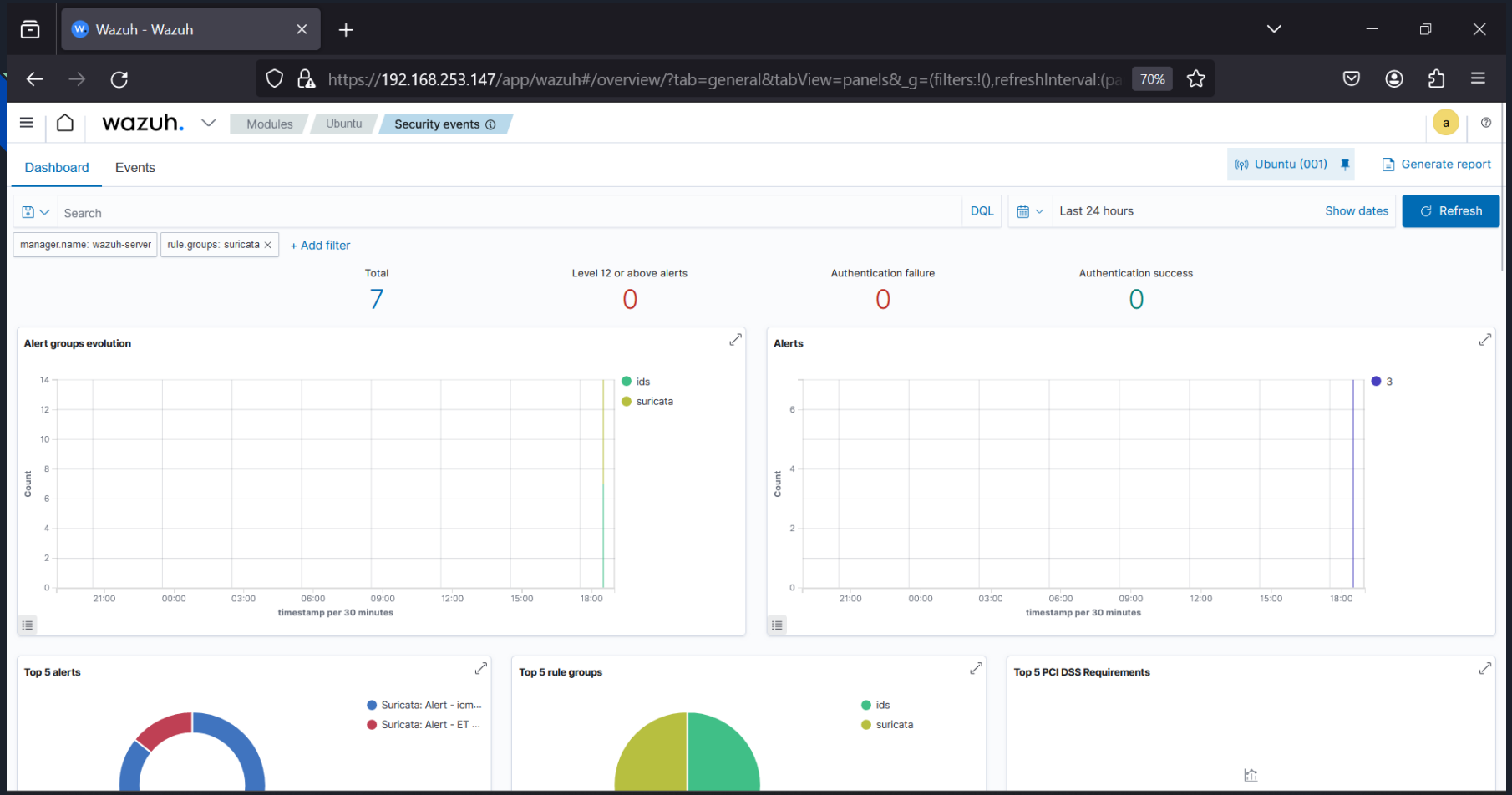

Wazuh - Wazuh
Wazuh - Wazuh
New Tab
https://192.168.253.147/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInterval:(pa
70%
wazuh.
Modules
Ubuntu
Security events
a
Security Alerts
Time
Technique(s)
Tactic(s)
Description
Level
Rule ID
Mar 31, 2024 @ 16:41:16.135
T1078
Defense Evasion, Persistence, Privilege Escalation, Initial Access
PAM: Login session opened.
3
5501
Mar 31, 2024 @ 16:40:44.112
sshd: Timeout while logging in.
4
5704
Mar 31, 2024 @ 16:40:30.194
Host Unblocked by firewall-drop Active Response
3
652
Mar 31, 2024 @ 16:38:50.036
Host Blocked by firewall-drop Active Response
3
651
Mar 31, 2024 @ 16:38:50.012
Host Blocked by firewall-drop Active Response
3
651
Mar 31, 2024 @ 16:38:49.961
T1110.001
T1021.004
Credential Access, Lateral Movement
sshd: authentication failed.
5
5760
Mar 31, 2024 @ 16:38:48.026
Host Blocked by firewall-drop Active Response
3
651
Mar 31, 2024 @ 16:38:48.010
Host Blocked by firewall-drop Active Response
3
651
Mar 31, 2024 @ 16:38:47.958
T1110.001
Credential Access
PAM: User login failed.
5
5503
Mar 31, 2024 @ 16:38:41.968
PAM: Login session closed.
3
5502
Rows per page: 10
1
2
3
4
5
43

