



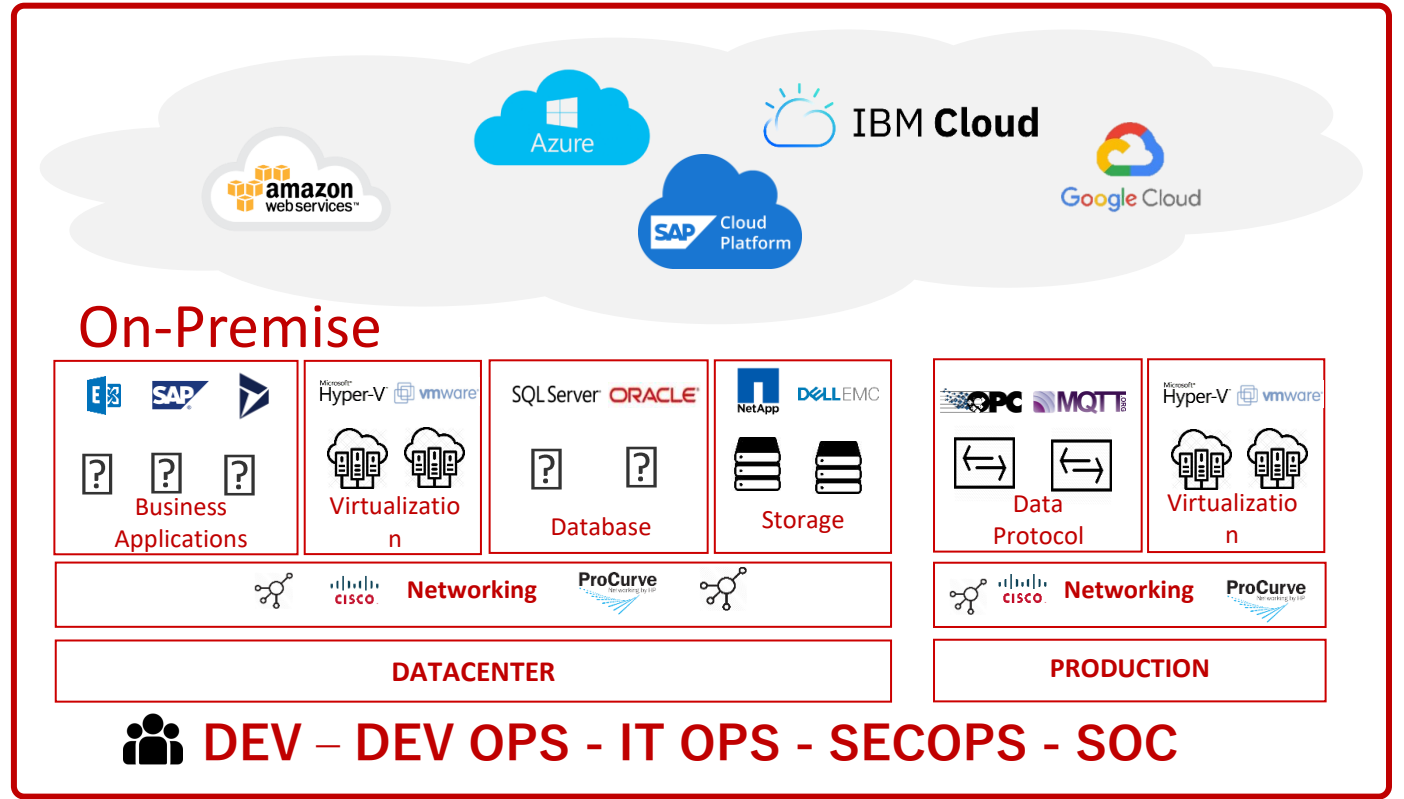
...more than
software,
your IT partner

Community meets Technology

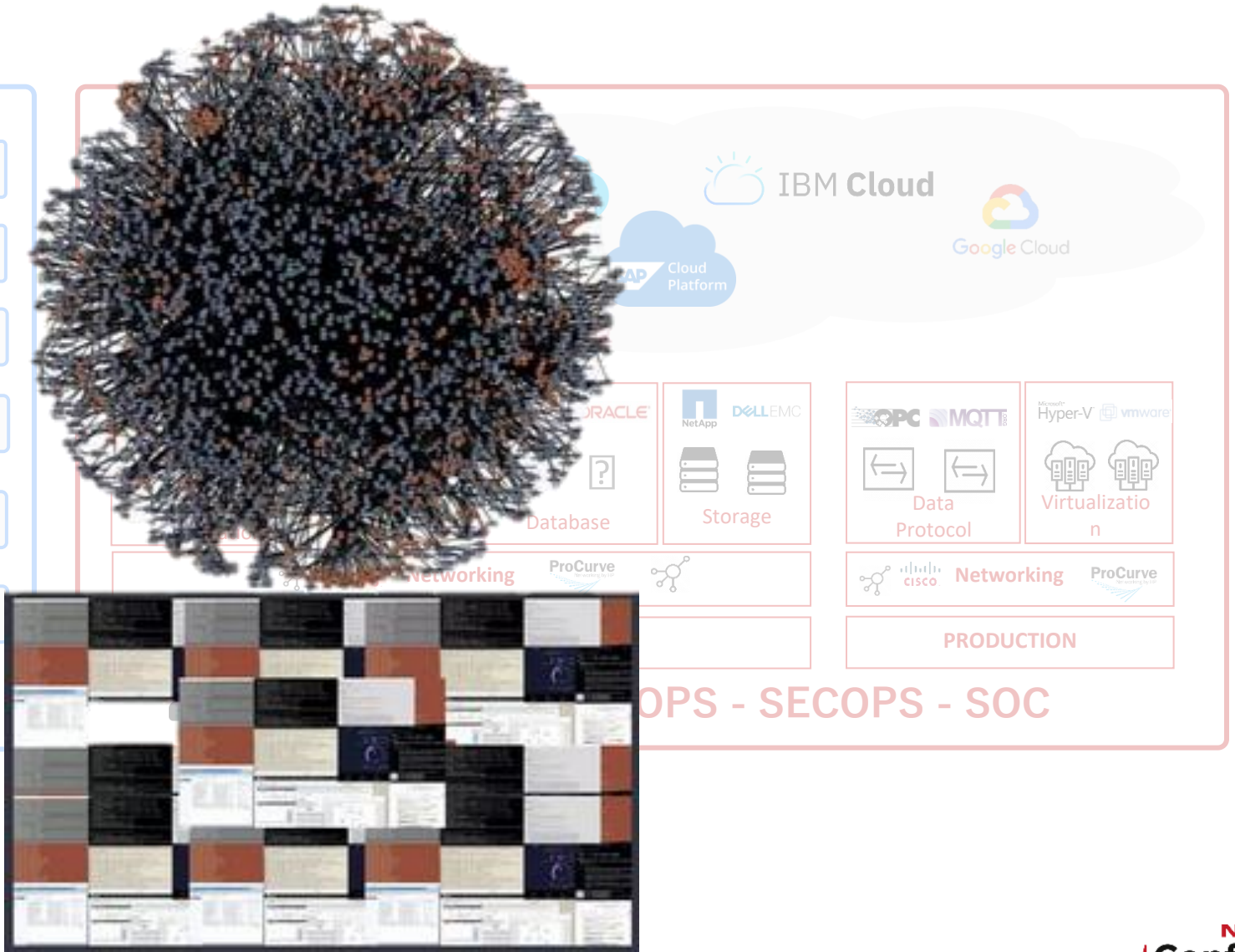
Die NetEye-Vision



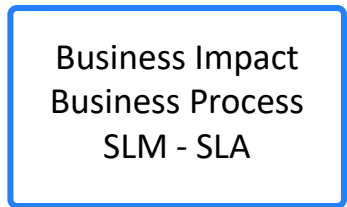
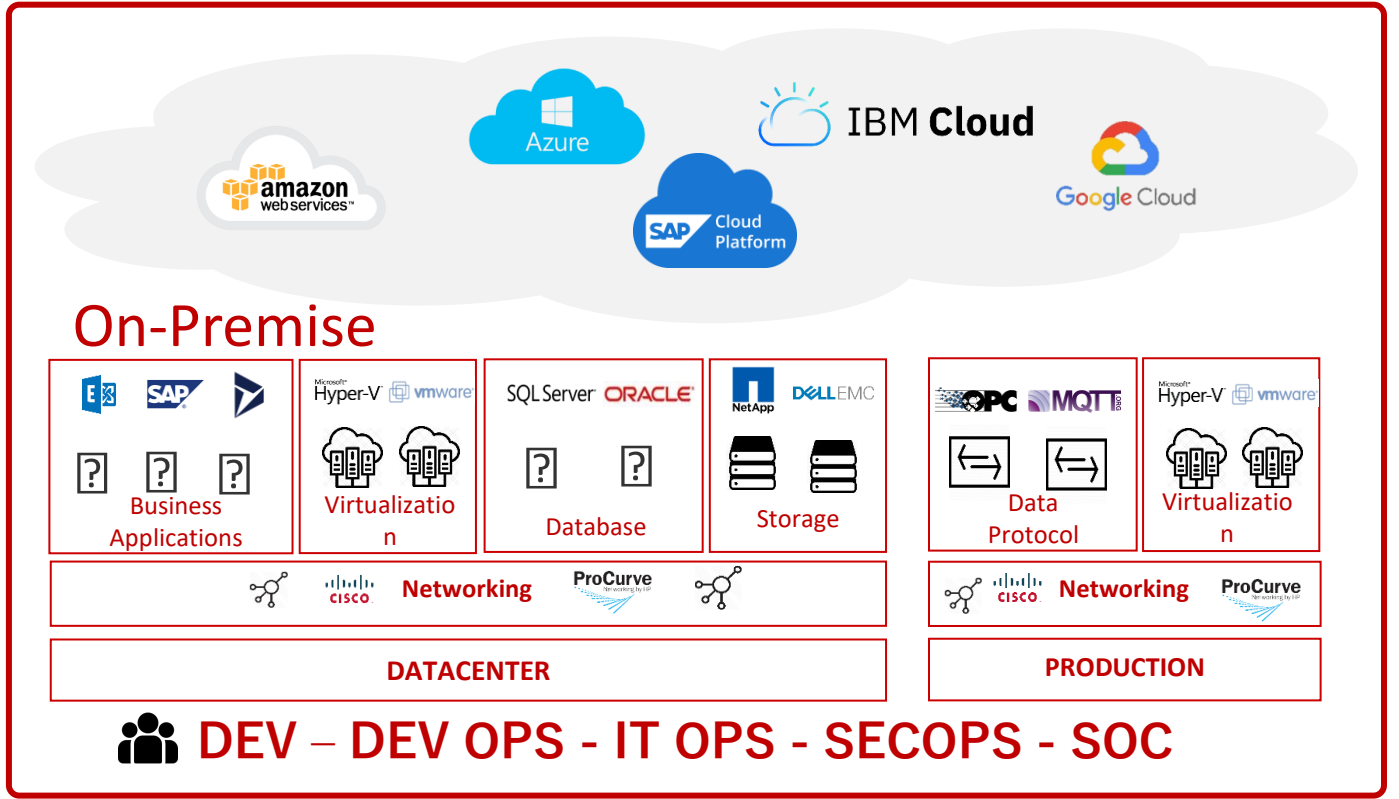
VISION



VISION



VISION



UNIFIED MONITORING PLATFORM

Organisation – Prozesse

Monitoring

Welche Störung liegt vor ?

Verfügbarkeit ?

Systemzustand ?

Entstörung

Antwortzeiten – Fit for use



Incident

Observability

Performance, Durchsatz ?

Sättigung, Skalarierbarkeit ?

Ressourcen – Kosten

Anomaly Detection – ML

User Experience



Problem

SIEM - SECURITY

Hinweis auf Threat Actor ?

Daten exfiltration ?

