Monitoring Data Analysis

Ivana Golub, PSNC

GN5-1 Network Development WP Co-lead

GN5-1

There are 17 NOC Functions

listed in

the 2023 SIG-NOC Tools survey

NOC Functions 2023
Monitoring
Problem Management
Ticketing
Knowledge Management and Documentation
Reporting and Statistics
Communication, Coordination and Chat
Configuration Management and Backup
Performance Management
Inventory Management
Resources Management
Out-of-band Access Management
Change Management
Training
Security Management
Data Aggregation, Representation, Visualization
DDoS Mitigation
Orchestration, automation and virtualisation

Source: SIG-NOC Tools Survey 2023

ACL	Ansible	ARBOR	**ARGUS**	BGMON	BGP FLOWSPEC	BGPALERTER	BGPMON
Blackholing	BOX	BWCTL	CA SPECTRUM	CACTI	Cisco NSO	CLEARPASS (ARUBA)	CONFLUENCE
CONSOLE SERVER		CORERO	CRICKET	CVS	DNS solution	Docker	DOCUWIKI	DRAC
DROPBOX	EDUMEET	ELASTICSEARCH		ELK STACK	E-mail	E-MAIL	EXCEL	FIPS
FIREWALL	**Firewall on Demand**		FIREWALLBUILDER	FITSM standards		FREERADIUS	FTTH /FTTx	GIT
GITLAB	GOOGLE DRIVE	**GRAFANA**	GRAYLOG	HADES	HP ILO	ICINGA	IDS	IM
IMS	INFLUXDB/INFLUX STACK	INFOBLOX	INTERMAPPER	IPERF	IPS	IRR	ISDN	JABBER
Jenkins scripting	JIRA	Junos Space	KENTIK	KERBEROS	KERBEROS·	KIBANA	Kubernetes	KVM
Landline	LIBRENMS	LIBRESPEED	LOGSTASH	LOOKING-GLASS		MAILING LISTS	MATTERMOST	MEDIAWIKI	MGEN
MICROSOFT ONEDRIVE	Mobile	MRTG	MUNIN	NAGIOS	NAV	NDT	NEMO
NETBOX	NEXTCLOUD	NFDUMP	NFSEN	NIST	NITS	NLNOG RING	Northstar	OBSERVIUM
OPENVIEW	OTRS	OWAMP/TWAMP	OWNCLOUD	OXIDIZED	**PerfSONAR**	PHPIPAM	PMACCT	**PMP**
PROMETHEUS	Provisioning	Puppet	Python scripting	RACKTABLES	RADIATOR	RANCID	RATE-LIMITING
REQUEST TRACKER	RIPE Atlas / Stats	RIPE RIS / BGPlay	ROCKETCHAT	RSA Software	RTBH
Rundeck	Salt	SERVICENOW	SHAREPOINT	SILK	SKYPE	SLACK	SMARTxAC	SMOKEPING
SPECTRUM	SPEEDTEST	SPLUNK	SUBVERSION	SURICATA	TABLEAU	TACACS+	TEAMS	THREAT INTELLIGENCE
TIMEMAP	TIMETOP	TWITTER	UTRS	VISIO	WEATHERMAP		WHATSAPP	**WIFIMON**	WIKI
WIRESHARK	ZABBIX	ZENDESK	ZENOSS	ZINO	ZOOM			

