

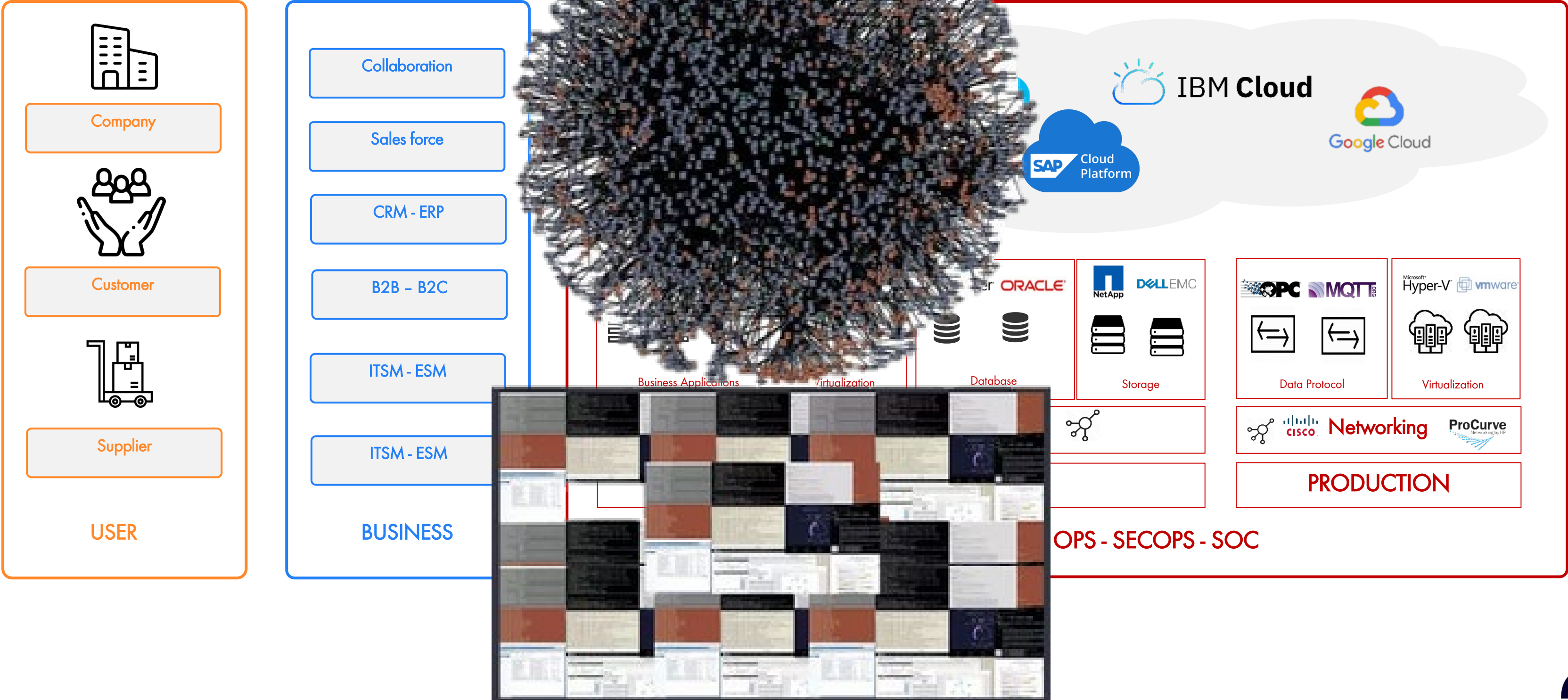


NetEye vision

Intelligenza artificiale: evoluzione e impatti

Georg Kostner, BU manager IT Systems & Service Management

VISION



VISION





Company



Customer



Supplier

USER

Collaboration

Sales force

CRM - ERP

B2B - B2C

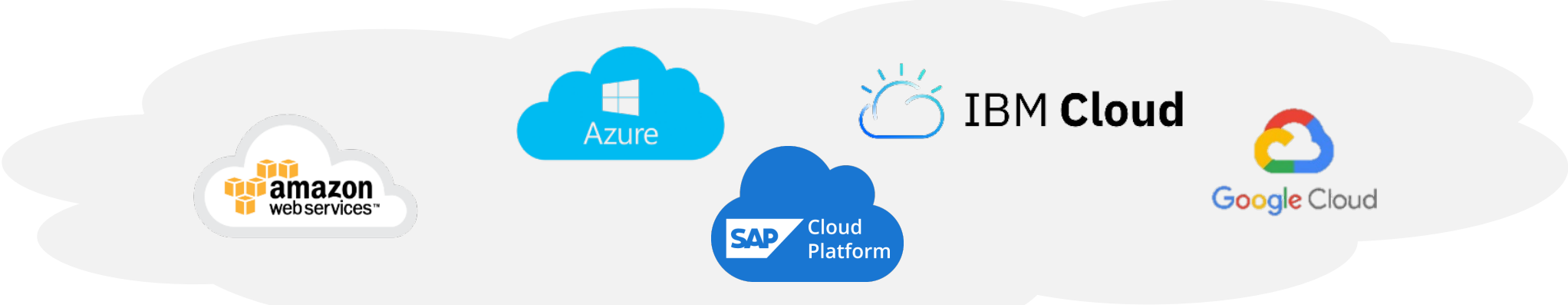
ITSM - ESM

ITSM - ESM


BUSINESS

Visual Mon
Web Mon
RUM

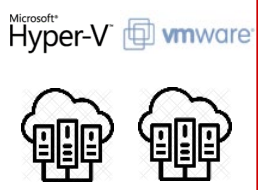
Business Impact
Business Process
SLM - SLA




On-Premise




Business Applications



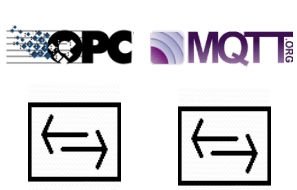
Virtualization



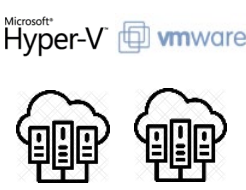
Database





Storage





Data Protocol



Virtualization



Networking



DATACENTER

DEV - DEV OPS - IT OPS - SECOPS - SOC

PRODUCTION

Datacenter Monitoring
Network Performance Monitoring

System Monitoring
Observability (Metric, Logs, Trace)
SLI - SLO

Automation
SIEM

UNIFIED MONITORING PLATFORM

ORGANIZATION - PROCESSES

NetEye

Monitoring

Service disruption?

Reliability?

Status?

Incident Management

Responsiveness – Fit for use



Incident

Observability

Performance?

Saturation, Scalability?

Resources – Cost

Anomaly Detection – ML

User Experience



Problem

SIEM - SECURITY

Threat Actor?

Data exfiltration?