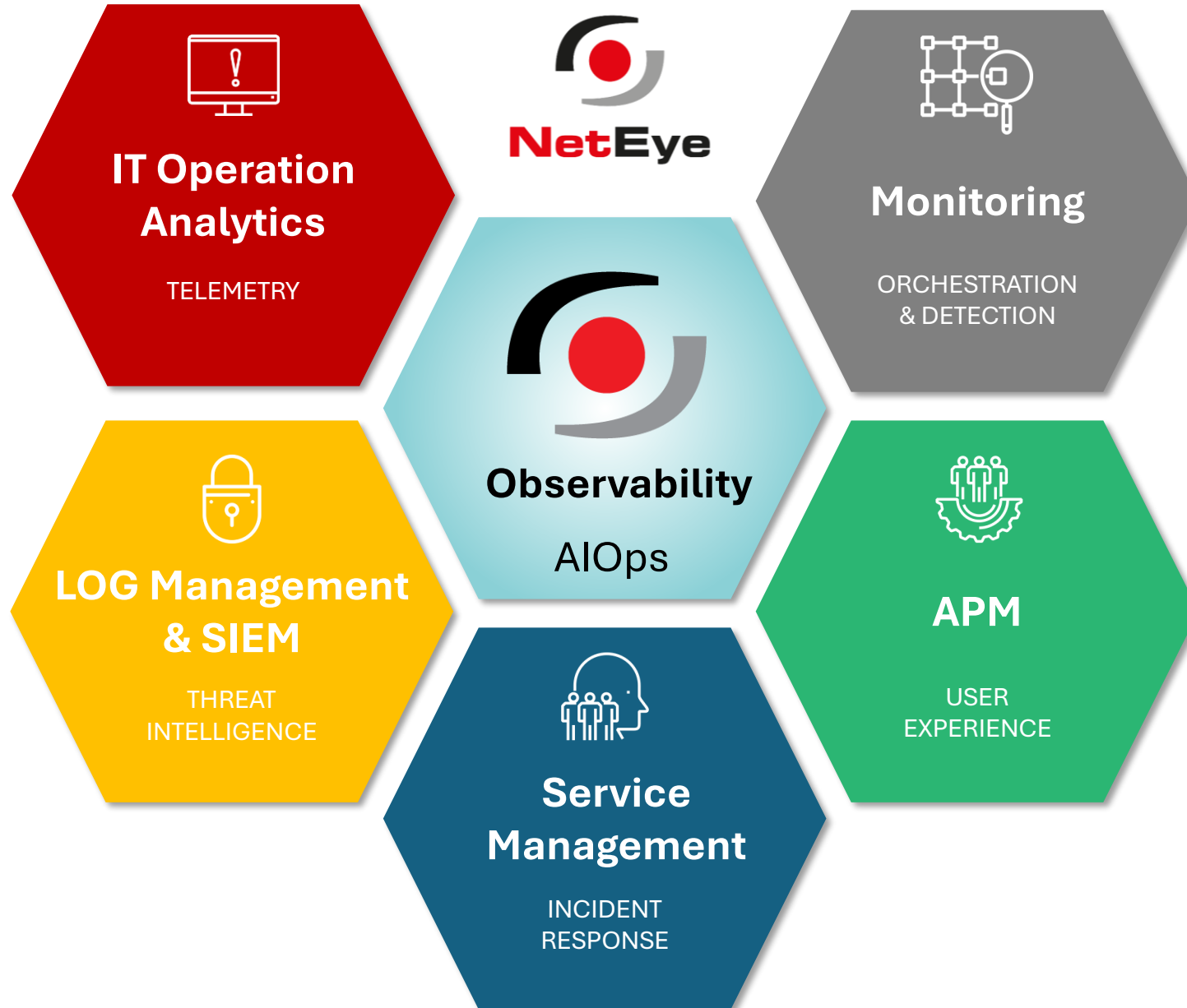
Erkennung – Detection Rules

Anomaly Detection - ML



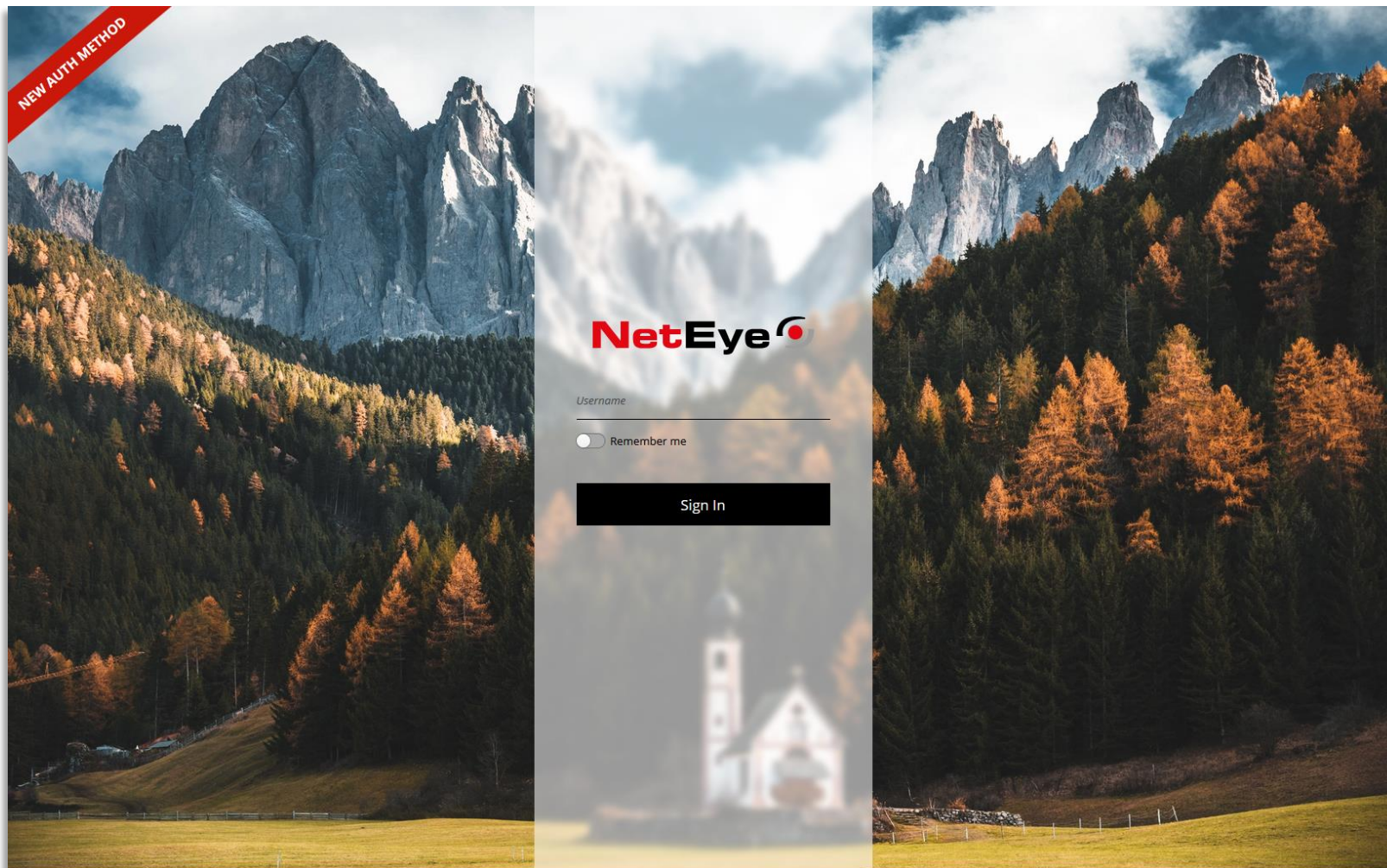
Security

UNIFIED MONITORING PLATFORM



NetEye: SSO Authentifizierung

Keycloak zur Integration mit Identity Provider



IdP Integration

OpenID - OAUTH

SAML

LDAP - AD

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

The screenshot shows the NetEye User Guide website. The top navigation bar includes the NetEye logo, 'User Guide', and a search bar. A left sidebar contains a navigation menu with categories like 'Introduction', 'Getting Started', 'Monitoring - Detection', and 'NetEye Update & Upgrade'. The main content area is titled 'Advanced Topics' and features a sub-section for 'The neteye Command'. Below this, there are sections for 'neteye install' and 'neteye update'. The 'neteye install' section lists tasks such as registering the machine to RHEL 8, setting up Red Hat Insights, reconfiguring NetEye services, restarting services, and creating certificates. The 'neteye update' section mentions parallel execution of configuration tasks. A right sidebar lists 'Advanced Topics' with links to 'neteye install', 'neteye update', 'neteye upgrade', and 'neteye update vs. neteye upgrade'.

