Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity

wazuh – prime esperienze

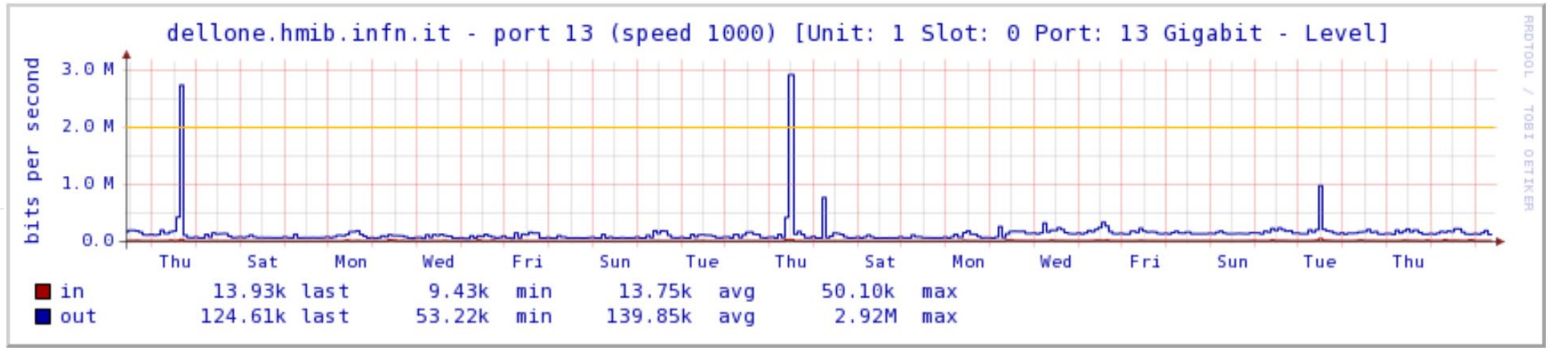
Luca G. Carbone

Mini WS CCR sulla Sicurezza Informatica

13-15/2/2023 - Padova

setup

Installato da qualche mese in modalità monolitica: manager, indexer e dashboard sulla stessa macchina (decentemente vestita: 8 core/16 GB RAM): solo un momento di afasia in tutto questo periodo – update indolori e ragionevole utilizzo risorse.



CPU 41 °C

8 CPU media: 2% max: 5%

View all CPUs

Carico 1 min: 0.33, 5 min: 0.36, 15 min: 0.32

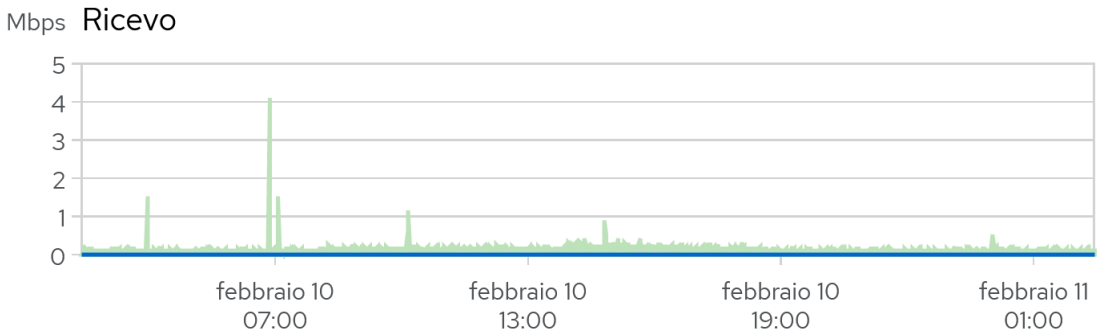
Servizio	%
user@1000	1.2
org.gnome.Shell@wayland	0.5

Memoria

RAM 3,99 GB disponibile

Swap 4,52 GB disponibile

Servizio	Usato
wazuh-indexer	7,19 GB
user@1000	3,53 GB
wazuh-manager	1,81 GB
org.gnome.Shell@wayla	1,03 GB



cosa può fare (1)

SECURITY INFORMATION MANAGEMENT

Security events

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

Integrity monitoring

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

AUDITING AND POLICY MONITORING

Policy monitoring

Verify that your systems are configured according to your security policies baseline.

System auditing

Audit users behavior, monitoring command execution and alerting on access to critical files.

CIS-CAT

Configuration assessment using Center of Internet Security scanner and SCAP checks.

Security configuration assessment

Scan your assets as part of a configuration assessment audit.

cosa può fare (2)

THREAT DETECTION AND RESPONSE

Vulnerabilities

Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK

Security events from the knowledge base of adversary tactics and techniques based on real-world observations

REGULATORY COMPLIANCE

PCI DSS

Global security standard for entities that process, store or transmit payment cardholder data.