Detection Rules

Anomaly Detection - ML

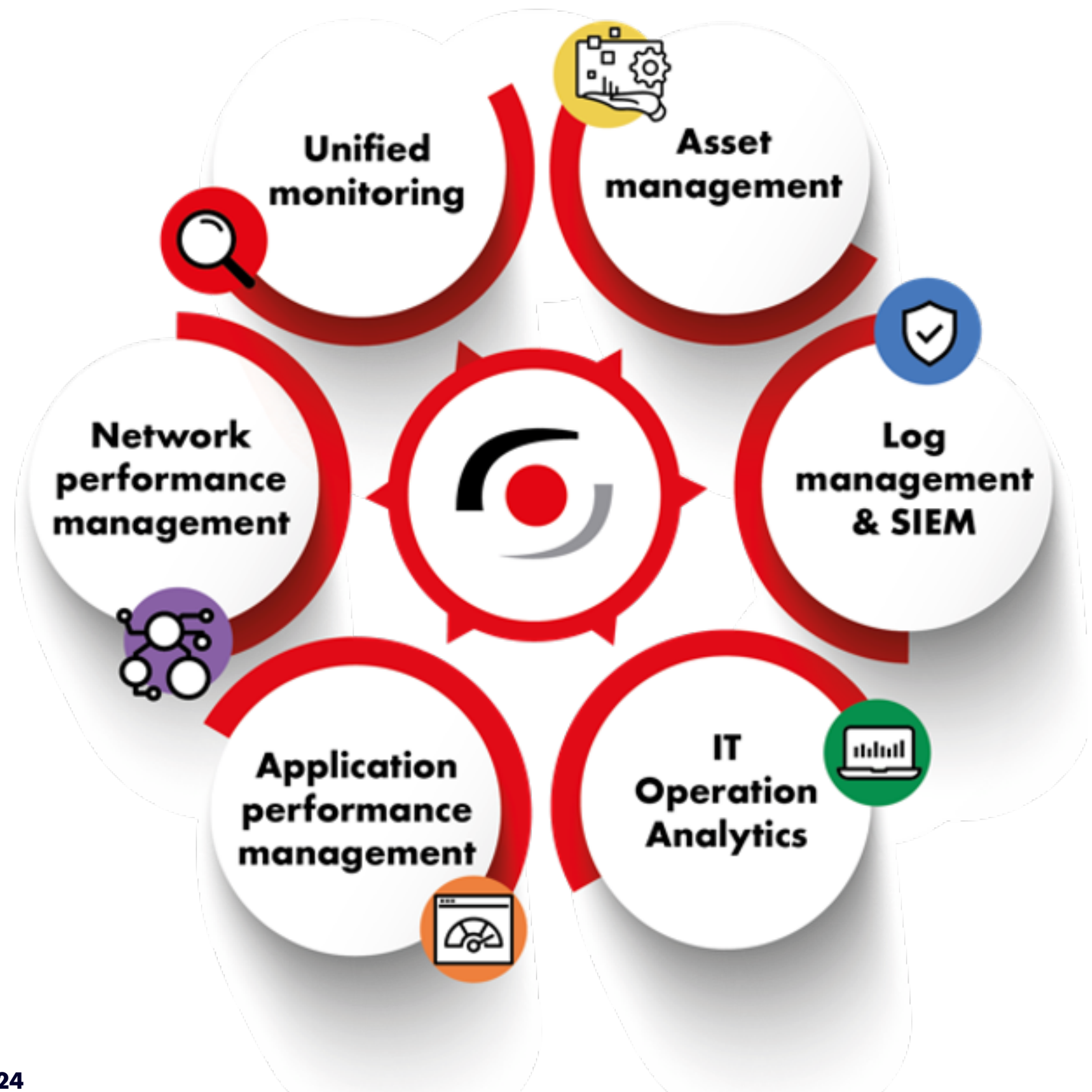


Security

RULE BASED ACCESS



UNIFIED MONITORING PLATFORM

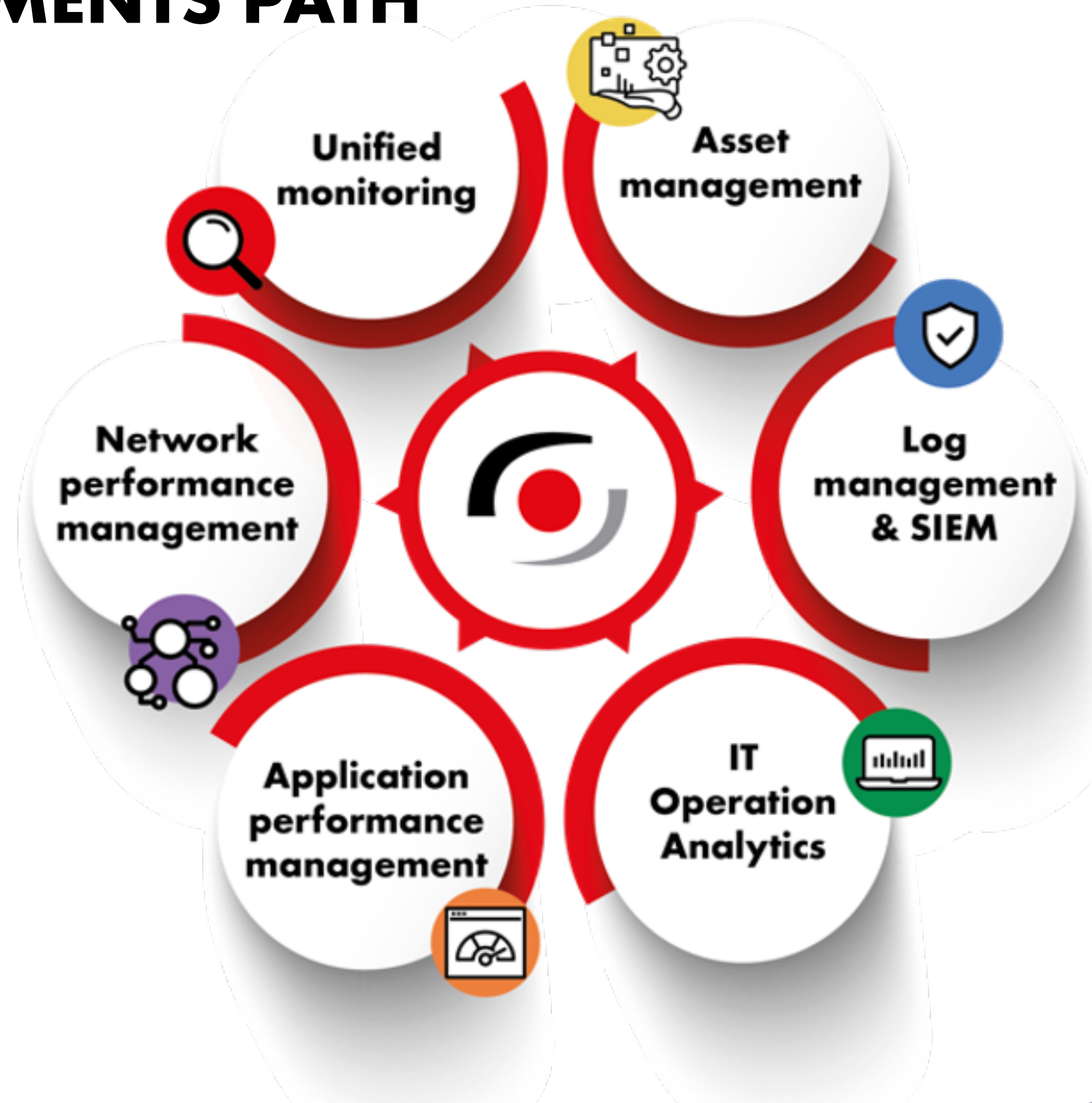


NetEye^{cloud}
since 2021



NETEYE DEPLOYMENTS PATH

NetEye
on prem



NetEye^{cloud}



NETEYE AUTHENTICATION

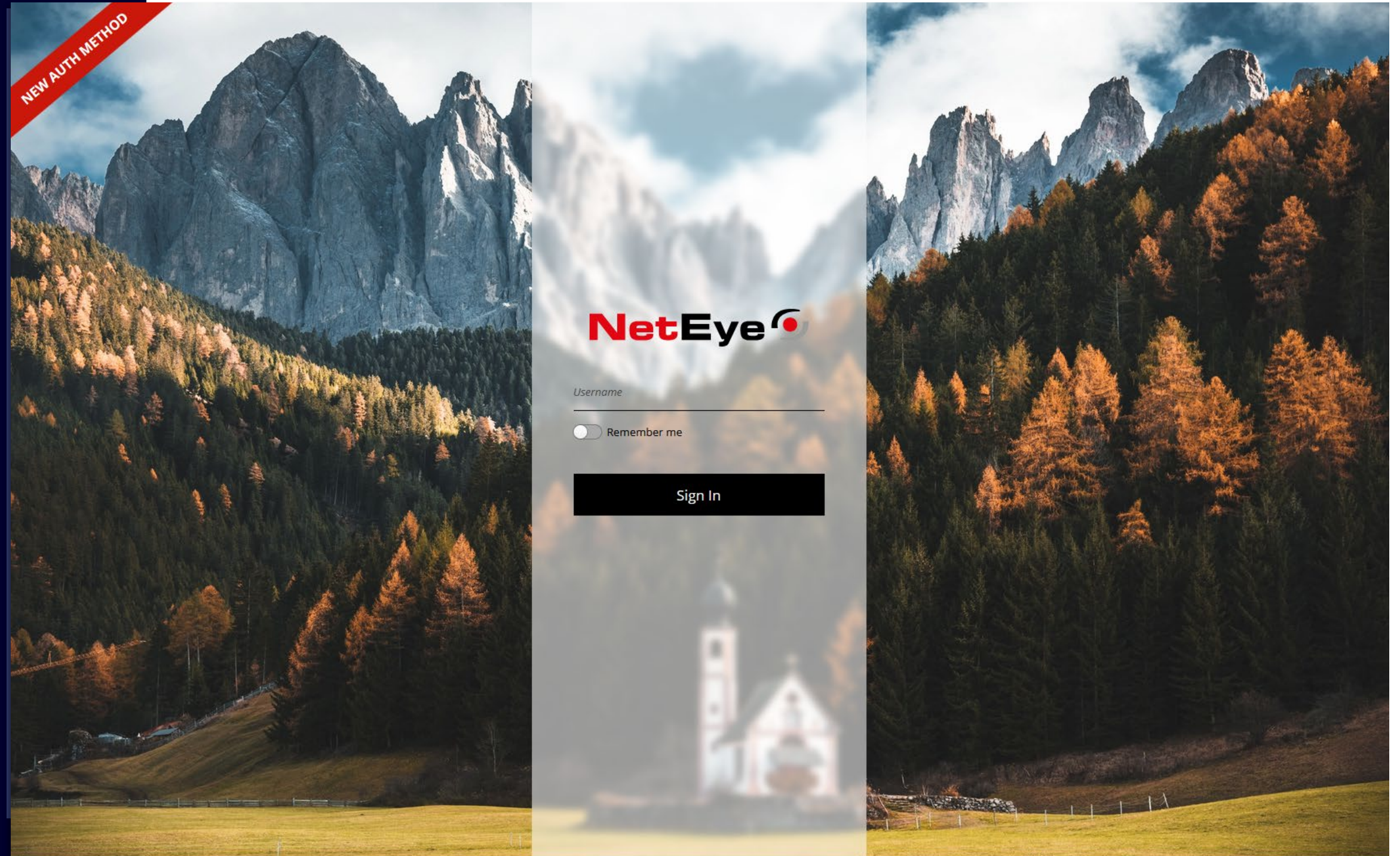
Single Sign On

IdP Integration

OpenID - OAUTH

SAML

LDAP - AD



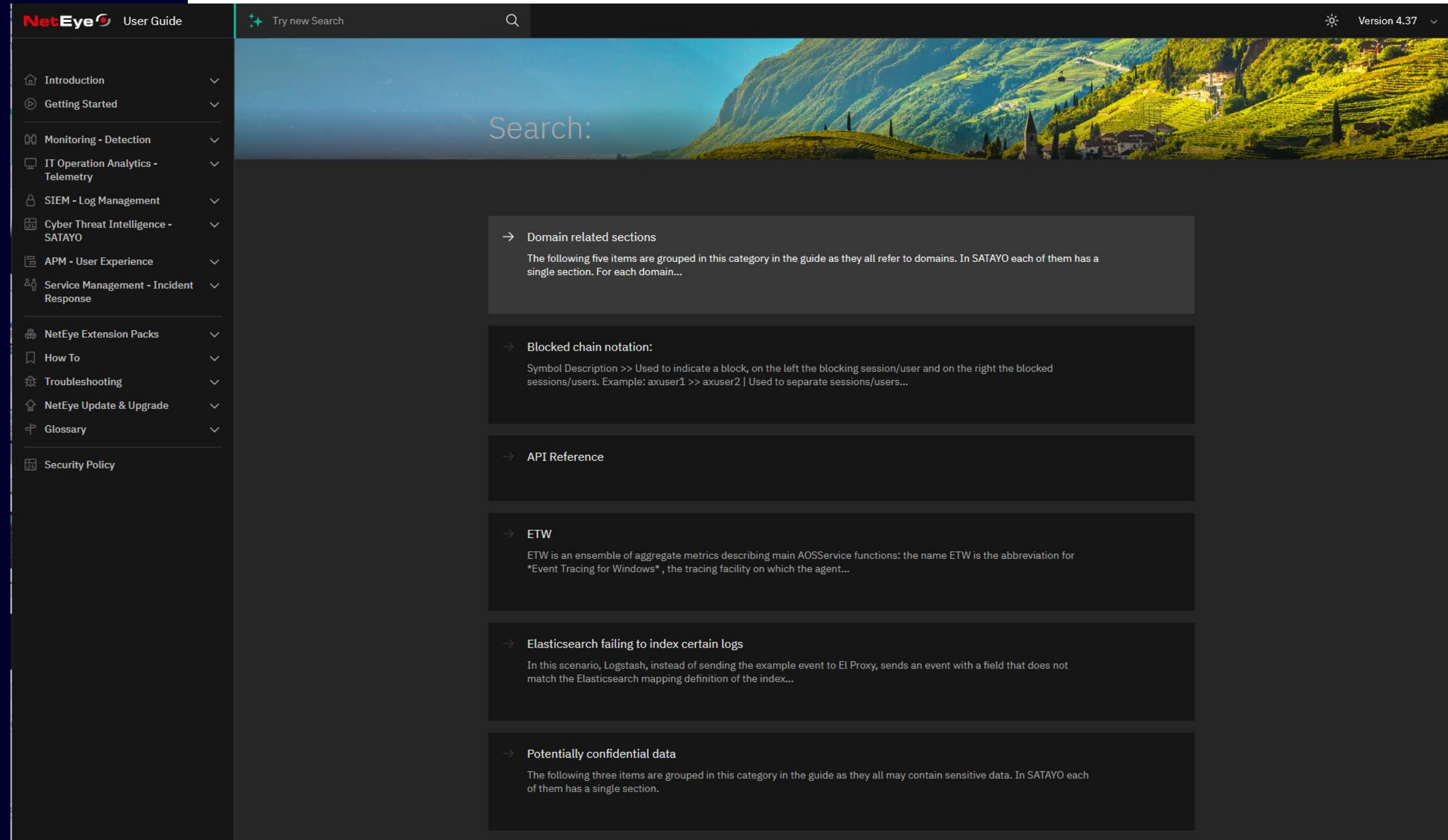
<https://www.keycloak.org/>



NETEYE GUIDE

Continuous improvement

Search Content Structure



The screenshot displays the NetEye User Guide interface. On the left is a dark sidebar with a 'User Guide' header and a list of categories: Introduction, Getting Started, Monitoring - Detection, IT Operation Analytics - Telemetry, SIEM - Log Management, Cyber Threat Intelligence - SATAYO, APM - User Experience, Service Management - Incident Response, NetEye Extension Packs, How To, Troubleshooting, NetEye Update & Upgrade, Glossary, and Security Policy. The main content area has a top header with 'Try new Search' and a search icon, and a version indicator 'Version 4.37'. Below the header is a large image of a mountain landscape with the word 'Search:' overlaid. The search results are listed in a dark theme with light text. Each result is preceded by a right-pointing arrow.

- Domain related sections
The following five items are grouped in this category in the guide as they all refer to domains. In SATAYO each of them has a single section. For each domain...
- Blocked chain notation:
Symbol Description >> Used to indicate a block, on the left the blocking session/user and on the right the blocked sessions/users. Example: axuser1 >> axuser2 | Used to separate sessions/users...
- API Reference
- ETW
ETW is an ensemble of aggregate metrics describing main AOSService functions: the name ETW is the abbreviation for *Event Tracing for Windows*, the tracing facility on which the agent...
- Elasticsearch failing to index certain logs
In this scenario, Logstash, instead of sending the example event to El Proxy, sends an event with a field that does not match the Elasticsearch mapping definition of the index...
- Potentially confidential data
The following three items are grouped in this category in the guide as they all may contain sensitive data. In SATAYO each of them has a single section.

