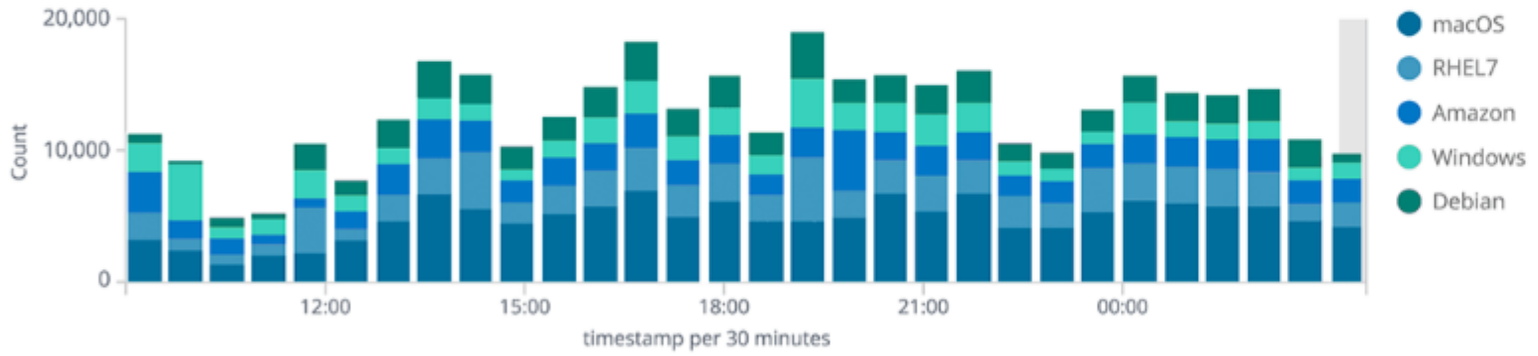
Search KQL Last 24 hours Show dates Refresh

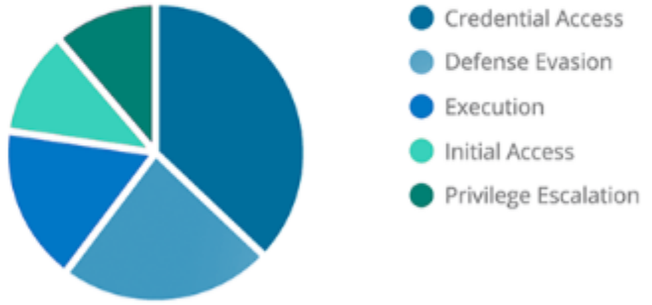
cluster.name: wazuh + Add filter

Total	Level 12 or above alerts	Authentication failure	Authentication success
226415	49	39232	51

Alerts evolution - Top 5 agents



Top Mitre ATT&K tactics



Security alerts

Time	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
> Aug 11, 2020 @ 10:13:49.493	Windows	T1218	Defense Evasion, Execution	Signed Script Proxy Execution: C:\Windows\System32\svchost.exe	10	255563
> Aug 10, 2020 @ 05:28:52.926	Amazon	T1110	Credential Access	sshd: Attempt to login using a non-existent user	5	5710

info@wazuh.com
https://wazuh.com

Agent 001 configuration

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	Kalilinux	192.168.29.131	Wazuh v4.8.0	kali	Kali GNU/Linux 2024.1	Jul 16, 2024 @ 12:01:05.000	Jul 17, 2024 @ 01:48:41.000

Group: default

Main configurations

Global configuration

Logging settings that apply to the agent

Write internal logs in plain text	yes
Write internal logs in JSON format	no

Communication

Settings related to the connection with the manager

Configuration profiles	kali, kali2024, kali2024.1
Time (in seconds) between agent checkings to the manager	10
Time (in seconds) before attempting to reconnect	60
force_reconnect_interval	-
ip_update_interval	-
Auto-restart the agent when receiving valid configuration from manager	yes
Remote configuration is enabled	yes
Method used to encrypt communications	aes

