Consorci de Serveis Universitaris de Catalunya

SIG-NOC Tools Survey 2023

Maria Isabel Gandía Carriedo

18th SIG-NOC Meeting
SUNET, Stockholm, 17-05-2023

Previous Work

- ✓ 1st Survey: July-October'11, published January'12.
  - NOCs' taxonomy, structures, resources, tools, standards…
  - 14 functions
  - 53 questions, 43 valid responses
  - Open boxes to add feedback
- ✓ 2nd Survey: December'15-February'16, published in June'16.
  - Tools, standards
  - 15 functions (14 + DDoS Mitigation)
  - 35 questions (66), 64 valid responses
  - Rating on importance (low/low-mid/mid-high/high) & quality (poor/fair/average/good/excellent)
- ✓ 3rd Survey: July-September'19, published in November'19.
  - Tools, standards
  - 16 functions (15 + Orchestration, Automation and Virtualisation)
  - 35 questions (74), 63 valid responses
  - Rating on importance (low/low-mid/mid-high/high) & quality (poor/fair/average/good/excellent)

What we will review today: the 4th SIG-NOC Tools Survey

- ✓ For all the survey:
  - The “big blocks” and how to sort them:
    - Basic information
    - Tools
    - Standards
  - Missing questions or answers

- ✓ The functionalities we will include.

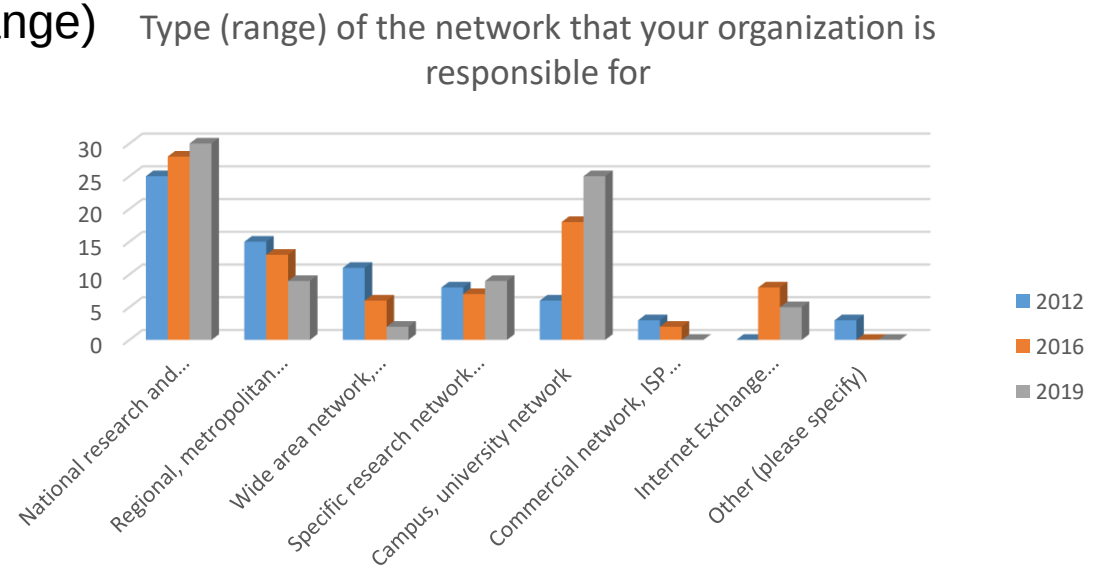
- ✓ For each functionality:
  - The name of the functionality
  - The definition
  - The tools that we will include
  - Missing tools

Basic information

1. Name (acronym) of your organisation

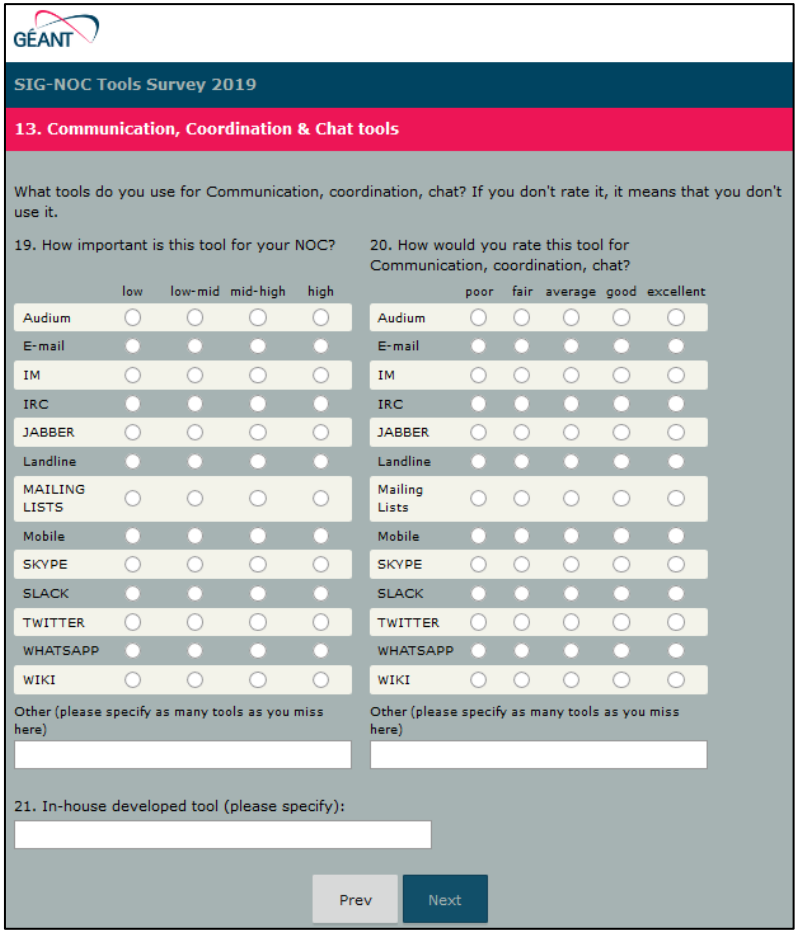
2. Type (range) of the network that your organisation is responsible for (Please choose all that apply):

- Wide area network among several countries
- National research and education network (NREN)
- Regional metropolitan network
- Campus university network
- Specific research network (any range)
- Commercial network (any range)
- Internet exchange
- Other:



NOC Tools – Introduction and Structure of the Survey

- ✓ For each one of the functions:
  - Short definition of <function>
  - Is your NOC responsible for <function>?
    - Yes → You are asked the questions below
    - No → Jump to the next function
  - What tools do you use for <function>?
    - How important is this tool for your NOC?
    - How would you rate this tool for <function>?