Suche
Inhalt
Struktur

<https://neteye.guide/>



NetEye: Core

Update – Upgrade – Install mit Ansible



Parallelisiert

Vereinfacht

Pflegbarer

OS Upgrade

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

Icinga: Icinga DB Web

Roadmap



The screenshot displays the Icinga DB Web interface. On the left, a 'Services' panel shows a list of services with their status (UP or DOWN) and performance metrics. The main panel shows the 'Host' view for 'docker-master', which is currently UP. It includes a 'Plugin Output' section showing 'PING OK - Packet loss = 0%, RTA = 0.18 ms'. Below this, there are sections for 'Services' (12 total, with 2 critical, 1 warning, 2 unknown, and 7 OK), 'Actions', 'Comments', 'Downtimes', 'Groups' (Linux Servers), 'Notifications', and 'Check Statistics'. The 'Check Statistics' section shows a timeline for the 'docker-master' check, with a 1.00 m interval and a 4.11 s execution time. The bottom status bar indicates 3020 services with 7 critical, 42 warning, 3 unknown, 958 OK, 44 pending, and 1966 disabled.

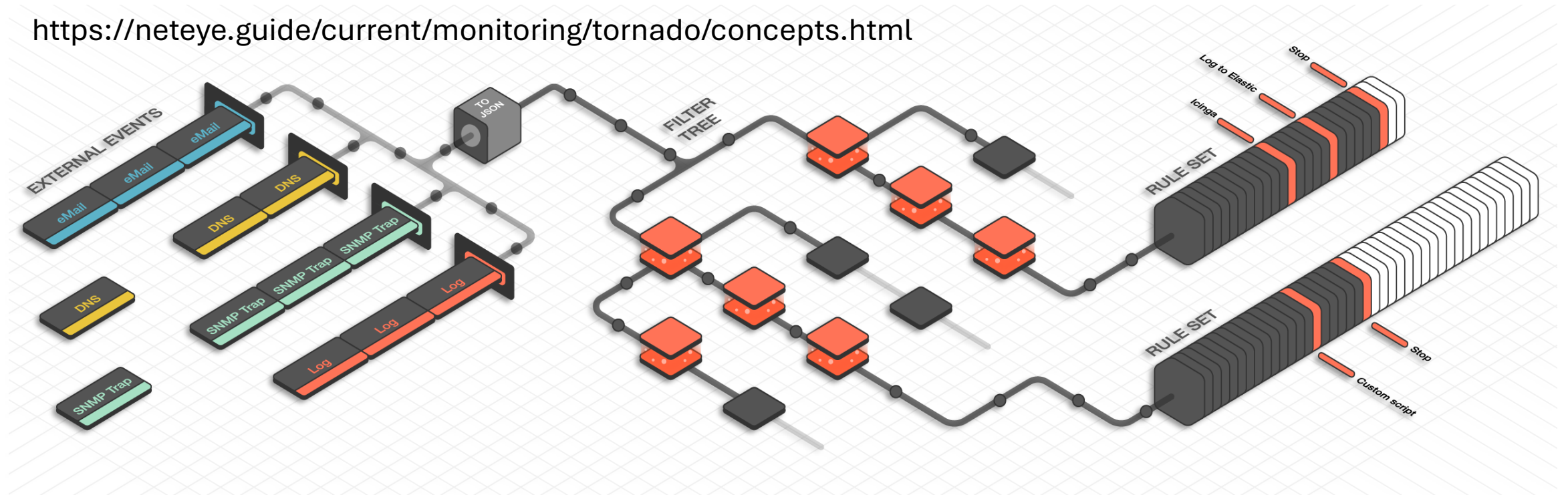
Performance
Skalierbarkeit
Darstellung
Filter

