GREYCORTEX
MENDEL

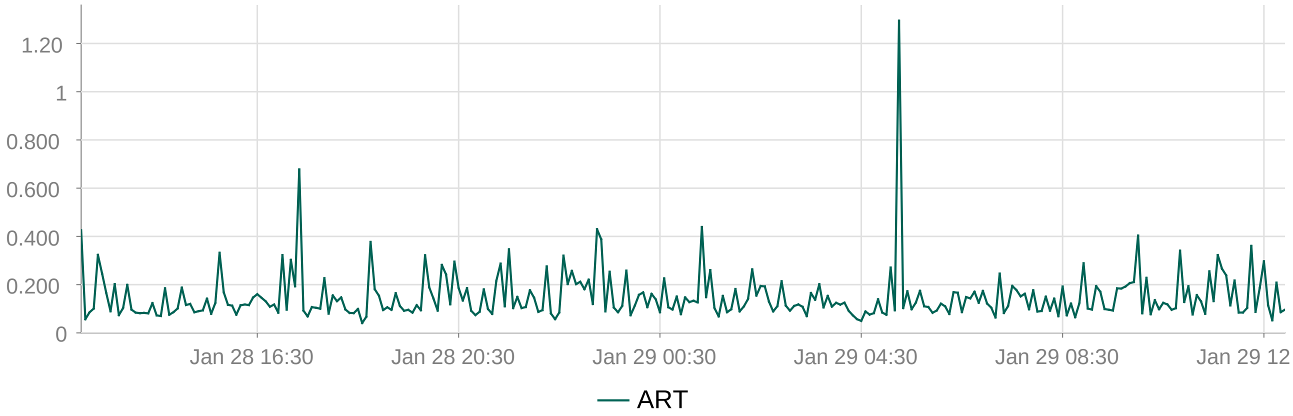
Sample report

2024-01-28 13:00 CET - 2024-01-29 13:00 CET

www.greycortex.com

Application Response Time

The line chart shows application response time measured in seconds.



CPU Detailed Overview

The chart shows utilization of CPU with detailed information about load of processes.

No records found.

