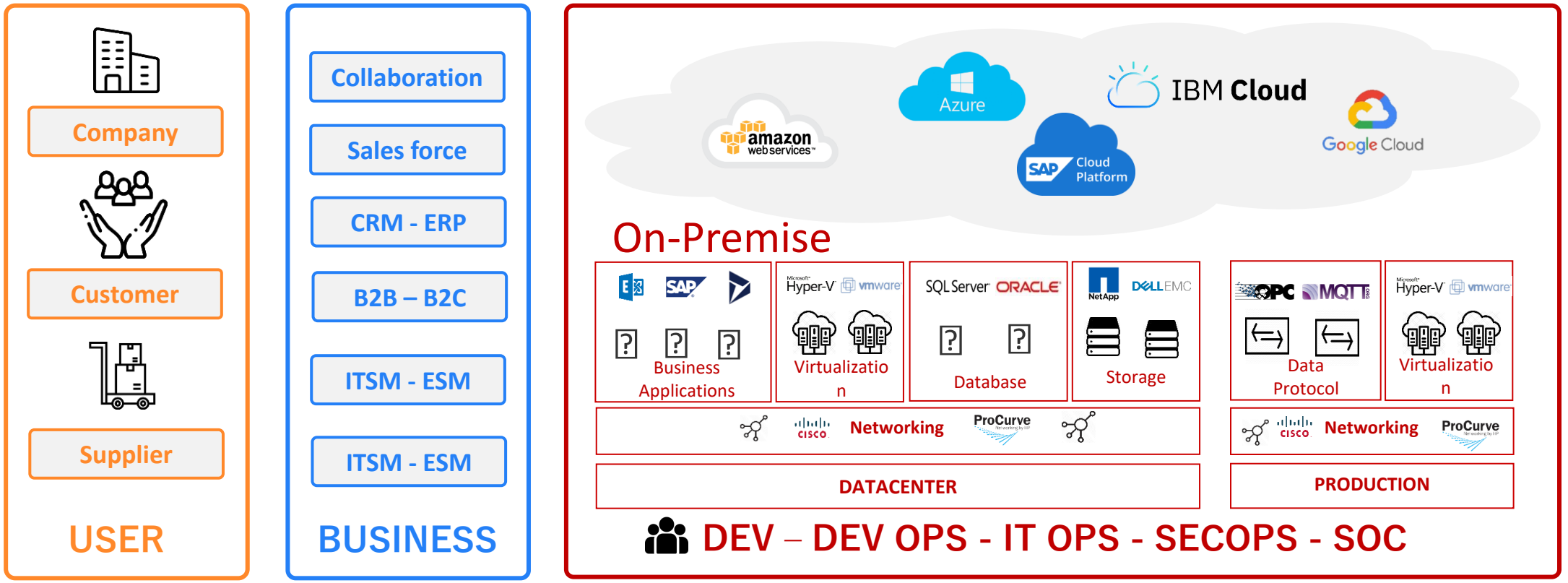
Community meets Technology

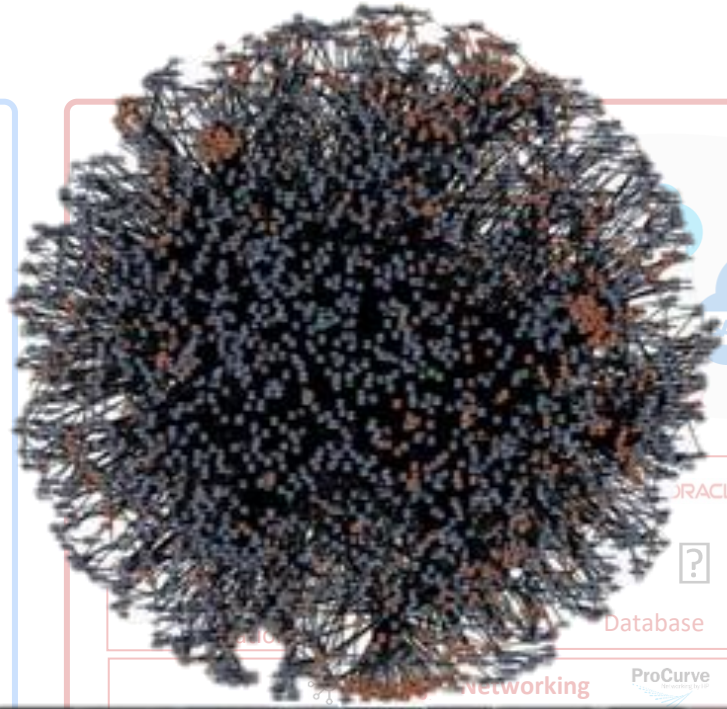
Die NetEye-Vision

WÜRTHPHOENIX

VISION


Company
Customer
Supplier
USER
Collaboration
Sales force
CRM - ERP
B2B – B2C
ITSM - ESM
ITSM - ESM
BUSINESS
amazon web services
Azure
IBM Cloud
SAP Cloud Platform
Google Cloud
On-Premise
Business Applications
Virtualization
Database
Storage
Data Protocol
Virtualization
Networking
Networking
DATACENTER
PRODUCTION
DEV – DEV OPS - IT OPS - SECOPS - SOC