Number of systems to collect various measurements

Number of Measurement Systems

- 🔵 All in 1
- 🟡 Between 2 and 4
- 🔴 5 or more
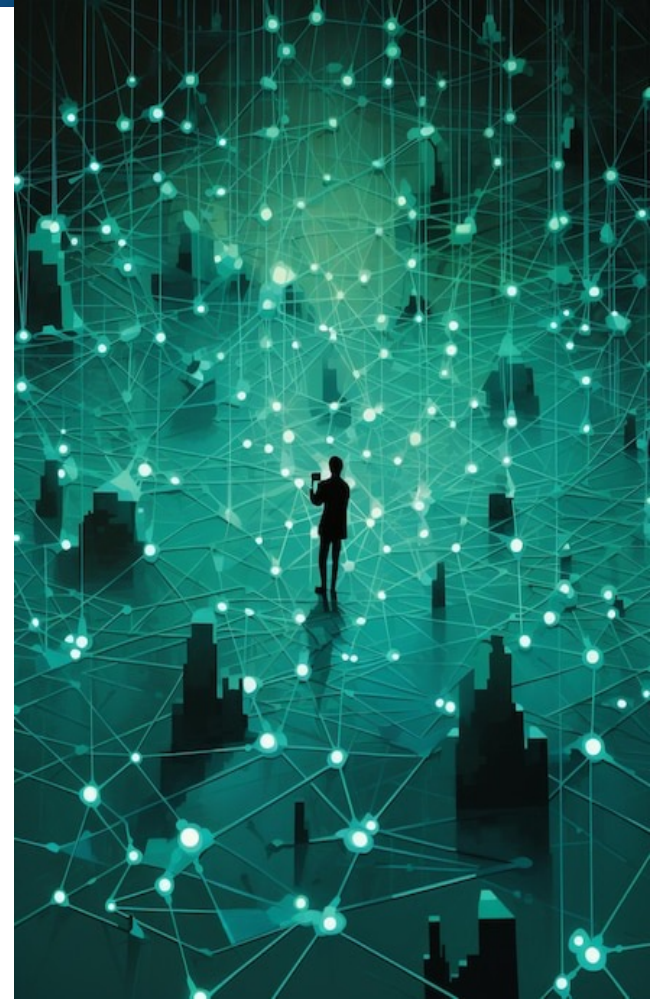
Source: MetrANOVA Survey 2023
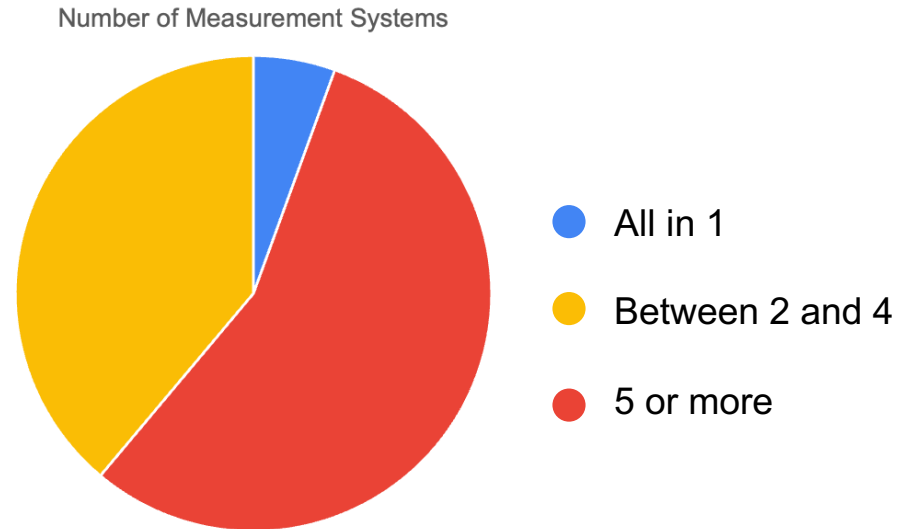
Do you know…

How many tools on average

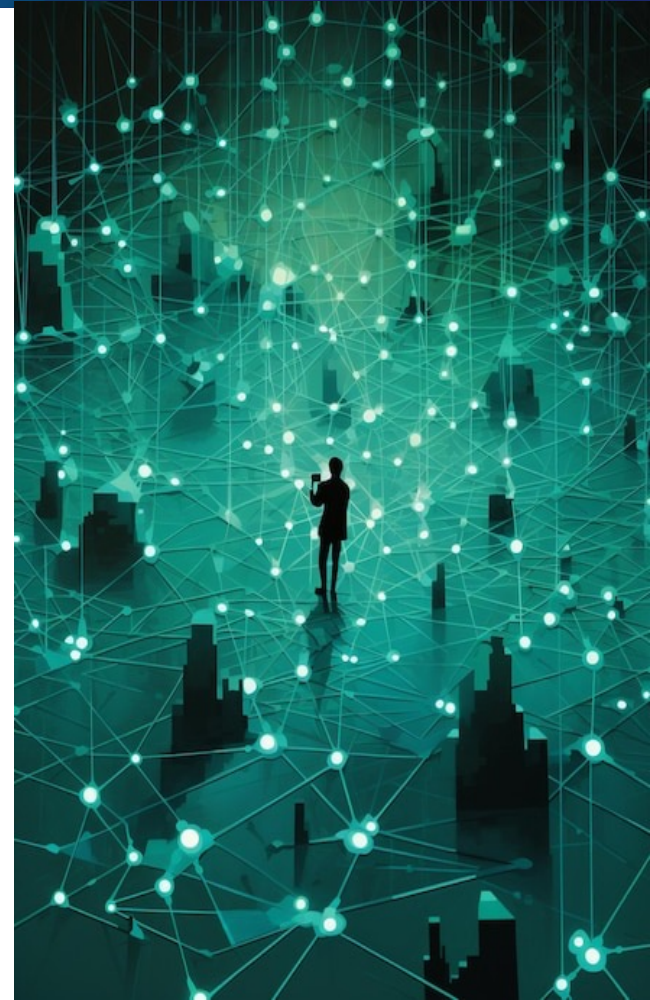**each organisation uses for…**
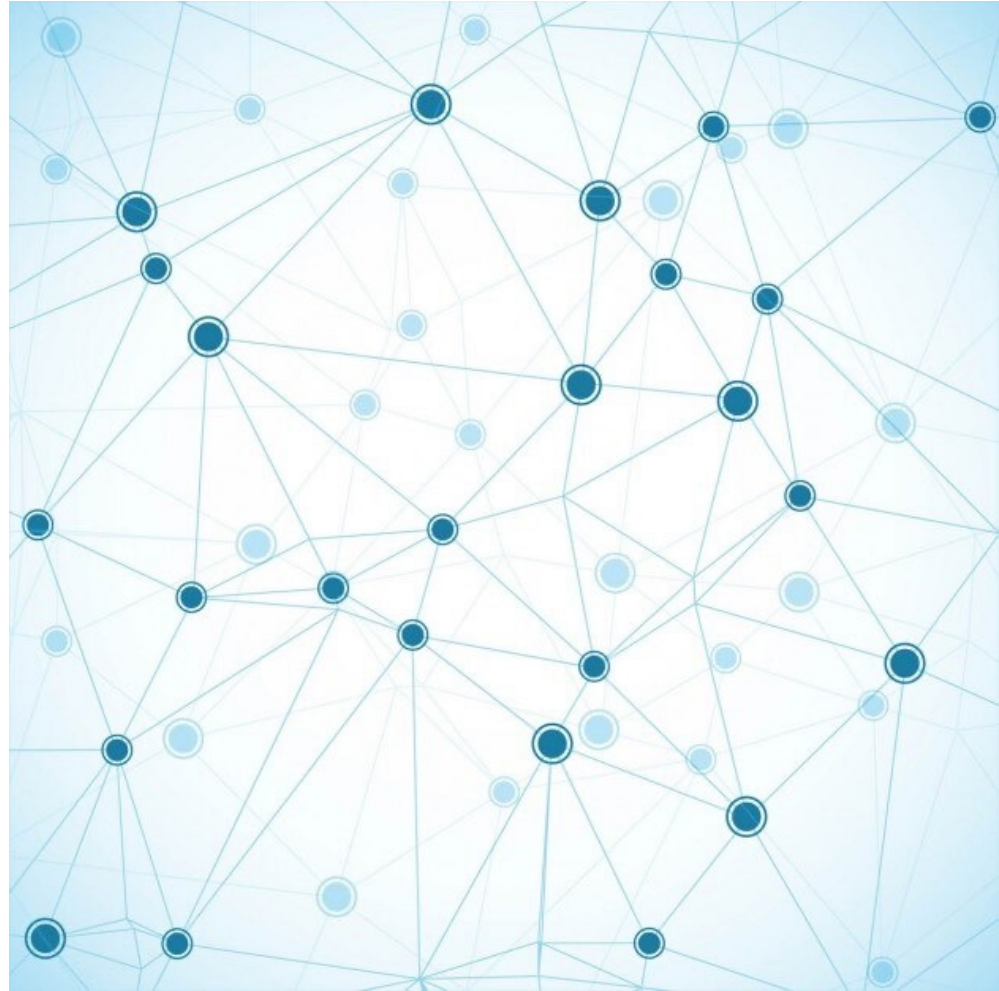
Monitoring:

Source: SIG-NOC Tools Survey 2023

Monitoring: **11.5**

Source: SIG-NOC Tools Survey 2023
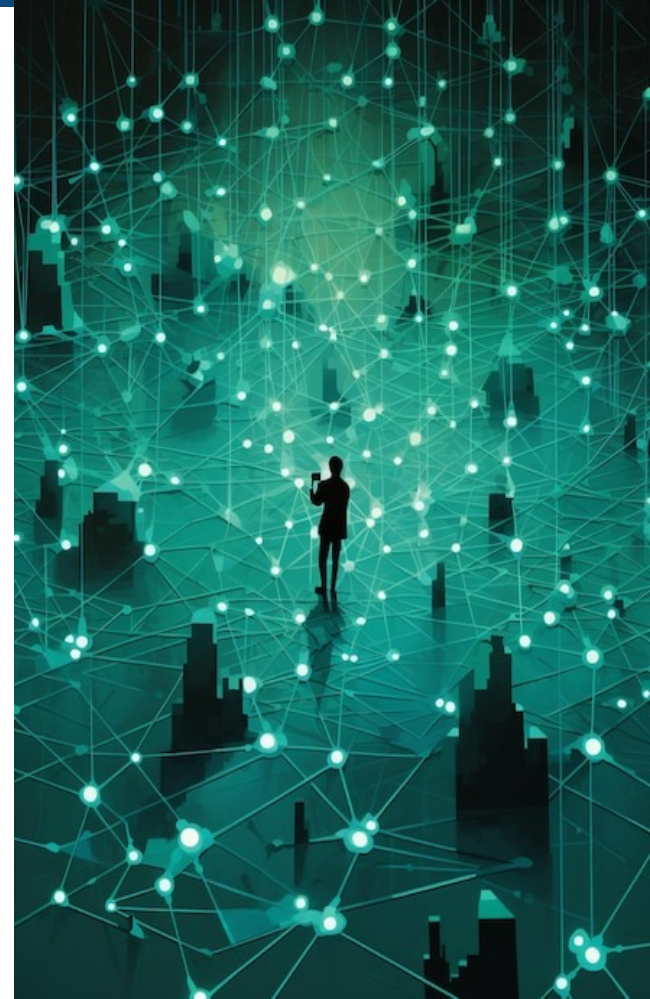
Monitoring: **11.5**

Problem management:

Source: SIG-NOC Tools Survey 2023

Monitoring: **11.5**

Problem management: **4.7**

Source: SIG-NOC Tools Survey 2023

Monitoring: **11.5**

Problem management: **4.7**

Data Aggregation, Representation and Visualisation:

Source: SIG-NOC Tools Survey 2023

Monitoring: **11.5**

Problem management: **4.7**

Data Aggregation, Representation and Visualisation: **3.8**

Source: SIG-NOC Tools Survey 2023
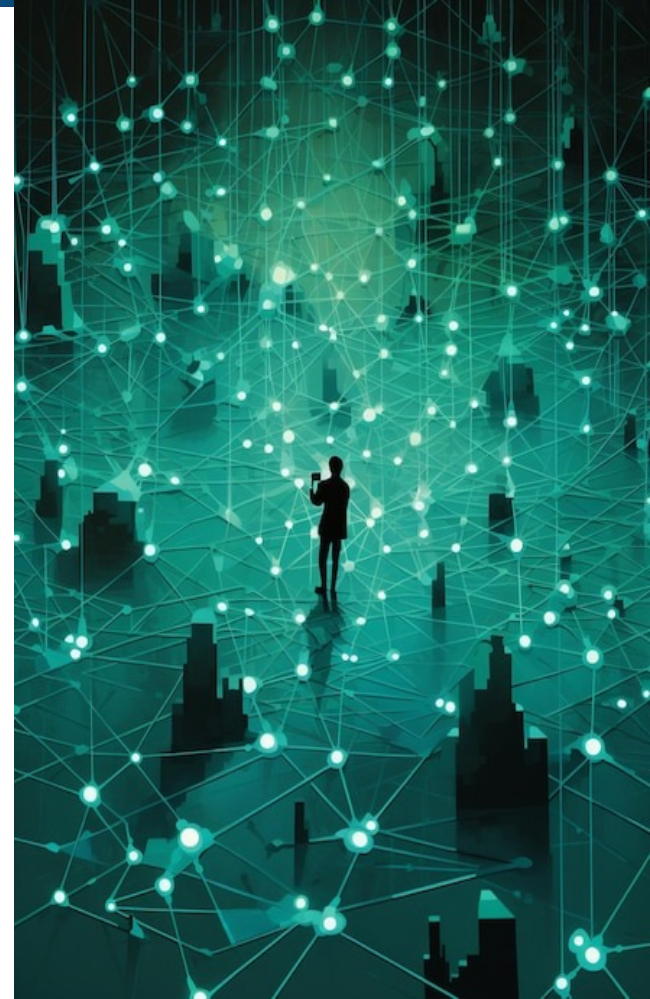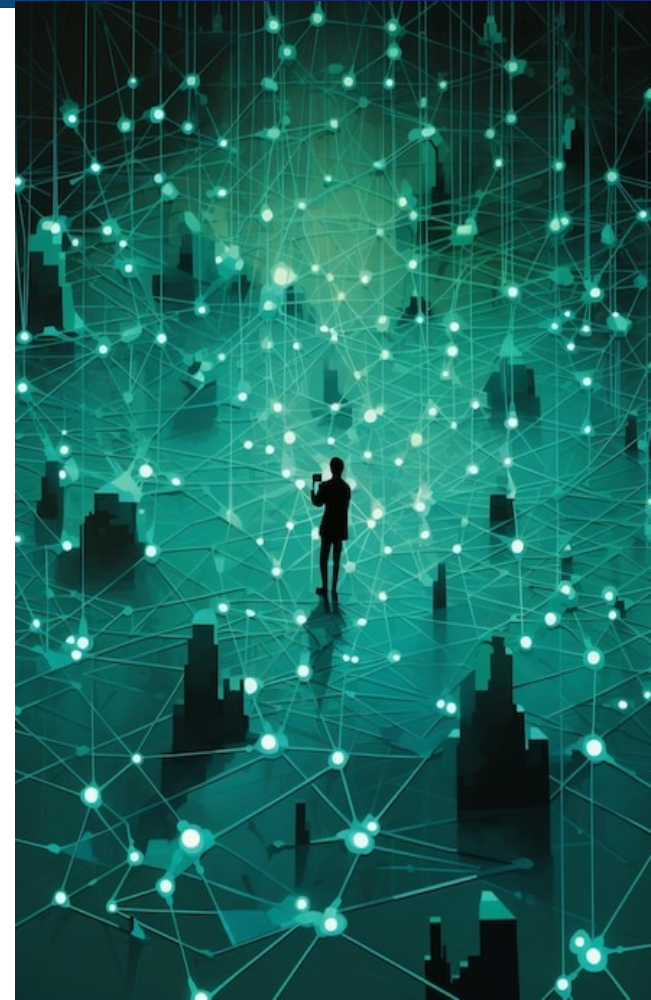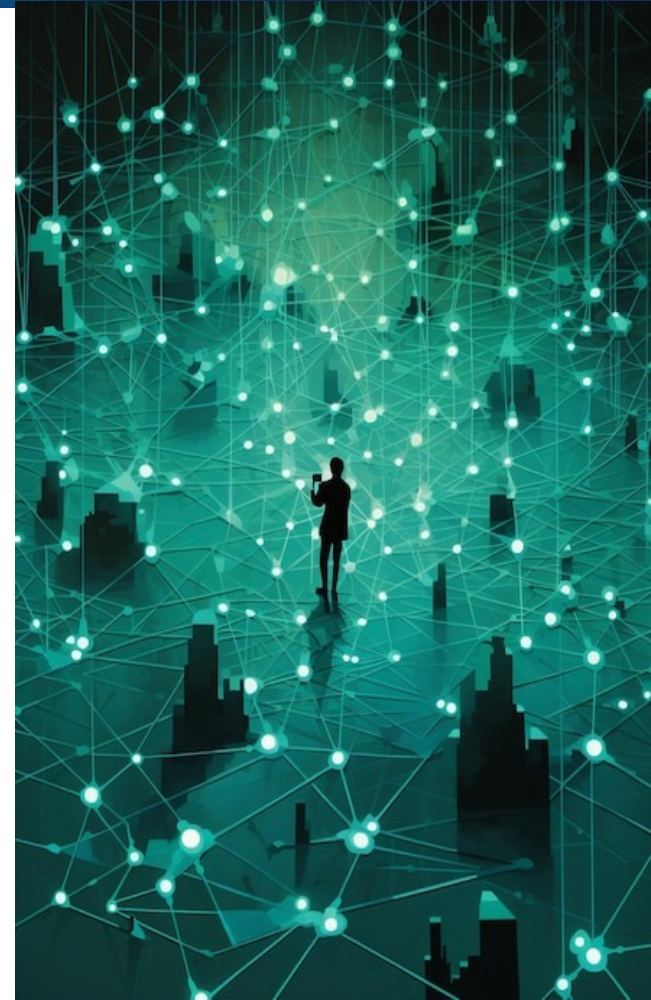
Monitoring: **11.5**