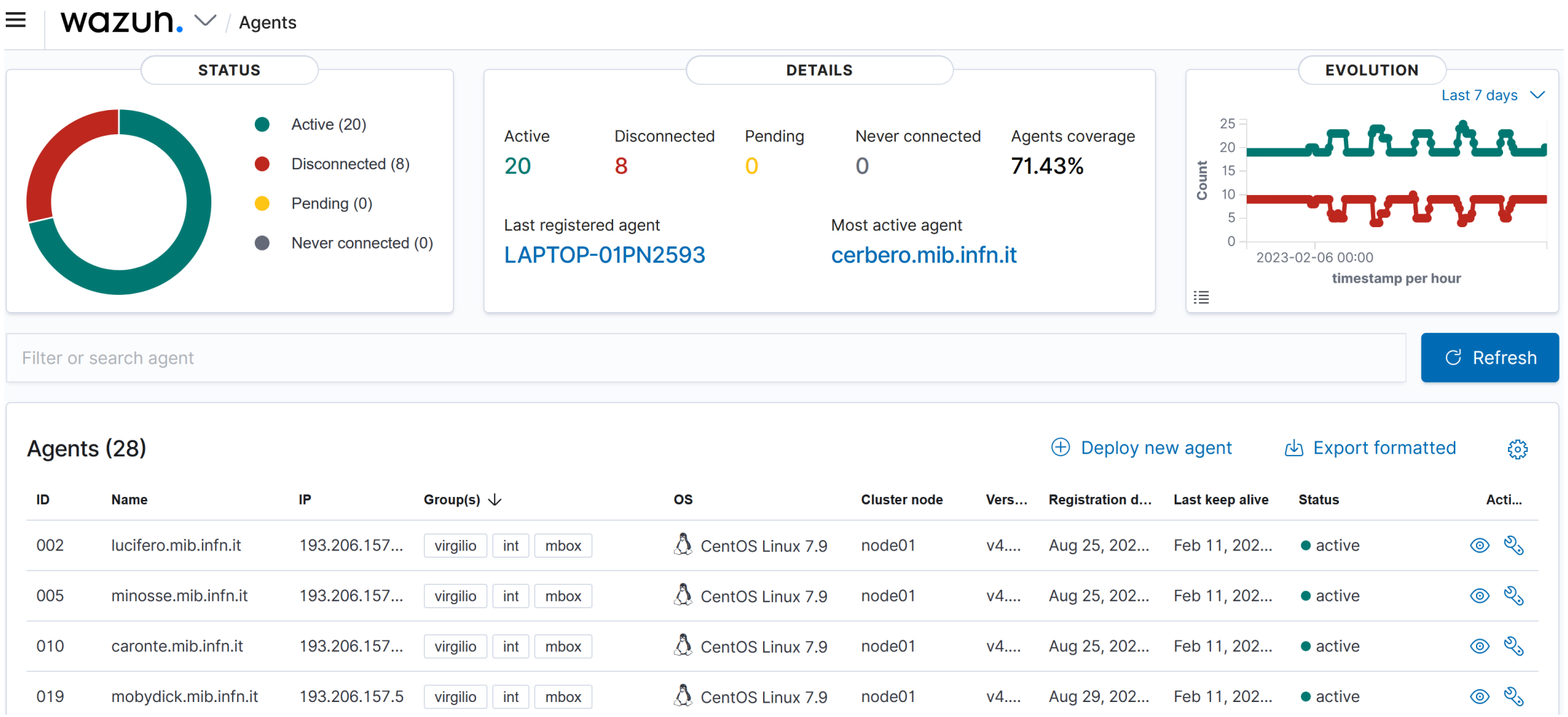
NIST 800-53

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

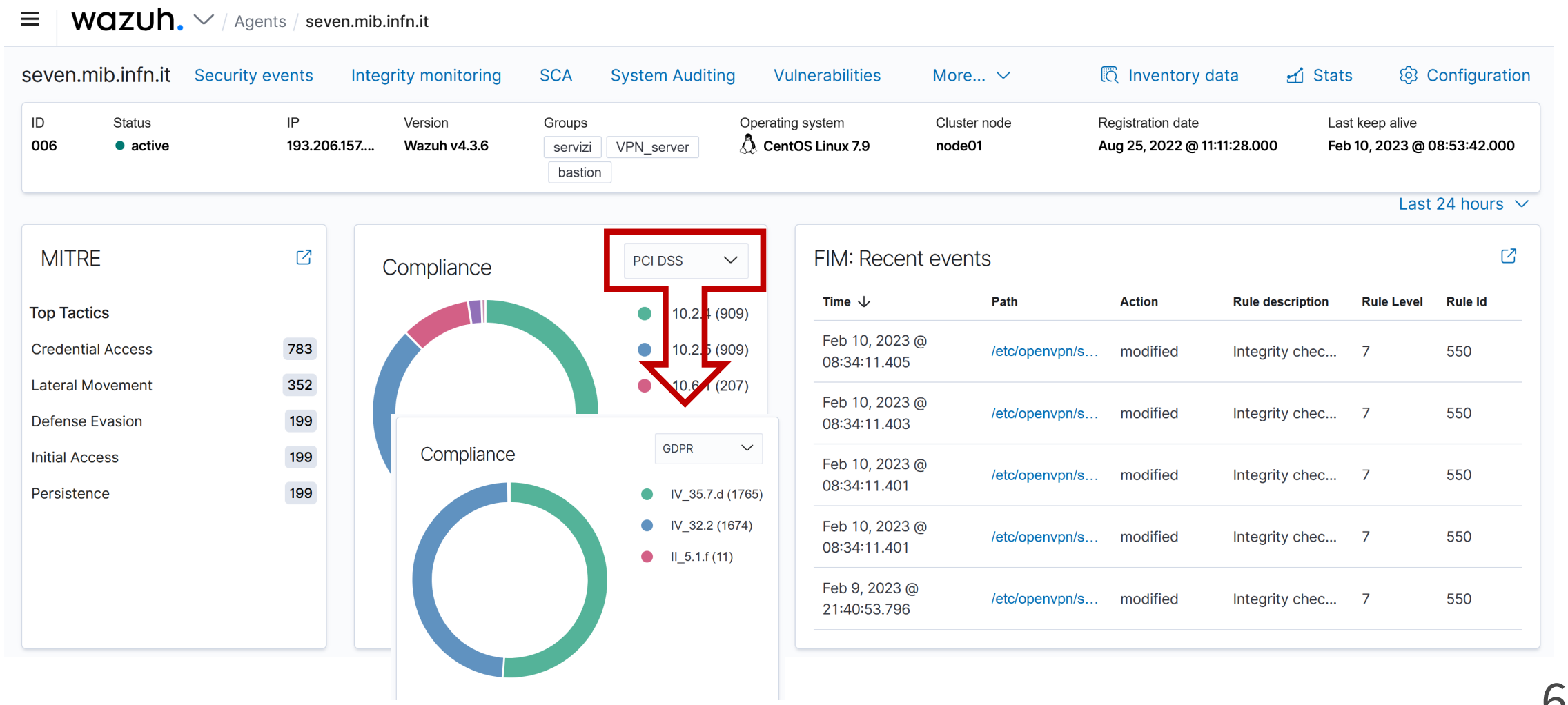
GDPR

General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

main dashboard



agent dashboard



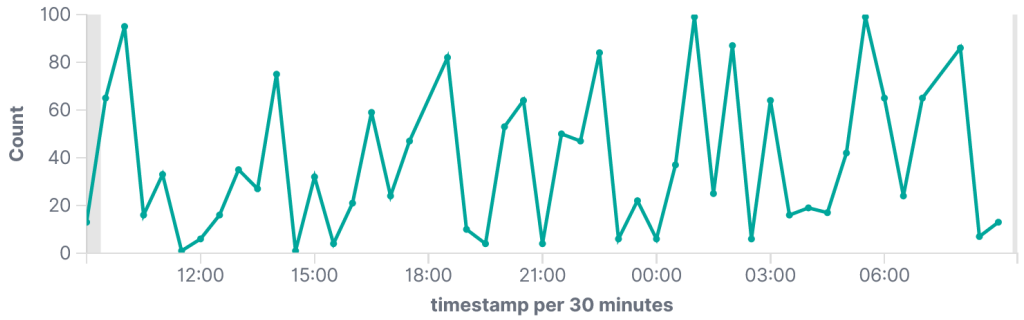
agent dashboard

seven.mib.infn.it | Security events | Integrity monitoring | SCA | System Auditing | More... | Inventory data | Stats | Configuration

ID	Status	IP	Version	Groups	Operating system	Cluster node	Registration date
006	active	193.206.157.70	Wazuh v4.3.6	servizi, VPN_server, bastion	CentOS Linux 7.9	node01	Aug 25, 2022 @ 11:11:28.000

Last keep alive
Feb 12, 2023 @ 09:22:16.000

Events count evolution



SCA: Last scan

CIS Benchmark for CentOS 7 cis_centos7_linux

This document provides prescriptive guidance for establishing a secure configuration posture for CentOS 7 systems running on x86 and x64 platforms. This document was tested against CentOS 7.

Pass	Fail	Total checks	Score
69	117	196	37%

Start time: Feb 12, 2023 @ 09:42:50.000 Duration: < 1s

seven: CIS benchmark

CIS Benchmark for CentOS 7

Export formatted Refresh

Pass	Fail	Not applicable	Score	End scan
69	117	10	37%	Feb 12, 2023 @ 09:42:50.000

Filter or search

ID	Title	Target	Result
6000	Ensure mounting of cramfs filesystems is disabled.	**Command:** modprobe -n -v cramfs	Failed
6001	Ensure mounting of squashfs filesystems is disabled.	**Command:** modprobe -n -v squashfs	Failed
6002	Ensure mounting of udf filesystems is disabled.	**Command:** modprobe -n -v udf	Failed
6003	Ensure mounting of FAT filesystems is disabled.	**Command:** modprobe -n -v vfat	Failed
6004	Ensure /tmp is configured.	**File:** /etc/fstab	Failed

seven: file changed alert

/etc/openvpn/server/status/ldap-ifpool

Details

Last analysis
Feb 10, 2023 @ 10:03:12.000

Last modified
Feb 10, 2023 @ 10:01:18.000

User
root

User ID
0

Group
root

Group ID
0

Size
0

Inode
33734787

MD5
d41d8cd98f00b204e9800998ecf8427e

SHA1
da39a3ee5e6b4b0d3255bfef95601890afd80709

SHA256
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Permissions
rw-------