⚠ The pre-defined responses in the survey are all the tools that were rated or mentioned by two or more respondents in the 2019 survey

Pre-defined Responses

- ✓ The pre-defined responses are the tools rated or mentioned by **two or more** respondents in the 2019 survey.
- ✓ Open boxes allow to include other tools, including in-house developed solutions, for each function.
- ✓ We are going to review the questions, the definitions and the pre-defined answers.

Do you find any missing or outdated tools or definitions? Any mistakes? Shout!

For each functionality we are going to review...

✓ This funcionality stands for... ← Short definition

Suggested tools:

- Tool1
- Tool2 (drop/change?)
- Tool3
- Tool4
- Tool5
- Tool6
- Tool7
- Tool8

In red, tools to erase from the survey, mostly because they were not mentioned or mentioned only once in 2019

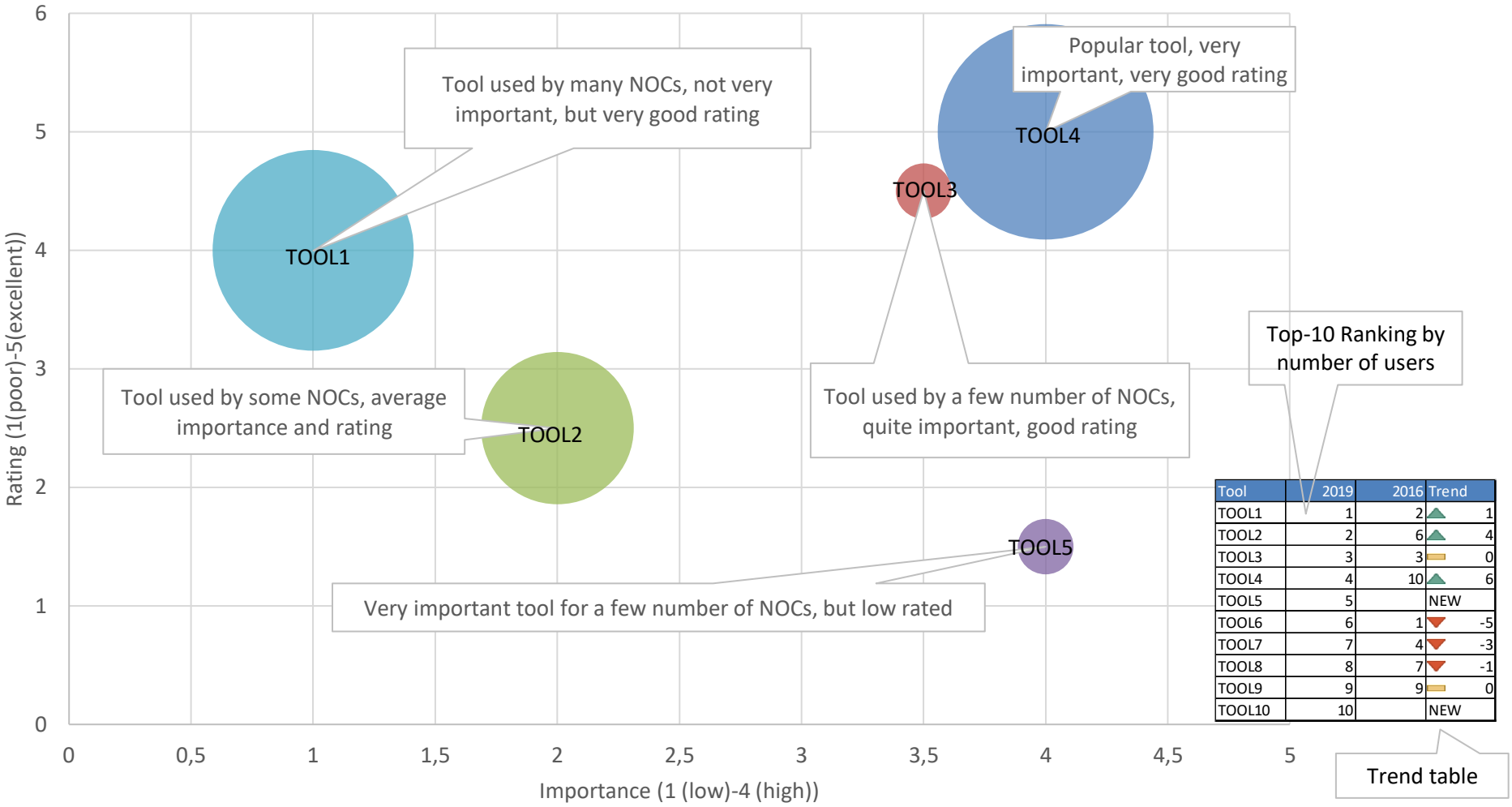
In green, possible answers to include in the survey, because they were mentioned more than once in 2019 / new suggestions

Tools mentioned only once in 2016 / 2019

Answers from one organization in 2016/2019:

~~Tool9~~	Tool12	Tool15
Tool10	Tool13	
Tool11	Tool14	

NOC Functions & Tools: Analysis of the Responses How-To

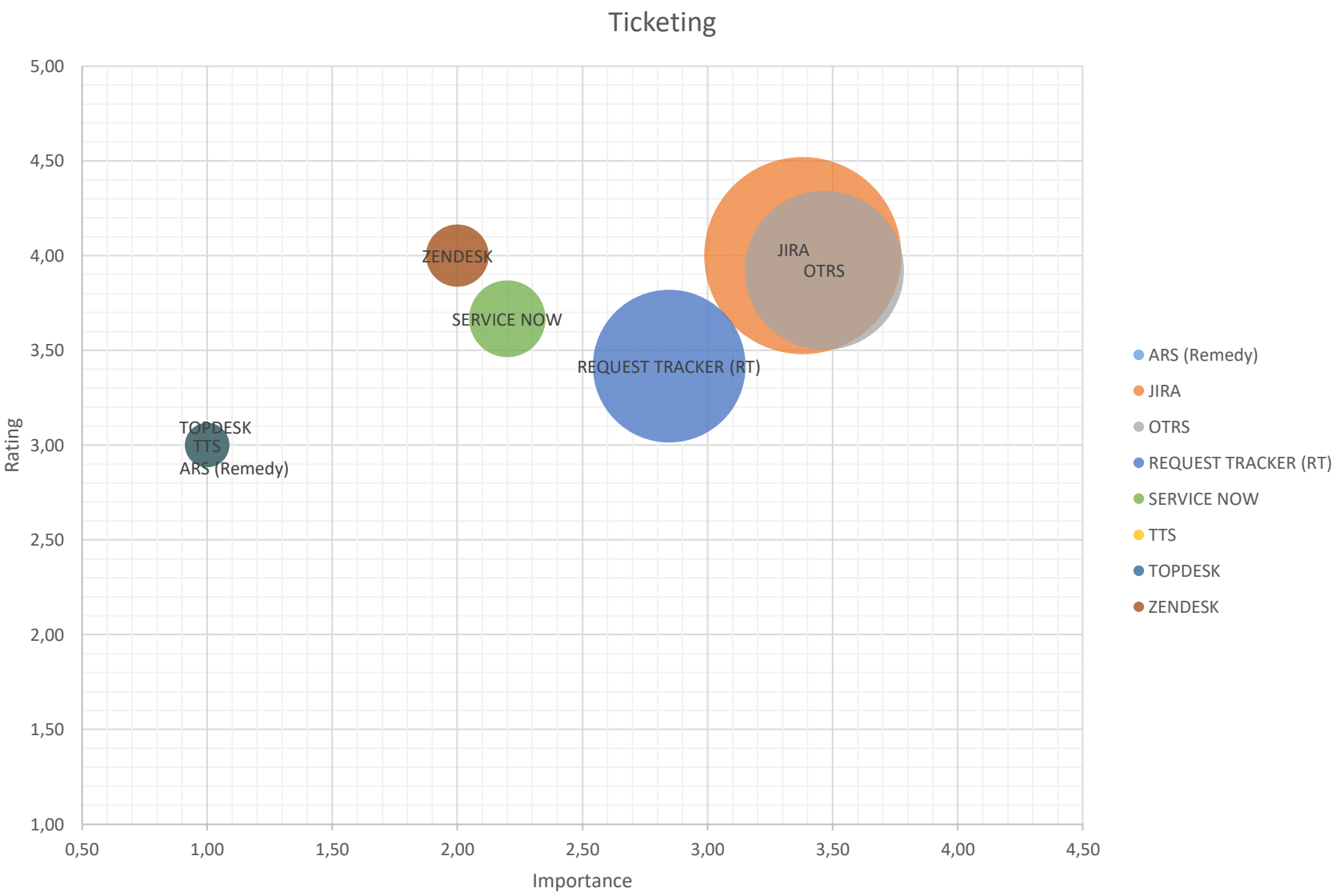


Tool	2019	2016	Trend
TOOL1	1	2	1
TOOL2	2	6	4
TOOL3	3	3	0
TOOL4	4	10	6
TOOL5	5		NEW
TOOL6	6	1	-5
TOOL7	7	4	-3
TOOL8	8	7	-1
TOOL9	9	9	0
TOOL10	10		NEW

Other not pre-defined tools mentioned by more than one institution, if any (in parentheses, the number of institutions that mention it)

Other tools: TOOL11 (5), TOOL12 (4), TOOL13(4), TOOL14 (2), TOOL15 (2), TOOL16 (2)