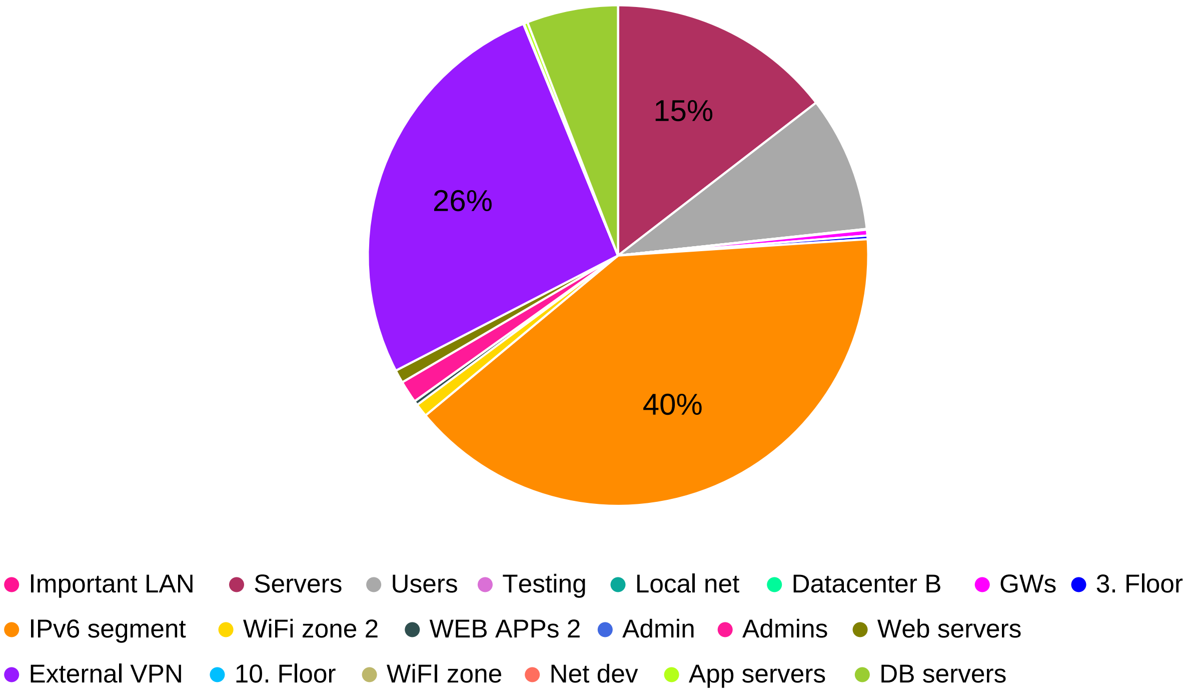
CPU Overview

The chart shows utilization of CPU. Cores value indicates the number of physical cores. The load represents total load of all cores including virtual threads.

No records found.

Data Traffic by Subnets

The pie chart shows data traffic by subnets.



Disk Detailed Overview

The chart shows detailed information about space usage of system partitions.

No records found.

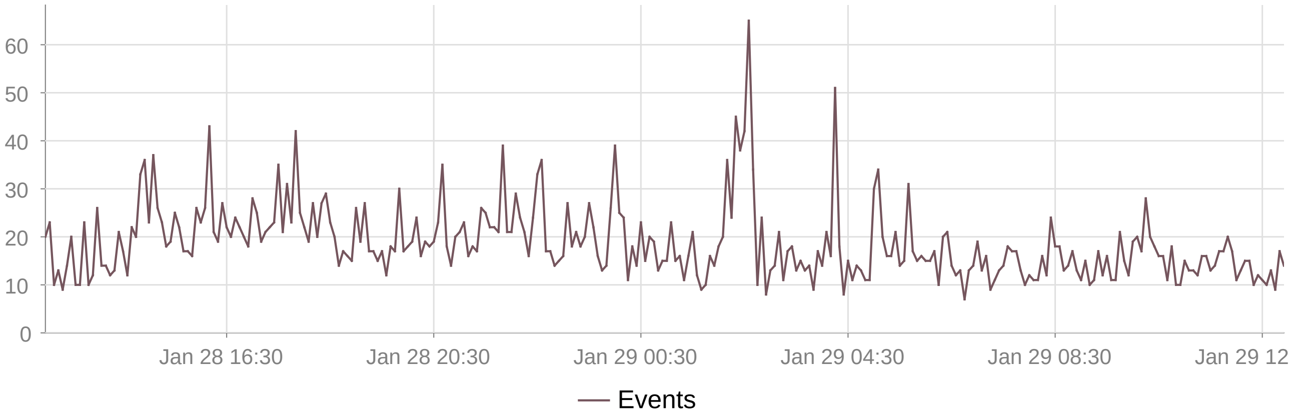
Disk Overview

The chart shows information about database space and its usage.

No records found.

