













OPENSOURCE SOC ENVIRONMENT

STEVEN OWEN

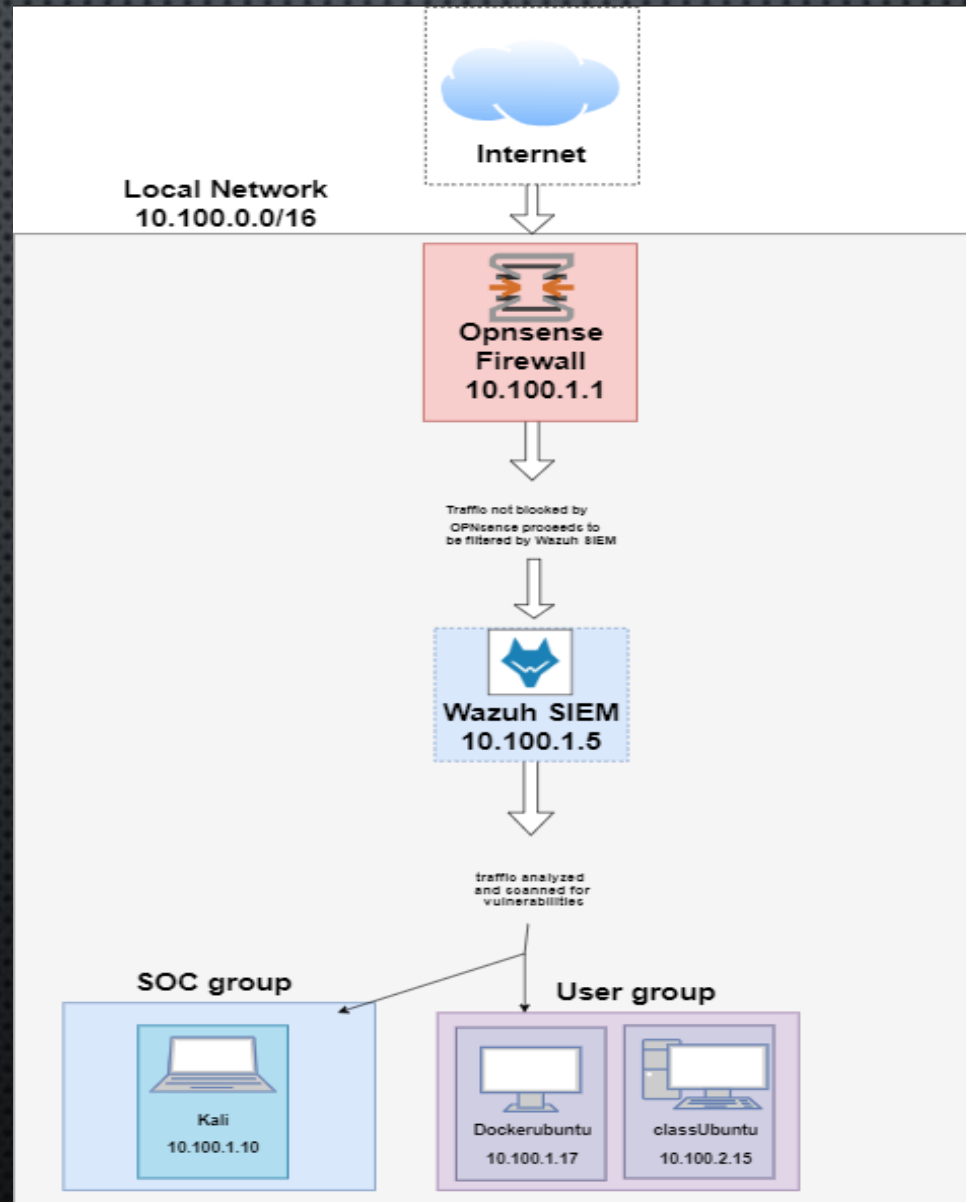
VIRTUAL MACHINES

 New group

	Wazuh v4.4.2 OVA  Powered Off
	OPNsense-firewall backup  Powered Off
	Newfolder_default_1678762788893_33604  Powered Off
	good kali  Powered Off
	UbuntuForDocker  Powered Off

 New group 3

TOPOLOGY



OPNSENSE



OPNSENSE DASHBOARD

Lobby

Dashboard

License

Password

Logout

Reporting

System

Interfaces

Firewall

VPN

Services

Zenarmor

Power

Help

Lobby: Dashboard

Add widget

2 columns

System Information

Name

OPNsense.localdomain

Versions

OPNsense 23.1.5_4-amd64
FreeBSD 13.1-RELEASE-p7
OpenSSL 1.1.1t 7 Feb 2023


Updates

Click to check for updates.