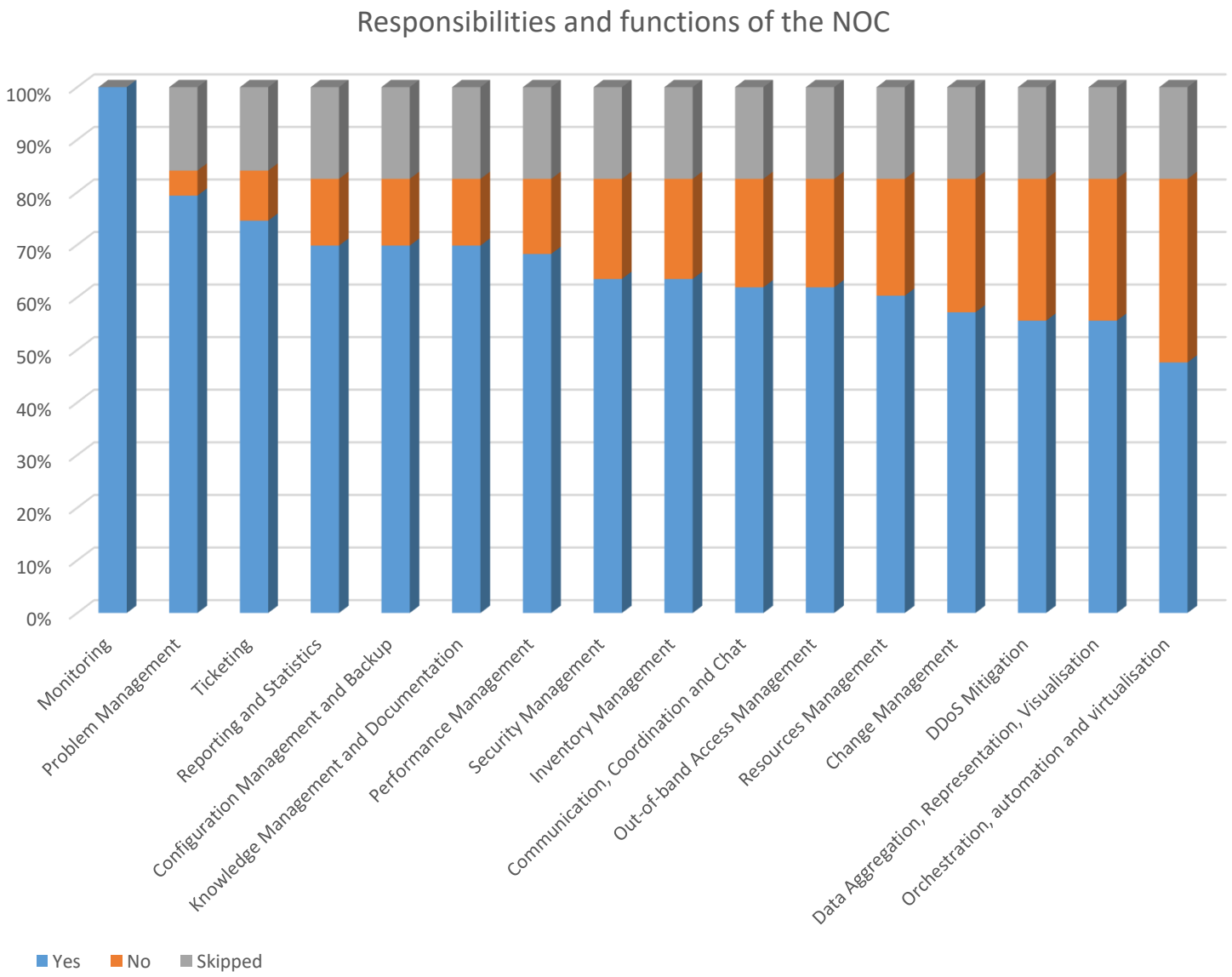
Example of graps from the last survey



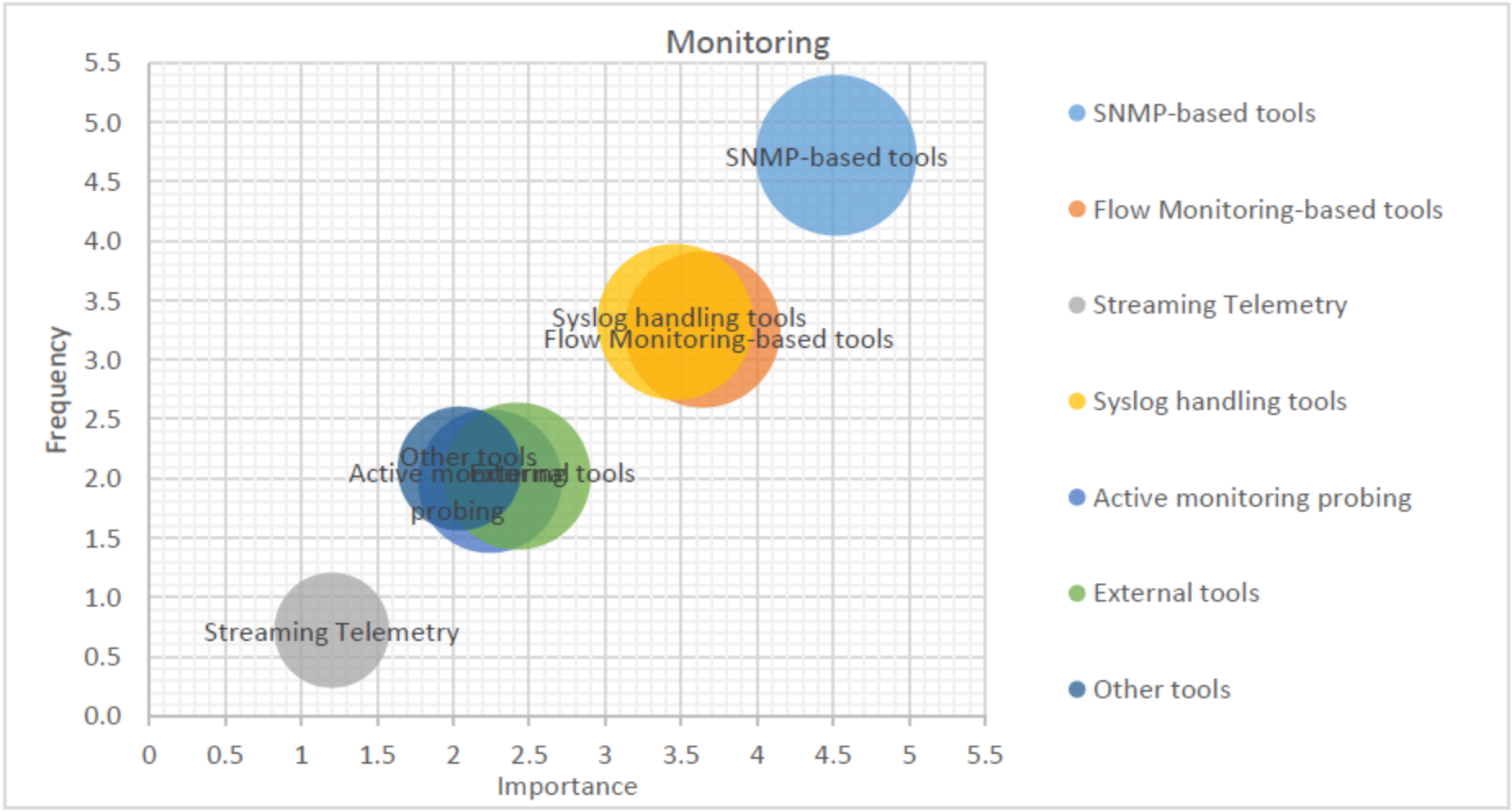
Tools: NOCs, Functions and Responsibilities since 2011

Functionality sorted by number of answers	2011	2016	2019	2023
Monitoring	✓	✓	✓	?
Problem management	✓	✓	✓	?
Ticketing	✓	✓	✓	?
Reporting & statistics	✓	✓	✓	?
Configuration management & backup	✓	✓	✓	?
Knowledge management/documentation	✓	✓	✓	?
Performance management	✓	✓	✓	?
Security management	✓	✓	✓	?
Inventory management	✓	✓	✓	?
Communication, coordination & chat	✓	✓	✓	?
Out-of-band-access	✓	✓	✓	?
Resource management	✓	✓	✓	?
Change management	✓	✓	✓	?
DDoS mitigation		✓	✓	?
Data aggregation	✓	✓	✓	?
Orchestration, Automation and Virtualisation			✓	?