Recent events

2 hits

seven: inventory - packages

wazuh. / Agents / seven.mib.infn.it / Inventory data

seven.mib.infn.it

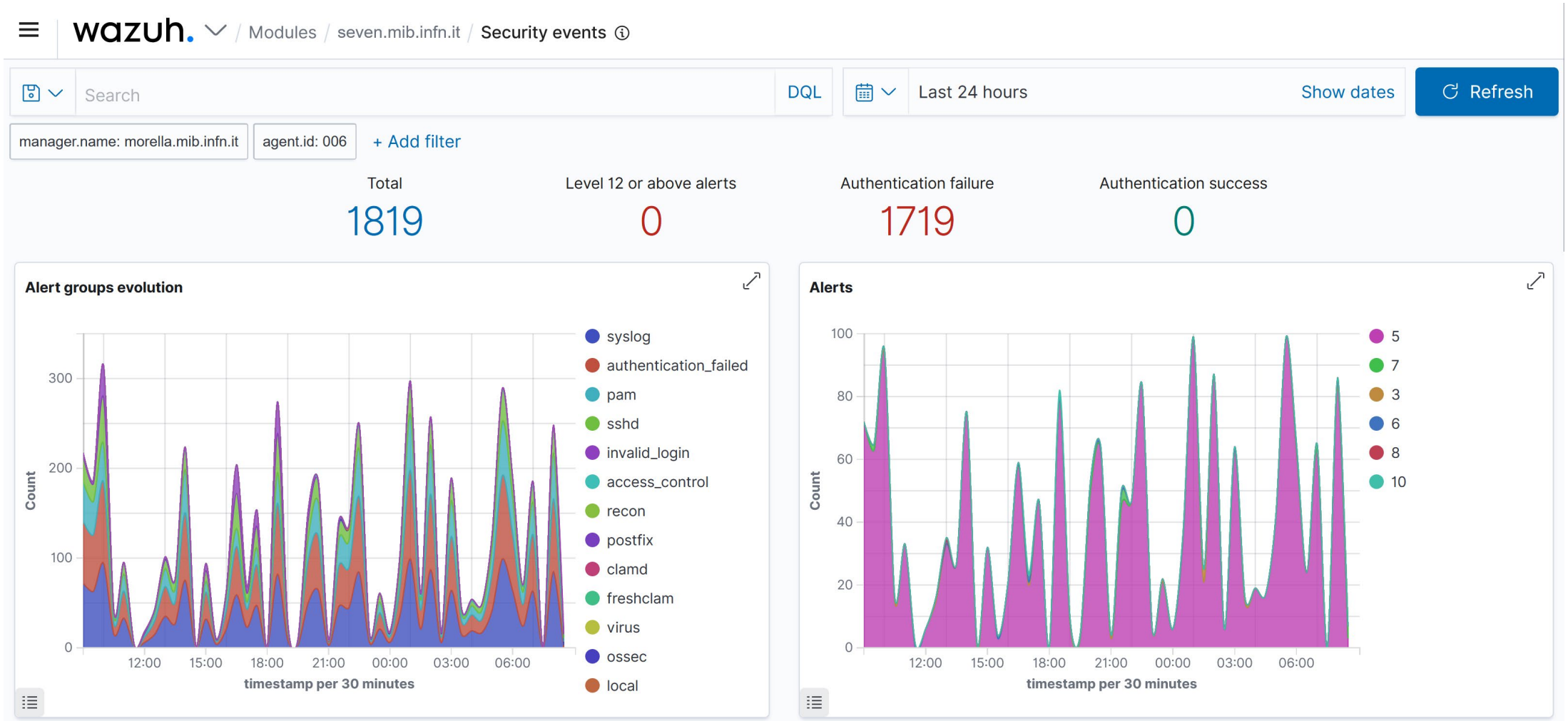
Generate report

Packages (782)

Filter packages...

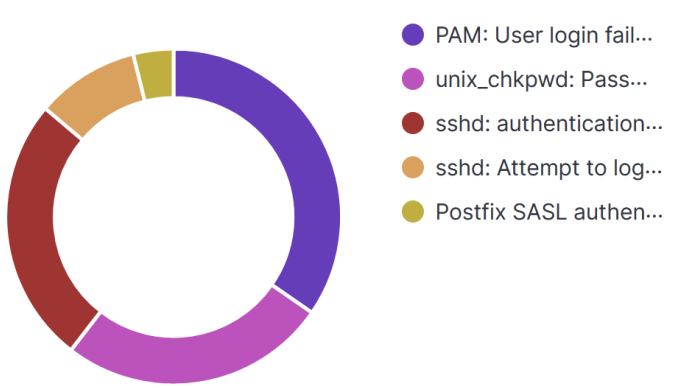
Name	Architecture	Version	Vendor	Description
dracut	x86_64	033-572.el7	CentOS	Initramfs generator using udev
libglvnd	x86_64	1:1.0.1-0.8.git5baa1e5.el7	CentOS	The GL Vendor-Neutral Dispatch library
libnetfilter_conntrack	x86_64	1.0.6-1.el7_3	CentOS	Netfilter conntrack userspace library
cronie-anacron	x86_64	1.4.11-23.el7	CentOS	Utility for running regular jobs
xorg-x11-font-utils	x86_64	1:7.5-21.el7	CentOS	X.Org X11 font utilities
xmlrpc-c	x86_64	1.32.5-1905.svn2451.el7	CentOS	A lightweight RPC library based on XML and HTTP
kmod-kvdo	x86_64	6.1.3.23-5.el7	CentOS	Kernel Modules for Virtual Data Optimizer
python-six	noarch	1.9.0-2.el7	CentOS	Python 2 and 3 compatibility utilities
tcpdump	x86_64	14:4.9.2-4.el7_7.1	CentOS	A network traffic monitoring tool
perl-constant	noarch	1.27-2.el7	CentOS	Perl pragma to declare constants

seven: security events

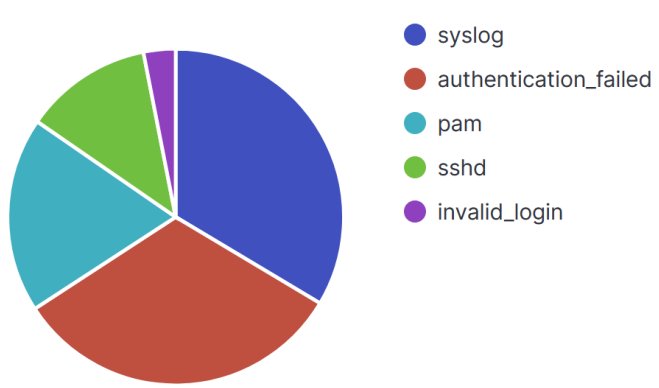


seven: security events

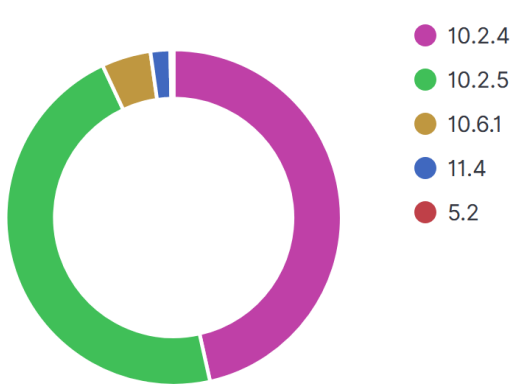
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



Security Alerts

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
Feb 12, 2023 @ 08:55:11.407			Postfix SASL authentication failure.	5	3332
Feb 12, 2023 @ 08:55:11.407			syslog: User authentication failure.	5	2501
Feb 12, 2023 @ 08:55:09.227	T1110.001	Credential Access	PAM: User login failed.	5	5503

