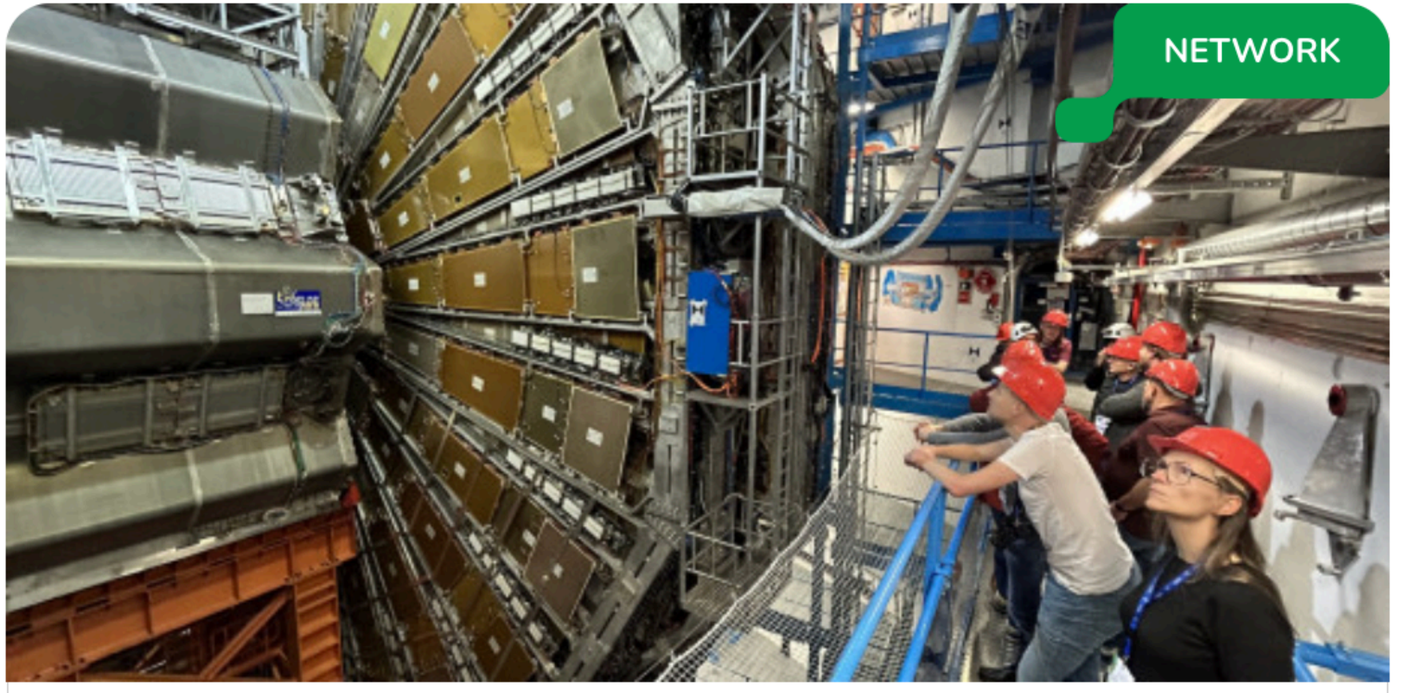
NOC, CERT & SOC

20th SIG-NOC (Helsinki, Finland)