Functionalities: Responsibilities and Functions of the NOC in 2019



NOC Tools – Monitoring - Methodologies



✓ Is any methodology missing?

NOC Tools – Monitoring

Observation and measurement of several parameters (from the link status or traffic on an interface or line to physical parameters, like temperature, humidity, etc).

Suggested tools:

Arbor/Netscout Peakflow/SP	ICINGA	NAGIOS	PMACCT	SPECTRUM
BGPMON	InfluxDB / Influx stack (4)	NAV	PROMETHEUS	SPLUNK
CACTI	INTERMAPPER	NFDUMP	RANCID	SURICATA
CRICKET	LibreNMS (3)	NFSEN	RIPE Atlas / Stats	WEATHERMAP
ELK STACK	LOOKING-GLASS	OBSERVIUM	RIPE RIS / BGPlay	ZABBIX
GRAFANA (5)	MRTG	OPENVIEW	SILK	ZENOSS
Graylog (2)	MUNIN	Oxidized (4)	SMARTxAC (2)	ZINO
		PERFSONAR	SMOKEPING	

1-answer 2019*:	Management Center	OpenNMS	Swatch	Rancid frontend
Ail-framework	Graphite	Request Tracker	Ciena OneControl	MRTG front-end,
AirManager	Infping	Scrutinizer	IBM Tivoli	Netflow analyser
Alerta	Intelmq	Sysmondash	Netdisco	RRDtool
ALLOT Netxplorer	IPERF	UNTANGLE NG	Net-minder	FTAS, G3
Ansible	IRIS (a South African	FIREWALL	Speedtest	SMARTxAC
Centreon	Network Management		Puppet	Turbo Krt
Ciena OneControl	Platform)	*** +18 in-house**	Racktables	Vialpe
Cisco PRIME	Nagvis		Patchmanager	
Corero	Netdisco		Splunk	
Dashing	Nfsen-ng	**1-answer-2016:**	Net Polygraph	
ECI Lightsoft	Nokia OMS	AS-Stats	NMS DWDM vendors	
EMMA	Omnivista	LibreNMS	GINS	
Extreme	OpenBMP/SNAS	CENTREON	minemon	

NOC Tools – Problem management / Incident management

The primary objectives of Problem Management are to prevent problems and resulting incidents from happening, to eliminate recurring incidents and to minimize the impact of incidents that cannot be prevented. Following the necessary steps in order to identify the source of a problem. Getting warnings about problems or incidents.
Please note communication and collaboration tools will be in a different section.

Suggested tools:

CONFLUENCE	OTRS	RIPE RIS /	ZINO
ELK stack	REQUEST	Bgplay	
JIRA	TRACKER	ServiceNow (2)	
NAGIOS	RIPE Atlas /	SPLUNK	
NLNOG RING	Stats	ZABBIX	

1-answer 2019*:	Graylog	ProactivaNet	GN6
AirManager	Icinga	SpiceWorks	Kibana
CLI	Llibrenms		HP Openview
Cricket	Netdisco	**In-house 2019**:	SpiceWorks
Gitlab (trouble tickets)	Nfsen	Own PM Tool	Observium
Grafana	Omnivista		Munin
	Openview	**1-answer 2016**:	
	Servicedesk		

NOC Tools – Ticketing

Process for the tracking of incidents, problems or tasks.

Suggested tools:

ARS (Remedy)	SERVICE NOW
JIRA	TTS
OTRS	TOPDESK
REQUEST TRACKER	ZENDESK

1-answer 2019:
CA Service Desk Manager
Gitlab
GLPI
Mantis
Openview ServiceDesk
ProactivaNet
ServiceDesk+
Salesforce SpiceWorks
Trac

In-house 2019:
e-mail (customer side), own PM tool (internally)
LAGUN
Ofbiz developed service
PHP in-house solution
TTS (trouble Ticket System)

1-answer 2016:
MANTIS Bug Tracker
TRAC
HP Openview SD
VC4 IMS
Clocking
SpiceWorks
GLPI
GN6
Ticketing for Drupal

NOC Tools – Reporting and statistics

Representation of data sources for reference and statistics. It includes capacity reporting and SLA reporting.

Suggested tools:

ARBOR	MUNIN	TABLEAU
CA SPECTRUM	NAGIOS	ZABBIX
CACTI	NFSEN	ZENOSS
GRAFANA	Observium (2)	ZINO
LibreNMS (2)	RT	
MRTG	SPLUNK	

1-answer 2019:	SQL Reporting	processing tools
AirManager	services	
Icinga	Tablaeu	**1-answer 2016:**
IXP-manager		Kibana
IRIS	**In-house 2019:**	LibreNMS
MRTG ==> Cricket	ESnet NetBeam and	Torrus
NFSEN ==> FlowMon	Portal	RRDtool
Omnivista	GINS	infovista
OpenNMS	Igor	sanet
OTRS	Report module	NAV
Pnp4nagios	Several statistic	NFDUMP
Scrutinizer	collection and	

NOC Tools – Configuration management and backup

Control and backup of the configuration for the routers switches and other pieces of equipment.