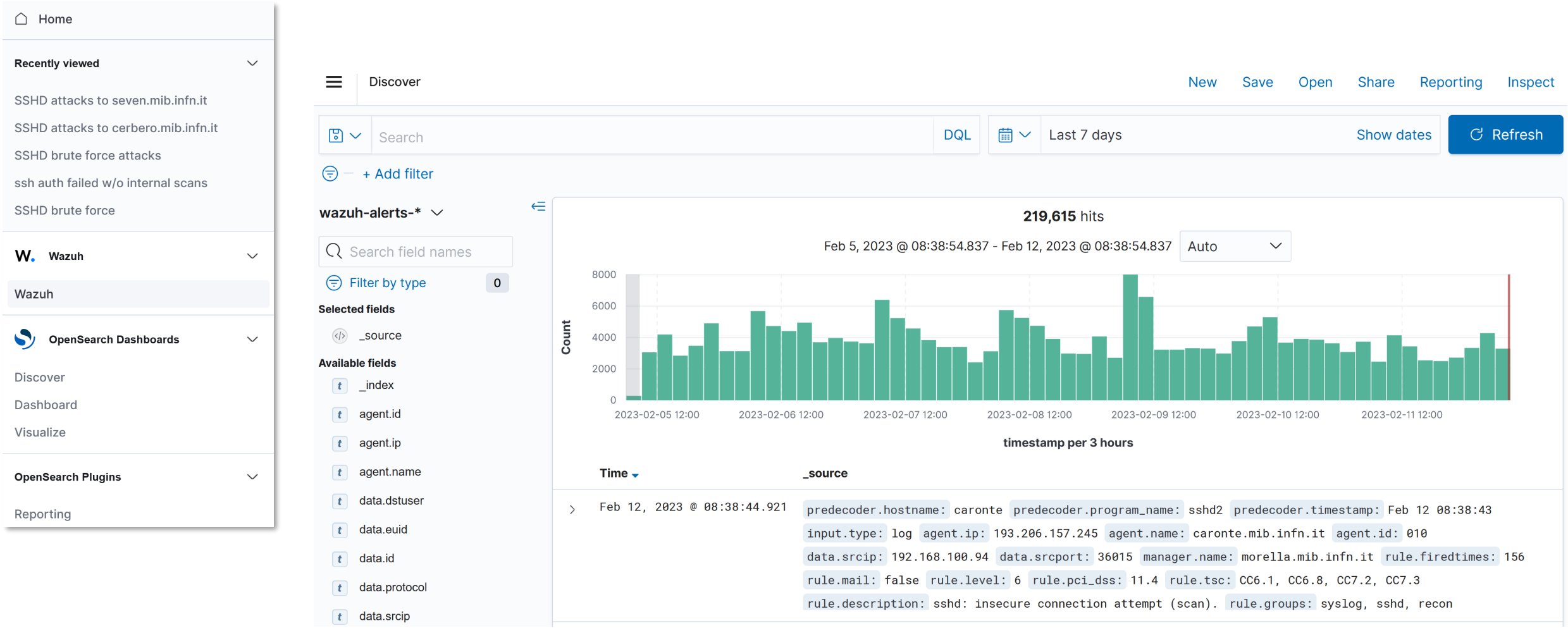
seven: security event details

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
Feb 12, 2023 @ 18:43:19.141	T1110.001 T1021.004 T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5	5710

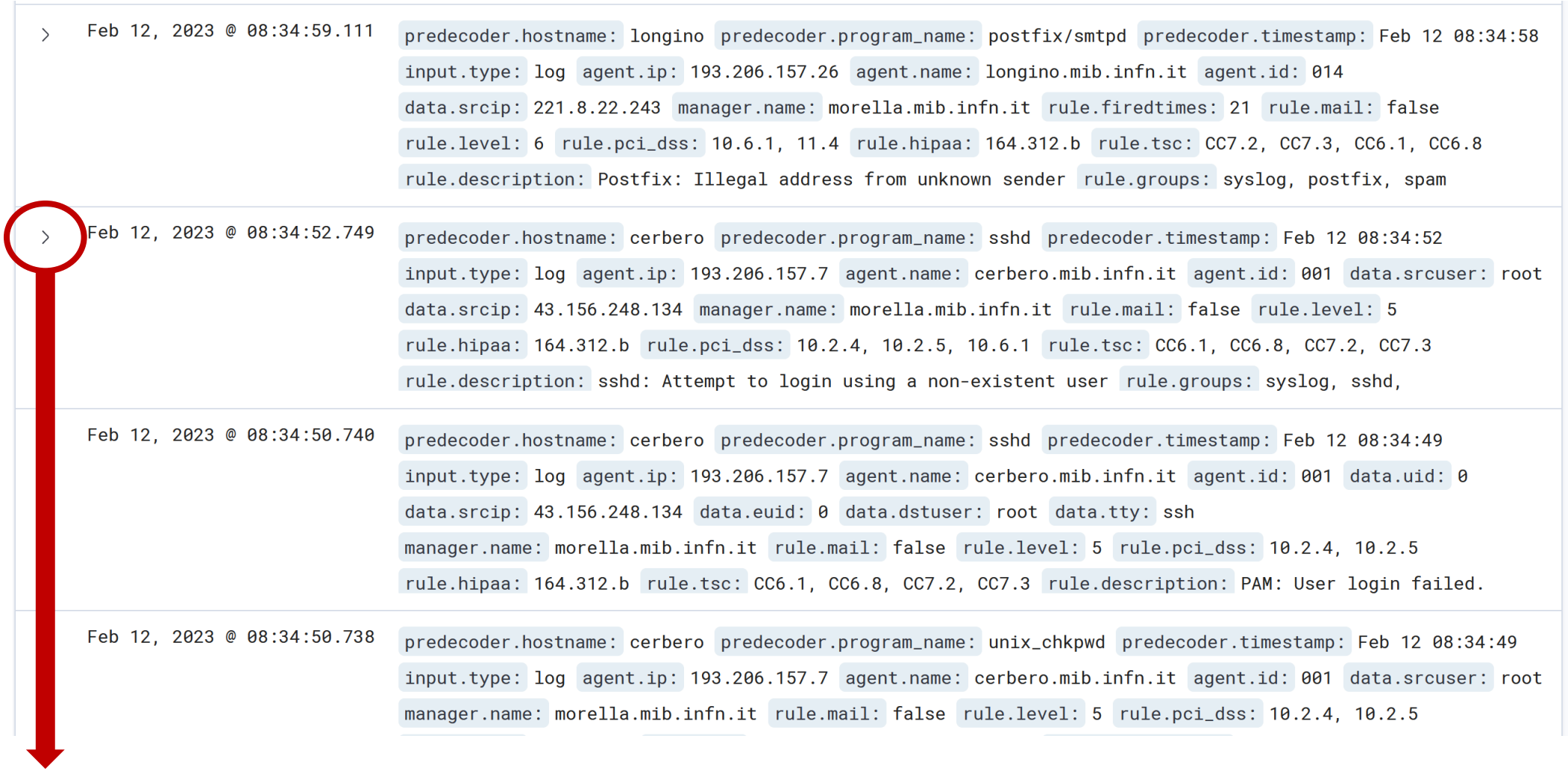
Table | JSON | Rule

@timestamp	2023-02-12T17:43:19.141Z
GeoLocation.city_name	Bengaluru
GeoLocation.country_name	India
GeoLocation.location.lat	12.9719
GeoLocation.location.lon	77.5937
GeoLocation.region_name	Karnataka
_id	WIC5RoYB_qD0gE1yaG2v
agent.id	006
agent.ip	193.206.157.70
agent.name	seven.mib.infn.it
data.srcip	139.59.92.30
data.srcuser	bench
decoder.name	sshd

discover


Home
Recently viewed
SSHD attacks to seven.mib.infn.it
SSHD attacks to cerbero.mib.infn.it
SSHD brute force attacks
ssh auth failed w/o internal scans
SSHD brute force
Wazuh
Wazuh
OpenSearch Dashboards
Discover
Dashboard
Visualize
OpenSearch Plugins
Reporting
Discover
New
Save
Open
Share
Reporting
Inspect
Search
DQL
Last 7 days
Show dates
Refresh
+ Add filter
wazuh-alerts-*
Search field names
Filter by type
0
Selected fields
_source
Available fields
_index
agent.id
agent.ip
agent.name
data.dstuser
data.euid
data.id
data.protocol
data.srcip
219,615 hits
Feb 5, 2023 @ 08:38:54.837 - Feb 12, 2023 @ 08:38:54.837
Auto
Count
8000
6000
4000
2000
0
2023-02-05 12:00
2023-02-06 12:00
2023-02-07 12:00
2023-02-08 12:00
2023-02-09 12:00
2023-02-10 12:00
2023-02-11 12:00
timestamp per 3 hours
Time
_source
Feb 12, 2023 @ 08:38:44.921
predecoder.hostname: caronte predecoder.program_name: sshd2 predecoder.timestamp: Feb 12 08:38:43
input.type: log agent.ip: 193.206.157.245 agent.name: caronte.mib.infn.it agent.id: 010
data.srcip: 192.168.100.94 data.srcport: 36015 manager.name: morella.mib.infn.it rule.firedtimes: 156
rule.mail: false rule.level: 6 rule.pci_dss: 11.4 rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3
rule.description: sshd: insecure connection attempt (scan). rule.groups: syslog, sshd, recon

discover



Feb 12, 2023 @ 08:34:59.111

predecoder.hostname: longino predecoder.program_name: postfix/smtpd predecoder.timestamp: Feb 12 08:34:58
input.type: log agent.ip: 193.206.157.26 agent.name: longino.mib.infn.it agent.id: 014
data.srcip: 221.8.22.243 manager.name: morella.mib.infn.it rule.firedtimes: 21 rule.mail: false
rule.level: 6 rule.pci_dss: 10.6.1, 11.4 rule.hipaa: 164.312.b rule.tsc: CC7.2, CC7.3, CC6.1, CC6.8
rule.description: Postfix: Illegal address from unknown sender rule.groups: syslog, postfix, spam