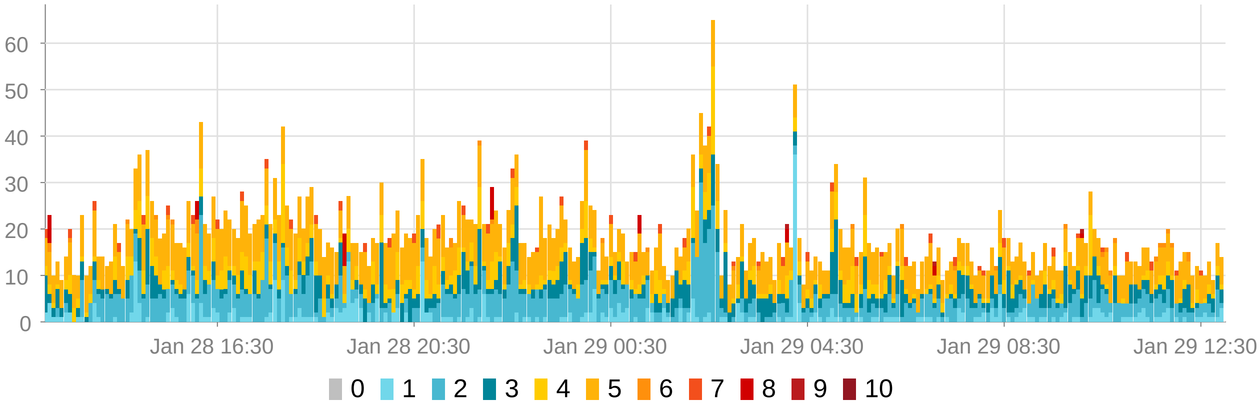
Events

The line chart shows number of detected events.



Events with severities

The bar chart shows number of events by severity.



Memory Detailed Overview

The chart shows detailed information of memory usage by processes.

No records found.

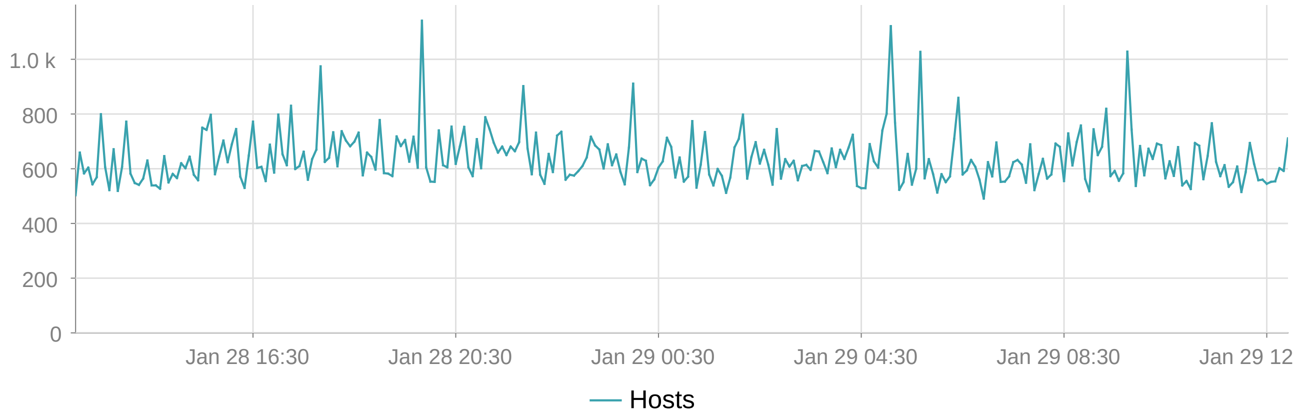
Memory Overview

The chart shows information about memory usage. It shows the total available RAM, the amount of used memory and also the maximum size of swap and the amount of swapped memory.

No records found.