Willem May 7th, 2024


SURF

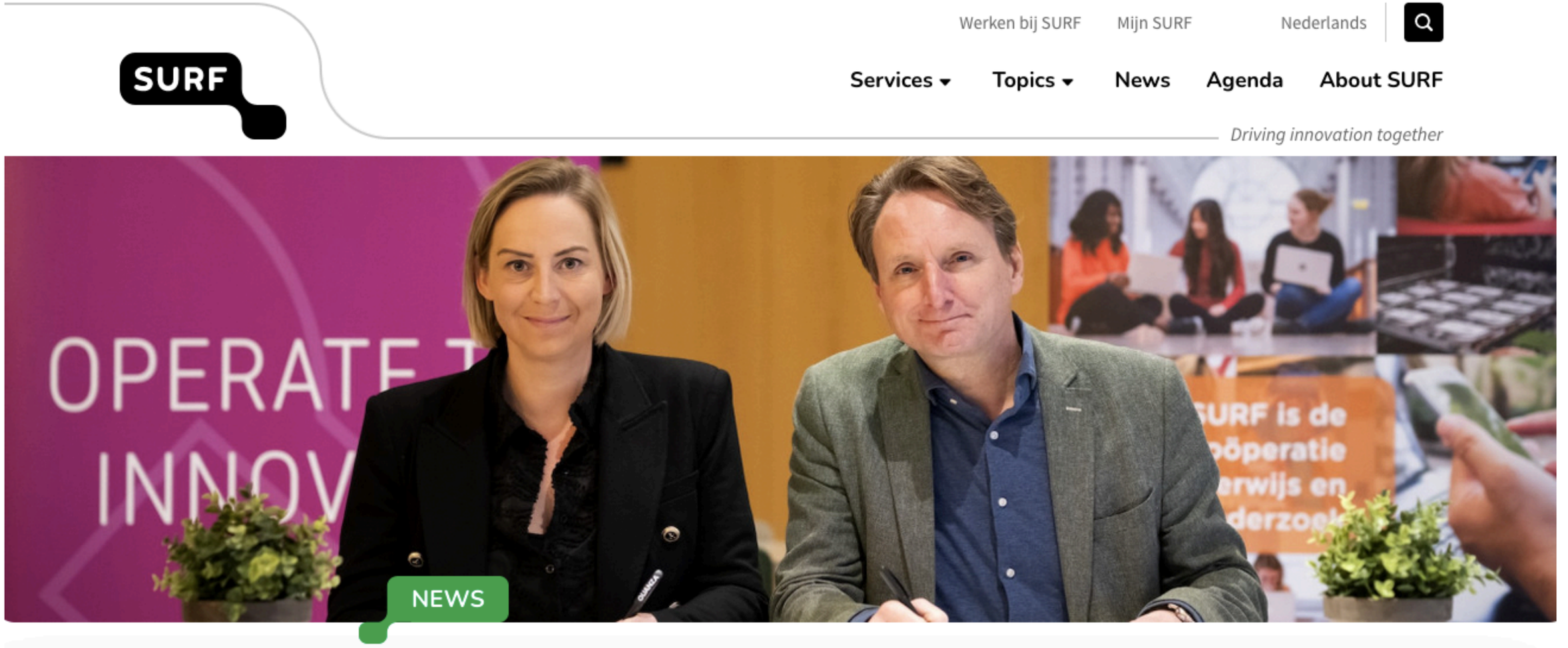


SURF and Nokia achieve data speed of 800Gbit per second on 1648km network connection →

Together with Nokia, Nikhef and CERN, SURF has tested the speed of data transfer between CERN in Geneva and Amsterdam. A data rate of 800Gbit per second was achieved on the 1648-kilometre fibre-optic connection. This means the connection is suitable for the future transmission of large-scale data streams, such as those from CERN's particle accelerator.


icinga


ICINGA
Search ...
Dashboard
Problems 73
Overview
History
1 1 day notifications
A Acknowledged services
E ECI notifications
H host problems
M Misc notifications
N non-BGP notifications
R Recent Acks
Current Incidents
Overdue
Muted
NOC_DASHBOARD
SN8 ACK
SN8 UNACK
Service Problems
CRITICAL Mar 26
bgp_10_13_37_1 on asd001a-jnx-09-tst.dcn.surf.net
10.13.37.1
65.7d idle - AS1104
CRITICAL Mar 26
bgp_210f_dead_beef_cafe__1 on asd001a-jnx-09-tst.dcn.surf.net
210f:dead:beef:cafe::1
65.7d idle - AS1104
CRITICAL Mar 26
bgp_145_125_99_1 on asd001a-jnx-09-tst.dcn.surf.net
145.125.99.1
65.7d idle - AS1140
CRITICAL Mar 26
bgp_145_125_0_49 on asd001a-jnx-09-tst.dcn.surf.net
145.125.0.49
65.7d idle - AS1140
CRITICAL Mar 24
ECI_HEARTBEAT on lightsoft-global
Heartbeat has stopped.
CRITICAL Mar 24
SNMPTRAP on unknown-trap-host
[Host: lo0-0.asd001a-jnx-08-tst.surf.net] ISIS-MIB::.iso.org.dod.in-ter-net.mgmt.mib-2.isisMIB.isisNotifications.isisRejectedAdjacency: isisNotificationSysLevelIndex:level2 isisNotificationCircIfIndex:Gauge32: 582 isisPduFragment:Hex-STRING: 83 14 01 00 11 01 00 00 02 00 00 10 12 40 11 00 1B:00 4B 01
Recently Recovered Services
OK 22m 15s
bgp_2001_7f8_1__a501_5557_1 on ASD001B-JNX-01
2001:7f8:1::a501:5557:1
0h51m established - AS15557 AMS-IX
OK 22m 16s
bgp_80_249_209_147 on ASD001B-JNX-01
CBV3-CO-4.gaoland.net
0h51m established - AS15557 AMS-IX
OK 22m 17s
bgp_2001_7f8_1__a501_5557_1 on ASD002A-JNX-01
2001:7f8:1::a501:5557:1
0h51m established - AS15557 AMS-IX
OK 22m 28s
bgp_80_249_209_147 on ASD002A-JNX-01
CBV3-CO-4.gaoland.net
0h50m established - AS15557 AMS-IX
OK 07:50
OPTICAL_ALARMS on tr001a-a96-01.dcn.surf.net
ok - no active alarms
OK 06:07
ping4 on nso-01.dcn.surf.net
PING OK - Packet loss = 0%, RTA = 0.41 ms
OK 03:03
PROCS on optnms-03.dcn.surf.net
PROCS OK: 989 processes
OK 01:45
bgp_2620_107_4008_44__1 on ASD051C-JNX-01
2620:107:4008:44::1
8h29m established - AS16509


Werken bij SURF
Mijn SURF
Nederlands
SURF
Services
Topics
News
Agenda
About SURF
Driving innovation together
NEWS


ZABBIX


No Internet Connection
Your computer is not connected to the Internet.
OK

When to call whom?

- At the Infrastructure Services Helpdesk you report malfunctions and operational actions related to the SURFnet network and SURFnet services. The SURFnet Helpdesk is always the first point of contact for institutions.
- The SURF NOC is available for questions about pending changes (changes or incidents) for which a ticket number already exists. You can reach the SURFnet NOC during office hours via **noc@surf.nl** and +31 88 787 36 60. Via the ticket number you can directly reach the appropriate NOC employee.

Please note: For disruptions in the local network and for disruptions not related to SURF services, please contact the helpdesk at your own institution.

Team Expert Network Management

Complex network management and special projects on the network are carried out by the Team Expert Network Management (TEN). Complex network management includes, for example, monitoring network capacity and responsibility for security. Major network renovations and complex changes at institutions affiliated to SURF are also carried out by the TEN, in consultation with Quanza.