Suggested tools:

CVS	OXIDIZED
GIT	RANCID
IMS	SUBVERSION

1-answer 2019:	**In-house 2019:**	CA Spectrum and
AirManager	Automator	FTP
Ansible	Backitup tool	Puppet
Backuppc	Backup scripts	Backuppc
Dude	CPE autoconfig	etckeeper
Extreme	Extreme	Racktables
Management Center	Management	Patchmanager
FTP	IROptika	Ciena NMS
HP IMC	Local script	SCCS
Netdot	Megaconf	veeam
NOC Project	Perl scripts	Imc
Rundeck	Several scripts	Rancid
Omnivista		emc
Prime-Infrastructure	**1-answer 2016**:	
Spectrum	RCS	

NOC Tools – Knowledge management / documentation

Storing and sharing knowledge information to improve the efficiency in an organization.

Suggested tools:

BOX	MEDIAWIKI	SHAREPOINT
CONFLUENCE	MICROSOFT ONEDRIVE	WIKI
DOCUWIKI	Nextcloud (3)	
DROPBOX	OTRS	
Gitlab (2)	OWNCLOUD	
GOOGLE DRIVE	REQUEST TRACKER	

1-answer 2019:		FosWiki
BSCW	**In-house 2019:**	Drupal CMS
Draw.io (Confluence plugin)	GARRBOX	File server
Gitbook	OnlyOffice	Subversion
Ikiwiki	Readthedocs	Plone
Microsoft Office	SAN / NAS	ownCloud
Moinmoin wiki. Not owncloud, but nextcloud!		SURFdrive
		OneDrive
Netbox	**1-answer 2016**:	KIND
ServiceNow	MoinMoin Wiki	GIS
XWIKI	TRACwiki	Comunitats
VC4 IMS	TiddlyWiki	

NOC Tools – Performance management

Following a procedure in order to identify the source of a performance problem on the network.

Suggested tools:

BWCTL	NDT	SMOKEPING
HADES	NLNOG RING tools	WIRESHARK
IPERF	OWAMP/TWAMP	ZINO
MGEN	PERFSONAR	
MRTG	RIPE Atlas	

1-answer 2019:	Icinga	https://github.com/jemcek/packETH
AirManager	Nfsen	FTAS
AKOStest (Slovenian **speed test** web app)	Mikrotik **speedtest**	Speed Test like tool
ALLOT Netxplorer	Munin	Bandwidth meter,
CA Performance Center	Rude/ crude measurements	Predictive treshold (Zenoss)
Cricket	Scrutinizer	
Grafana	**Speedtest**	**1-answer 2016:**
HawkEye	SNMP	RRD
HTML5 **speedtest**	Weathermap	Spirent appliances
https://github.com/adolfintel/**speedtest**	**In-house 2019:**	Speedtest
	packETH	NAV

NOC Tools - Security management

Control of IT resources to avoid third parts from attacking the resources of an institution.

Suggested tools:

ACL	KERBEROS
BGMON	RADIATOR
ClearPass (Aruba) (2)	REQUEST TRACKER
E-MAIL SECURITY APPLIANCE	RSA Software
FIREWALL	TACACS+
FIREWALLBUILDER	THREAT INTELLIGENCE
FREERADIUS	Web security appliance
IPS	
IDS	

1-answer 2019:	Minemeld	Netflow analyser
AIL-Framework	RPKI	
AirManager	UNTANGLE NG	
Anti-DDoS (F5 BigIP)	FIREWALL	
Cisco Umbrella		
FortiAnalyzer	**1-answer 2016**:	
IntelMQ	RTIR	

NOC Tools – Inventory management

Organization and control of information about an institution's devices materials and products.

Suggested tools:

EXCEL	IRR	RANCID
IMS	Netbox(2)	WIKI
Jira (3)	RACKTABLES	

1-answer 2019:
AirManager Otrs-cmdb
Ansible-Inventory
CMDB
Combodo itop
EMMA
GLPI
Netdot
Omnivista
OpenDCIM
Oxidized
PhpIPAM
ProactivaNet

In-house 2019:
Automator (one module is inventory management)
Custom perl web software
DFN GIS
Equipment inventory
GARR database
In-house CMDB IIR
KIND
Ofbiz developed tool
PHP Development
Skladišče (inventory of devices)
Web interface to store data in Oracle DB
Xixare

1-answer 2016:
Patchmanager
HP Openview SDesk
HP Openview NNM
Ciena NMS
filemaker
netdisco
Observium
KIND
CMT
GarrDB
GIS
GN6

NOC Tools – Communication coordination chat

Communication with people, either in the same institution or in other institutions.

Suggested tools:

E-mail	SLACK
IM	TWITTER
IRC	WHATSAPP
JABBER	WIKI
Landline	
MAILING LISTS	
Mobile	
SKYPE	

1-answer 2019:	Onlyoffice Videoconferencing (Polycom)	(webbased sender for mailing lists) SharePoint
Connectme		
Mattermost		
Nextcloud Chat		
Riot-im		
Rocket.Chat	**1-answer 2016**:	
ServiceNow	Asterisk	
Telegram	Kamailio	
Threema	CallDav	
Trello	ServiceInfo	

NOC Tools – Out-of-band Access

Access to the network devices of an institution from an external network.

We didn't ask about tools in 2019. Should we ask again?:

These are the options we included in 2016:

ADSL
CONSOLE SERVER
DRAC
HP ILO
ISDN
KVM (not the hypervisor)
Landline
Mobile tech

1-answer 2016:	**1 answer 2011:**
DWDM OSC	DRAC
POTS	IPMI

NOC Tools – Resources management

Organization and control of logical resources such as IP addresses, AS numbers circuit numbers, topology, documentation etc.