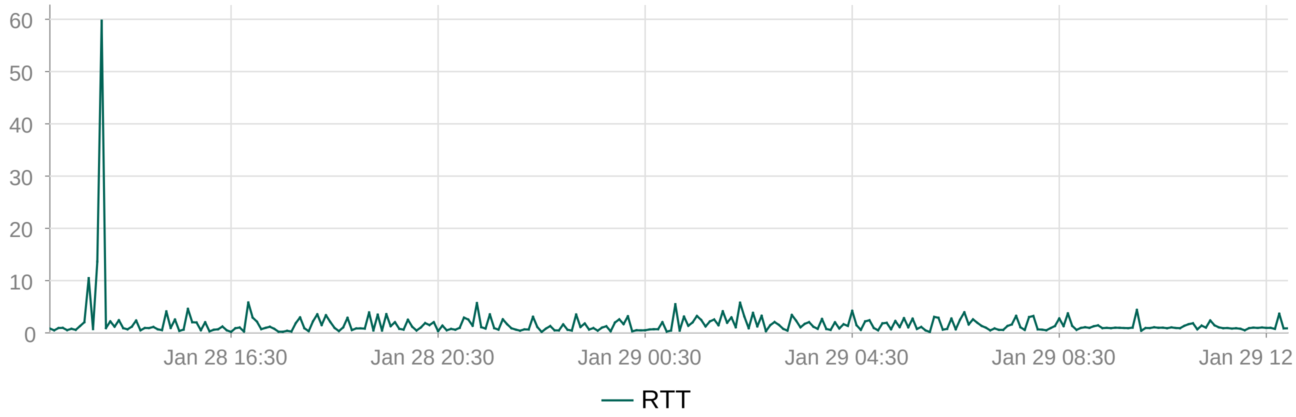
Number of Monitored Hosts

The line chart shows the number of active hosts on the network.



Round Trip Time

The line chart shows round trip time measured in seconds.



Top Countries

The table shows countries ordered by its risk. Risk calculation is based on severity and number of events.

Risk	Country	Hosts	Events
Critical	Romania	6	9
High	Czech Republic	11	83
High	Russian Federation	20	30
High	Ukraine	8	29

Risk	Country	Hosts	Events
High	Belgium	8	15
High	Japan	6	15
High	Italy	4	4
High	South Africa	1	2
High	Canada	1	1
High	Europe	1	1

Top Countries by Traffic

The table shows top countries ordered by their data traffic.

Country	Flows	Traffic
France	237.6 k	104.6 G
Czech Republic	558.7 k	76.4 G
Netherlands	83.1 k	58.0 G
Russian Federation	106.6 k	17.6 G
Ireland	401.8 k	9.1 G
Poland	25.8 k	6.9 G
United States	1.2 M	6.5 G
Germany	11.8 M	4.4 G
Slovakia	65.3 k	4.3 G
United Kingdom	80.7 k	2.3 G

Top Destination Countries

The table shows destination countries ordered by its risk. Destination means target country in occurred events. Risk calculation is based on severity and number of events.

Risk	Country	Hosts	Events
Critical	Romania	1	3

Risk	Country	Hosts	Events
High	Belgium	3	9
High	Czech Republic	5	8
High	Russian Federation	4	4
High	South Africa	1	2
High	Canada	1	1
High	Europe	1	1
High	Greece	1	1
High	Italy	1	1
High	Japan	1	1

Top Destination Hosts

The table shows destination hosts ordered by its risk. The destination means the hosts that are targeted in the event. Risk calculation is based on severity and number of events.

Risk	Host	Events
Medium	10.22.10.163	4
Medium	10.22.10.249	2
Medium	10.22.9.196	1
Medium	hat-mehit (10.22.9.198)	1
Medium	atum (10.22.182.127)	1
Medium	10.22.15.234	19
Medium	10.22.15.12	3
Medium	10.22.181.107	3
Medium	10.22.9.213	1
Low	thales (fd00:dead:beef:e811:0:48a7:0:9d24)	47

Top Events

The table shows events ordered by severity and their number of occurrences. Hosts column means how many hosts are engaged in the event.

Severity	Name	Hosts	Occurrences
9	Periodic: Repetitive Connections (every 30 minutes in 6 hours)	2	3
8	Periodic: Repetitive Connections (every 30 minutes in 6 hours)	29	34
7	Discovery: Forbidden remote service (forbidden by policies)	3	87
7	Trojan: IRC Nick change on non-standard port	2	1
6	Outlier: Data at Host	3	9
6	Periodic: Possible Malware Check-in on HTTP/S	7	6
6	Outlier: Incoming data at Host	3	5
6	Telnet: TELNET login failed	6	4
6	P2P: TOR 1.0 Server Key Retrieval	2	3
6	Discovery: New Host (forbidden by policies)	3	2

Top External Destinations

The table shows external hosts, when internal hosts originated communication. External hosts are ordered by its risk.