Problem management: **4.7**

Data Aggregation, Representation and Visualisation: **3.8**

Ticketing: **1.5**

Knowledge Management: **5.2**

Reporting and Statistics: **4.4**

Bidirectional Communication: **6.4**

Unidirectional Communication: **2.8**

Configuration Management and Backup: **2.3**

Performance Management: **5.7**

Inventory Management: **2.6**

Resources Management: **2.4**

Out-of-Band Access Management: **3.4**

Change Management: **2.4**

Security Management: **6**

Source: SIG-NOC Tools Survey 2023

FUNCTIONALITIES

- Monitoring
- Problem Management
- Ticketing
- Knowledge Management and Documentation
- Reporting and Statistics
- Communication, Coordination and Chat - Bidirectional
- Communication, Coordination and Chat - Unidirectional
- Configuration Management and Backup
- Performance Management
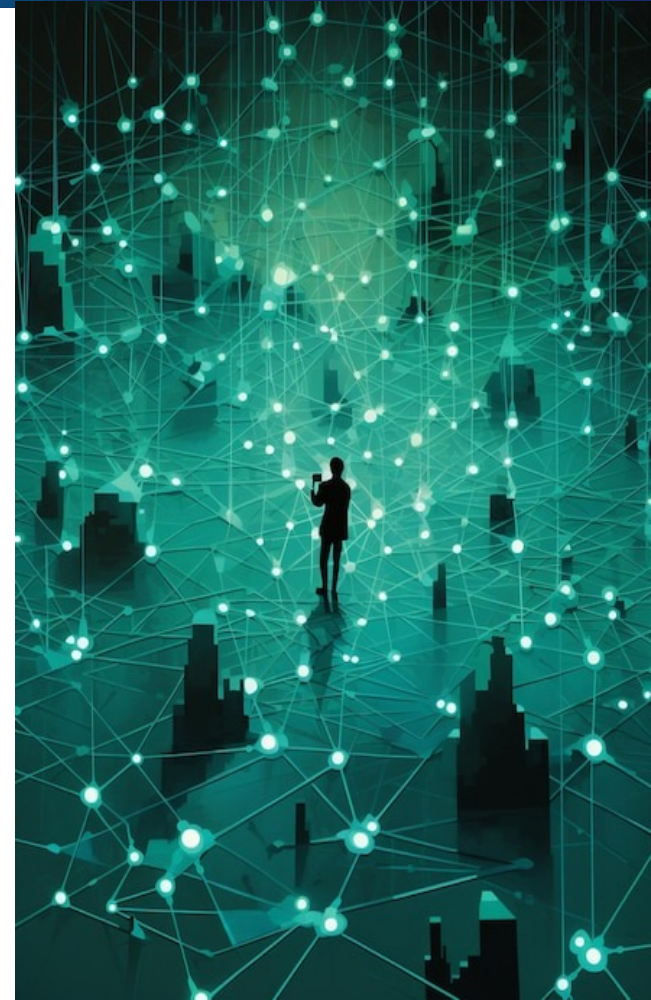- Inventory Management
- Resources Management
- Out-of-band Access Management
- Change Management
- Security Management
- Data Aggregation, Representation, Visualisation
- DDoS Mitigation
- Orchestration, automation and virtualisation

https://wiki.geant.org/display/SIGNOC/SIG-NOC+Tools+Survey+2023

2023 Tools Matrix

SIG-NOC

	CACTI	CONFLUENCE	E-mail	GRAFANA	JIRA	MAILING LISTS	MRTG	NAGIOS	OTRS	RANCID	REQUEST TRACKER	RIPE Atlas / Stats	SPLUNK	WIKI	ZABBIX
# FUNCTIONALITIES	3	4	2	4	4	2	3	3	4	3	6	3	4	5	3
Monitoring	21			35			25	27			18		25	17		20
Problem Management		17			17			22	13		15	19	11		16
Ticketing					14				11		15				
Knowledge Management and Documentation		19							11		10			17	
Reporting and Statistics	13			20			6	9			19		11		9
Communication, Coordination and Chat - Bidirectional			32			24								7	
Communication, Coordination and Chat - Unidirectional			28			27								9	
Configuration Management and Backup										16					
Performance Management				21			10					15			
Inventory Management					5					11				9	
Resources Management		7												13	
Out-of-band Access Management															
Change Management		7			11				9		9				
Security Management											8				
Data Aggregation, Representation, Visualisation	12			20									7		
DDoS Mitigation															
Orchestration, automation and virtualisation															
Usage	46	50	60	96	47	51	41	58	44	45	76	59	46	55	45