Mitigation	Detection Engines	Telemetry Sources	Current Traffic Allowed (Estimated)		Current Traffic Blocked (Estimated)	
Enabled	1	4	199,741 Mbps	24,186,071 Packets per Second	0 Mbps	0 Packets per Second

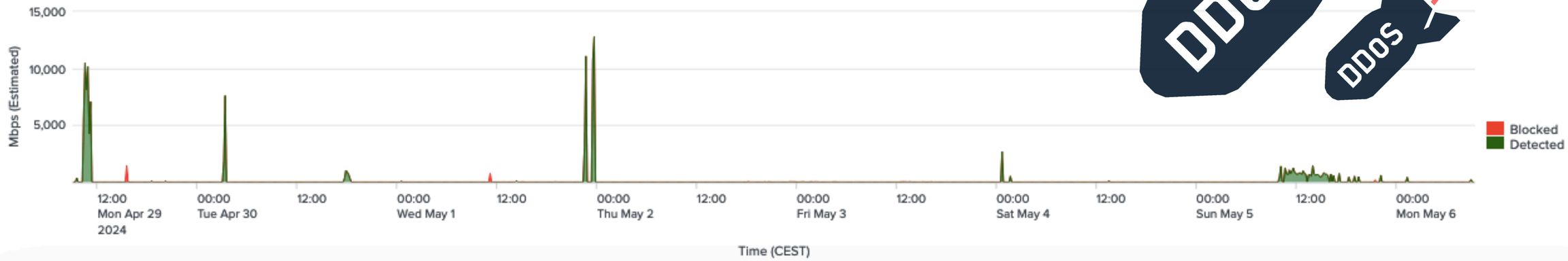
Telemetry

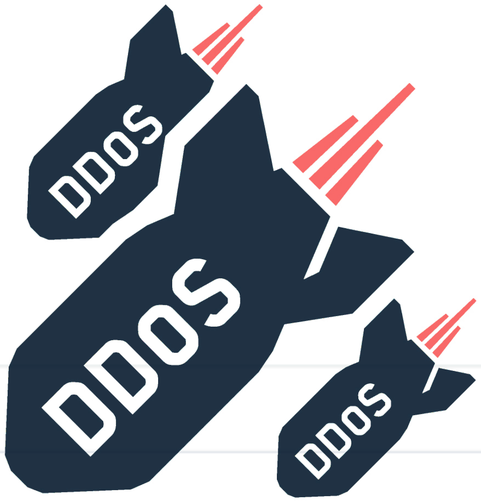
Source: All

Aggregation: by Action

Include Allowed Traffic: Yes | No

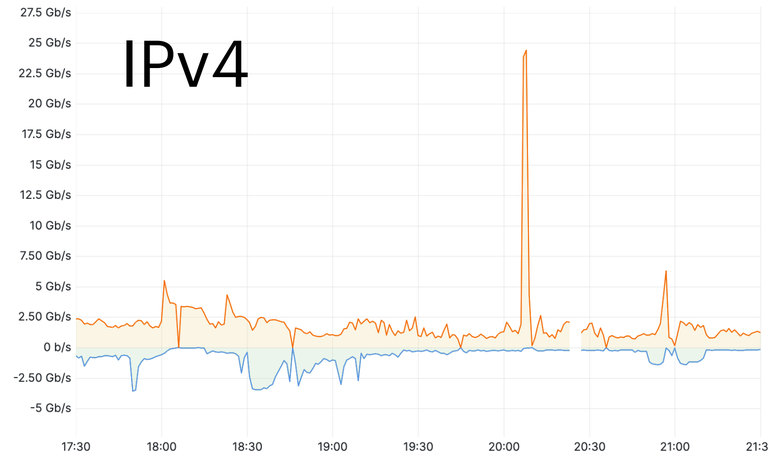
Units: Mbps | PPS





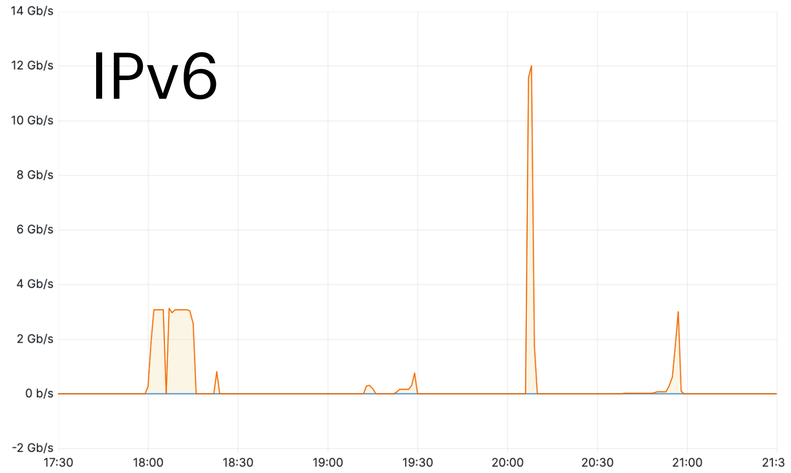

O'NEILL
O'NEILL
O'NEILL

WUR IP: cce8b757-386e-4243-a557-d07617dd94a7 bits/sec

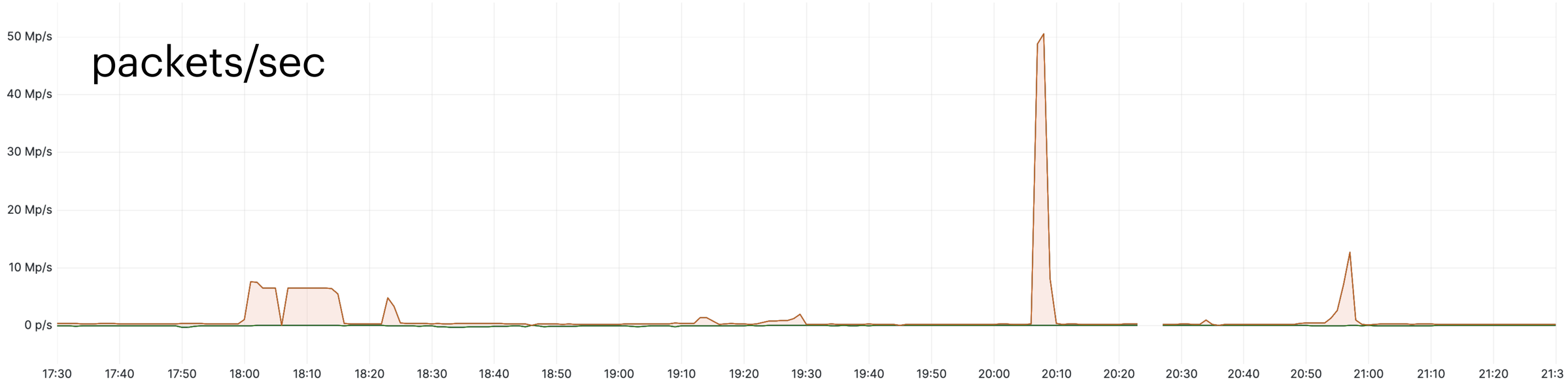


WAGENINGEN
UNIVERSITY & RESEARCH

WUR IPv6: cce8b757-386e-4243-a557-d07617dd94a7 bits/sec