Risk	Host	Events
Critical	🇷🇴 79.118.182.202	3
High	🇧🇪 2a02:a03f:2e7f:ea00:689f:96f6:e3:d5d7	6
High	🇿🇦 105.233.73.61	2
High	🇧🇪 2a02:a03f:1485:ab00:69cf:3785:d62a:f44c	2
High	🇨🇦 2001:56a:f102:ef00:e55c:5fec:14cd:af4c	1
High	🇺🇦 2001:67c:f8:1224:a4ec:febe:8dfe:2746	1
High	🇵🇹 2001:8a0:70d1:f401:fd33:5f4:266b:69ca	1
High	🇮🇹 2001:b07:6449:a591:c88a:4a70:265a:f410	1
High	🇪🇺 2001:2002:4e47:6162:2d13:c578:9d0c:e48	1
High	2002:54f:c047::54f:c047	1

Top External Hosts

The table shows external hosts ordered by its risk. Risk calculation is based on severity and number of events.

Risk	Host	Events
Critical	79.118.182.202	3
High	2a02:a03f:2e7f:ea00:689f:96f6:e3:d5d7	6
High	105.233.73.61	2
High	2a02:a03f:1485:ab00:69cf:3785:d62a:f44c	2
High	2001:56a:f102:ef00:e55c:5fec:14cd:af4c	1
High	2001:67c:f8:1224:a4ec:febe:8dfe:2746	1
High	2001:8a0:70d1:f401:fd33:5f4:266b:69ca	1
High	2001:b07:6449:a591:c88a:4a70:265a:f410	1
High	2001:2002:4e47:6162:2d13:c578:9d0c:e48	1
High	240d:1a:180:7700:ca2a:14ff:fe55:ac1b	1

Top External Sources

The table shows external hosts, which originated communication with internal hosts. External hosts are ordered by its risk.

Risk	Host	Events
Medium	112.167.217.22	7
Medium	68.102.166.186	2
Medium	122.54.145.102	2
Medium	175.210.24.232	2
Medium	220.132.72.63	2
Medium	119.246.23.83	9
Medium	169.54.233.124	9
Medium	113.236.117.187	8
Medium	123.193.228.191	6

Risk	Host	Events
Medium	🇹🇼 123.195.253.108	6

Top Hosts by Risk

The table shows hosts ordered by its risk. Risk calculation is based on severity and number of events.

Risk	Host	Events
Critical	bes.greycortex.com (10.22.182.253)	4
High	fd00:dead:beef:e8d:5f76:dbff:fb58:d218	32
High	peitha.greycortex.com (10.22.8.250)	2
High	anhur.greycortex.com (10.22.10.107)	648
High	crios.greycortex.com (10.22.10.246)	40
High	10.22.182.143	2
Medium	jiangyin.greycortex.com (10.22.8.85)	945
Medium	bellerophon.greycortex.com (10.22.10.242)	18
Medium	10.22.10.163	4
Medium	10.22.11.109	4

Top Hosts by Traffic

The table shows hosts ordered by network traffic. Highest network traffic is on the top and the number of the rows is adjustable.

Host	Traffic
seasmoke.greycortex.com (10.22.14.27)	103.19 G
harvest.greycortex.com (fd00:dead:beef:e811:0:48a7:0:3e8)	74.43 G
edmure.greycortex.com (fd00:dead:beef:e811:0:48a7:0:1129)	42.28 G
eurus.greycortex.com (10.22.176.33)	25.44 G
fd00:dead:beef:4f3:c27b:2eed:45b:cb16	14.35 G
bellerophon.greycortex.com (10.22.10.242)	13.32 G
fd00:dead:beef:4ff0:c97:f0a1:4d8a:fc47	12.51 G
kuhn.greycortex.com (10.22.15.195)	10.91 G

Host	Traffic
aristotle.greycortex.com (10.22.15.229)	8.28 G
fd00:dead:beef:3df9:8bec:bea8:8cd0:b917	8.21 G

Top Hosts by Traffic at Mail Services

The table shows hosts ordered by highest traffic at mail services (IMAP, IMAPS, POP3, SPOP3, SMTP, SMTPS).