Tornado

Complex Event Processing



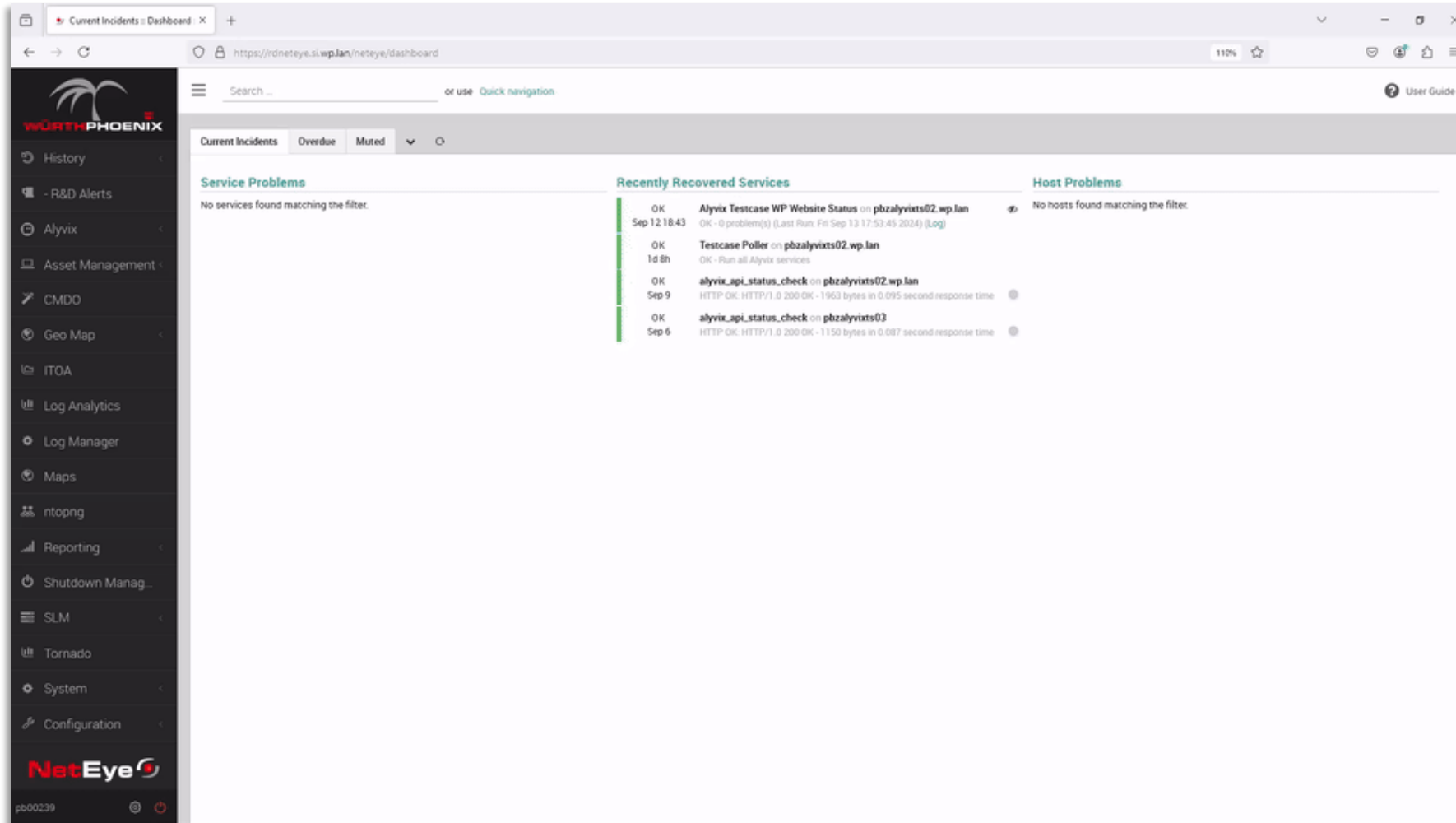
<https://neteye.guide/current/monitoring/tornado/concepts.html>