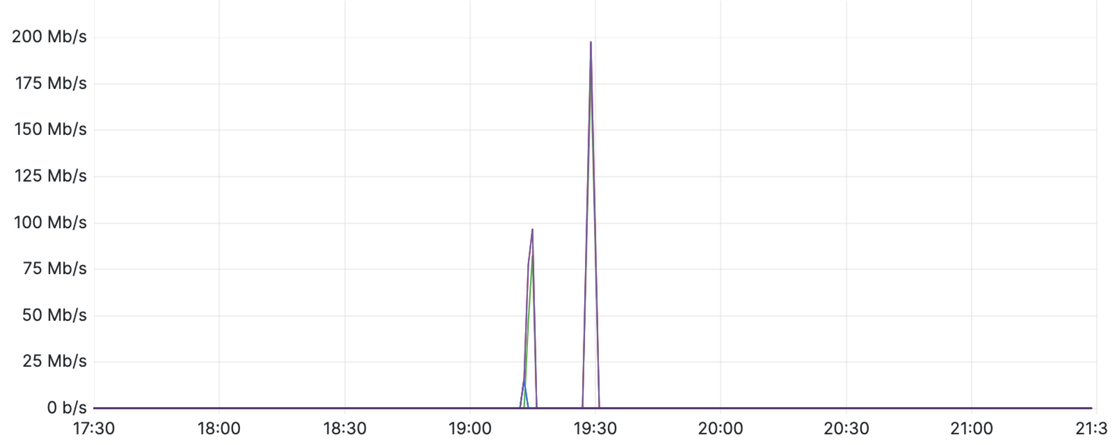


WUR IP: cce8b757-386e-4243-a557-d07617dd94a7 packets



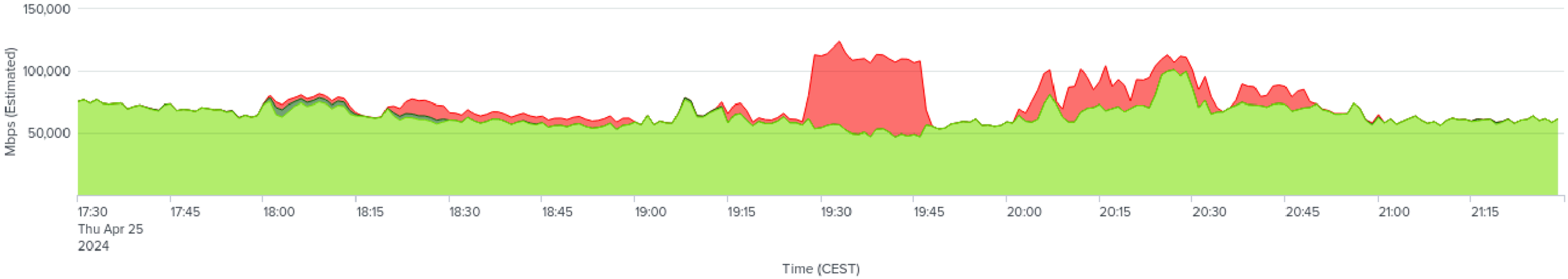
CERT filter hits IPv4

CERT filter hits IPv6



Units

Mbps | PPS



Who ya gonna call?


SURF CERT
2023

SURF SOC

FOX IT
part of nccgroup

DPI

flow

network sensor

LOGs

splunk>

FORWARDER

SIEM

splunk>

SOC

detection

magic

CTMp

FOX IT
part of nccgroup

NOTIFICATION

New incident

VNC server response

misc-activity | web-application-activity | Low risk | Misuse of systems

ALERTS
2

Case created: 2024-01-02, 12:49 CET
Case ID: 60
Instance: Default / surfnet-1/mon0: Amsterdam (DPI sensor)