List of managers to connect

Address	Port	Max_retries	Retry_interval	Protocol
192.168.29.42	1514	5	10	tcp

enabled	yes
delay_after_enrollment	20
port	1515
agent_name	Kalilinux
ssl_cipher	HIGH:!ADH:!EXP:!MD5:!RC4:!3DES:!CAMELLIA:@STRENGTH
auto_method	no

Anti-flooding settings

Agent bucket parameters to avoid event flooding

Buffer disabled	no
Queue size	5000
Events per second	500

Agent labels

User-defined information about the agent included in alerts

Auditing and policy monitoring

Policy monitoring

Configuration to ensure compliance with security policies, standards and hardening guides

General

Policy monitoring service disabled	no
Base directory	-
Rootkit files database path	etc/shared/rootkit_files.txt
Rootkit trojans database path	etc/shared/rootkit_trojans.txt
Scan the entire system	no
Skip scan on CIFS/NFS mounts	yes
Frequency (in seconds) to run the scan	43200
Check /dev path	yes
Check files	yes
Check network interfaces	yes
Check processes IDs	yes
Check network ports	yes
Check anomalous system objects	yes
Check trojans	yes
Check UNIX audit	no

Security configuration assessment

Interval	43200
Security configuration assessment enabled	yes
Scan on start	yes
Skip scan on CIFS/NFS mounts	yes
Policies	/var/ossec/ruleset/sca/sca_unix_audit.yml

CIS-CAT

Configuration assessment using CIS scanner and SCAP checks

CIS-CAT integration disabled	yes
Scan on start	yes
Interval between scan executions	86400
Path to Java executable directory	wodles/java
Path to CIS-CAT executable directory	wodles/ciscat
ciscat_binary	CIS-CAT.sh
Timeout (in seconds) for scan executions	1800

System threats and incident response

Osquery

Expose an operating system as a high-performance relational database

Osquery integration disabled	yes
Auto-run the Osquery daemon	yes
Use defined labels as decorators	yes
Path to the Osquery results log file	/var/log/osquery/osqueryd.results.log
Path to the Osquery configuration file	/etc/osquery/osquery.conf

Inventory data

Gather relevant information about the operating system, hardware, networking and packages

Syscollector integration disabled	no
Scan on start	yes
Interval between system scans	3600
Scan network interfaces	yes
Scan operating system info	yes
Scan hardware info	yes
Scan installed packages	yes
Scan listening network ports	yes
Scan all network ports	no
Scan current processes	yes
sync_max_eps	10

Active response

Active threat addressing by immediate response

Active response disabled	no

Commands

Configuration options of the Command wodle

This module is not configured. Please take a look on how to configure it in commands configuration.

Log data analysis

Log collection

Log analysis from text files, Windows events or syslog outputs

Command

Logformat	Command	Alias	Ignore_binaries	Target	Frequency
command	df -P	df -P	no	agent	360

Full command

Logformat	Command	Alias	Ignore_binaries	Target	Frequency
full_command	netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:digit:]]\+\ \+[[:digit:]]\+\ \+ \(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 == \3 == \4 \5/' | sort -k 4 -g | sed 's/ == \(.*\) ==/:\1/' | sed 1,2d	netstat listening ports	no	agent	360
full_command	last -n 20	last -n 20	no	agent	360

File	Logformat	Ignore_binaries	Only-future-events	Target
/var/log/nginx/access.log	apache	no	yes	agent
/var/log/nginx/error.log	apache	no	yes	agent
/var/log/apache2/error.log	apache	no	yes	agent
/var/log/apache2/access.log	apache	no	yes	agent

Syslog

File	Logformat	Ignore_binaries	Only-future-events	Target
/var/ossec/logs/active-responses.log	syslog	no	yes	agent
/var/log/dpkg.log	syslog	no	yes	agent