External Event

Integration

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

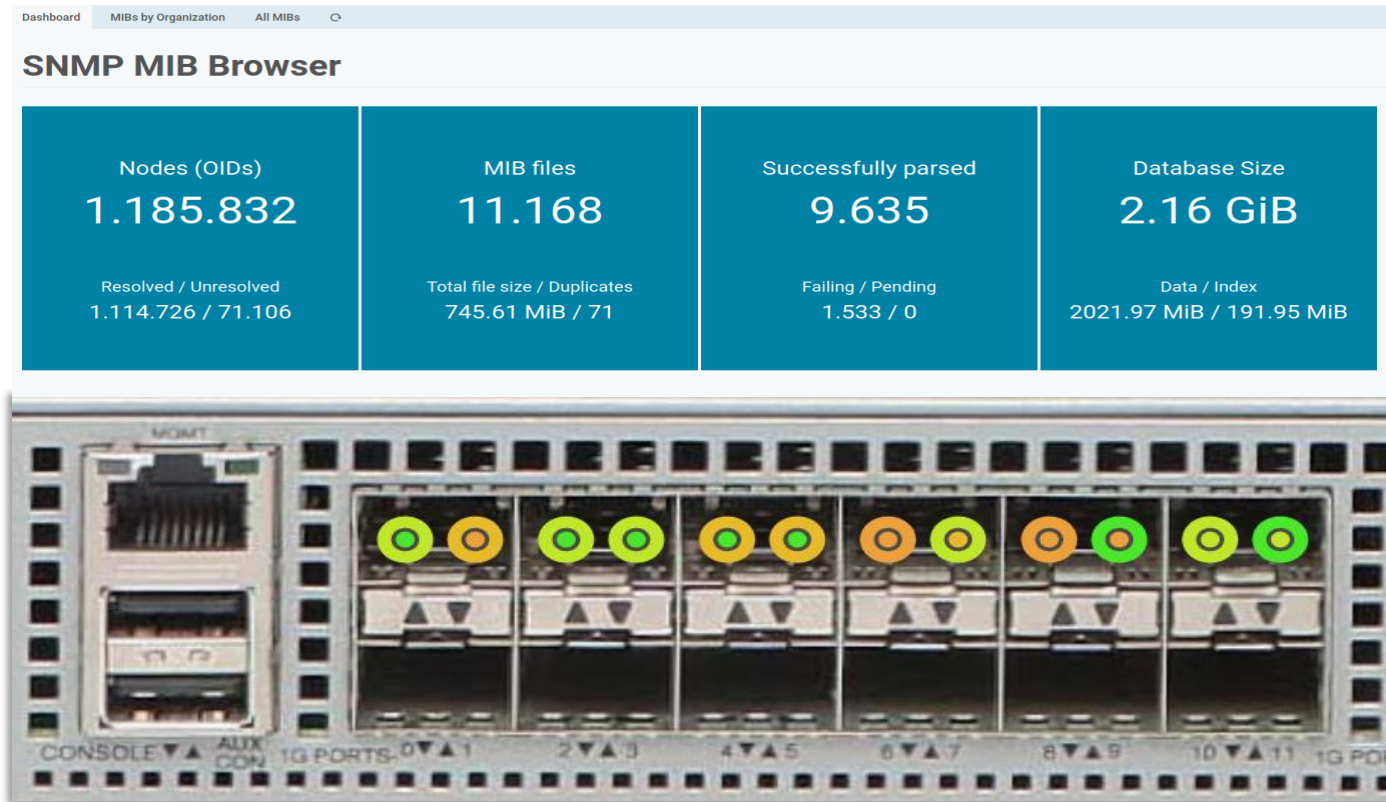


Usability
Event Test
Iterator
...

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

SNMP: Monitoring at scale

Roadmap (neues Modul)



SNMP MIB Browser

SNMP Inventory

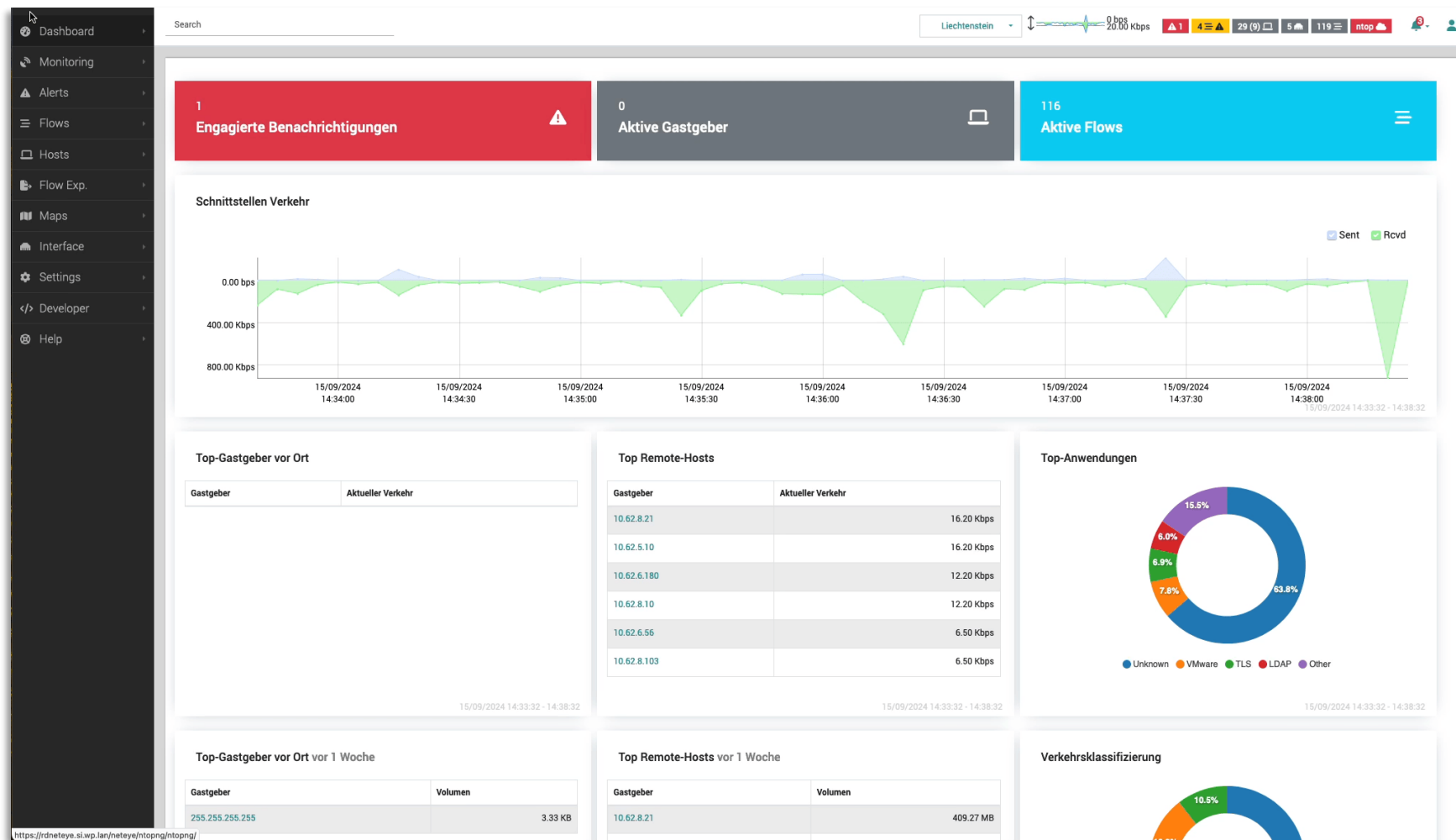
SNMP Polling at a scale 15sec

SNMP Polling in a distributed way



NTOPNG: Synthetic monitoring

Release 6.2



UI Verbesserungen
 Mitre Att&ck
 Historical Flow
 Replay
 Periodic Reports
 -60% Memory