CPU type

12th Gen Intel(R) Core(TM) i5-12400 (2 cores, 2 threads)

CPU usage



Load average

0.99, 1.06, 1.17

Uptime

01:02:57

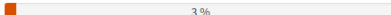
Current date/time

Sun Jun 4 15:03:11 EDT 2023

Last config change

Sun Jun 4 15:00:37 EDT 2023

CPU usage

3 %


State table size

0 % (154/815000)

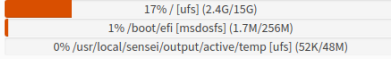
MBUF usage

0 % (4064/507618)

Memory usage

3 % (3157/8154 MB)

Disk usage



Services

Service	Description		
configd	System Configuration Daemon		
cron	Cron		
dhcpcd	DHCPv4 Server		
dhcpcd6	DHCPv6 Server		
login	Users and Groups		
ntpd	Network Time Daemon		
openssh	Secure Shell Daemon		
pf	Packet Filter		
radvd	Router Advertisement Daemon		
routing	System routing		
squid	Web Proxy		
suricata	Intrusion Detection		
sysctl	System tunables		
syslog-ng	Syslog-ng Daemon		
unbound	Unbound DNS		
webgui	Web GUI		

OPNsense (c) 2014-2023 Deciso B.V.

https://10.100.1.1/index.php

OPNSENSE WEB PROXY

Forward proxy--with a self-signed certificate--enables OPNsense to Intercept and filter traffic.

General Proxy Settings

Forward Proxy

Proxy Auto-Config

Remote Access Control Lists

Support

advanced mode

Proxy interfaces

LAN

Clear All

Proxy port

3128

Enable Transparent HTTP proxy

☒

Enable SSL inspection

☒

Log SNI information only

☐

SSL Proxy port

3129

CA to use

OPNsense-webca

SSL no bump sites

Clear AllCopyPaste

Apply

System: Trust: Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	
OPNsense-webca	YES	self-signed	0	emailAddress=homelab@homelab.com, ST=NY, O=homelab, L=NY, CN=opnsense-webca, C=US Valid From: Sun, 04 Jun 2023 09:10:16 -0400 Valid Until: Sat, 06 Sep 2025 09:10:16 -0400	<div><div>+</div><div><div></div><div></div><div></div><div></div></div></div>

FIREWALL LAN RULES TO ALLOW PROXY INTERCEPT

OPNsense

<

root@OPNsense.localdomain

Q

Reporting

System

Interfaces

Firewall

- Aliases
- Categories
- Groups
- NAT
- Rules
 - Floating
 - LAN
 - Loopback
 - WAN
- Shaper
- Settings
- Log Files
- Diagnostics

VPN

Services

Firewall: Rules: LAN

Select category

Inspect

The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

Apply changes

		Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description ?	
										Automatically generated rules	24
		IPv4 TCP/UDP	LAN net	*	*	80 (HTTP)	*	*		block http bypass	
		IPv4 TCP/UDP	LAN net	*	*	443 (HTTPS)	*	*		block https proxy	
		IPv4 *	LAN net	*	*	*	*	*		Default allow LAN to any rule	
		IPv6 *	LAN net	*	*	*	*	*		Default allow LAN IPv6 to any rule	
		IPv4 TCP	LAN net	*	127.0.0.1	3128	*	*		redirect traffic to proxy	
		IPv4 TCP	LAN net	*	127.0.0.1	3129	*	*		redirect traffic to proxy	
	pass	✗ block			✗ reject			log	→ in	⚡ first match	
	pass (disabled)	✗ block (disabled)			✗ reject (disabled)			log (disabled)	← out	⚡ last match	
										Active/Inactive Schedule (click to view/edit)	
										Alias (click to view/edit)	