<https://neteye.guide/>



NETEYE CORE

Update, Upgrade, Install via Ansible

Parallel execution
Simplified
Maintainability
Log(s) - debug

```
ok: [localhost] => {
  "dnf_result": {
    "changed": true,
    "failed": false,
    "msg": "",
    "rc": 0,
    "results": [
      "Installed: icingaweb2-module-alyvix-configurator-0.55.1-1.noarch",
      "Installed: elastic-stack-configurator-1:8.14.3_neteye3.65.0-1.noarch",
      "Installed: neteye-setup-configurator-1:1.130.2-1.noarch",
      "Installed: elastic-blockchain-proxy-configurator-1.3.0-1.noarch",
      "Installed: icingaweb2-module-tornado-configurator-2.16.4-1.noarch",
      "Removed: elastic-blockchain-proxy-configurator-1.2.5-2.noarch",
      "Removed: elastic-stack-configurator-1:8.14.3_neteye3.64.2-1.noarch",
      "Removed: neteye-setup-configurator-1:1.130.1-1.noarch",
      "Removed: icingaweb2-module-alyvix-configurator-0.55.0-1.noarch",
      "Removed: icingaweb2-module-tornado-configurator-2.15.2-1.noarch"
    ]
  }
}

PLAY RECAP *****
localhost                : ok=16  changed=3  unreachable=0  failed=0  skipped=5  rescued=0  ignored=0

*****
* We are starting the update of NetEye *
* This activity can take a non trivial amount of time *
* to complete. *
* Please do not press ctrl+c or other commands *
* until the NetEye update has finished. *
*****

You can follow the update logs for every service in the following folder: /neteye/local/os/log/neteye_command/update/20240717-140301
icingaweb2                [5/5]: Done in 8s
icingaweb2-module-tornado [1/1]: Done in 50s
neteye-setup              [1/1]: Done in 14s
snmptrapd-neteye-config   [1/3]: Started Playbook
alyvix                    [1/1]: Done in 3s

0:24/00:28 1x
```

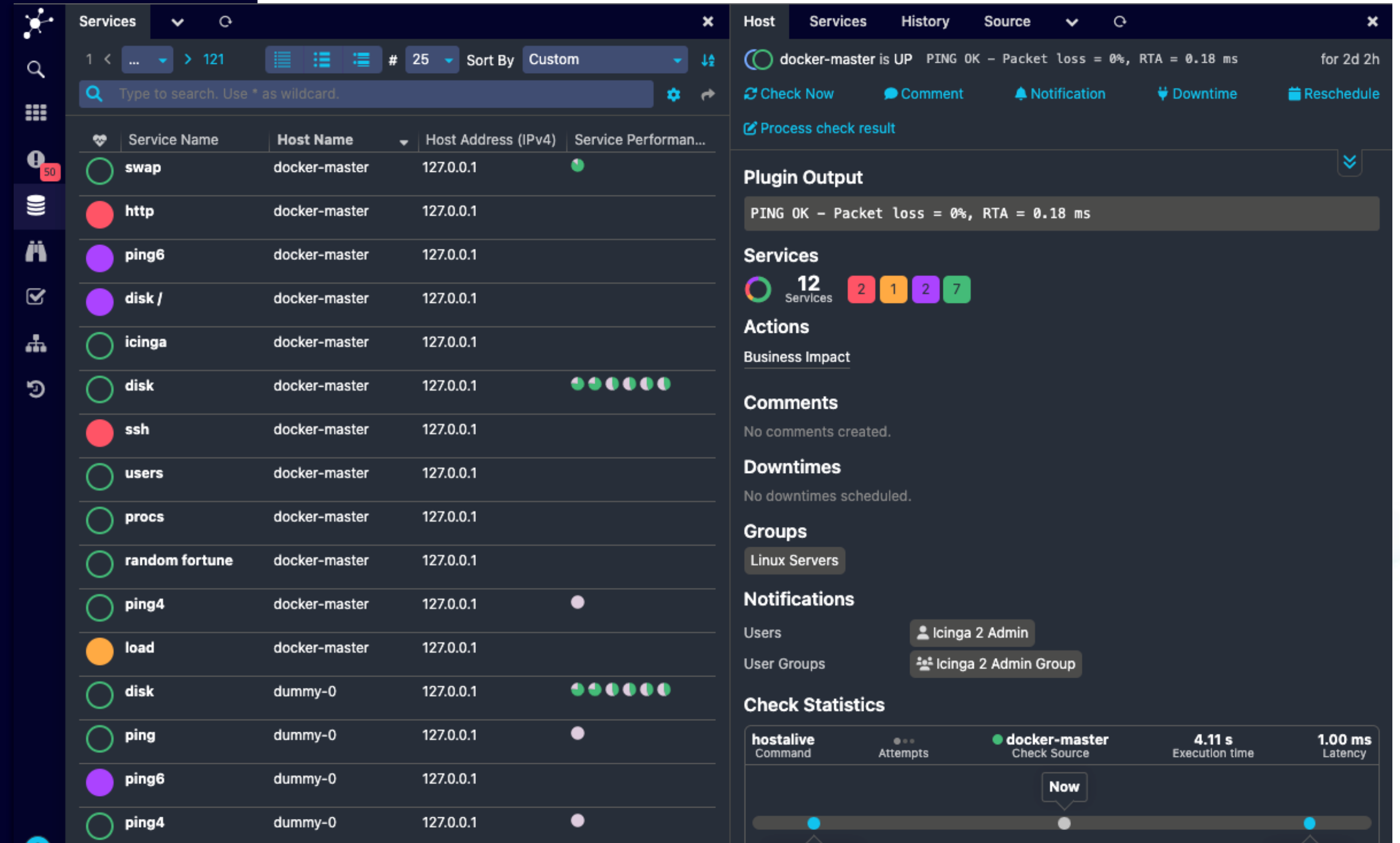
<https://github.com/ansible/ansible>



ICINGA DB WEB

Roadmap

Performance
Scalability
Web UX
Filter



The screenshot displays the Icinga DB Web interface, divided into two main panels. The left panel shows a list of services under the 'Services' tab, with a search bar and various filters. The right panel shows the details for a specific host, 'docker-master', under the 'Host' tab, including a status bar, plugin output, and various statistics.

Services List:

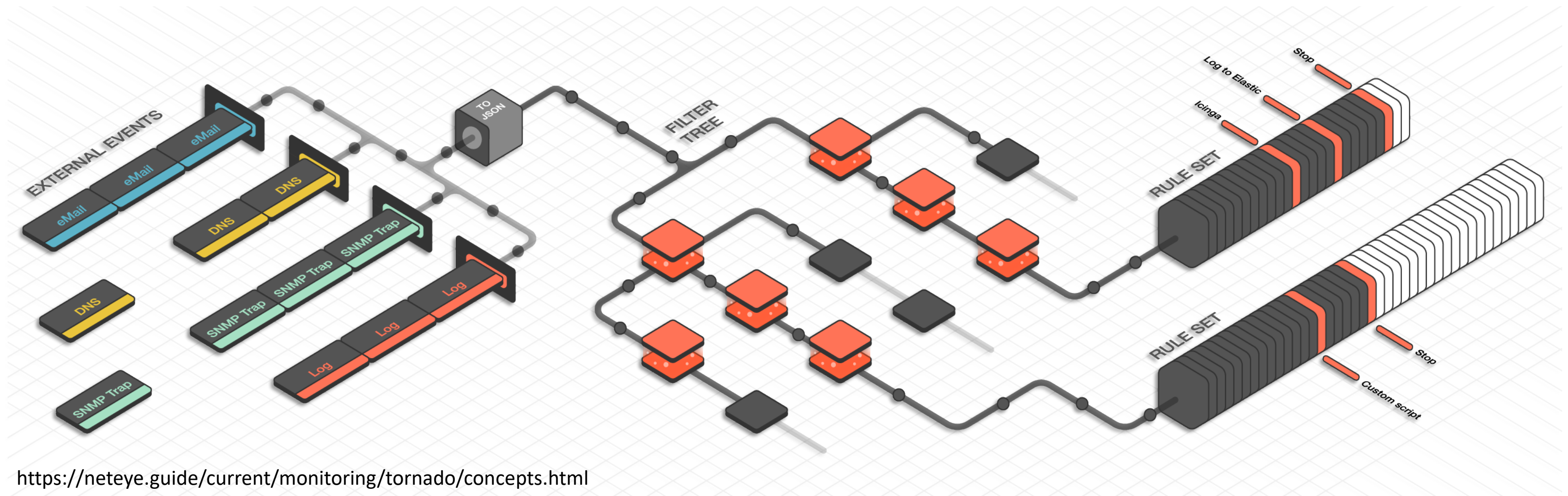
Service Name	Host Name	Host Address (IPv4)	Service Performance
swap	docker-master	127.0.0.1	●
http	docker-master	127.0.0.1	●
ping6	docker-master	127.0.0.1	●
disk /	docker-master	127.0.0.1	●
icinga	docker-master	127.0.0.1	●
disk	docker-master	127.0.0.1	● ● ● ● ● ● ● ●
ssh	docker-master	127.0.0.1	●
users	docker-master	127.0.0.1	●
procs	docker-master	127.0.0.1	●
random fortune	docker-master	127.0.0.1	●
ping4	docker-master	127.0.0.1	●
load	docker-master	127.0.0.1	●
disk	dummy-0	127.0.0.1	● ● ● ● ● ● ● ●
ping	dummy-0	127.0.0.1	●
ping6	dummy-0	127.0.0.1	●
ping4	dummy-0	127.0.0.1	●

Host Details (docker-master):

- Status: docker-master is UP PING OK - Packet loss = 0%, RTA = 0.18 ms for 2d 2h
- Actions: Check Now, Comment, Notification, Downtime, Reschedule
- Process check result
- Plugin Output: PING OK - Packet loss = 0%, RTA = 0.18 ms
- Services: 12 Services (2 red, 1 orange, 2 purple, 7 green)
- Actions: Business Impact
- Comments: No comments created.
- Downtimes: No downtimes scheduled.
- Groups: Linux Servers
- Notifications: Users (Icinga 2 Admin), User Groups (Icinga 2 Admin Group)
- Check Statistics: hostalive Command, Attempts, docker-master Check Source, 4.11 s Execution time, 1.00 ms Latency

TORNADO

External Event Integration



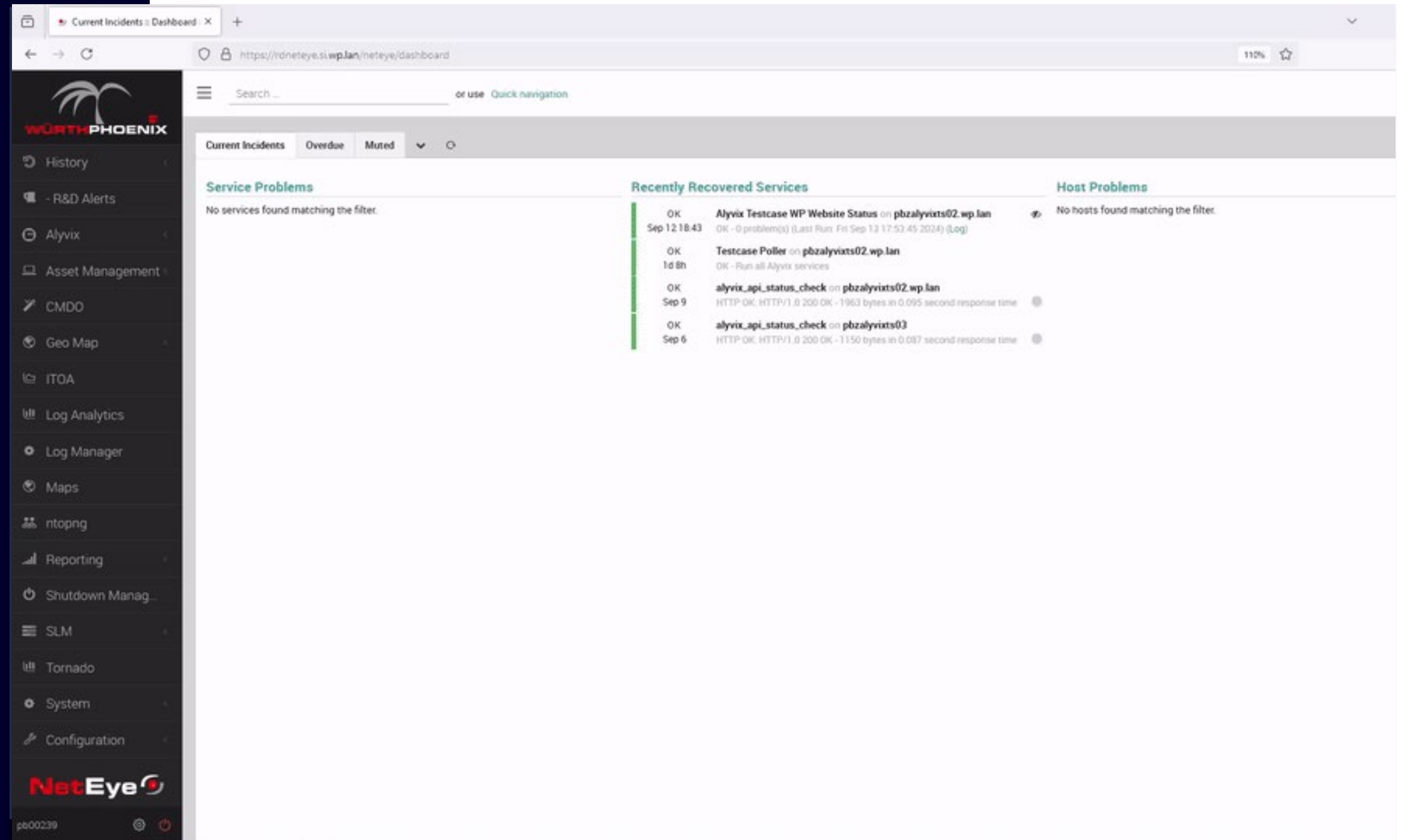
- Webhooks
- Syslog
- SMS
- SNMP Traps
- Email
- ...

TORNADO

Complex Event Processing

Usability
Event Test
Iterator

...