Tools mentioned in the survey more than 40 times

Source: SIG-NOC Tools Survey 2023

# FUNCTIONALITIES	CACTI	CONFLUENCE	E-mail	GRAFANA	JIRA	MAILING LISTS	MRTG	NAGIOS	OTRS	RANCID	REQUEST TRACKER	RIPE Atlas / Stats	SPLUNK	WIKI	ZABBIX
# FUNCTIONALITIES	3	4	2	4	4	2	3	3	4	3	6	3	4	5	3
Monitoring	21			35			25	27		18		25	17		20
Problem Management		17			17			22	13		15	19	11		16
Ticketing				14					11		15				
Knowledge Management and Documentation		19							11		10			17	
Reporting and Statistics	13			20			6	9			19		11		9
Communication, Coordination and Chat - Bidirectional		32			24									7	
Communication, Coordination and Chat - Unidirectional		28			27									9	
Configuration Management and Backup										16					
Performance Management				21			10					15			
Inventory Management					5					11				9	
Resources Management		7												13	
Out-of-band Access Management															
Change Management		7			11				9		9				
Security Management											8				
Data Aggregation, Representation, Visualisation	12			20									7		
DDoS Mitigation															
Orchestration, automation and virtualisation															
Usage	46	50	60	96	47	51	41	58	44	45	76	59	46	55	45

Convergence of most frequently used tools

Do any of your systems today combine multiple sources of data or augment your measurements with metadata from a source of truth type database?

Combining multiple data sources
including from a Source of Truth system

● Yes (1/3)

● No (2/3)
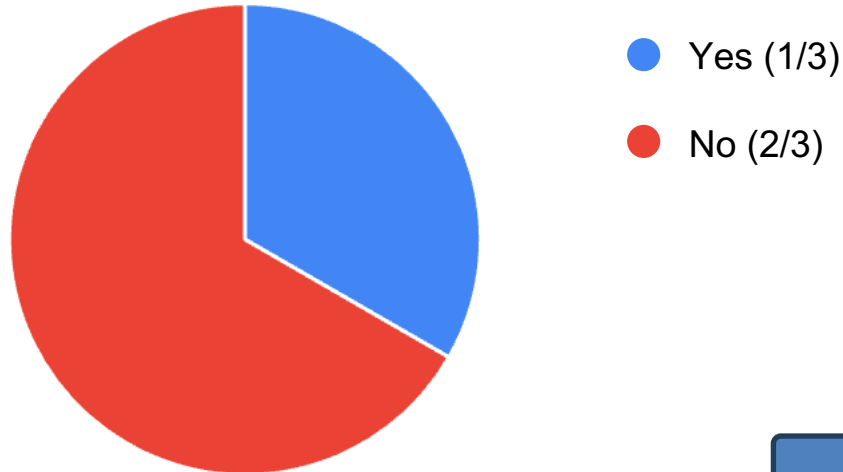
Source: MetrANOVA Survey 2023

Measurement Pain Points

- **System integration**
- **Data cross-correlation**, correlation of data sets
- **One dashboard** for multiple data sources
- Common **data models** between different vendors
- **Metatagging** in databases
- **Event extractions** from telemetry and optical data sets
- Network source of truth
- Offering high level **flow reports** to our membership
- Using netflow data for network design and operations
- Bit error rates
- Streaming Telemetry
- More accurate measurements
- Accurately show the status and capabilities for wireless links

Source: MetrANOVA Survey 2023

NOC Monitoring and Management Data

- Measurements from optical systems
- Port level counters and stats
- Interface status and statistics
- BGP peering / route feeds
- Routing updates
- Delay, Jitter, Packet loss
- Network flow data
- Host level metrics
- Application level metrics

Source: MetrANOVA Survey 2023
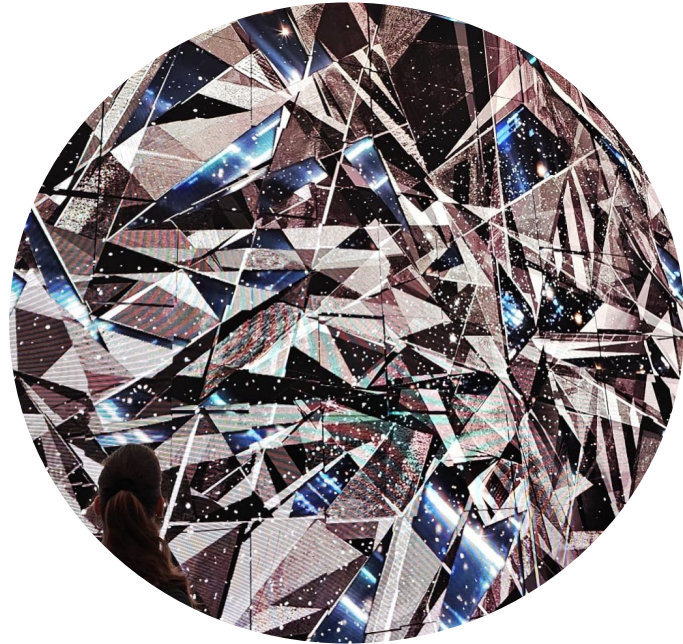
Usage of Monitoring Data