ZENARMOR

Next-Gen Firewall



OPNSENSE ZENARMOR PLUGINS

OPNsense

<

root@OPNsense.localdomain

Q

Lobby

Reporting

System

Access

Configuration

Firmware

Status

Settings

Changelog

Updates

Plugins

Packages

Reporter

Log File

Gateways

High Availability

Routes

Settings

Trust

Wizard

Log Files

Diagnostics

Interfaces

System: Firmware

Status

Settings

Changelog

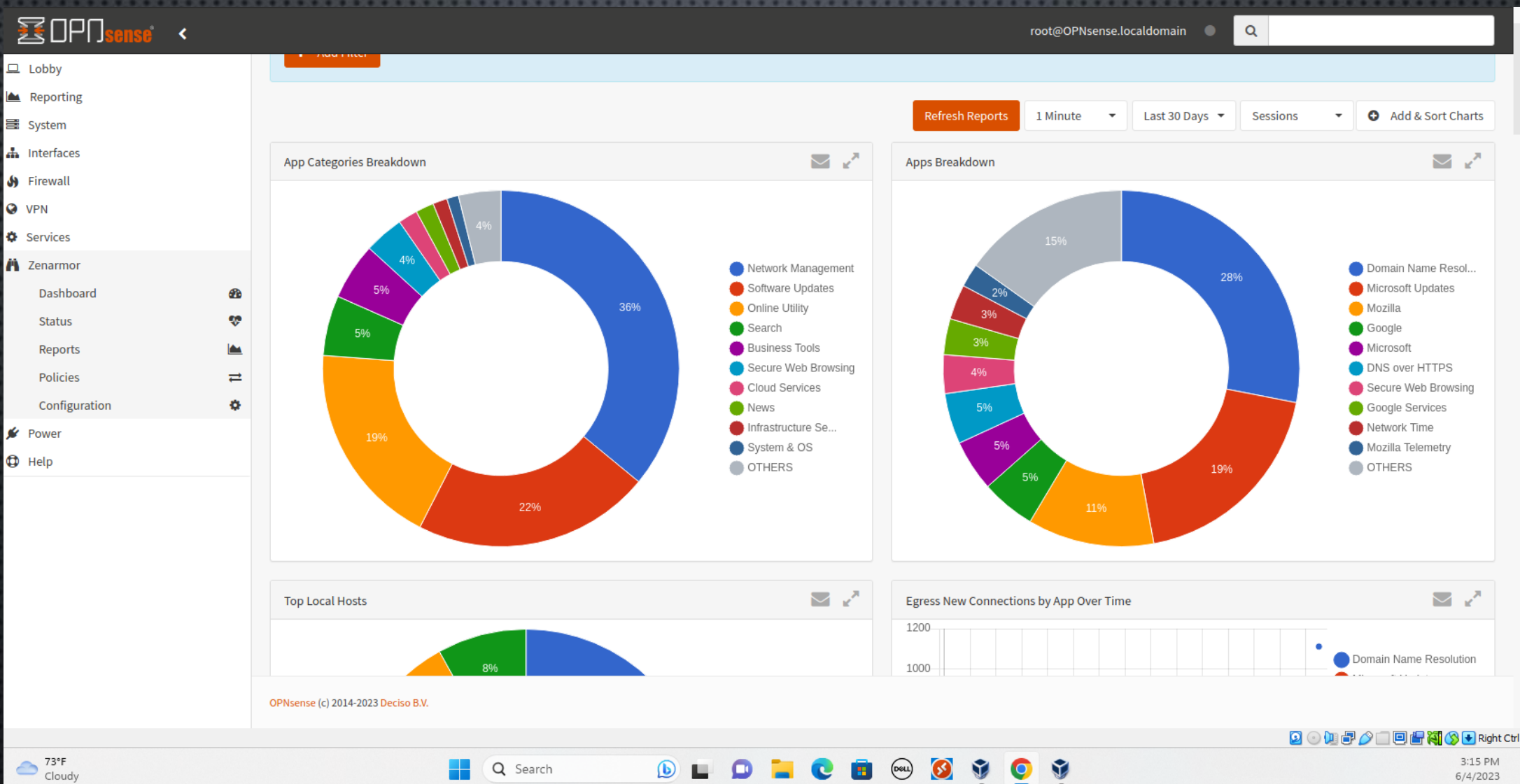
Updates

Plugins

Packages

Name	Version	Size	Repository	Comment	
os-sensei (installed)	1.13.1	205MiB	SunnyValley	Next Generation Firewall Extensions for OPNsense (ZENARMOR)	<div><div></div><div></div></div>
os-sensei-updater (installed)	1.13	4.79KiB	SunnyValley	OPNsense ZENARMOR Plugin Updater	<div><div></div><div></div></div>
os-sunnyvalley (installed)	1.2_3	643B	OPNsense	Vendor Repository for Zenarmor (a.k.a Sensei, Next Generation Firewall Extensions)	<div><div></div><div></div></div>
os-virtualbox (installed)	1.0_1	516B	OPNsense	VirtualBox guest additions	<div><div></div><div></div></div>
os-acme-client	3.17	714KiB	OPNsense	ACME Client	<div><div></div><div>+</div></div>
os-apcupsd	1.1	56.6KiB	OPNsense	APCUPSD - APC UPS daemon	<div><div></div><div>+</div></div>
os-api-backup	1.1	3.80KiB	OPNsense	Provide the functionality to download the config.xml	<div><div></div><div>+</div></div>
os-bind	1.26_5	145KiB	OPNsense	BIND domain name service	<div><div></div><div>+</div></div>
os-c-icap	1.7_3	50.1KiB	OPNsense	c-icap connects the web proxy with a virus scanner	<div><div></div><div>+</div></div>
os-cache	1.0_1	520B	OPNsense	Webserver cache	<div><div></div><div>+</div></div>
os-chrony	1.5_1	20.4KiB	OPNsense	Chrony time synchronisation	<div><div></div><div>+</div></div>
os-clamav	1.8	47.7KiB	OPNsense	Antivirus engine for detecting malicious threats	<div><div></div><div>+</div></div>