Feb 12, 2023 @ 08:34:52.749

predecoder.hostname: cerbero predecoder.program_name: sshd predecoder.timestamp: Feb 12 08:34:52
input.type: log agent.ip: 193.206.157.7 agent.name: cerbero.mib.infn.it agent.id: 001 data.srcuser: root
data.srcip: 43.156.248.134 manager.name: morella.mib.infn.it rule.mail: false rule.level: 5
rule.hipaa: 164.312.b rule.pci_dss: 10.2.4, 10.2.5, 10.6.1 rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3
rule.description: sshd: Attempt to login using a non-existent user rule.groups: syslog, sshd,

Feb 12, 2023 @ 08:34:50.740

predecoder.hostname: cerbero predecoder.program_name: sshd predecoder.timestamp: Feb 12 08:34:49
input.type: log agent.ip: 193.206.157.7 agent.name: cerbero.mib.infn.it agent.id: 001 data.uid: 0
data.srcip: 43.156.248.134 data.euid: 0 data.dstuser: root data.tty: ssh
manager.name: morella.mib.infn.it rule.mail: false rule.level: 5 rule.pci_dss: 10.2.4, 10.2.5
rule.hipaa: 164.312.b rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3 rule.description: PAM: User login failed.

Feb 12, 2023 @ 08:34:50.738

predecoder.hostname: cerbero predecoder.program_name: unix_chkpwd predecoder.timestamp: Feb 12 08:34:49
input.type: log agent.ip: 193.206.157.7 agent.name: cerbero.mib.infn.it agent.id: 001 data.srcuser: root
manager.name: morella.mib.infn.it rule.mail: false rule.level: 5 rule.pci_dss: 10.2.4, 10.2.5

discover - event zoom

t	GeoLocation.country_name	South Korea
	GeoLocation.location	{ "lon": 126.9741, "lat": 37.5112 }
t	_index	wazuh-alerts-4.x-2023.02.12
t	agent.id	001
t	agent.ip	193.206.157.7
t	agent.name	cerbero.mib.infn.it
t	data.srcip	211.245.106.55
t	data.srcuser	root
t	decoder.name	sshd
t	decoder.parent	sshd
t	full_log	Feb 12 08:38:42 cerbero sshd[27932]: Failed password for invalid user root from 211.245.106.55 port 52104 ssh2

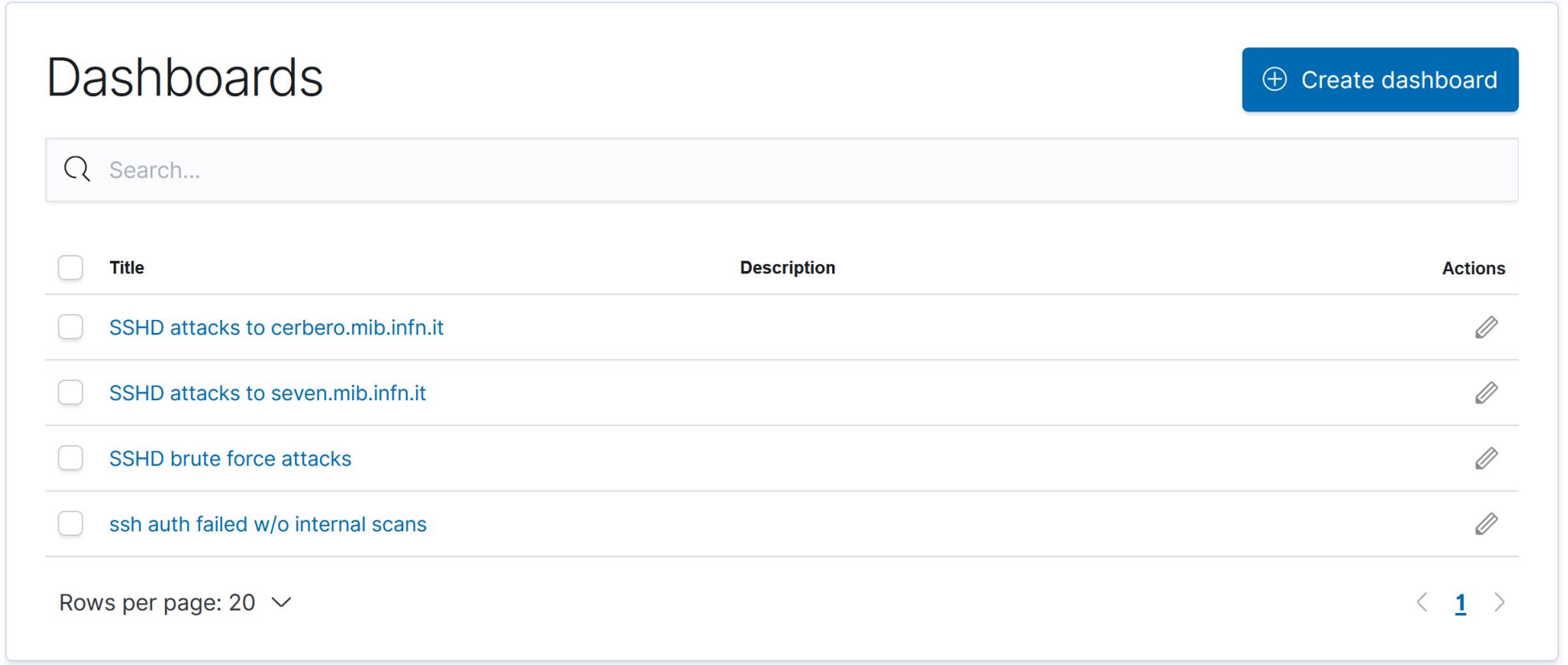
discover - event zoom

Feb 12, 2023 @ 04:57:28.712	T1110	Credential Access	sshd: Multiple access attempts using a denied user.	10	5719

Table JSON Rule

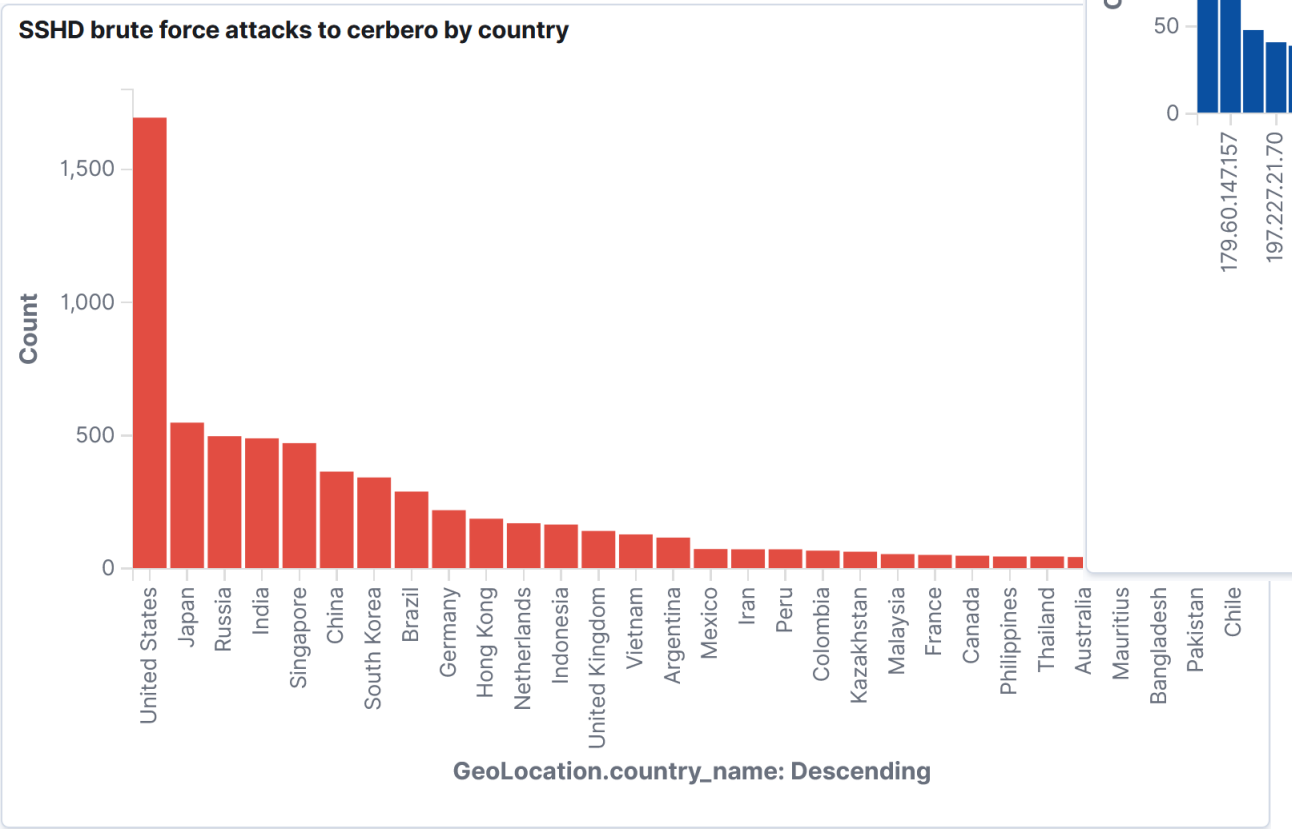
@timestamp	2023-02-12T03:57:28.712Z
GeoLocation.country_name	Peru
GeoLocation.location.lat	-12.0433
GeoLocation.location.lon	-77.0283
_id	_VDFQ4YB_qD0gE1yXi5m
agent.id	001
agent.ip	193.206.157.7
agent.name	cerbero.mib.infn.it
data.dstuser	root
data.srcip	179.6.12.59
decoder.name	sshd
decoder.parent	sshd
full_log	Feb 12 04:57:28 cerbero sshd[19617]: User root from 179.6.12.59 not allowed because listed in DenyUsers