Troubleshooting

Network planning

User reporting

Usage of Monitoring Data

Troubleshooting

> Where is the problem?
> What is the problem?
> What has caused the problem?
> Which device / service is affected? …

Network planning

> Which device(s) should I replace / add / remove?
> Which links should be upgraded?
> Which services should I change/upgrade/retire? …

User reporting

> Who is using which service?
> How often, how much?
> What is user experience for the service?
> Which service performance the user experiences? …

Challenges

- Multiple data sources
- Huge amount of data

- Data correlation
- Integration
- Representation

- Tools
- Automation
- AI

And now YOU!

Nils Arne Eggen

Norwegian footballer and manager

(1941 - 2022)

Nils Arne Eggen (born 17 September 1941 , died 19 January 2022) was a Norwegian football player , football coach and lecturer.

As a player, he won three league golds and one cup gold. As a coach, he was the most successful Norwegian football coach of all time with 15 league championships and six cup championships. One of the series championships as a coach was for Moss , the rest with Rosenborg Ballklub , where he was coach for six periods: [8] 1971–1972, 1976, 1978–1982, 1988–1997, 1999–2002 and 2010. He led Rosenborg for six seasons to The Double , [9] and for seven seasons he led Rosenborg to the Champions League group stage.

Nils Arne Eggen's sporting success gave him a unique status in Trønder sports. His ideas about 4-3-3, fun and attacking football, and the goodfoot theory have inspired many football coaches to play according to his philosophy in Norway and abroad. In 2020, Eggen was voted Trønder's most influential person in sports, ahead of Olympic champions such as Hjalmar Andersen and Petter Northug . [10]

You are a NOC engineer!

You are a NOC engineer!
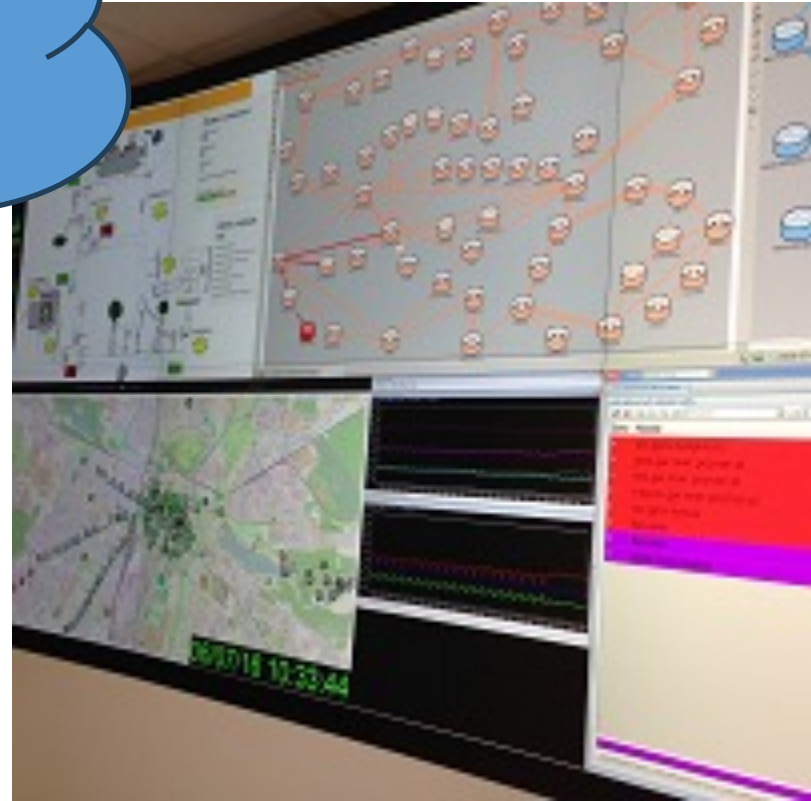
Responsible for managing your network

NILS ARNE EGGEN

You are a NOC engineer/manager,

Responsible for managing your network

You have all the Network Management tools and systems you want!