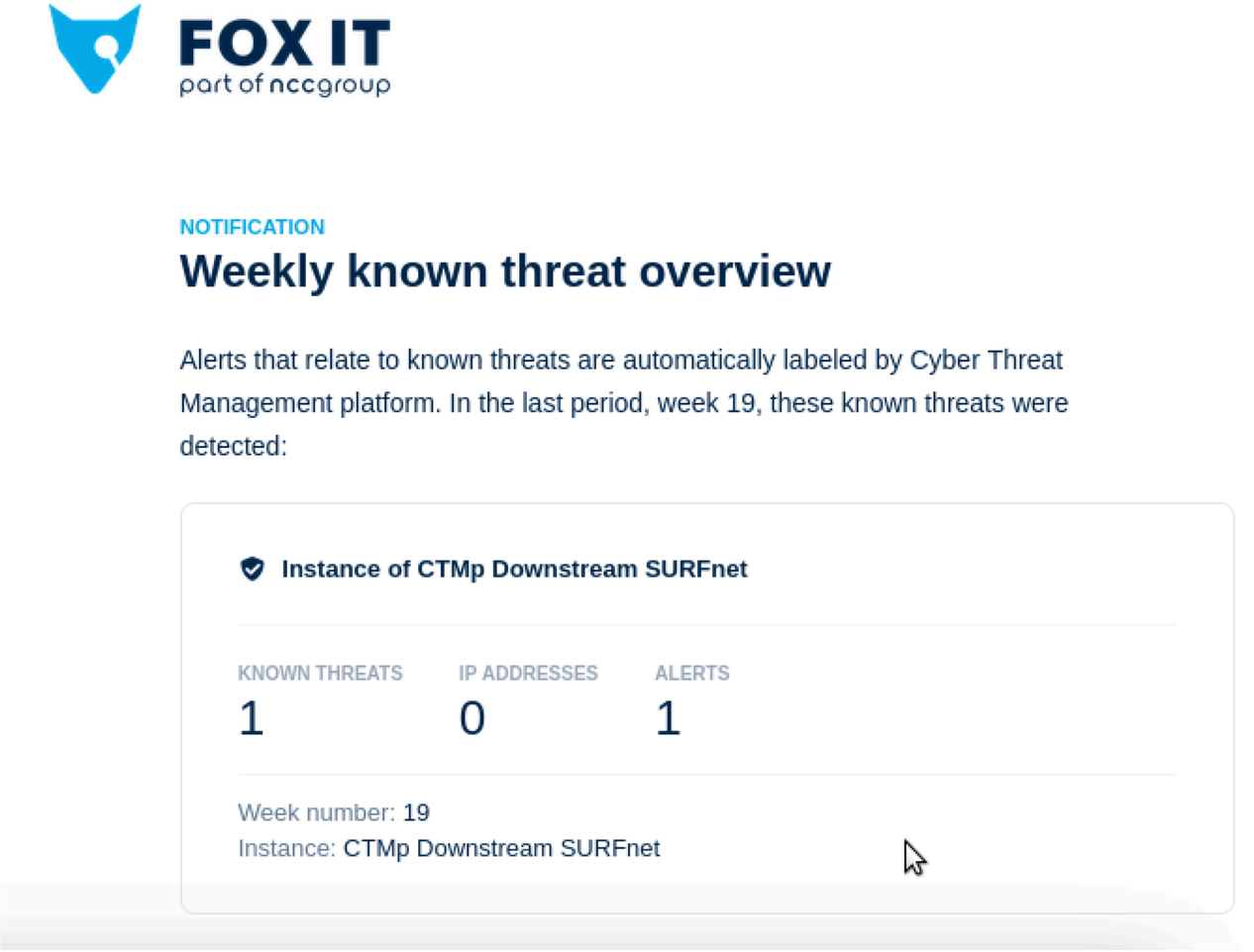
Go to **https://soc.fox-it.com/squo3ad7die3/cases/60/local/** or use the following button to view the case.

View case

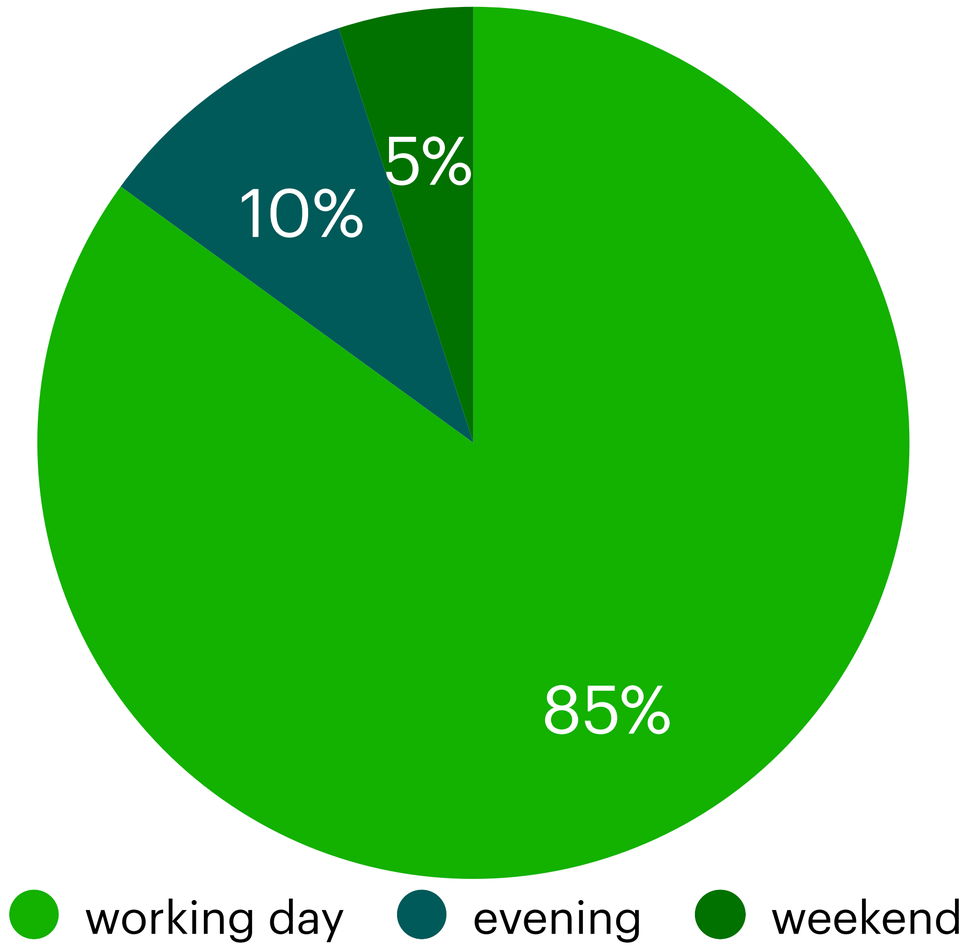
You receive this email because of your notification settings. You can change these settings on **https://soc.fox-it.com/squo3ad7die3/users/68/local/**