os-collectd	1.4_1	36.8KiB	OPNsense	Collect system and application performance metrics periodically	<div><div></div><div>+</div></div>
os-crowdsec	1.0.5	63.2KiB	OPNsense	Lightweight and collaborative security engine	<div><div></div><div>+</div></div>
os-ddclient	1.13_2	97.6KiB	OPNsense	Dynamic DNS client	<div><div></div><div>+</div></div>
os-debug	1.5	434B	OPNsense	Debugging Tools	<div><div></div><div>+</div></div>

OPNSENSE ZENARMOR DASHBOARD



ZENARMOR POLICIES

OPNsense

<

root@OPNsense.localdomain

Q

Lobby

Reporting

System

Interfaces

Firewall

VPN

Services

Zenarmor

Dashboard

Status

Reports

Policies

Configuration

Power

Help

zenarmor > Policies

Business Edition | [Report Bug](#) | [Contact Team](#) | [My Account](#)

+ Add New Policy

Policy Name	Status	Security	App Controls	Web Controls	Actions	Order
Default	<div></div>	Enabled	Permissive	Enabled	<div></div> <div></div>	

ZENARMOR WEB CONTROLS

Policy ConfigurationSecurityApp ControlsWeb ControlsExclusions

Enforce Safe Search | Preset profile: ☐ Permissive ☐ Moderate Control ☐ High Control ☒ Custom

Search...

Web Categories

Ad Trackers

Adult

Advertisements

Alcohol and Tobacco

Arts and Culture

Blacklist

Blogs

Business Services

Chats

Clothing and Fashion

Content Delivery Networks

Cult and Occult

Dating

Education

Entertainment

Financial Services

Forums

User Defined Categories

Auto White List Hosts

Auto Block List Hosts

New Category

OPNsense

root@OPNsense.localdomain

Q

LobbyReportingSystemInterfacesFirewallVPNServicesZenarmorDashboardStatusReportsPoliciesConfigurationPowerHelp

Policy ConfigurationSecurityApp ControlsWeb ControlsExclusions

Whitelists

example.com

Describe for exclusion site

FilterAddClear

You can enter hostnames, domains and IP addresses. Domains match all subdomains. CIDR notation is acceptable for IP addresses.
host.sub.domain.com, domain.com, 172.16.1.1, 10.10.0.0/16).