Host	Service	Traffic
larissa.greycortex.com (10.22.176.107)	IMAP (143)	452.3 M
larissa.greycortex.com (10.22.176.107)	IMAPS (993)	287.53 M
khons.greycortex.com (10.22.8.224)	IMAPS (993)	241.18 M
fd00:dead:beef:e8d:39d7:4972:9aa3:fb8	IMAPS (993)	50.64 M
khons.greycortex.com (10.22.8.224)	IMAP (143)	37.5 M
khons.greycortex.com (10.22.8.224)	SMTP (25)	36.69 M
fd00:dead:beef:e8d:e231:407d:fc13:f057	POP3S (995)	19.03 M
fd00:dead:beef:a85b:b265:8ef2:ca55:2a2	IMAP (143)	17.19 M
fd00:dead:beef:a85b:70c0:7518:462c:61f0	IMAPS (993)	14.92 M
hemsut.greycortex.com (10.22.11.168)	IMAPS (993)	13.43 M

Top Hosts by Traffic at Web Services

The table shows hosts ordered by highest traffic at web services (HTTP or HTTPS).

Host	Service	Traffic
eurus.greycortex.com (10.22.176.33)	HTTPS (443)	21.26 G
kuhn.greycortex.com (10.22.15.195)	HTTPS (443)	10.91 G
aristotle.greycortex.com (10.22.15.229)	HTTPS (443)	8.28 G
fd00:dead:beef:3df9:8bec:bea8:8cd0:b917	HTTPS (443)	8.21 G
antheia.greycortex.com (10.22.15.73)	HTTPS (443)	8.1 G
persephone.greycortex.com (10.22.15.20)	HTTPS (443)	8.05 G
buto.greycortex.com (10.22.176.147)	HTTP (80)	7.89 G

Host	Service	Traffic
clotho.greycortex.com (10.22.15.156)	HTTPS (443)	7.53 G
eowyn.greycortex.com (10.22.15.55)	HTTPS (443)	7.0 G
nekhbet.greycortex.com (fd00:dead:beef:e8e8:0:48a7:0:64e8)	HTTP (80)	5.88 G

Top Operating Systems

The table shows top operating systems used in the network ordered by the number of hosts on which the system was detected.

Operating system	Hosts
Windows 7/Server 2008 R2 (NT 6.1)	522
Windows 10/Server 2016/Server 2019 (NT 10.0)	141
Windows Vista/Server 2008 (NT 6.0)	58
Linux	57
Windows 8.1/Server 2012/R2 (NT 6.3)	50
Linux Debian based	33
Windows 8/Server 2012 (NT 6.2)	13
Apple iOS	7
Windows 2000/XP/Server 2003 (NT 5.x)	6
Android 4	6

Top Sensors

The table shows top sensors ordered by number of events.

Severity	Sensor	Events
9	demo	5.4 k

Top Services by Risk

The table shows services by its risk. Risk is based on severity and number of events. Hosts column means how many hosts are engaged in the event.

Risk	Service	Hosts	Events
Critical	32738	1	3
High	49001	18	18
High	51413	6	12
High	32744	1	2
High	11444	1	1
High	12525	1	1
High	7773	1	48
High	XMPP (5269)	1	38
High	80	6	26
High	81	1	8

Top Services by Traffic

The table shows services ordered by highest data traffic.

Service	Type	Traffic
HTTPS (443)	LOCAL	111.18 G
RTSP (554)	LOCAL	104.65 G
Rsync (873)	LOCAL	87.66 G
HTTPS (443)	REMOTE	62.48 G
NDL-AAS (3128)	LOCAL	39.81 G
NDL-AAS (3128)	REMOTE	39.8 G
HTTP (80)	REMOTE	19.79 G
HTTP (80)	LOCAL	16.56 G
SSH (22)	LOCAL	8.75 G
Rsync (873)	REMOTE	1.17 G

Top Source Countries

The table shows source countries ordered by its risk. Source means origin country in occurred events. Risk calculation is based on severity and number of events.