Kind regards,
Fox-IT Security Operations Center

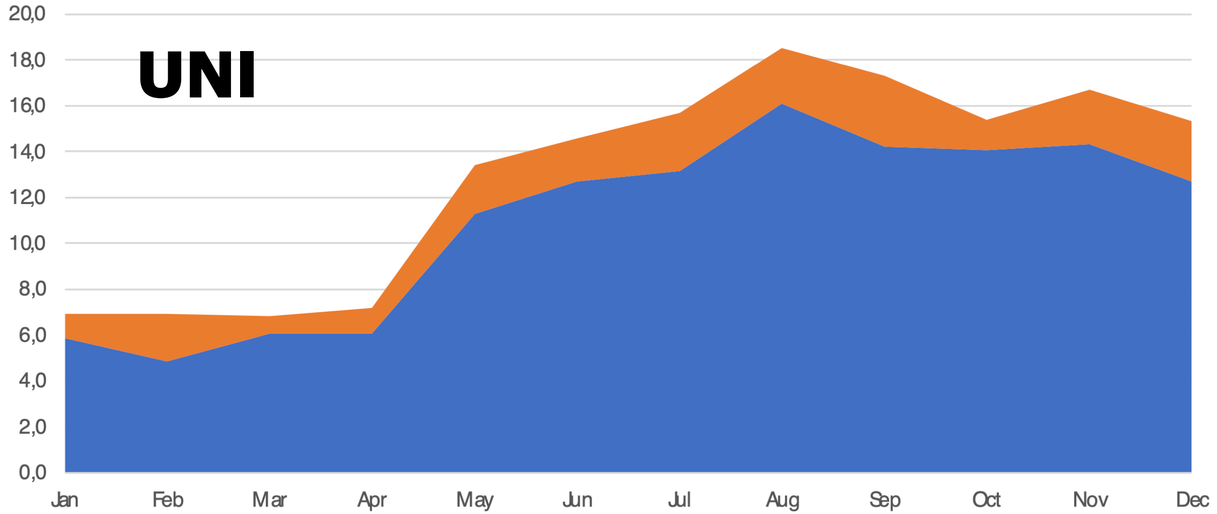
FOR A MORE SECURE SOCIETY

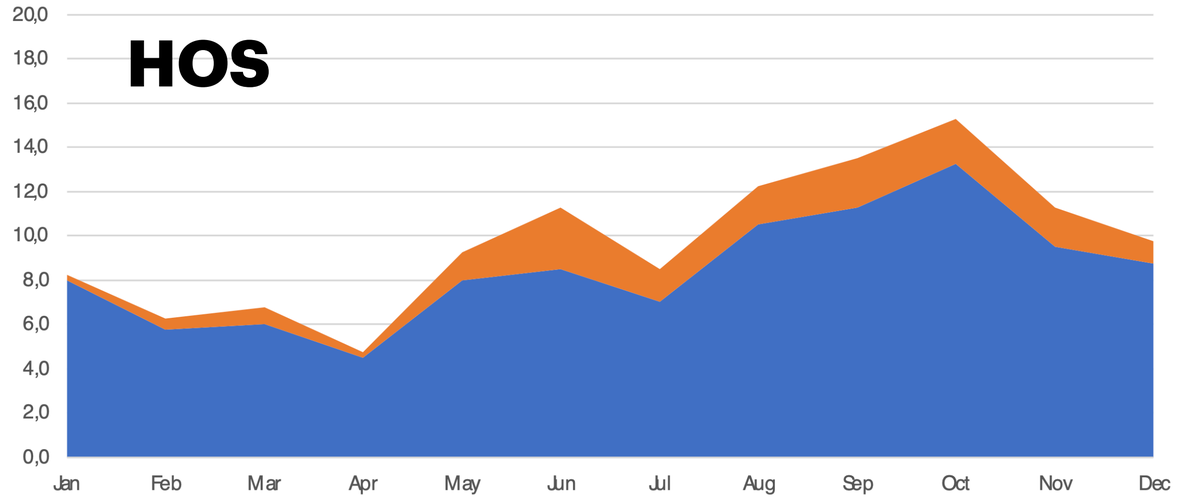


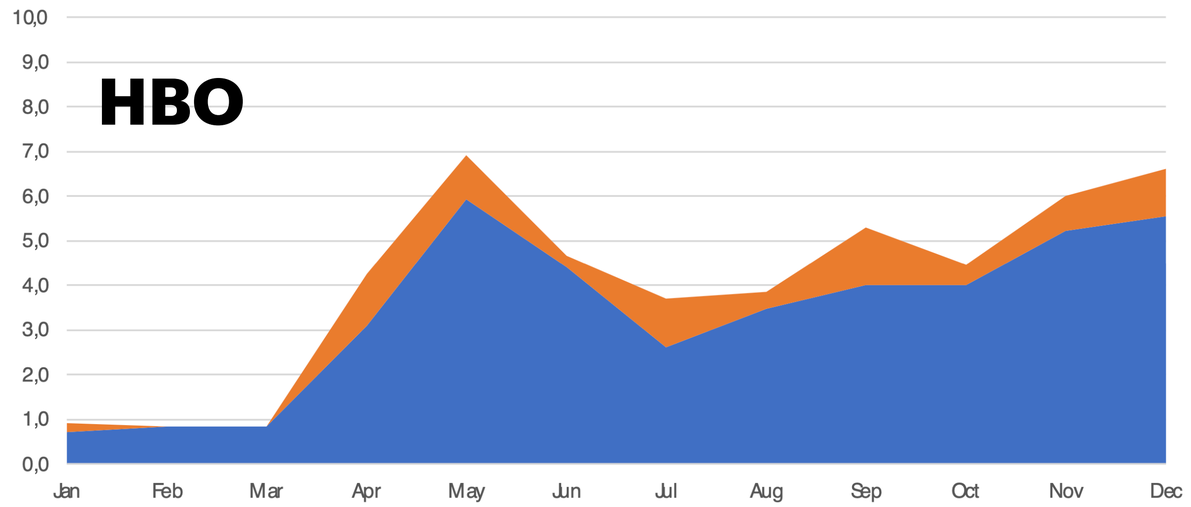

Open
24/7

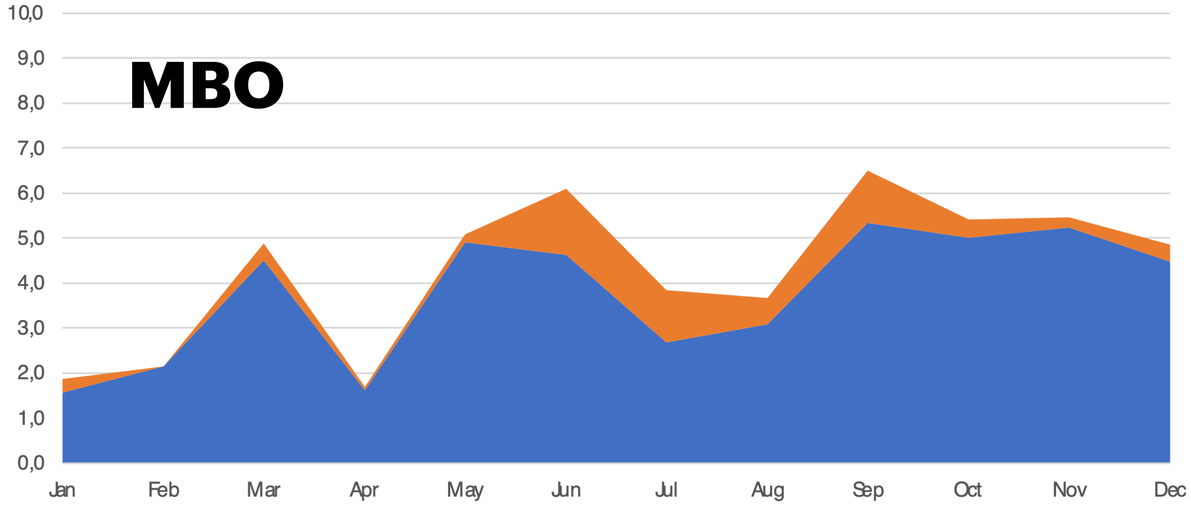

5%
10%
85%
working day
evening
weekend

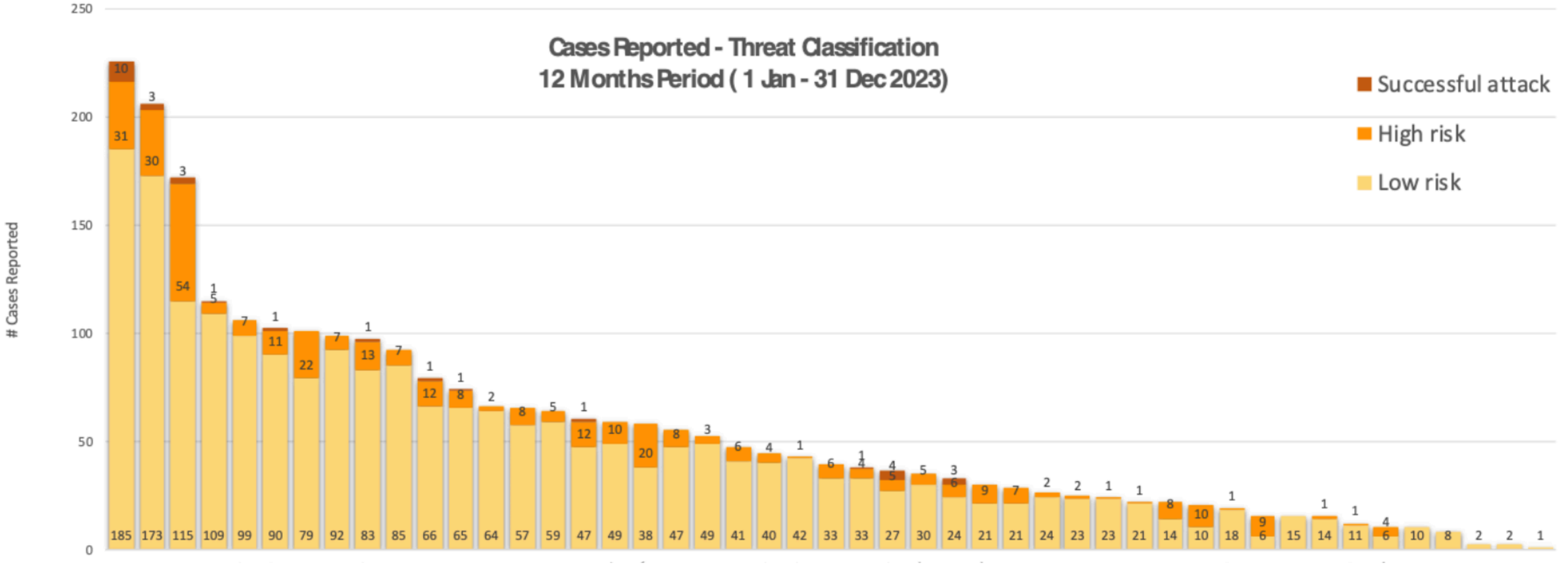
Incidents 2023