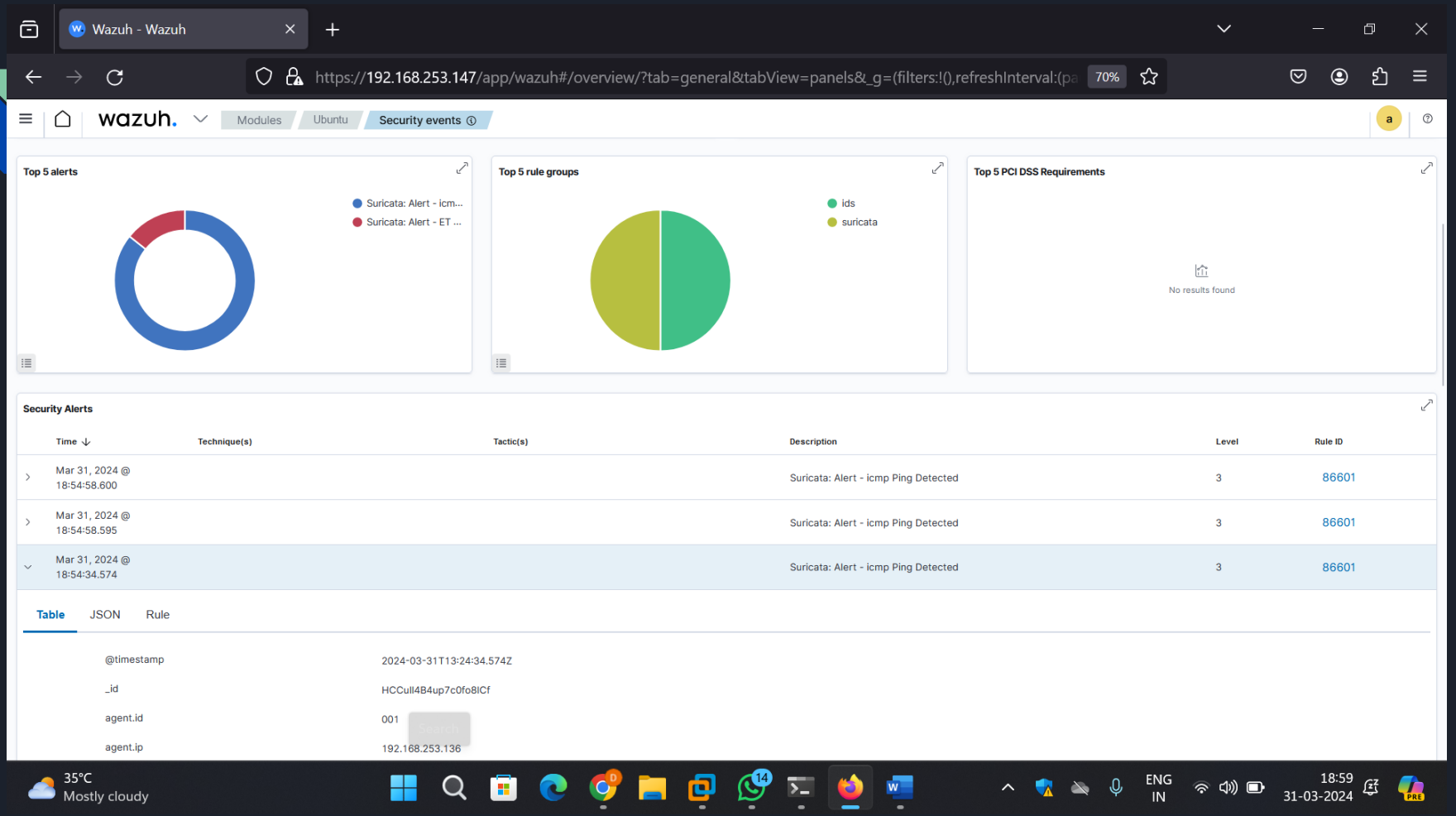
Mitigation

```
disha@disha-virtual-machine:~$ exit
logout
Connection to 192.168.253.136 closed.

C:\Users\pdish>ssh disha@192.168.253.136
disha@192.168.253.136's password:
Permission denied, please try again.
disha@192.168.253.136's password:
ssh_dispatch_run_fatal: Connection to 192.168.253.136 port 22: Connection timed out

C:\Users\pdish>
C:\Users\pdish>
C:\Users\pdish>ssh disha@192.168.253.136
ssh: connect to host 192.168.253.136 port 22: Connection timed out

C:\Users\pdish>
```

6. IDS Detection (Network Detection)

1. **Complex Network Landscape**: The proliferation of diverse devices in networks presents challenges in detecting and responding to threats in real-time due to the sheer volume and variety of nodes.
2. **Evolution of Security Technology**: To streamline threat response efforts, Extended Detection and Response (XDR) solutions have emerged, leveraging automation to analyze data from monitored endpoints and swiftly respond to suspicious activities.
3. **Suricata Intrusion Detection System**: Suricata, an advanced intrusion detection system, is capable of scrutinizing network events and triggering alerts upon detecting potentially malicious behavior, offering a proactive defense against network threats.
4. **Integration with Wazuh**: By integrating Suricata with the Wazuh active response module, administrators can augment the XDR capabilities of Wazuh. This integration enables automated responses to specific events detected by Suricata on monitored endpoints, enhancing overall threat mitigation efforts.
5. **Endpoint Protection Against Network Attacks**: This blog post delves into the practical implementation of leveraging Suricata and the Wazuh active response module to fortify endpoint security against network-based threats, providing a comprehensive defense strategy for modern network environments.