Risk	Country	Hosts	Events
Medium	United States	54	251
Medium	Taiwan	82	136
Medium	Korea, Republic of	23	34
Medium	Philippines	2	3
Medium	China	100	396
Medium	Hong Kong	16	61
Medium	Ukraine	7	28
Medium	Brazil	13	21
Medium	Romania	5	6
Medium	Mexico	5	5

Top Source Hosts

The table shows source hosts ordered by its risk. Source means the hosts that originated the event. Risk calculation is based on severity and number of events.

Risk	Host	Events
Critical	bes (10.22.182.253)	4
High	fd00:dead:beef:e8d:5f76:dbff:fb58:d218	32
High	peitha (10.22.8.250)	2
High	anhur (10.22.10.107)	647
High	crios (10.22.10.246)	40
High	10.22.182.143	2
Medium	jiangyin (10.22.8.85)	932
Medium	bellerophon (10.22.10.242)	18
Medium	10.22.11.109	4
Medium	imhotep (fd00:dead:beef:e8d:a6d3:e9e3:fc2a:5f36)	2

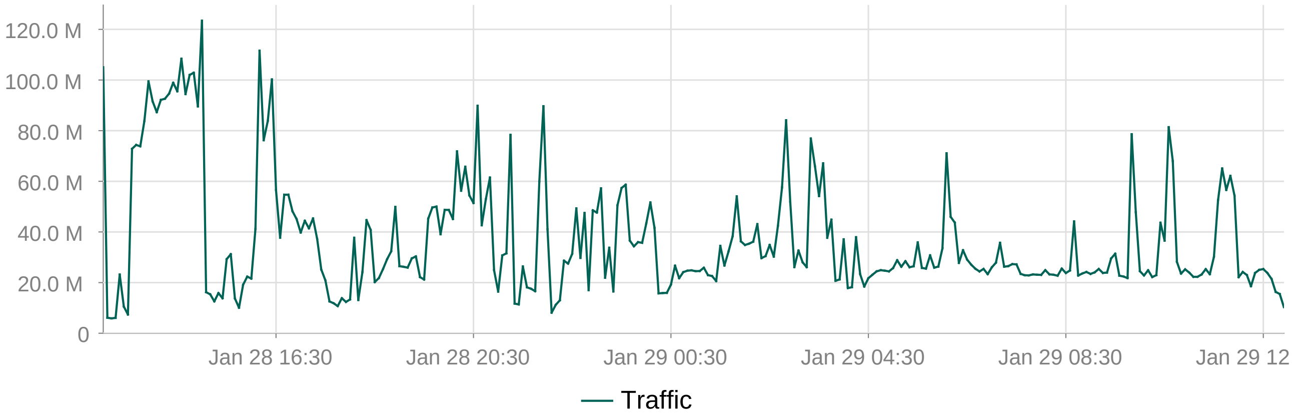
Top Users by Events

The table shows users ordered by number of events occurred related to a user.

Risk	User	Events
Info	Jessica Joseph (jjoseph_4801)	2
Info	Joe Medina (jmedina_988)	1
Info	Kelly Howard (khoward_3630)	1