Suggested tools:

6CONNECT	IPPlan	WIKI
BLUECAT	OMNIGRAFFLE	
CONFLUENCE	PhpIPAM (3)	
EXCEL	RACKTABLES	
INFOBLOX	VISIO	

1-answer 2019:	Homegrown database for IP-addresses	Webform which is fed by a script that makes SNMP based routing table polls and DNS queries.
EfficientIP SOLIDServer	Igor	
IXP-manager	In-house CMDB	
Microsoft IPAM	Internal IPam	
Netbox	IP Adress Management (IPAM)	**1-answer 2016:**
Netdot	IPIS (tracks IP assignments and syncs to RIPE DB)	GIS
Nocproject.org	Perl scripts	GestioIP
PowerPoint	PHP Development	HP Openview SDesk
ProactivaNet	Web-based list of networks and router-interfaces	Phpipam
	Web developed APP	KIND
In-house 2019:	Web interface to Oracle DB	GIS
Custom perl web software		BDCOM
DFN GIS		
Equipment inventory		
GESIP		

NOC Tools – Change management

Controlling and recording of changes in values technologies etc.

Suggested tools:

CONFLUENCE
GITLAB
JIRA
OTRS
REQUEST TRACKER
ServiceNow(2)

1-answer 2019:
Combodo itop
Git
MeisterTask,
ProactivaNet
RANCID
Trello

In-house 2019:
Change tracker
Storing
configuration history
DFN GIS
In-house 'planned maintenance calendar' web app

1-answer 2016:
Redmine
gitlab
Racktables
Patchmanager
HP Openview Sdesk
pymetric
Wiki
GN6

NOC Tools – DDoS Mitigation – Mechanisms - Detection

DoS mitigation is a set of techniques for resisting distributed denial-of-service (DDoS) attacks on networks attached to the Internet by protecting the target and relay networks.

What kind of DDoS Detection solutions do you use?

Suggested Mechanisms for Detection:

Threat intelligence
DNS solution
Firewall on Demand (2)
Netflow-based tools (2)

What kind of DDoS Mitigation solutions do you use?

Suggested Mechanisms for Mitigation:

Hardware platforms on-site in-line
Hardware platforms on-site off-line
Cloud solutions
No special tool, but blackholes, ACLS, etc

1-answer 2019:
Arbor (3) (Peakflow SP)
Fastnetmon (2)
FoD (2)
DDoS mitigation
DFN Nemo
Firewall
Kentik
Minemel Netflow
Netflow based scripts
Radware Riorey
Syslog

In-house 2019:
FoD (4)
RTBH (4)
DFN Nada
Fortinet 1500D
Minemeld

This question was probably misunderstood (as some answers are tools, and that was the next question)

NOC Tools – DDoS Mitigation Tools

Suggested tools:

Akamai Solutions Arbor/Netscout Cloud solutions Arbor/Netscout Hardware Solutions (Peakflow, SP, TMS,…)	Blackholing Cloudflare solutions. Dyn solutions Firewall on Demand BGP FLOWSPEC RATE-LIMITING	RTBH UTRS

1-answer 2019: F5 BigIP Next generation firewall PaloAlto **Remote triggered black hole** **In-house 2019:**	AutoBH DDoS Protector Black Wall DFN Mitigation platform Nemo+Nada ExaFS Tool based on	**RTBH** **1-answer 2016:** FastNetMon

NOC Tools - Data aggregation, representation, visualisation

Aggregate live data from various tools and represent/visualize them in a human readable way.

Suggested tools:

CACTI
Cricket(2)
ELASTICSEARCH
GRAFANA
KIBANA
LOGSTASH
Observium (2)
SPLUNK
WEATHERMAP

1-answer 2019:
EMMA
Icinga
IXP-manager
Munin
Librenms
Prometheus
Zabbix

In-house 2019:
DMON(under construction)
FTAS
G3
GINS
In-house CMDB
Nemo
ServiceNow
SURFnet
NetworkDashboard
TurboKrt

1-answer 2016:
MRTG, Tivoli maps, Juniper RIM
Zino
Zenoss
CheckMK
Observium

NOC Tools – Automation and Orchestration

Automation describes a task or function accomplished without human intervention in a network, like configuration, management, testing, deployment, and operations of physical and virtual devices.

Orchestration describes the arranging and coordination of automated tasks, ultimately resulting in a consolidated process or workflow to automatically define and modify the behavior of the network.

What kind of tasks do you automate?

Provisioning
Routing Configuration
Network discovery

How many devices are you automating tasks for?

Core (number)
Access

NOC Tools – Automation and Orchestration

Suggested tools and languages:

Ansible	Northstar
Chef	Puppet
Cisco NSO	Python scripting
Dockers	Salt
Jenkins scripting	ServiceNow
Junos Space	Terraform
Kubernetes	

1-answer 2019:	DFN GIS
Bash scripts	Inventory monitor
Dude	MegaConf, AutoBH
EMMA	Perl and javascripts scripts
Perl	Scripts to mass generate and deploy configuration and update related databases.
Zabbix	
In-house 2019:	SURFnet WorkflowEngine
Automator	
Custom bash, expect and perl scripts	

Standards

- ✓ What is the estimated level of adoption of the given standard or methodology at your NOC? + How many of your NOC people are certified or trained (in percentage)?