Wazuh - Wazuh
https://192.168.253.147/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInterval:(pa
70%
wazuh.
Modules
Ubuntu
Security events
Dashboard
Events
Ubuntu (001)
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh-server
rule.groups: suricata
+ Add filter
Total
7
Level 12 or above alerts
0
Authentication failure
0
Authentication success
0
Alert groups evolution
ids
suricata
Count
timestamp per 30 minutes
Alerts
3
Top 5 alerts
Suricata: Alert - icm...
Suricata: Alert - ET ...
Top 5 rule groups
ids
suricata
Top 5 PCI DSS Requirements
35°C
Mostly cloudy
ENG
IN
18:58
31-03-2024


Wazuh - Wazuh
https://192.168.253.147/app/wazuh#/overview/?tab=general&tabView=panels&_g=(filters:!(),refreshInterval:(pa
70%
wazuh.
Modules
Ubuntu
Security events
Top 5 alerts
Suricata: Alert - icm...
Suricata: Alert - ET ...
Top 5 rule groups
ids
suricata
Top 5 PCI DSS Requirements
No results found
Security Alerts
Time
Technique(s)
Tactic(s)
Description
Level
Rule ID
Mar 31, 2024 @ 18:54:58.600
Suricata: Alert - icmp Ping Detected
3
86601
Mar 31, 2024 @ 18:54:58.595
Suricata: Alert - icmp Ping Detected
3
86601
Mar 31, 2024 @ 18:54:34.574
Suricata: Alert - icmp Ping Detected
3
86601
Table
JSON
Rule
@timestamp
2024-03-31T13:24:34.574Z
_id
HCCuII4B4up7c0fo8ICf
agent.id
001
agent.ip
192.168.253.136
35°C
Mostly cloudy
ENG
IN
18:59
31-03-2024

agent.id	001
agent.ip	192.168.253.136
agent.name	Ubuntu
data.alert.action	allowed
data.alert.gid	1
data.alert.rev	1
data.alert.severity	3
data.alert.signature	icmp Ping Detected
data.alert.signature_id	1
data.community_id	1:E5Og7v75tk3Fj94mOwtE8bMHkEI=
data.dest_ip	192.168.253.1
data.dest_port	0
data.direction	to_client
data.event_type	alert
data.flow.bytes_toclient	74
data.flow.bytes_toserver	74
data.flow.dest_ip	192.168.253.136
data.flow.pkts_toclient	1
data.flow.pkts_toserver	1
data.flow.src_ip	192.168.253.1
data.flow.start	2024-03-31T18:54:34.485743+0530

```
root@disha-virtual-machine:/var/ossec/etc# sudo tail -f /var/log/suricata/eve.json | jq 'select(.event_type=="alert")'
{
  "timestamp": "2024-03-31T18:48:58.584582+0530",
  "flow_id": 821912653187721,
  "in_iface": "ens33",
  "event_type": "alert",
  "src_ip": "192.168.253.1",
  "src_port": 0,
  "dest_ip": "192.168.253.136",
  "dest_port": 0,
  "proto": "ICMP",
  "icmp_type": 8,
  "icmp_code": 0,
  "pkt_src": "wire/pcap",
  "community_id": "1:E5Og7v75tk3Fj94mOwtE8bMHkEI=",
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 1,
    "rev": 1,
    "signature": "icmp Ping Detected",
    "category": "",
    "severity": 3
  },
  "direction": "to_server",
  "flow": {
    "pkts_toserver": 1,
    "pkts_toclient": 0,
    "bytes_toserver": 74,
    "bytes_toclient": 0,
    "start": "2024-03-31T18:48:58.584582+0530",
```

Open

*suricata.yaml
/etc/suricata

```
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.4.
suricata-version: "7.0"

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.175.0/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DC_SERVERS: "$HOME_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
    ENIP_SERVER: "$HOME_NET"

  port-groups:
    HTTP_PORTS: "80"
    SHELLCODE_PORTS: "!80"
    ORACLE_PORTS: 1521
    SSH_PORTS: 22
    DNP3_PORTS: 20000
    MODBUS_PORTS: 502
```