Integrity monitoring

Identify changes in content, permissions, ownership, and attributes of files

General

Integrity monitoring disabled	no
Interval (in seconds) to run the integrity scan	43200
Skip scan on CIFS/NFS mounts	yes
skip_dev	yes
skip_sys	yes

skip_proc	yes
Scan on start	yes
max_files_per_second	-
No diff directories	/etc/ssl/private.key
Ignored files and directories	/etc/mtab /etc/hosts.deny /etc/mail/statistics /etc/random-seed /etc/random.seed /etc/adjtime /etc/httpd/logs /etc/utmpx /etc/wtmpx /etc/cups/certs /etc/dumpdates /etc/svc/volatile
ignore_sregex	.log$\|.swp$
allow_remote_prefilter_cmd	no
max_eps	50
process_priority	10
database	disk

Who data

Restart audit	yes
Startup healthcheck	yes

Disk quota

enabled	yes
limit	1048576

File size

enabled	yes
limit	51200

Synchronization

enabled	yes
queue_size	16384
interval	300
max_eps	10
response_timeout	30
max_interval	3600
thread_pool	1

File limit

enabled	yes
entries	100000

Monitored directories

RT: Real time | WD: Who-data | Per.: Permission | MT: Modification time | SL: Symbolic link | RL: Recursion level

-	RT	WD	Changes	MD5	SHA1	Per.	Size	Owner	Group	MT	Inode	SHA256	SL	RL
/bin	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	256
/boot	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	256
/etc	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	256
/root	yes	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	256
/sbin	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	256
/usr/bin	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	256
/usr/sbin	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	256

Wazuh Report:-

File Integrity Monitoring

info@wazuh.com
https://wazuh.com

Integrity monitoring report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	Linux_Server	192.168.44.149	Wazuh v4.7.5	kali	Kali GNU/Linux 2024.1	Jun 4, 2024 @ 12:54:04.000	Jun 8, 2024 @ 06:30:16.000

Group: default

Alerts related to file changes, including permissions, content, ownership and attributes.

2024-06-07T06:30:15 to 2024-06-08T06:30:15

manager.name: kali AND rule.groups: syscheck AND agent.id: 002

Last file integrity monitoring scan was executed from 2024-06-08T10:06:27+00:00 to 2024-06-08T10:06:38+00:00.

Last 10 deleted files

Path	Date
/root/smit.txt	2024-06-08T10:08:33.946Z

Last 10 modified files

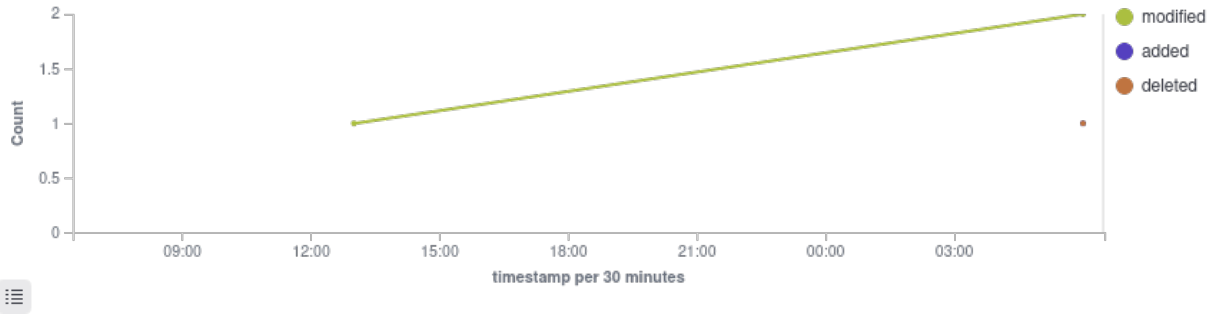
Path	Date
/root/smit.txt	2024-06-08T10:08:26.321Z
/root/.zsh_history	2024-06-08T10:03:31.955Z