Import list from file

Download Whitelist

Delete list

Id	Site	Desc	Global	Action
<input checked="" type="checkbox"/>	Send this re-categorization as a feedback to zenarmor Team to improve web categorization.			

Blacklists

example.com

Describe for exclusion site

FilterAddClear

You can enter hostnames, domains and IP addresses. Domains match all subdomains. CIDR notation is acceptable for IP addresses.
host.sub.domain.com, domain.com, 172.16.1.1, 10.10.0.0/16).

Import list from file

Download Blacklist

Delete list

Id	Site	Desc	Global	Action
1	Instagram.com		<input type="checkbox"/>	
2	facebook.com		<input type="checkbox"/>	

Save Changes

Policy ConfigurationSecurityApp ControlsWeb ControlsExclusions

Essential Security

full help

Block Bad IP

Block Non-existent Domain

Block Malware Activity

Block Phishing Servers

Block Spam sites

Block Hacking Sites

Block Parked Domains

Block Potentially Dangerous Sites

Block Firstly Seen Sites

Block Undecided Not Safe Sites

Block Undecided Safe Sites

Advanced Security

full help

Block Recent Malware/Phishing/Virus Outbreaks

NEW Block Botnet C&C

Block Proxy

Block Dead Sites

Block Dynamic DNS Sites

Block Local IP

Block Newly Registered Sites

Block Newly Recovered Sites

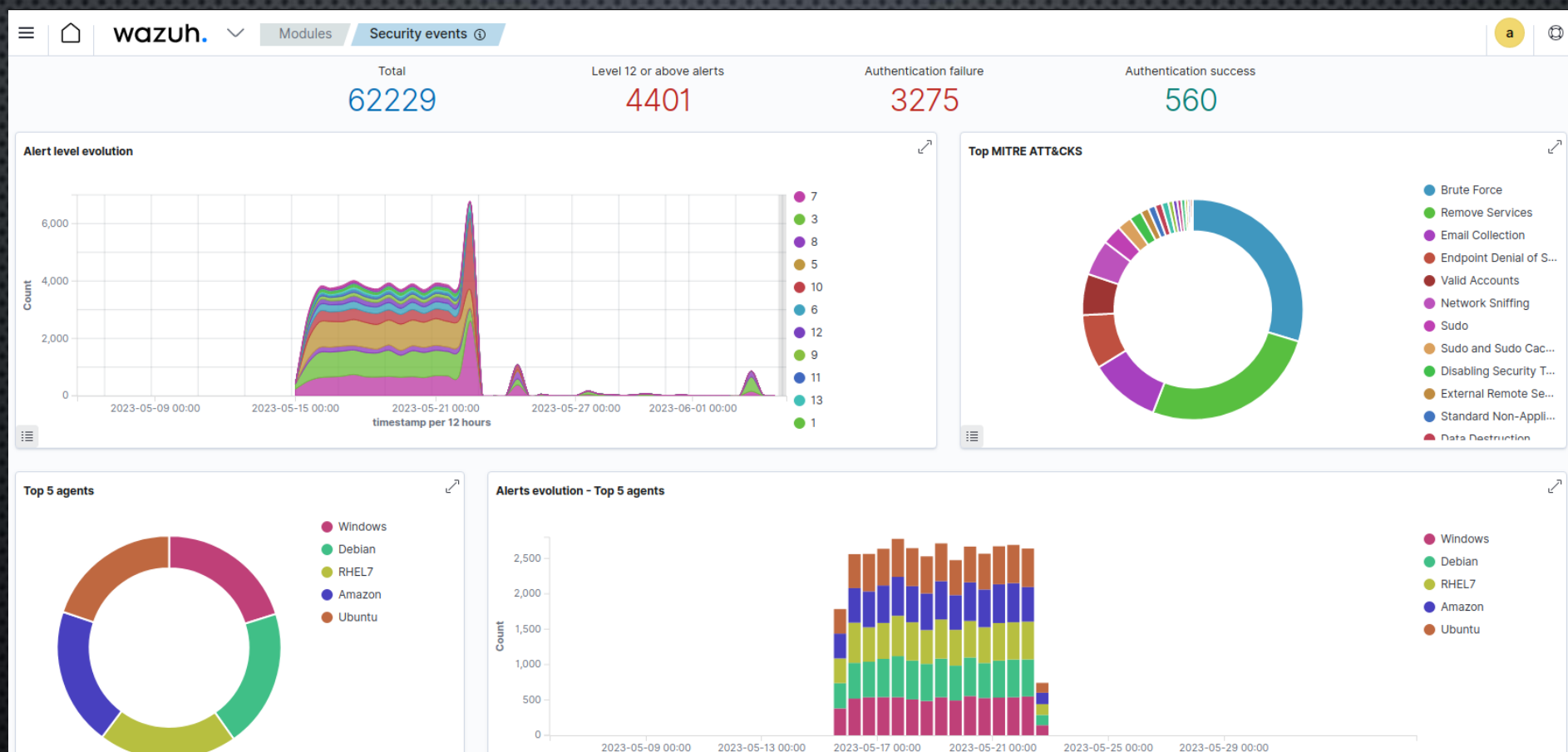
Block Botnet DGA Domains (Coming soon)