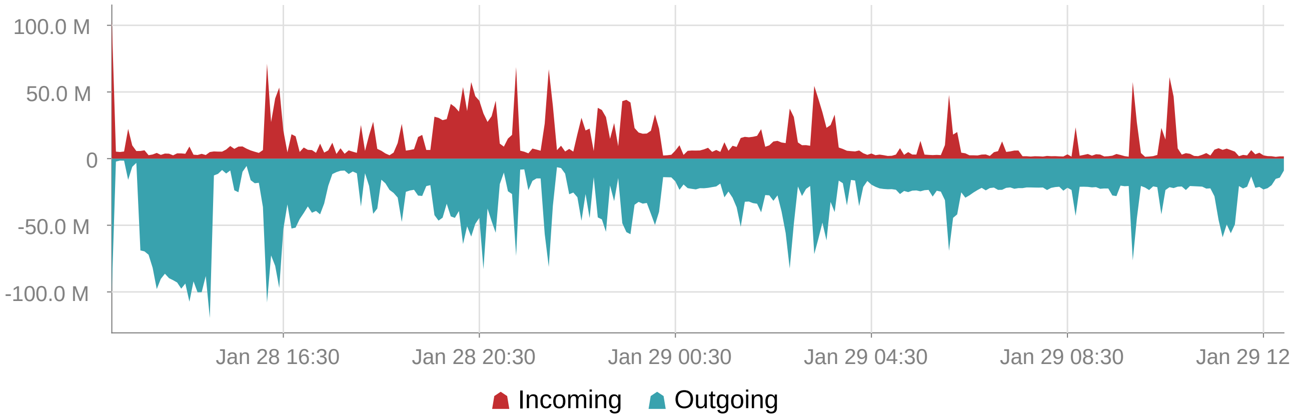
Total Network Traffic

The line chart shows overall network traffic.



Traffic by Direction

The chart shows incoming and outgoing network traffic.



Traffic Detailed Overview

The chart shows detailed information about incoming traffic to the network interfaces.

No records found.

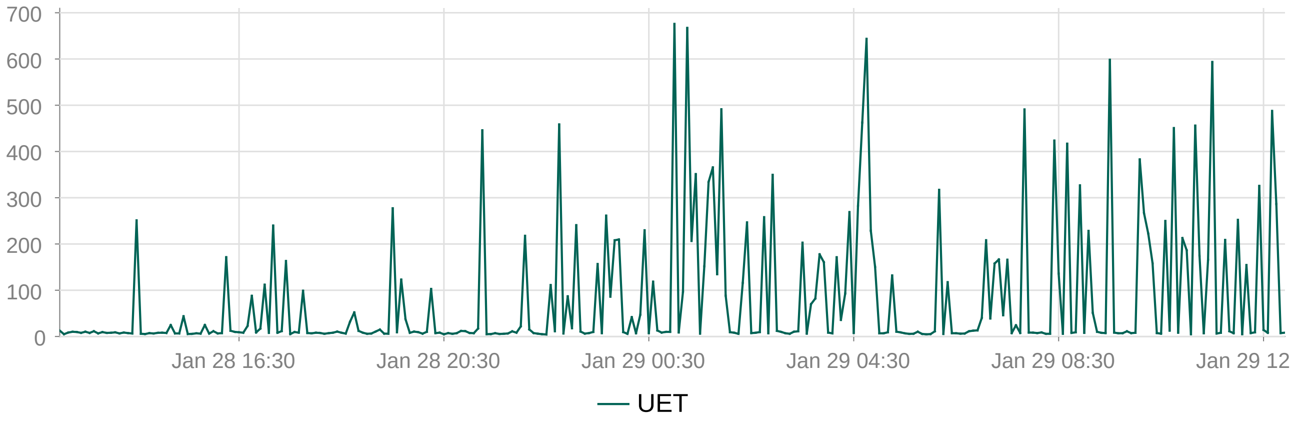
Traffic Overview

The chart shows how much traffic is received on the network interface. SPAN is traffic measured on mirrored ports and Management shows amount of traffic received on the management interface.

No records found.

User Experience Time

The line chart shows user experience time measured in seconds.



About this report:

Generated:	2024-01-29 13:20 CET
Sensor:	demo
Interval:	2024-01-28 13:00 CET - 2024-01-29 13:00 CET
Appliance Type:	all-in-one
Licensed To:	test@greycortex.com
License Expiration:	2025-12-31
Current Version:	4.2.0