Files added

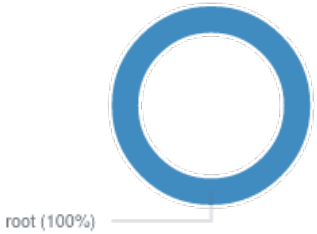
Files deleted

Files modified

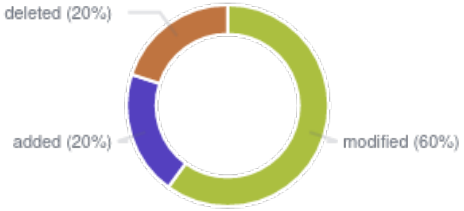
Events



Most active users



Actions



Alerts summary

Path	Description	Count
/root/.zsh_history	Integrity checksum changed.	2
/root/smit.txt	File added to the system.	1
/root/smit.txt	File deleted.	1
/root/smit.txt	Integrity checksum changed.	1

info@wazuh.com
https://wazuh.com

Security events report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	Linux_Server	192.168.44.149	Wazuh v4.7.5	kali	Kali GNU/Linux 2024.1	Jun 4, 2024 @ 12:54:04.000	Jun 8, 2024 @ 06:46:16.000

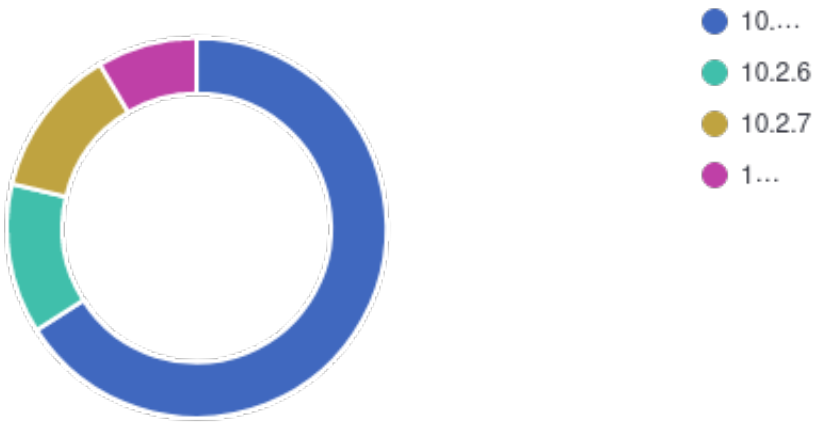
Group: default

Browse through your security alerts, identifying issues and threats in your environment.