Block DNS Tunneling (Coming soon)



WAZUH

WAZUH DASHBOARD



SLACK ALERTS AND CONFIGURATION

homelab

homelabalerts

+ Add a bookmark

Agent (001) - kali

Location netstat listening ports

Rule ID 533 (Level 7)

Today at 11:17 AM

wazuh-alerts APP 11:59 AM

WAZUH Alert

Listened ports status (netstat) changed (new port opened or closed).

ossec: output: 'netstat listening ports':

tcp 127.0.0.1:33041 0.0.0.0:* 544/containerd

udp 0.0.0.0:33381 0.0.0.0:* 2019/firefox-esr

Agent (001) - kali

Location netstat listening ports

Rule ID 533 (Level 7)

Today at 11:59 AM

Manager configuration

Edit ossec.conf of Manager

```
<integration>
  <name>slack</name>
  <hook_url>https://hooks.slack.com/services/T059BKV5MSS/B059BLTPDRU/5QggAjdSdKvVFI6vikLL6M5</hook_url>
  <level>5</level>
  <alert_format>json</alert_format>
</integration>

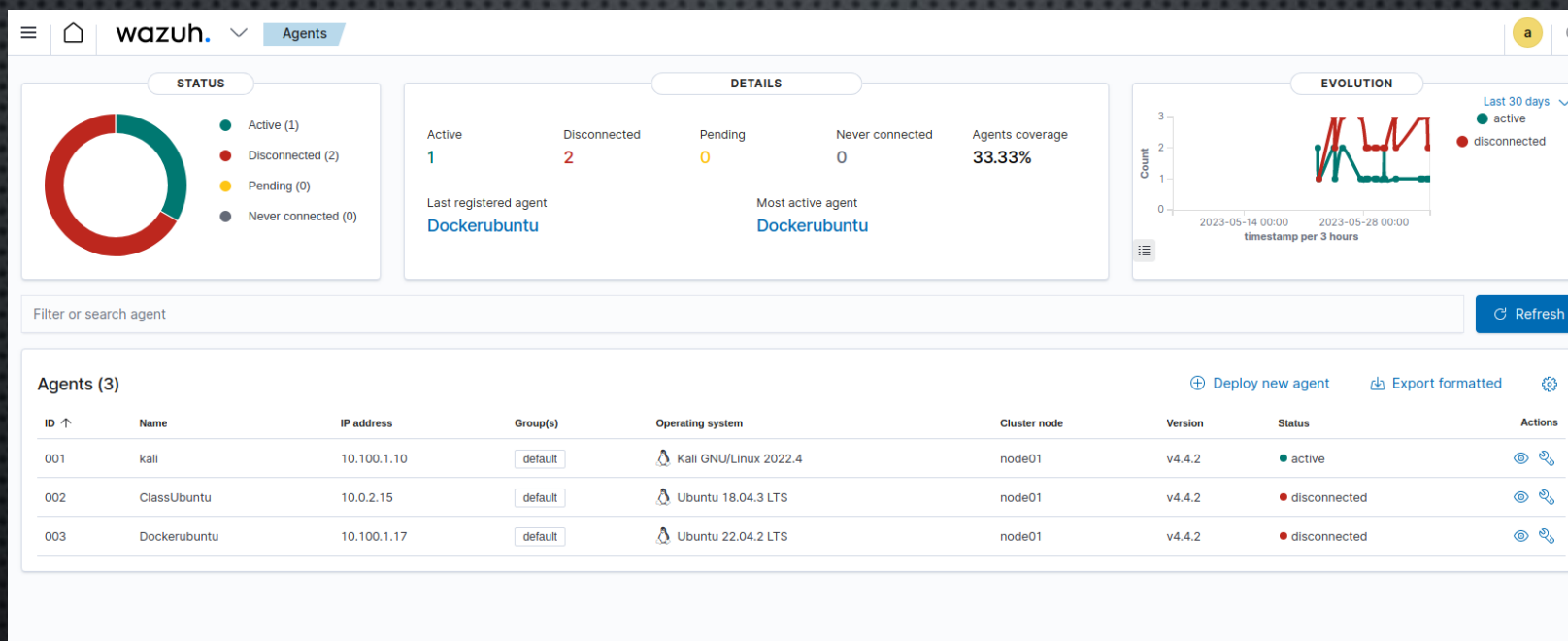
<alerts>
  <log_alert_level>3</log_alert_level>
  <email_alert_level>12</email_alert_level>
</alerts>

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

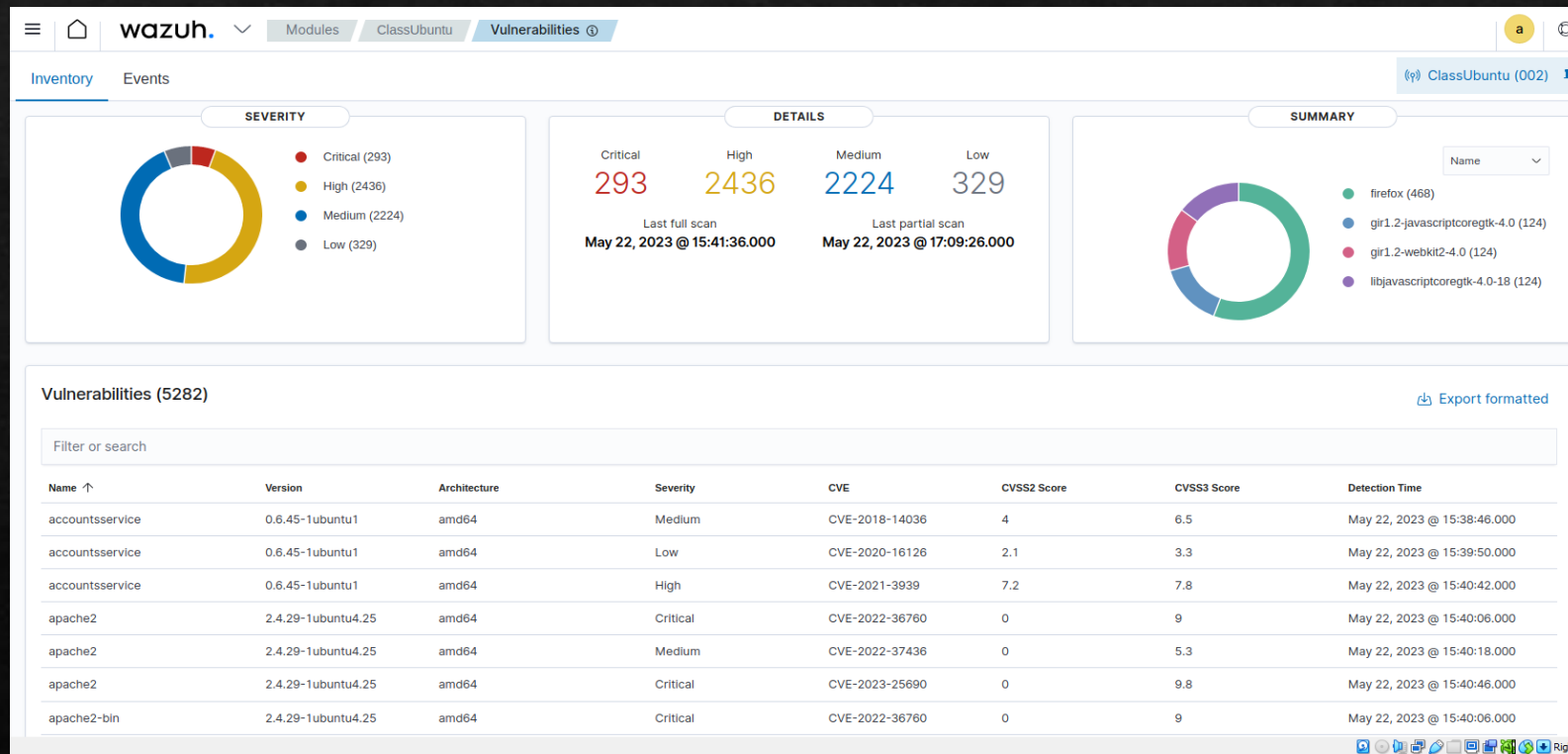
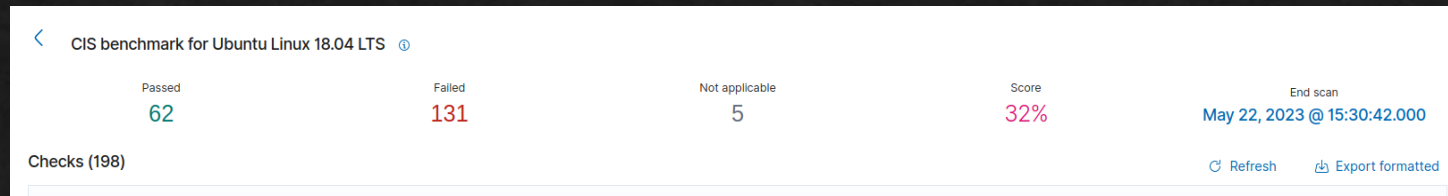
<remote>
  <connection>secure</connection>
  <port>1514</port>
  <protocol>tcp</protocol>
  <queue_size>131072</queue_size>
</remote>

<!-- Policy monitoring -->
<rootcheck>
  <disabled>yes</disabled>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
```

