

```
Connecting to packages.wazuh.com (packages.wazuh.com)|18.154.48.95|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10774582 (10M) [application/vnd.debian.binary-package]
Saving to: 'wazuh-agent_4.9.2-1_amd64.deb'

wazuh-agent_4.9.2-1 100%[=====] 10.28M 26.5MB/s in 0.4s

2024-11-20 13:39:08 (26.5 MB/s) - 'wazuh-agent_4.9.2-1_amd64.deb' saved [10774582/10774582]

Selecting previously unselected package wazuh-agent.
(Reading database ... 167703 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.9.2-1_amd64.deb ...
Unpacking wazuh-agent (4.9.2-1) ...
Setting up wazuh-agent (4.9.2-1) ...
root@debian:/home/debian# sudo systemctl daemon-reload
root@debian:/home/debian# sudo systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service
→ /lib/systemd/system/wazuh-agent.service.
root@debian:/home/debian# sudo systemctl start wazuh-agent
root@debian:/home/debian#
```

W.

EndpointsDebian

a

Threat HuntingFile Integrity MonitoringConfiguration AssessmentMore...

Debian (002)Inventory dataStatsConfiguration

ID	Status	IP address	Version	Groups	Operating system	Cluster node	Registration date	Last keep alive
002	active	192.168.1.148	Wazuh v4.9.2	default	Debian GNU/Linux 12	node01	Nov 20, 2024 @ 19:39:55.000	Nov 20, 2024 @ 19:40:40.000

Last 24 hours

MITRE ATT&CK

Top Tactics

Defense Evasion1

Compliance

PCI DSS

10.6.1 (7)

10.2.6 (2)

FIM: Recent events

Time ↓	Path	Action	Rule description	Rule Lev...	Rule Id
No recent events					

Events count evolution

SCA: Lastest scans

Center for Internet Security Debian Family Linux Benchmark v1.0.0cis_debian12

Policy	End scan	Passed	Failed	Not ap...	Score
Center for Internet Security Debian Family Linux Benchmark v1.0.0	Nov 20, 2024 @ 19:40:30.000	62	82	37	43%

```
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/access.log</location>
</localfile>
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/error.log</location>
</localfile>
```

GNU nano 7.2

/var/www/html/wp-config.php

```
define( 'WP_DEBUG', true );
define( 'WP_DEBUG_LOG', true );
define( 'WP_DEBUG_DISPLAY', false );
```

```
root@debian:/home/debian# ssh usuarioinvalido@192.168.1.148
The authenticity of host '192.168.1.148 (192.168.1.148)' can't be established.
ED25519 key fingerprint is SHA256:pkpG0s13GQe+oyIAFtQuUF02hFxDWvW9xyrXf/1ItnA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.148' (ED25519) to the list of known hosts.
usuarioinvalido@192.168.1.148's password:
Permission denied, please try again.
usuarioinvalido@192.168.1.148's password:
Permission denied, please try again.
usuarioinvalido@192.168.1.148's password:
usuarioinvalido@192.168.1.148: Permission denied (publickey,password).
root@debian:/home/debian# ssh usuarioinvalido@192.168.1.148
usuarioinvalido@192.168.1.148's password:
Permission denied, please try again.
usuarioinvalido@192.168.1.148's password:
Permission denied, please try again.
usuarioinvalido@192.168.1.148's password:
usuarioinvalido@192.168.1.148: Permission denied (publickey,password).
root@debian:/home/debian#
```

234

- Total -

0

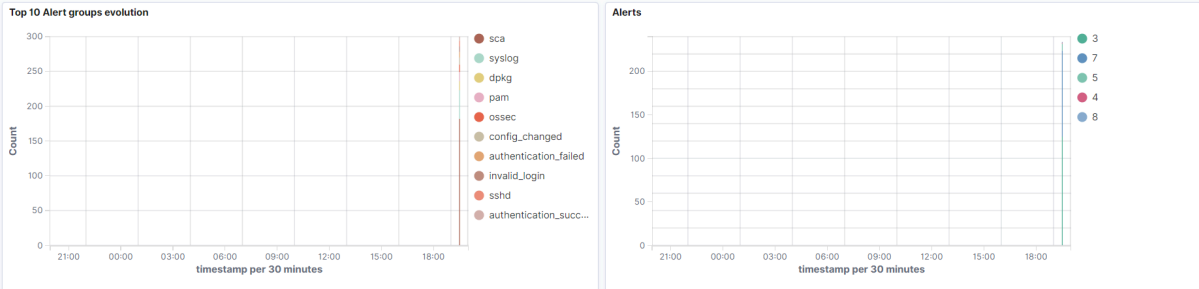
- Level 12 or above alerts -

8

- Authentication failure -

6

- Authentication success -



Export Formatted

473 columns hidden

Density

1 fields sorted

Full screen

Nov 19, 2024 @ 19:57:28.369 - Nov 20, 2024 @ 19:57:28.369

timestamp	agent.name	rule.description	rule.level	rule.id
Nov 20, 2024 @ 19:55:57.559	Debian	sshd: Attempt to login using a non-exist...	5	5710
Nov 20, 2024 @ 19:55:57.559	Debian	sshd: Attempt to login using a non-exist...	5	5710
Nov 20, 2024 @ 19:55:57.558	Debian	sshd: Attempt to login using a non-exist...	5	5710
Nov 20, 2024 @ 19:55:57.508	Debian	sshd: Attempt to login using a non-exist...	5	5710
Nov 20, 2024 @ 19:55:53.506	Debian	sshd: Attempt to login using a non-exist...	5	5710
Nov 20, 2024 @ 19:55:53.506	Debian	sshd: Attempt to login using a non-exist...	5	5710
Nov 20, 2024 @ 19:55:51.505	Debian	sshd: Attempt to login using a non-exist...	5	5710
Nov 20, 2024 @ 19:55:35.546	Debian	PAM: Login session closed.	3	5502
Nov 20, 2024 @ 19:55:35.501	Debian	Successful sudo to ROOT executed.	3	5402
Nov 20, 2024 @ 19:55:35.501	Debian	PAM: Login session opened.	3	5501
Nov 20, 2024 @ 19:55:27.496	Debian	PAM: Login session closed.	3	5502
Nov 20, 2024 @ 19:55:23.494	Debian	Successful sudo to ROOT executed.	3	5402
Nov 20, 2024 @ 19:55:23.494	Debian	PAM: Login session opened.	3	5501
Nov 20, 2024 @ 19:55:17.510	Debian	PAM: Login session closed.	3	5502

Rows per page: 15

<

1

2

3

4

5

...

16

>