2024-06-07T06:46:14 to 2024-06-08T06:46:14

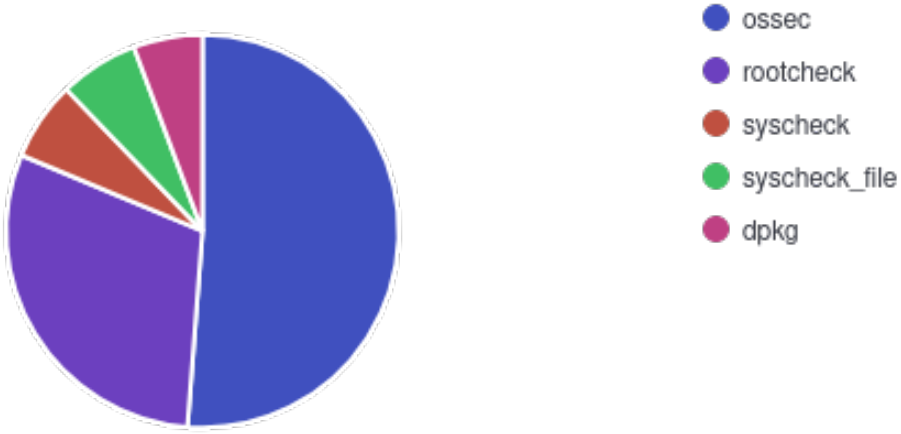
manager.name: kali AND agent.id: 002

Top 5 PCI DSS requirements

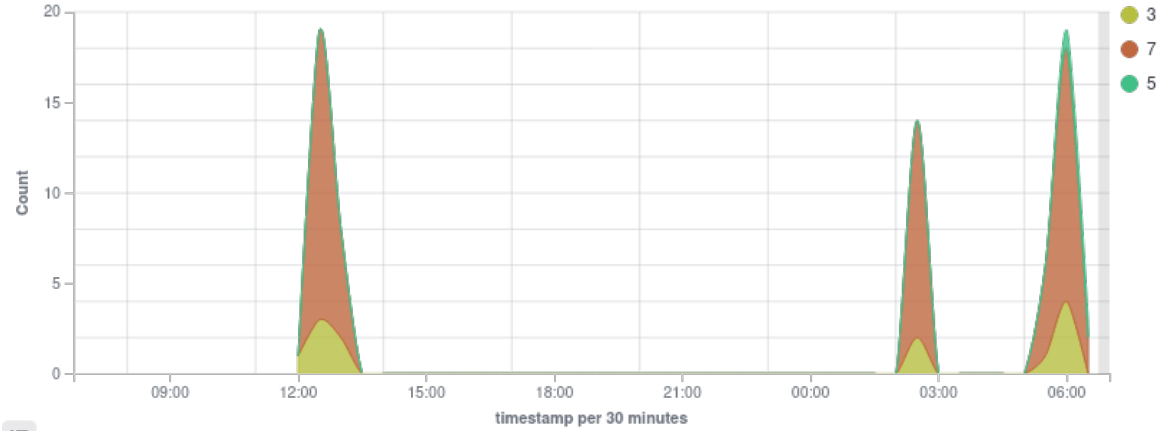


Top 5 alerts

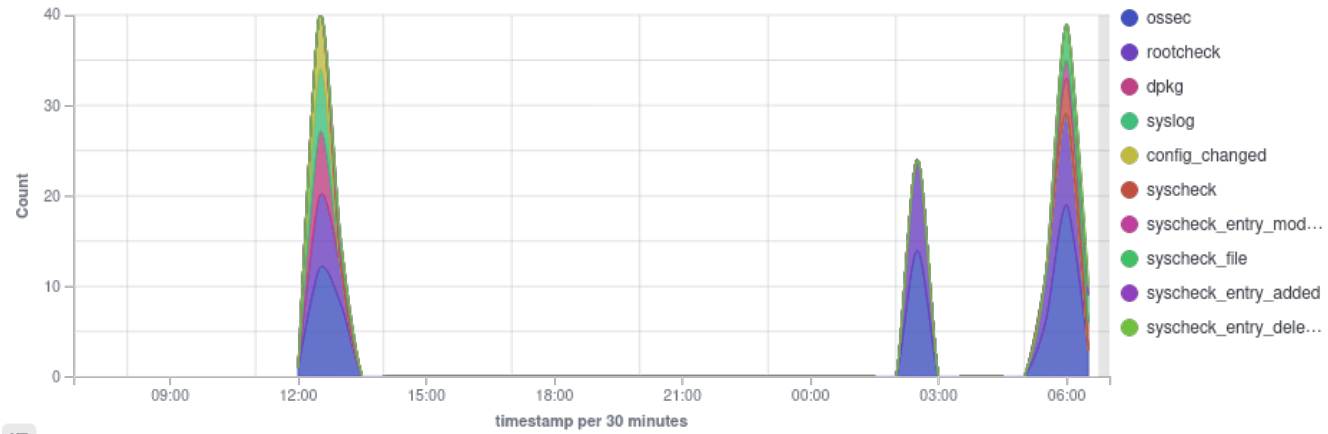
Top 5 rule groups



Alerts



Alert groups evolution



Alerts summary

Rule ID	Description	Level	Count
510	Host-based anomaly detection event (rootcheck).	7	37
503	Wazuh agent started.	3	8
533	Listened ports status (netstat) changed (new port opened or closed).	7	6
550	Integrity checksum changed.	7	5
506	Wazuh agent stopped.	3	4
2902	New dpkg (Debian Package) installed.	7	3
2904	Dpkg (Debian Package) half configured.	7	3
553	File deleted.	7	3
554	File added to the system.	5	3
2901	New dpkg (Debian Package) requested to install.	3	1

Groups summary

Groups	Count
ossec	66
rootcheck	37
syscheck	11
syscheck_file	11
dpkg	7
syslog	7
config_changed	6
syscheck_entry_modified	5
syscheck_entry_added	3
syscheck_entry_deleted	3