ACL	Ansible	ARBOR	ARGUS	BGMON		BGPALERTER	BGPMON
Blackholing	BOX	BWCTL	CA SPECTRUM	CACTI	Cisco NSO	CLEARPASS (ARUBA)	CONFLUENCE
CONSOLE SERVER		CORERO	CRICKET	CVS	DNS solution	Docker	DOCUWIKI	DRAC
DROPBOX	EDUMEET	ELASTICSEARCH		ELK STACK	E-mail	E-MAIL	EXCEL	FIPS
FIREWALL	Firewall on Demand		FIREWALLBUILDER		FITSM standards		FREERADIUS	FTTH /FTTx	GIT
GITLAB	GOOGLE DRIVE		GRAFANA	GRAYLOG	HADES	HP ILO	ICINGA	IDS	IM
IMS	INFLUXDB/INFLUX STACK		INFOBLOX	INTERMAPPER	IPERF	IPS	IRR	ISDN	JABBER
Jenkins scripting		JIRA	Junos Space	KENTIK	KERBEROS	KERBEROS·	KIBANA	Kubernetes	KVM
Landline	LIBRENMS	LIBRESPEED	LOGSTASH	LOOKING-GLASS		MAILING LISTS	MATTERMOST	MEDIAWIKI	MGEN
MICROSOFT ONEDRIVE		Mobile	MRTG	MUNIN	NAGIOS	NAV	NDT	NEMO
NETBOX	NEXTCLOUD	NFDUMP	NFSEN	NIST	NITS	NLNOG RING	Northstar	OBSERVIUM
OPENVIEW	OTRS	OWAMP/TWAMP		OWNCLOUD	OXIDIZED	PerfSONAR	PHPIPAM	PMACCT	PMP
PROMETHEUS	Provisioning	Puppet	Python scripting		RACKTABLES	RADIATOR	RANCID	RATE-LIMITING
REQUEST TRACKER		RIPE Atlas / Stats		RIPE RIS / BGPlay		ROCKETCHAT	RSA Software	RTBH
Rundeck	Salt	SERVICENOW	SHAREPOINT	SILK	SKYPE	SLACK	SMARTxAC	SMOKEPING
SPECTRUM	SPEEDTEST	SPLUNK	SUBVERSION	SURICATA	TABLEAU	TACACS+	TEAMS	THREAT INTELLIGENCE
TIMEMAP	TIMETOP	TWITTER	UTRS	VISIO	WEATHERMAP		WHATSAPP	WIFIMON	WIKI
WIRESHARK	ZABBIX	ZENDESK	ZENOSS	ZINO	ZOOM			

Task 1: What do I need to know?

Which questions

do I need to be able to answer about my network / system related to:

1. Troubleshooting

2. Planning

3. User reporting

Write at least 2 questions per each of the topics.

Task 2: Transformation

For each of the questions

specify the data that you need

in order to be able to answer the question, and

name the tool where the data can be found.

Task 2: Transformation

For each of the questions **specify the data that you need** in order to be able to answer the question, and **name the tool where the data can be found.**

- Measurements from Optical Systems
- Port level counters and stats
- Interface status and statistics
- BGP peering / route feeds
- Routing updates
- Delay, Jitter, Packet loss
- Network flow data
- Host level metrics
- Application level metrics
- ...

		ARGUS	BGMON	BGP FLOWSPEC				
	6WCTL	CA SPECTRUM	CACTI	Cisco NSO	CLEARPASS (ARUBA)			
		CORERO	CRICKET	CVS	DNS solution	Docker	DOCUWIKI	Dn.
	EDUMEET	ELASTICSEARCH		ELK STACK	E-mail	E-MAIL	EXCEL	FIPS
...L		Firewall on Demand		FIREWALLBUILDER	FITSM standards		FREERADIUS	FTTH /FTTx
...AB	GOOGLE DRIVE		GRAFANA	GRAYLOG	HADES	HP ILO	ICINGA	IDS	IM
...S	INFLUXDB/INFLUX STACK		INFOBLOX	INTERMAPPER	IPERF	IPS	IRR	ISDN	JABBE.
enkins scripting		JIRA		Junos Space	KENTIK	KERBEROS	KERBEROS.	KIBANA	Kubernetes	KVM
Landline	LIBRENMS	LIBRESPEED		LOGSTASH	LOOKING-GLASS		MAILING LISTS	MATTERMOST	MEDIAWIKI	MGEN
MICROSOFT ONEDRIVE		Mobile		MRTG	MUNIN	NAGIOS	NAV	NDT	NEMO
...ETBOX	NEXTCLOUD	NFDUMP		NFSEN	NIST	NITS	NLNOG RING	Northstar	OBSERVIUM
...PENVIEW	OTRS		OWAMP/TWAMP		OWNCLOUD	OXIDIZED	PerfSONAR	PHPIPAM	PMACCT	PMP
...METHEUS Provisioning	Puppet		Python scripting		RACKTABLES	RADIATOR	RANCID	RATE-LIMITING
...TRACKER		RIPE Atlas / Stats		RIPE RIS / BGPlay		ROCKETCHAT	RSA Software	RTBH
	Salt	SERVICENOW	SHAREPOINT	SILK	SKYPE	SLACK	SMARTxAC	SMOKEPI.
	...OTEST	SPLUNK	SUBVERSION	SURICATA	TABLEAU	TACACS+	TEAMS	TH.
		...WITTER	UTRS	VISIO	WEATHERMAP		WHATS.
		...ENOSS	ZINO	ZOOM		

NOC Functions 2023
Monitoring
Problem Management
Ticketing
Knowledge Management and Documentation
Reporting and Statistics
Communication, Coordination and Chat
Configuration Management and Backup
Performance Management
Inventory Management
Resources Management
Out-of-band Access Management
Change Management
Training
Security Management
Data Aggregation, Representation, Visualizatio...
DDoS Mitigation
Orchestration, automation and virtualisation

Task 3: Automation journey

For each of the questions from all three categories, **define the process** that needs to be followed **to get the answers** to your questions.

Task 3: Automation journey

For each of the questions from all three categories, **define the process** that needs to be followed **to get the answers** to your questions.

- How is the process triggered

- What is the first step that needs to be done

- Second, third,……. last

- How it terminates?

- What are the results and how are they visualised.

Thank You!

netdev@lists.geant.org