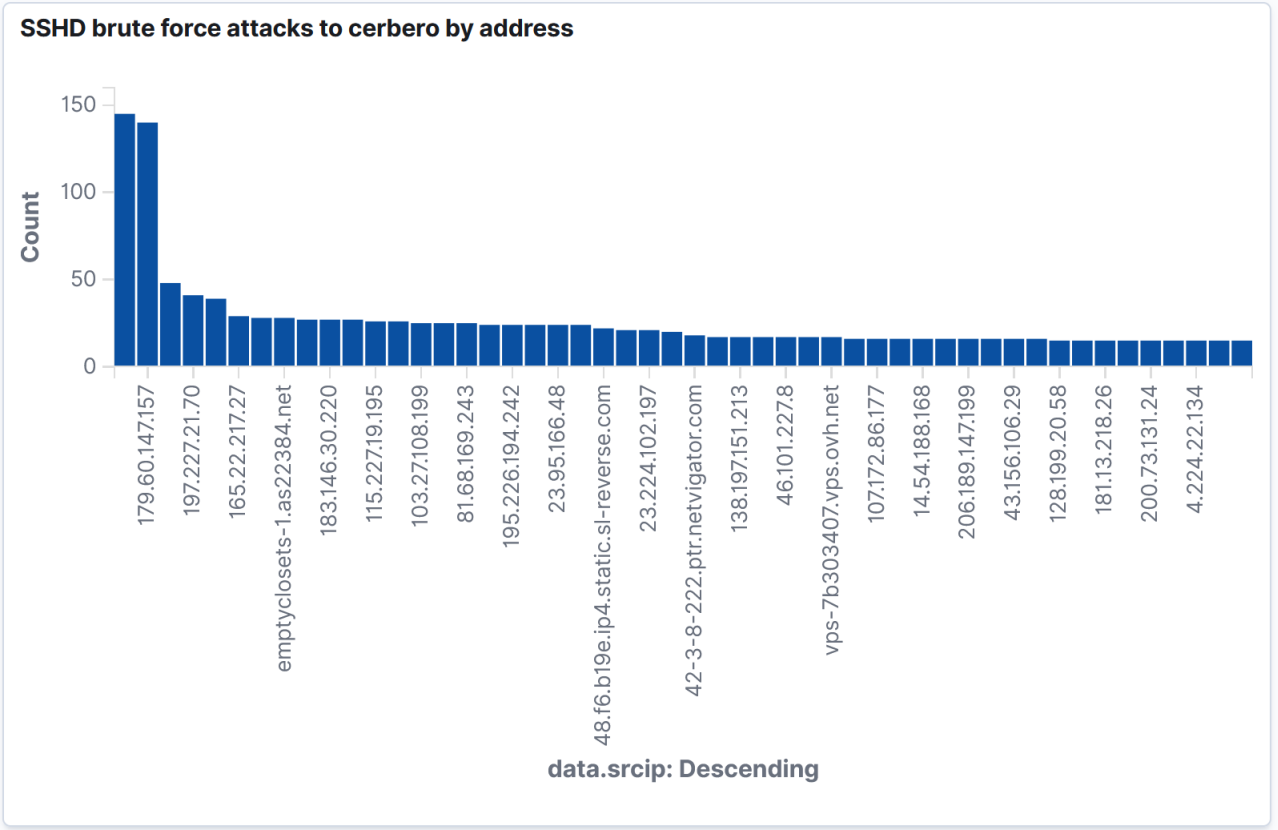
custom dashboards



brute force attacks to cerbero

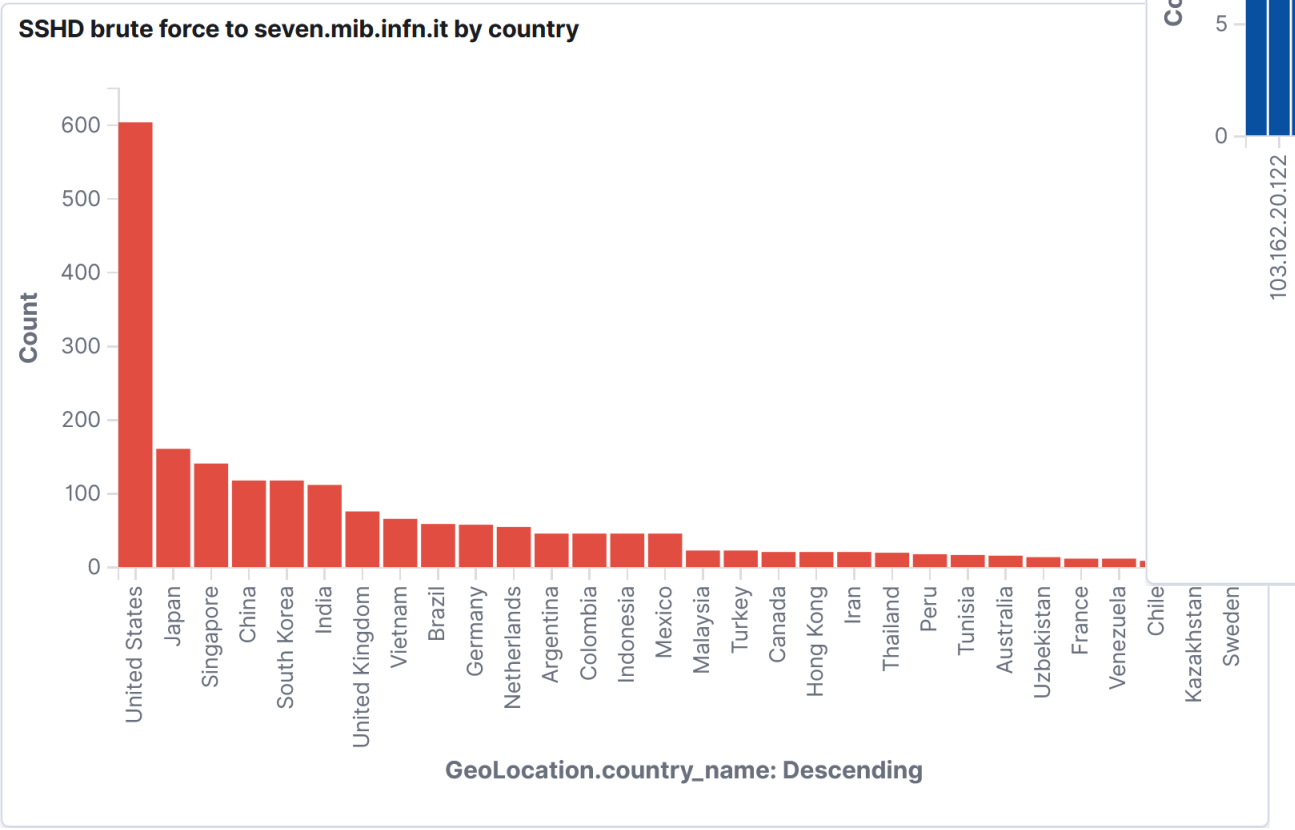
7 days span
fail2ban only

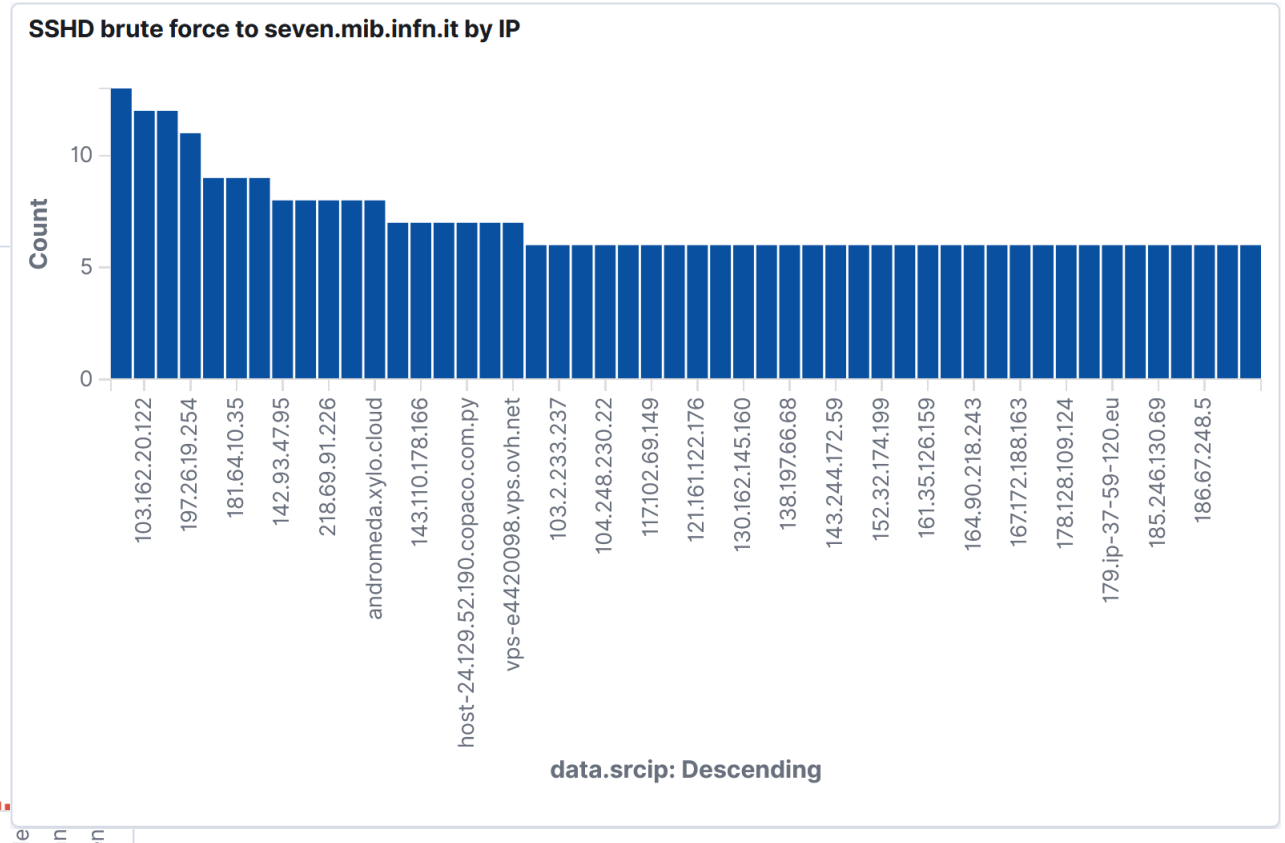




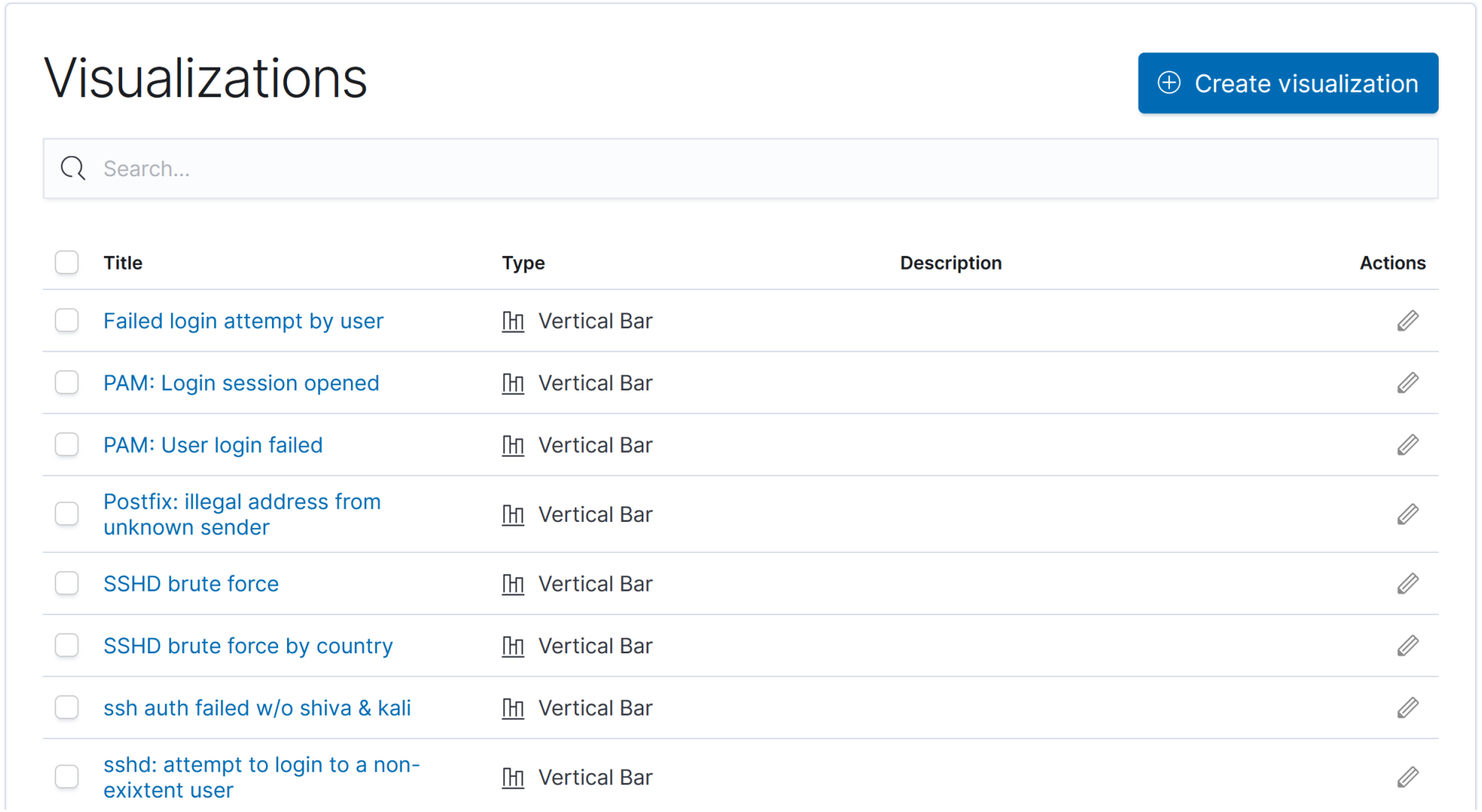
brute force attacks to seven

7 days span
~15 klines ipset blacklist

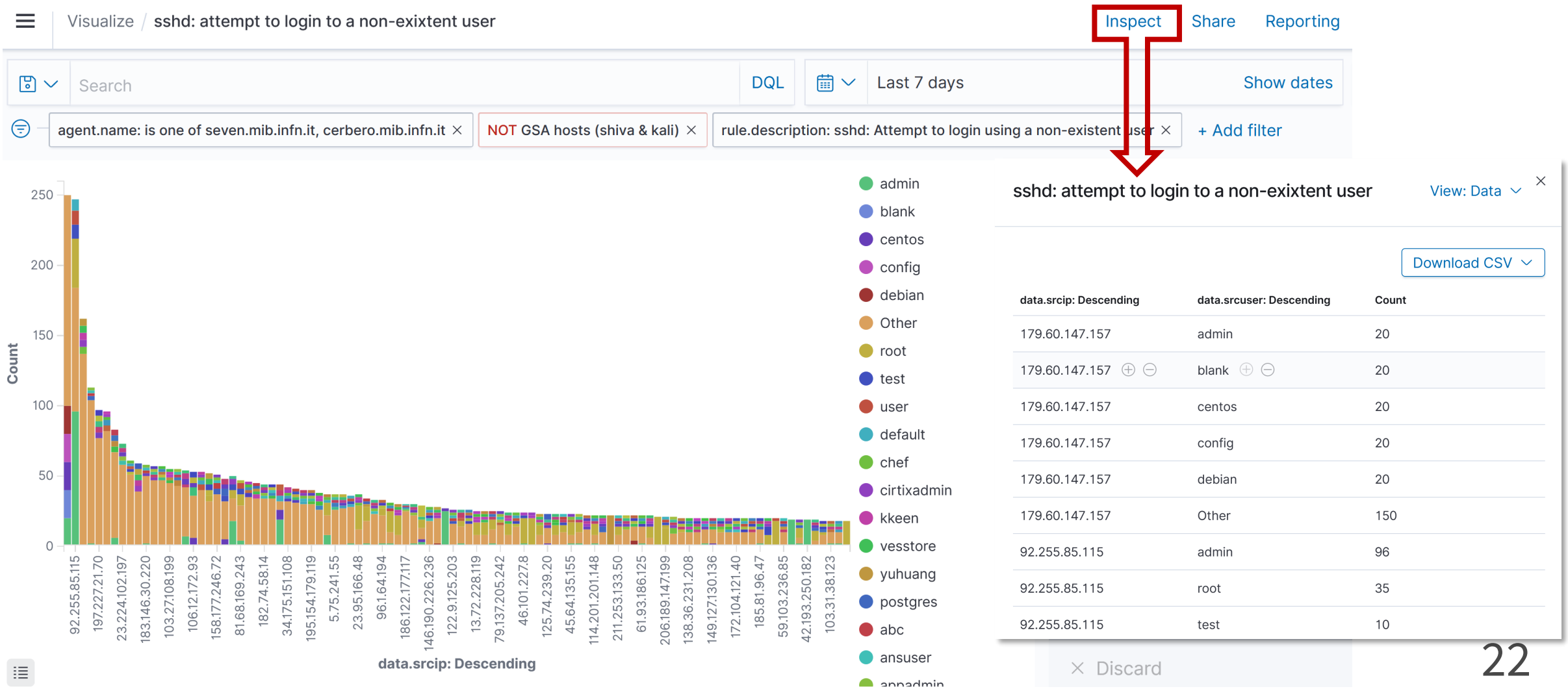




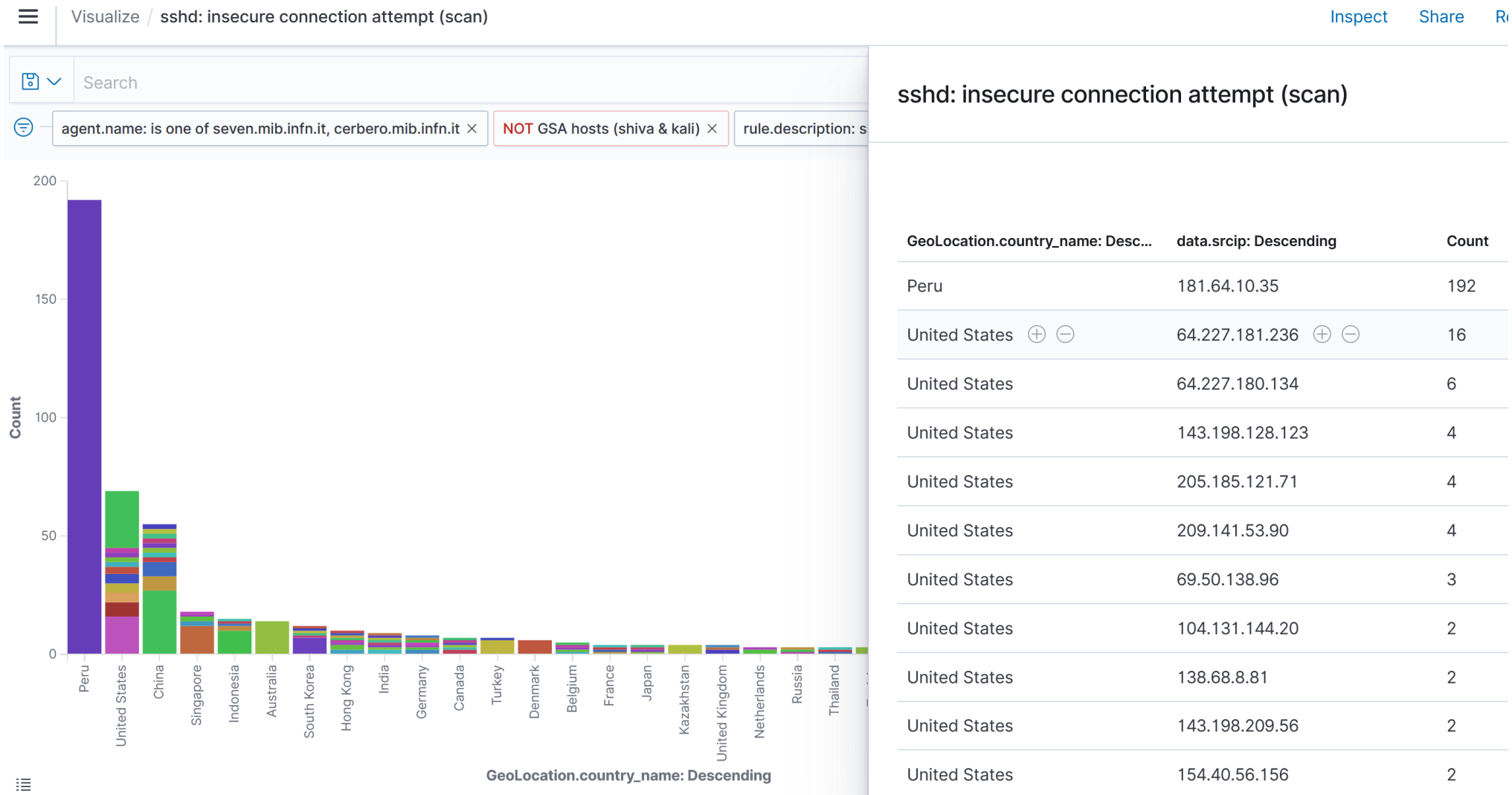
visualizations



visualization example



visualization example



GeoLocation.country_name: Desc...	data.srcip: Descending	Count
Peru	181.64.10.35	192
United States	64.227.181.236	16
United States	64.227.180.134	6
United States	143.198.128.123	4
United States	205.185.121.71	4
United States	209.141.53.90	4
United States	69.50.138.96	3
United States	104.131.144.20	2
United States	138.68.8.81	2
United States	143.198.209.56	2
United States	154.40.56.156	2

valutazione/things to do

Strumento potentissimo (e raccomandato caldamente) per:

- **analisi log/eventi di sicurezza**
- **controllo integrità**
- **compliance/aderenza a policy**
- **…**

Una montagna di cose da fare:

- **fondamentale: allarmistica/reporting** - si possono definire monitor/trigger/alert
- integrazione in ambiente standard – bisogna capire quali log si possono dare in pasto a wazuh out of the box con una ragionevole certezze di poterli usare effiacemente
- definizione setup fisico/virtuale standard
- studio gerarchia di server per deployment distribuito (?)