WAZUH CONNECTED AGENTS



"CLASSUBUNTU" AUDIT



WAZUH ACTIVE RESPONSE

```
<!--  
<active-response>  
  <command>firewall-drop</command>  
  <location>kali</location>  
  <rules_id>5720</rules_id>  
  <timeout>1000</timeout>  
</active-response>  
-->
```

```
<active-response>  
  <command>route-null</command>  
  <location></location>  
  <rules_id>5710</rules_id>  
  <timeout>1000</timeout>  
</active-response>
```

ID ↑	Description
5710	sshd: Attempt to login using a non-existent user

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

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

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

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

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

ACTIVE RESPONSE COMMANDS

CURRENT WHITE LISTED DOMAINS

127.0.0.1

LOCALHOST.LOCALDOMAIN

172.31.0.2

DISABLE-ACCOUNT: WAZUH USES THIS ACTIVE RESPONSE ON LINUX/UNIX ENDPOINTS TO DISABLE THE ACCOUNT FOR THE USER IN THE DSTUSER FIELD OF A WAZUH ALERT

FIREWALL-DROP: USES IPTABLES TO BLOCK MALICIOUS IP ADDRESSES

HOST-DENY:

WHEN THIS COMMAND IS TRIGGERED, WAZUH WILL ADD THE IP ADDRESS TO THE /ETC/HOSTS.DENY FILE, WHICH WILL PREVENT THE IP ADDRESS FROM BEING ABLE TO CONNECT TO THE SYSTEM

THE HOST-DENY ACTIVE RESPONSE COMMAND CAN BE USED TO HELP PROTECT SYSTEMS FROM A VARIETY OF THREATS, SUCH AS:

- SSH BRUTE FORCE ATTACKS
- PORT SCANS
- DENIAL-OF-SERVICE ATTACKS

ROUTE-NULL/WIN_ROUTE-NULL:

THE WAZUH ROUTE-NULL ACTIVE RESPONSE COMMAND IS USED TO ROUTE ALL TRAFFIC FROM A SPECIFIC IP ADDRESS TO A NONEXISTENT DESTINATION

NETSH: WHEN THIS RULE IS TRIGGERED, WAZUH WILL EXECUTE THE NETSH COMMAND TO BLOCK THE IP ADDRESS. THE BLOCK WILL BE IN EFFECT FOR 1 HOUR

DEMONSTRATION



THANK YOU