<https://neteye.guide/current/monitoring/tornado/concepts.html>

SNMP MONITORING AT SCALE

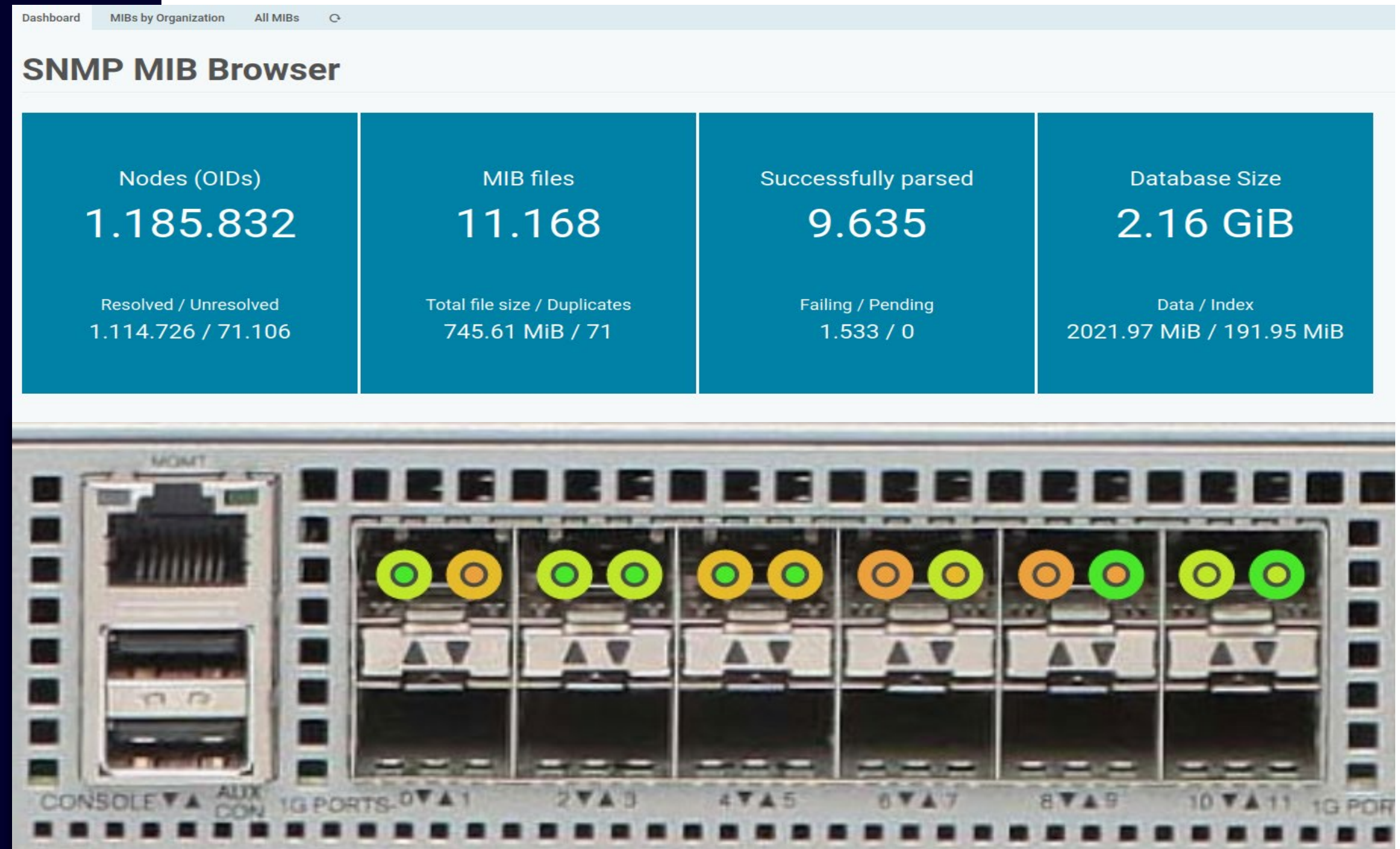
Roadmap (new module)