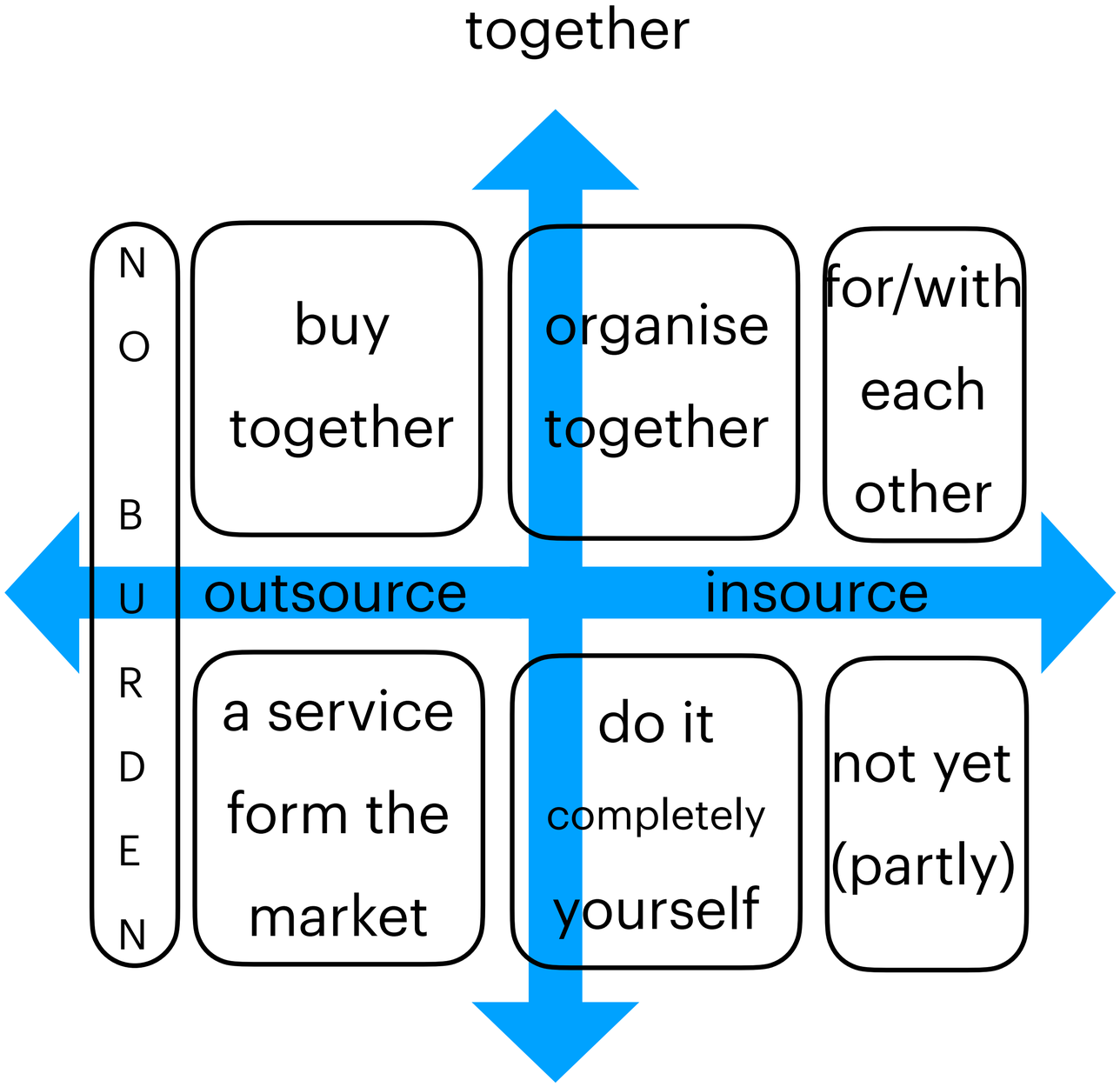





Cases Reported - Threat Classification
12 Months Period (1 Jan - 31 Dec 2023)
Cases Reported
Successful attack
High risk
Low risk
250
200
150
100
50
0
10 3 3 1 1 1 1 1 1 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
31 30 54 5 7 11 22 7 13 7 12 8 8 5 12 10 20 8 3 6 4 1 6 4 5 5 6 9 7 2 2 1 1 8 10 1 9 6 15 14 14 11 6 10 8 2 2 1
185 173 115 109 99 90 79 92 83 85 66 65 64 57 59 47 49 38 47 49 41 40 42 33 33 27 30 24 21 21 24 23 23 21 14 10 18 6 15 14 11 6 10 8 2 2 1


don't call us
we'll call you...

retainer


together
buy
together
organise
together
for/with
each
other
NOBU
outsource
insource
RDEN
a service
form the
market
do it
completely
yourself
not yet
(partly)
Individual


NOC
SURF CERT
SOC