Open *suricata.yaml /etc/suricata Save

```
2127    #   (e.g. ports: [all])
2128    #
2129    # This parameter has no effect if auto-config is disabled.
2130    #
2131    ports: [0-1,2-3]
2132
2133    # When auto-config is enabled the hashmode specifies the algorithm for
2134    # determining to which stream a given packet is to be delivered.
2135    # This can be any valid Napatech NTPL hashmode command.
2136    #
2137    # The most common hashmode commands are:  hash2tuple, hash2tuplesorted,
2138    # hash5tuple, hash5tuplesorted and roundrobin.
2139    #
2140    # See Napatech NTPL documentation other hashmodes and details on their use.
2141    #
2142    # This parameter has no effect if auto-config is disabled.
2143    #
2144    hashmode: hash5tuplesorted
2145
2146 ##
2147 ## Configure Suricata to load Suricata-Update managed rules.
2148 ##
2149
2150 default-rule-path: /var/lib/suricata/rules
2151
2152 rule-files:
2153   - suricata.rules
2154   - local.rules
2155 ##
2156 ## Auxiliary configuration files.
2157 ##
2158
2159 classification-file: /etc/suricata/classification.config
2160 reference-config-file: /etc/suricata/reference.config
2161 # threshold-file: /etc/suricata/threshold.config
2162
2163 ##
2164 ## Include other configs
2165 ##
2166
2167 # Includes:  Files included here will be handled as if they were in-lined
2168 # in this configuration file. Files with relative pathnames will be
2169 # searched for in the same directory as this configuration file. You may
2170 # use absolute pathnames too.
2171 #include:
2172 #  - include1.yaml
2173 #  - include2.yaml
```

YAML Tab Width: 8 Ln 2154, Col 16 INS

Open ossec.conf /var/ossec/etc Save

```
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/auth.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/syslog</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/dpkg.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/kern.log</location>
  </localfile>

  <localfile>
  <log_format>audit</log_format>
  <location>/var/log/audit/audit.log</location>
  </localfile>

<!-- Logcollector for udev suricata detected Logs -->
  <localfile>
  <log_format>syslog</log_format>
  <location>/var/log/suricata/eve.json</location>
  </localfile>


</ossec_config>

  <!-- Logcollector for udev USB detected Logs -->

<ossec_config>
  <localfile>
    <log_format>json</log_format>
    <location>/var/log/usb_detect.json</location>
  </localfile>
</ossec_config>
```

HTML Tab Width: 8 Ln 1, Col 1 INS

```
root@disha-virtual-machine:/# cd /var/log/suricata/
root@disha-virtual-machine:/var/log/suricata# ls
certs  core  eve.json  fast.log  files  stats.log  suricata.log  suricata-start.log
root@disha-virtual-machine:/var/log/suricata# cat fast.log
03/31/2024-18:06:03.074838  [**] [1:1:1] icmp Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.253.1:8 -> 19
2.168.253.136:0
03/31/2024-18:06:03.074941  [**] [1:1:1] icmp Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.253.136:0 ->
192.168.253.1:0
03/31/2024-18:46:49.014279  [**] [1:2013505:4] ET POLICY GNU/Linux YUM User-Agent Outbound likely related to package management [**]
 [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 192.168.253.147:48708 -> 108.157.238.120:80
03/31/2024-18:48:58.584582  [**] [1:1:1] icmp Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.253.1:8 -> 19
2.168.253.136:0
03/31/2024-18:48:58.584652  [**] [1:1:1] icmp Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.253.136:0 ->
192.168.253.1:0
03/31/2024-18:54:34.485743  [**] [1:1:1] icmp Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.253.1:8 -> 19
2.168.253.136:0
03/31/2024-18:54:34.485899  [**] [1:1:1] icmp Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.253.136:0 ->
192.168.253.1:0
03/31/2024-18:54:57.897559  [**] [1:1:1] icmp Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.253.147:8 ->
192.168.253.136:0
03/31/2024-18:54:57.897675  [**] [1:1:1] icmp Ping Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.253.136:0 ->
192.168.253.147:0
root@disha-virtual-machine:/var/log/suricata#
```