<https://ntop.org/>

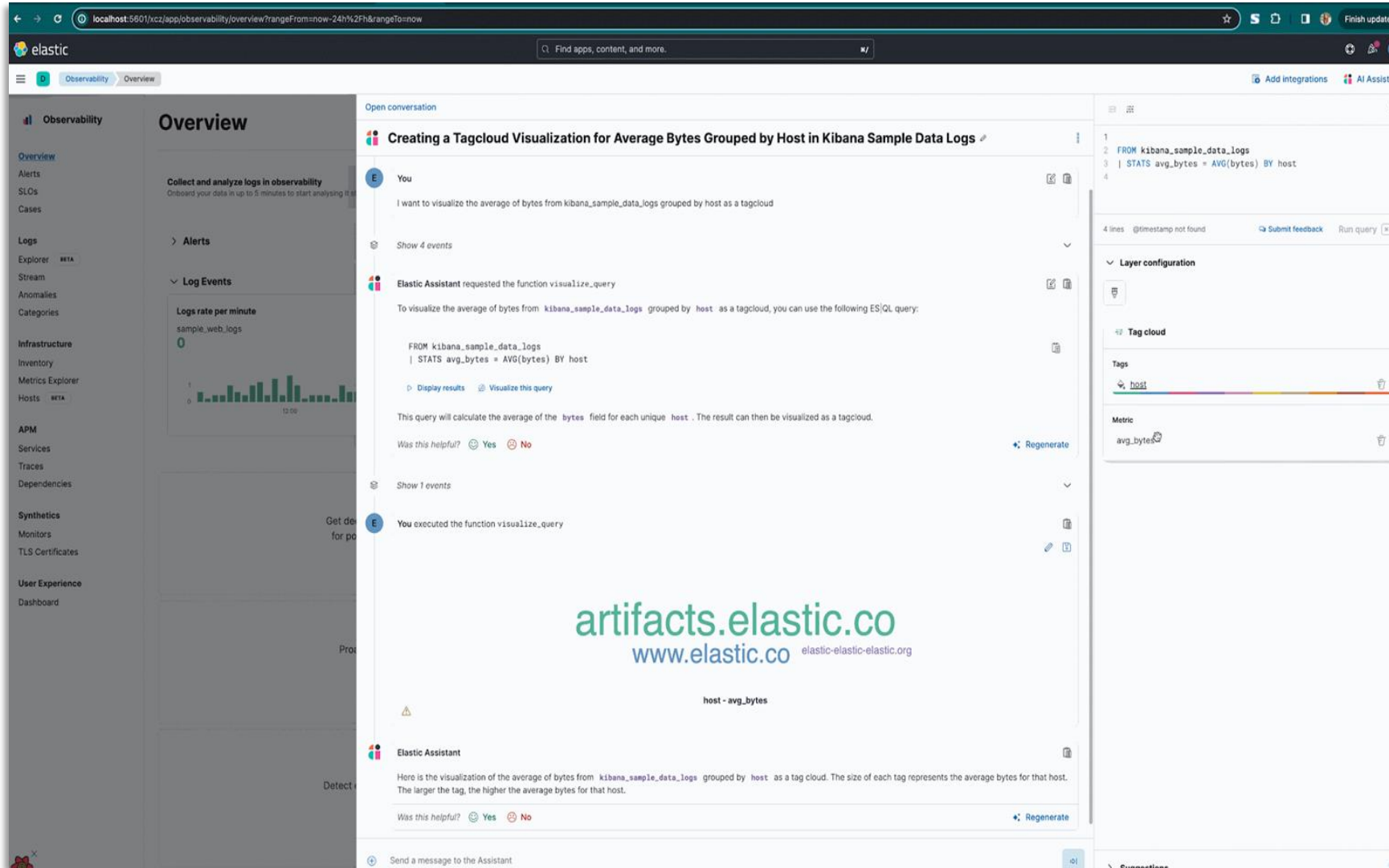
Elastic: Release 8.15 News

Release 8.15



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

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

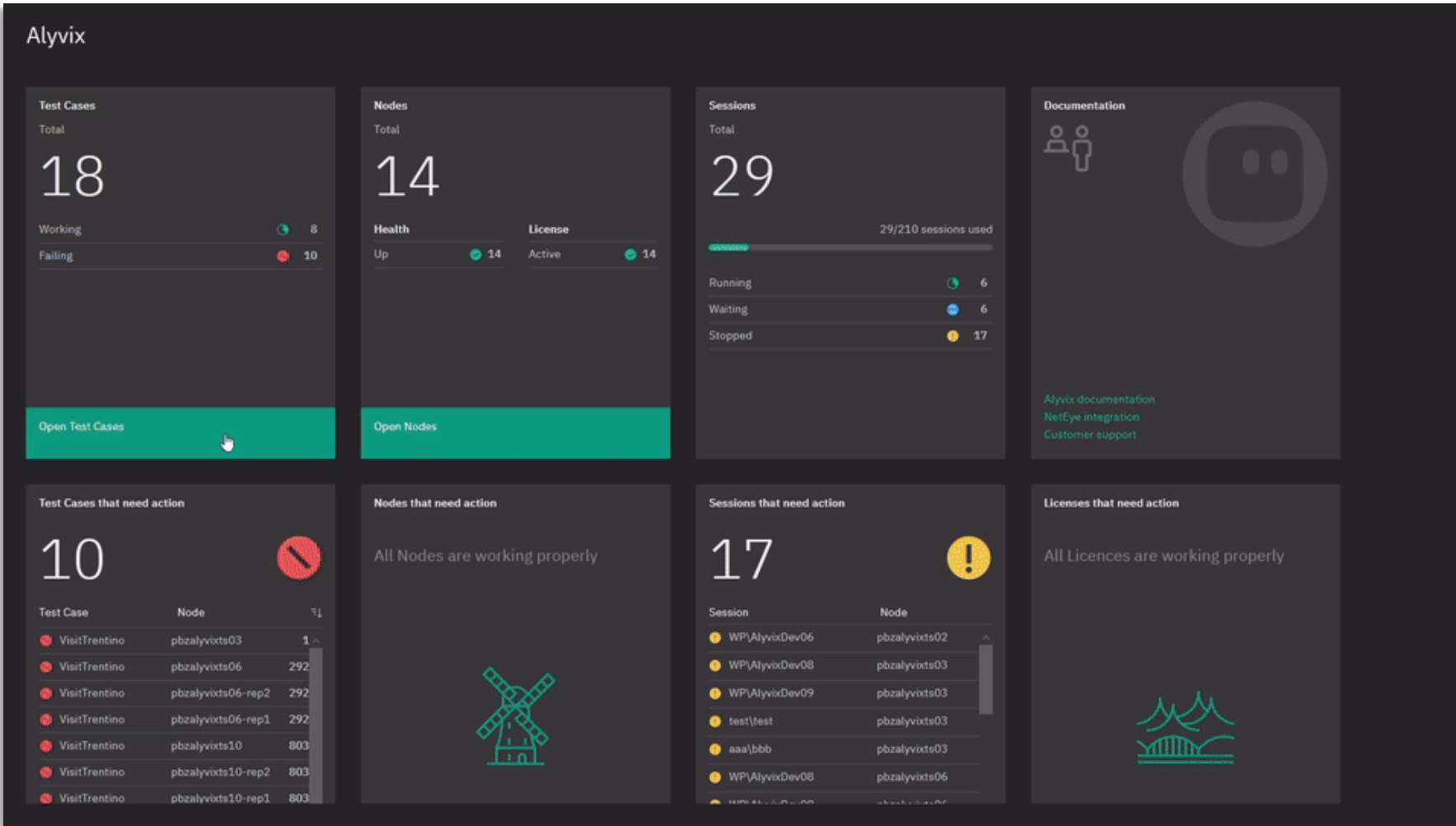


The screenshot shows the Elastic Observability AI Assistant interface. The main window displays a conversation titled "Creating a Tagcloud Visualization for Average Bytes Grouped by Host in Kibana Sample Data Logs". The user asks: "I want to visualize the average of bytes from kibana_sample_data_logs 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`. The user then asks for a visualization, and the assistant provides a Tagcloud visualization configuration with the tag "host" and the metric "avg_bytes". The interface also shows a "Layer configuration" panel and a "Tag cloud" visualization area.

Verkürzung des Arbeitsablaufs für User bei der Verwendung des Observability KI-Assistenten

Alyvix: Synthetic monitoring

Quantifizieren Sie Ihre User Experience



Test Cases
Total: 18
Working: 8
Failing: 10

Nodes
Total: 14
Health: Up 14, License: Active 14

Sessions
Total: 29 (29/210 sessions used)
Running: 6
Waiting: 6