SNMP MIB Browser

SNMP Inventory

SNMP Polling at a scale
15sec

SNMP Polling in a
distributed way



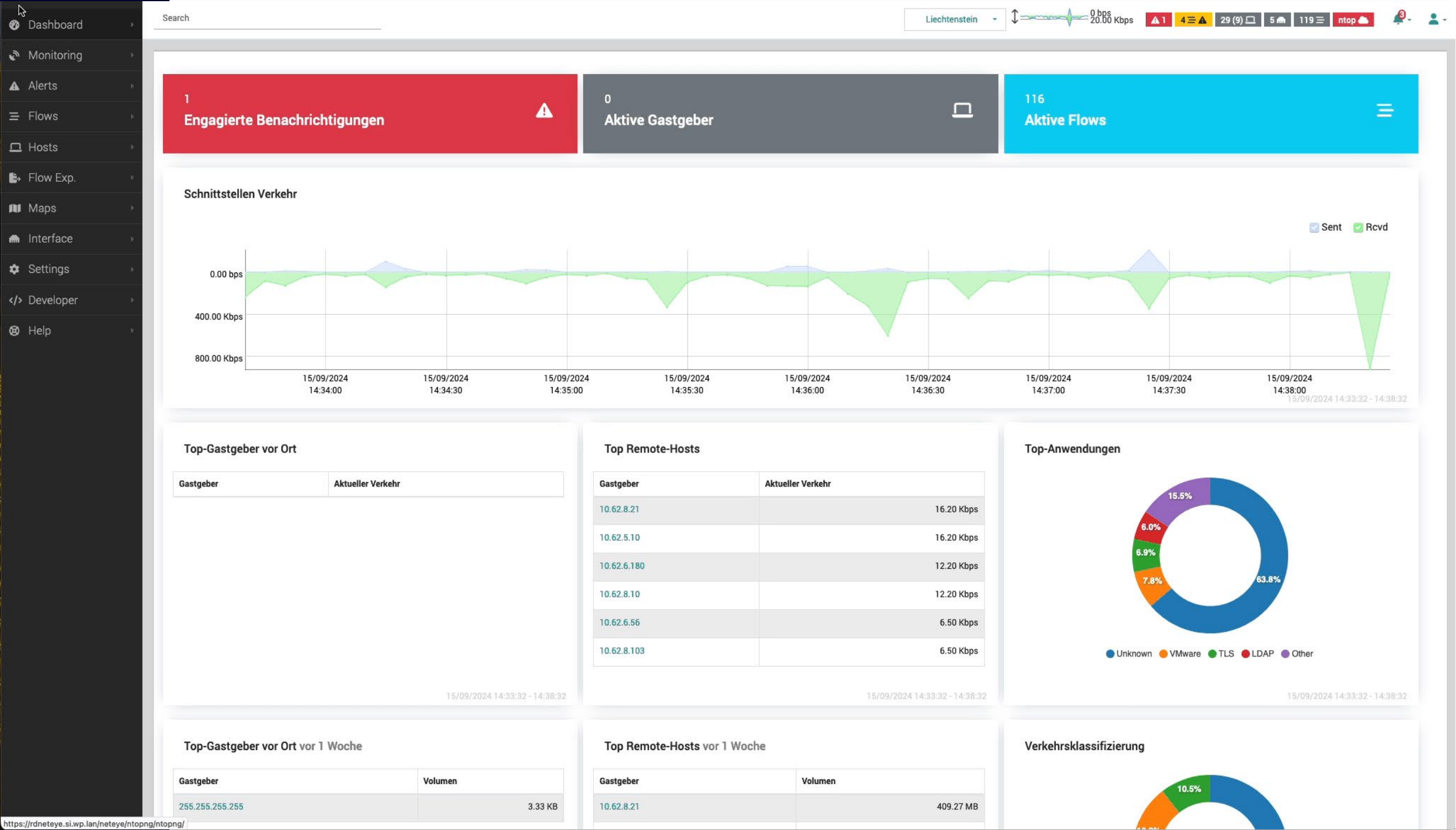
Thanks to



NTOPNG

Release 6.2

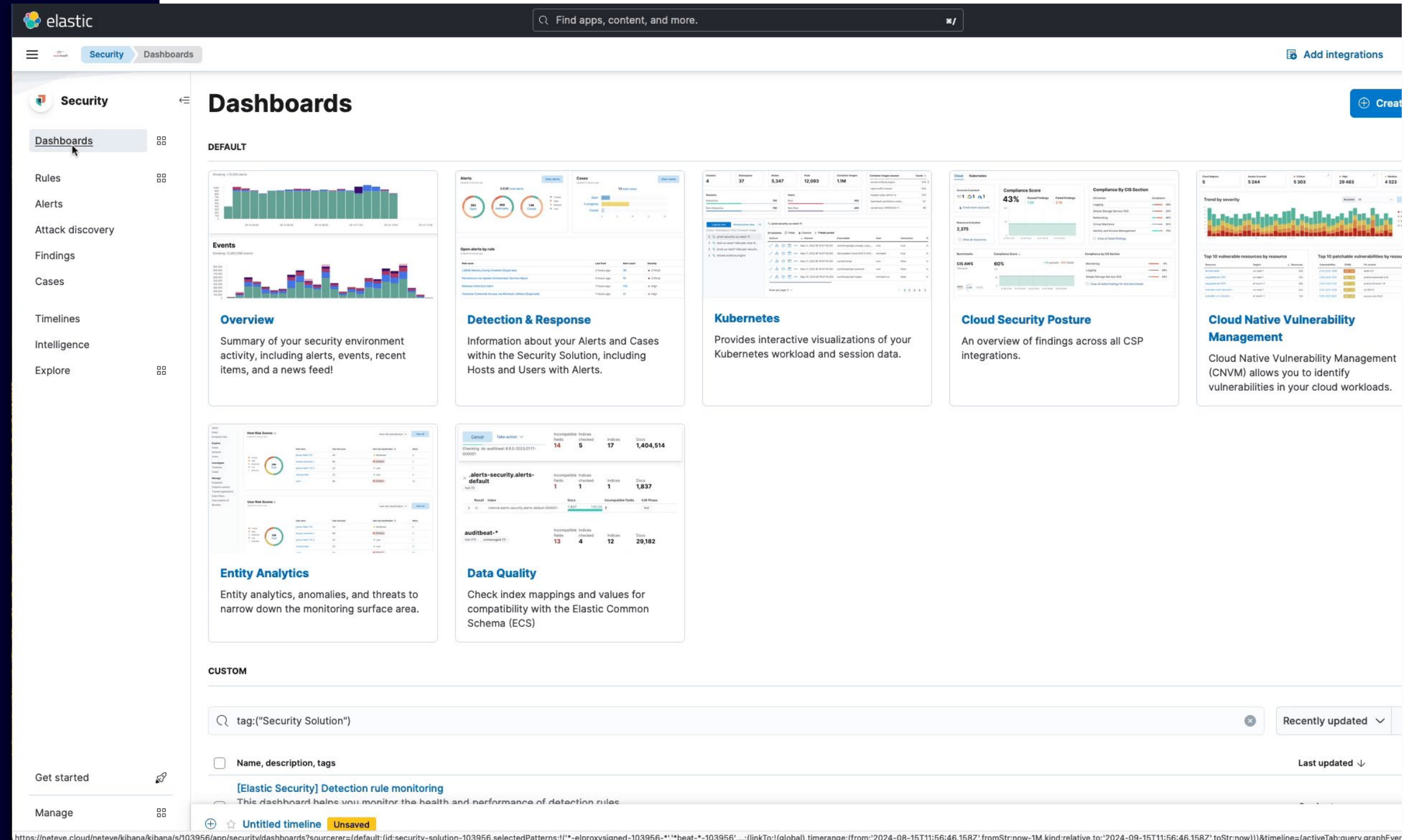
UX Improvemtns
Mitre Att&ck
Historical Flow
Replay
Periodic Reports
-60% Memory



ELASTIC RELEASE 8.15

News

Dashboards
Detection Response
Entity Analysis
Data Quality ECS
Mitre Att&ck

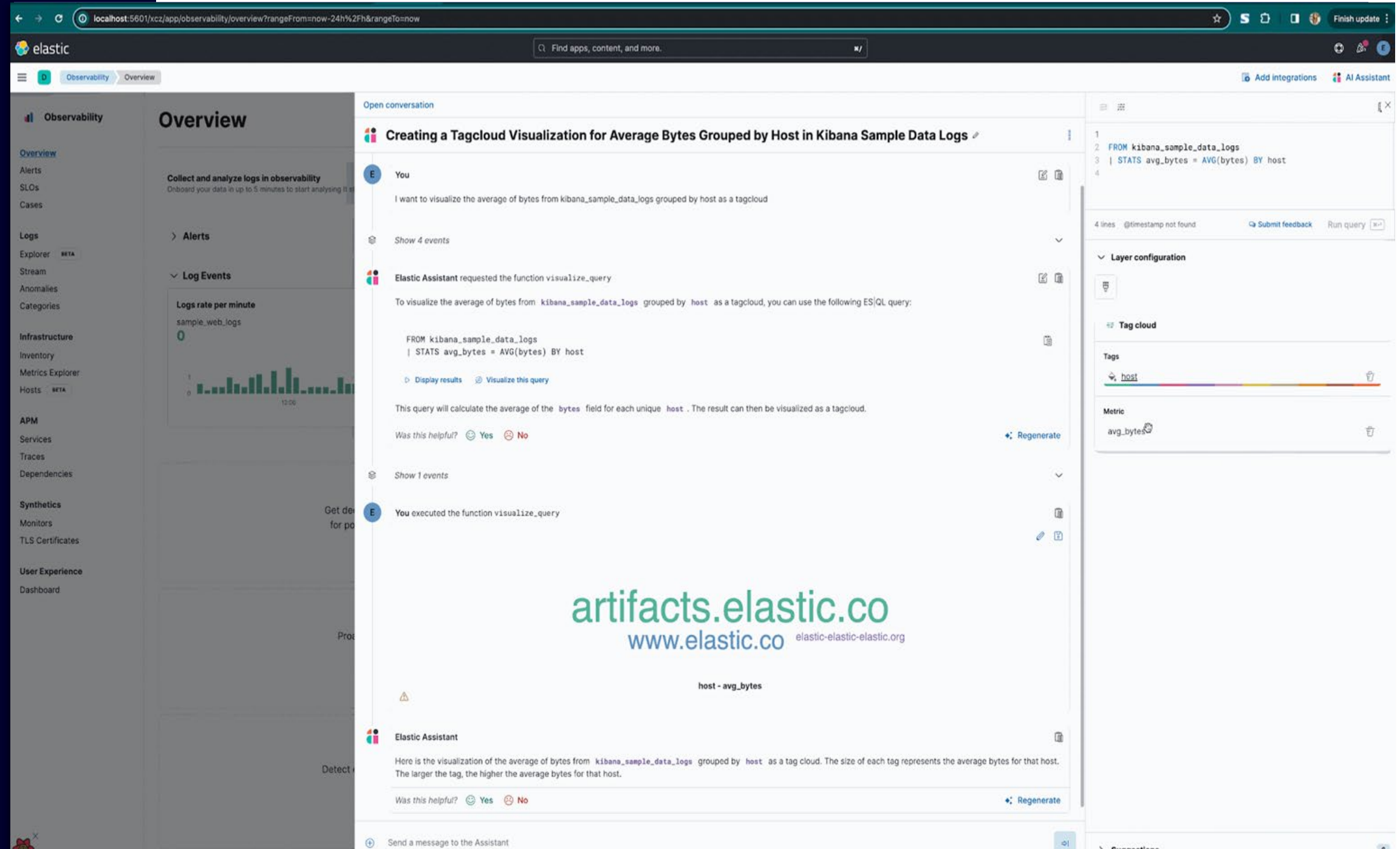


<https://demo.elastic.co/>

ELASTIC RELEASE 8.15

*ES/QL - Security
Observability AI assistant*

Streamlining the
workflow for users when
using the Observability
AI Assistant



The screenshot displays the Elastic Observability AI Assistant interface. The left sidebar shows the 'Observability' menu with options like Overview, Alerts, SLOs, Cases, Logs, Explorer, Stream, Anomalies, Categories, Infrastructure, Inventory, Metrics Explorer, Hosts, APM, Services, Traces, Dependencies, Synthetics, Monitors, TLS Certificates, User Experience, and Dashboard. The main panel shows a conversation with the AI Assistant. The user asks: 'I want to visualize the average of bytes from kibana_sample_data_logs grouped by host as a tagcloud'. The assistant responds with an ES/QL query:

```
FROM kibana_sample_data_logs
| STATS avg_bytes = AVG(bytes) BY host
```