ISO	ITIL
ISO 20000	NITS
ISO 27001	FIPS
eTOM	

Standards

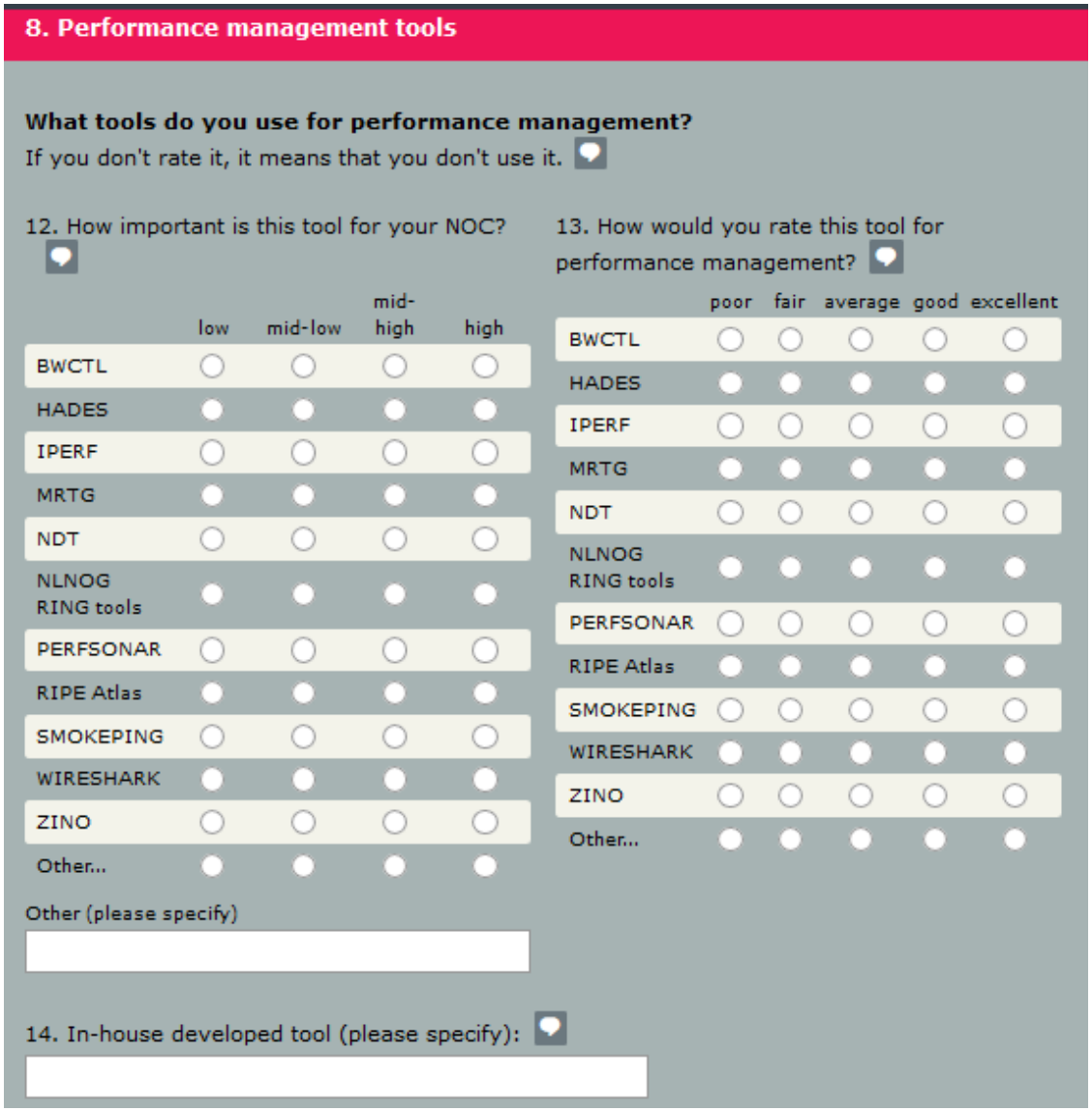
- What technical training(s) are provided either in-house or contracted to your NOC personnel? Please, describe them all (open question).

- Mentoring inside organisation
- ITIL Foundations for NOC technicians, ITIL Service Capability Modules (SOA, OSA, PPO, RCV) and Managing Through Lifecycle (MALC) (ITIL Expert certification) for NOC Manager. Cisco CCNA, Attendance to NOG Forums (Network Operators Group), Communication workshops.
- We include technical training in our tenders (about the equipment or the service we buy in the tender)
- Mentoring top to bottom, technical courses of equipment vendors (Cisco, Juniper...), self-learning...
- ITIL foundations to all involved staff members.
- Trainings provided by vendors when a new equipment/software is deployed.
- ISO awareness and risk management through Cyber security training
- Network Working Group meetings at SWITCH Community.
- Cisco Academy, Mikrotik Training, in-house training
- Occasional trainings by vendors
- In most cases, training courses in-house by the providers

Shall we add them as options?

- Attendance to NOG meetings
- Cisco Academy
- ISO Training
- ITIL Training
- Mentoring inside organisation
- Mikrotik Training
- Network eAcademy (GÉANT)
- Training provided by vendors when new equipment/software is deployed

SurveyMonkey-friendly style



8. Performance management tools

What tools do you use for performance management?

If you don't rate it, it means that you don't use it.

12. How important is this tool for your NOC?

	low	mid-low	mid-high	high
BWCTL	○	○	○	○
HADES	○	○	○	○
IPERF	○	○	○	○
MRTG	○	○	○	○
NDT	○	○	○	○
NLNOG RING tools	○	○	○	○
PERFSONAR	○	○	○	○
RIPE Atlas	○	○	○	○
SMOKEPING	○	○	○	○
WIRESHARK	○	○	○	○
ZINO	○	○	○	○
Other...	○	○	○	○

Other (please specify)

13. How would you rate this tool for performance management?

	poor	fair	average	good	excellent
BWCTL	○	○	○	○	○
HADES	○	○	○	○	○
IPERF	○	○	○	○	○
MRTG	○	○	○	○	○
NDT	○	○	○	○	○
NLNOG RING tools	○	○	○	○	○
PERFSONAR	○	○	○	○	○
RIPE Atlas	○	○	○	○	○
SMOKEPING	○	○	○	○	○
WIRESHARK	○	○	○	○	○
ZINO	○	○	○	○	○
Other...	○	○	○	○	○

14. In-house developed tool (please specify):

Easy to click

Proposed Deadlines*

- ✓ 31-5 to send feedback to sig-noc-al@lists.geant.org (you)
- ✓ 30-6 to send the final survey to sig-noc@lists.geant.org (us)
- ✓ 30-9 to answer the survey (you)
- ✓ 31-10 to have the results (us)

* Not set in stone

Consorci de Serveis Universitaris de Catalunya

Thank you!

Questions? Suggestions?

Please, send us your feedback!

sig-noc-al@lists.geant.org
mariaisabel.gandia@csuc.cat