Stopped: 17

Documentation
Alyvix documentation
NetEye integration
Customer support

Test Cases that need action
10

Test Case	Node	
VisitTrentino	pbzalyvixts03	1
VisitTrentino	pbzalyvixts06	292
VisitTrentino	pbzalyvixts06-rep2	292
VisitTrentino	pbzalyvixts06-rep1	292
VisitTrentino	pbzalyvixts10	803
VisitTrentino	pbzalyvixts10-rep2	803
VisitTrentino	pbzalyvixts10-rep1	803

Nodes that need action
All Nodes are working properly

Sessions that need action
17

Session	Node
WP\AlyvixDev06	pbzalyvixts02
WP\AlyvixDev08	pbzalyvixts03
WP\AlyvixDev09	pbzalyvixts03
test\test	pbzalyvixts03
aaa\bbb	pbzalyvixts03
WP\AlyvixDev08	pbzalyvixts06

Licenses that need action
All Licences are working properly

Workflow Test case
Run Bots

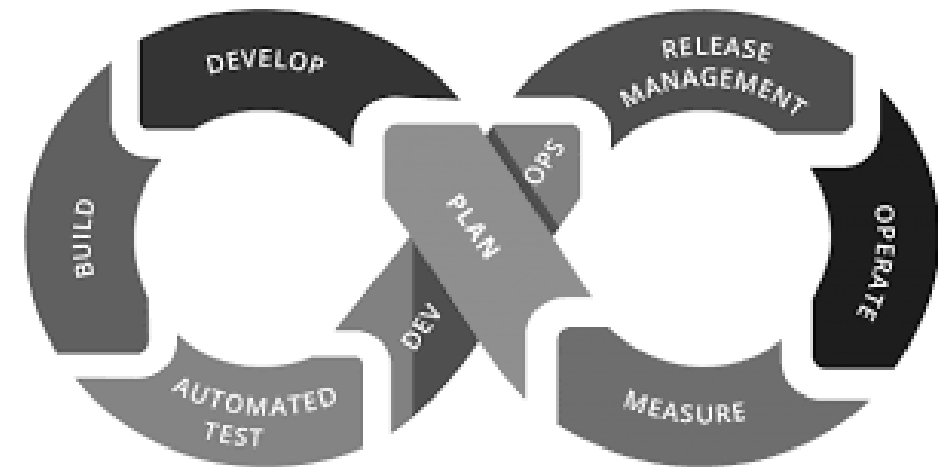
Analyse - Insights

Aktionen



- OAUTH, OpenID über alle interne Module
- Update – Upgrade mit Ansible
- Vom PCS Cluster -> Appl. Cluster, no DRBD
 - Mariadb, Timeseries,...
- RedHat OS 9
- Integration alle Module
- Tornado
 - Usability
 - Enrichments mit Icinga Objects
- Security (Externe Assessments, interne Reviews, interne Audits)

WITH DEVOPS ADOPTION





info@wuerth-
phoenix.com
www.wuerth-
phoenix.com