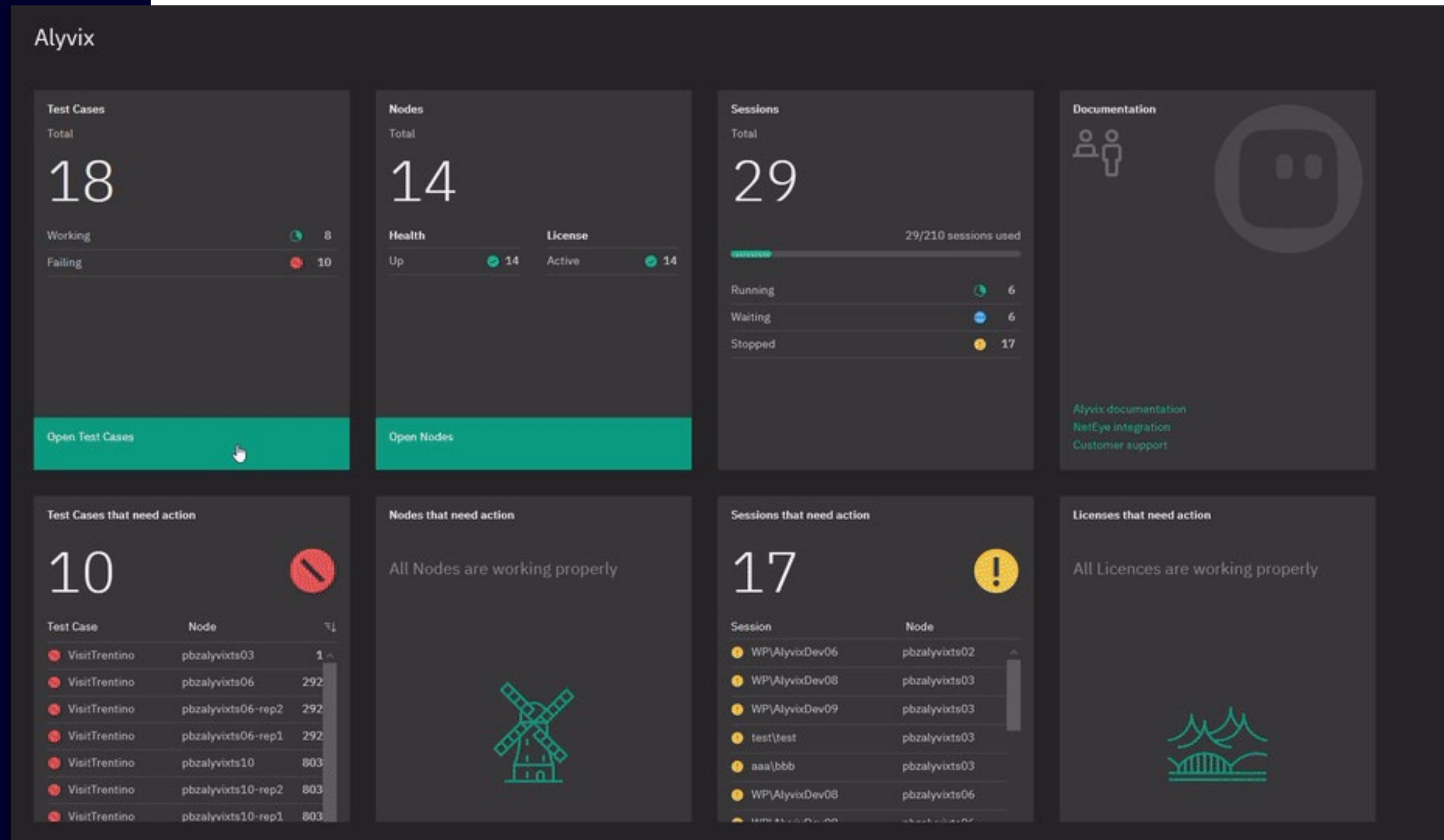
 and provides instructions on how to visualize the results as a tagcloud. The right sidebar shows the 'Layer configuration' for the 'Tag cloud' visualization, with tags set to 'host' and the metric set to 'avg_bytes'.

<https://demo.elastic.co/>

ALYVIX SYNTHETIC MONITORING

Quantify your user experience

Workflow Test case
Run Bots
Analyze - Insights
Actions



<https://alyvix.com/>

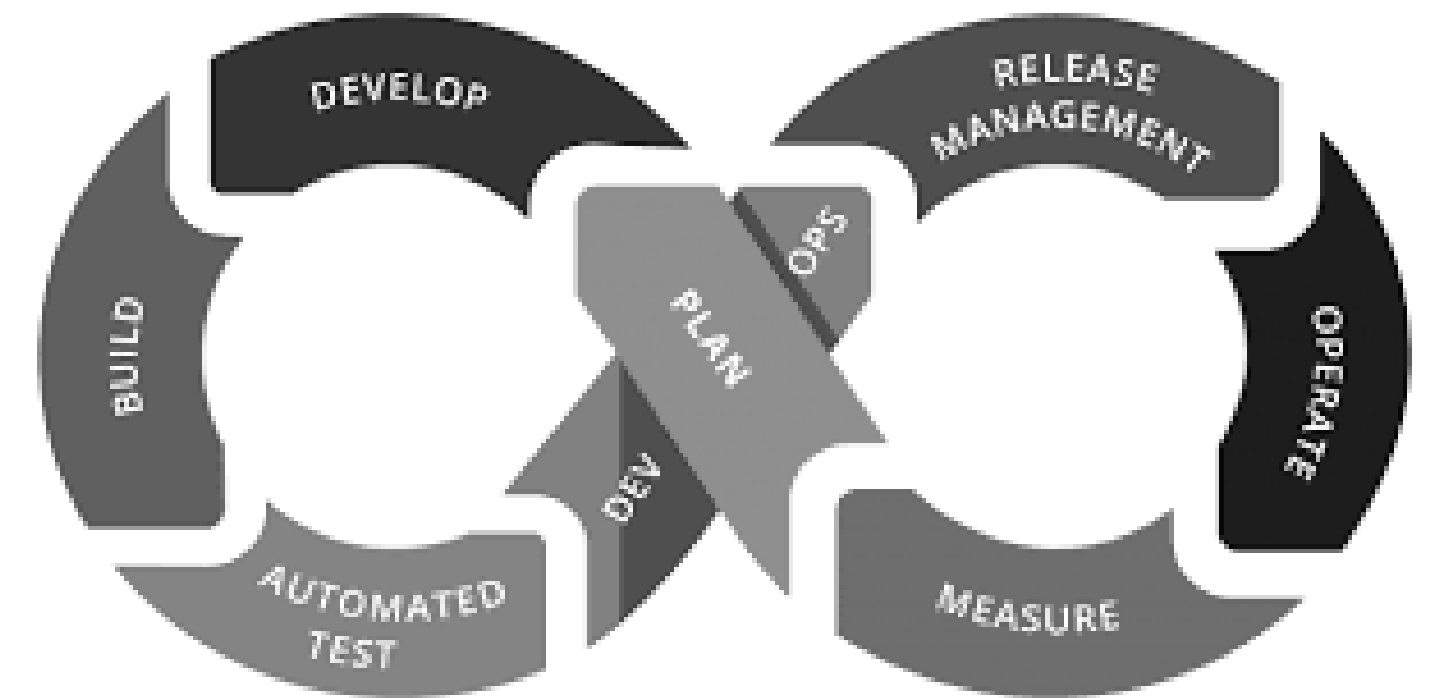


NETEYE

Outlook...

- Introduce two weeks Sprint Release for fast reaction
- Update – Upgrade with Ansible without standby node
- Blockchain for SOC ADS - GDPR
- OAUTH for all internal modules
- Move from PCS Cluster to Appl. Cluster, no DRBD
- RedHat OS 9
- Integration of all modules
- Tornado
 - Usability
 - Enrichments with Icinga Objects
- Security (external assessments, internal reviews, internal audits)

WITH **DEVOPS** ADOPTION



**THANK
YOU.**