VISION



Company

Customer

Supplier

USER

Collaboration

Sales force

CRM - ERP

B2B – B2C

ITSM - ESM

ITSM - ESM

BUSINESS

IBM Cloud

Google Cloud

Cloud Platform

Database

Storage

Data Protocol

Virtualizatio n

Networking

ProCurve

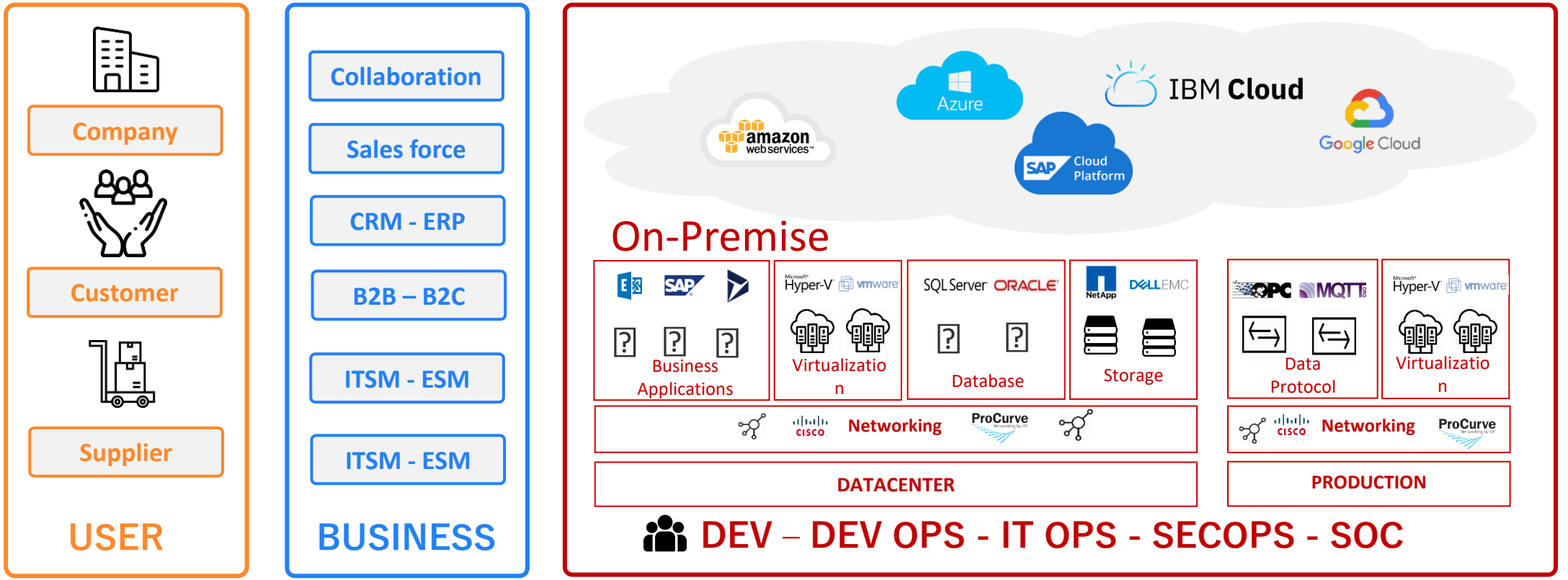
Networking

ProCurve

PRODUCTION

OPS - SECOPS - SOC

VISION



NetEye

Visual Mon
Web Mon
RUM

Business Impact
Business Process
SLM - SLA

Datacenter Mon
Network Performance Mon

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

Automation
SIEM

UNIFIED MONITORING PLATFORM

NetEye Conference DACH 2024

Organisation – Prozesse

Monitoring

Welche Störung liegt vor ?

Verfügbarkeit ?

Systemzustand ?

Entstörung

Antwortszeiten – Fit for use

NOC

Incident

Observability

Performance, Durchsatz ?

Sättigung, Sklarierbarkeit ?

Ressourcen – Kosten

Anomaly Detection – ML

User Experience

SRE  DevOps

Problem

SIEM - SECURITY

Hinweis auf Threat Actor ?

Daten exfiltration ?

Erkennung – Detection Rules

Anomaly Detection - ML

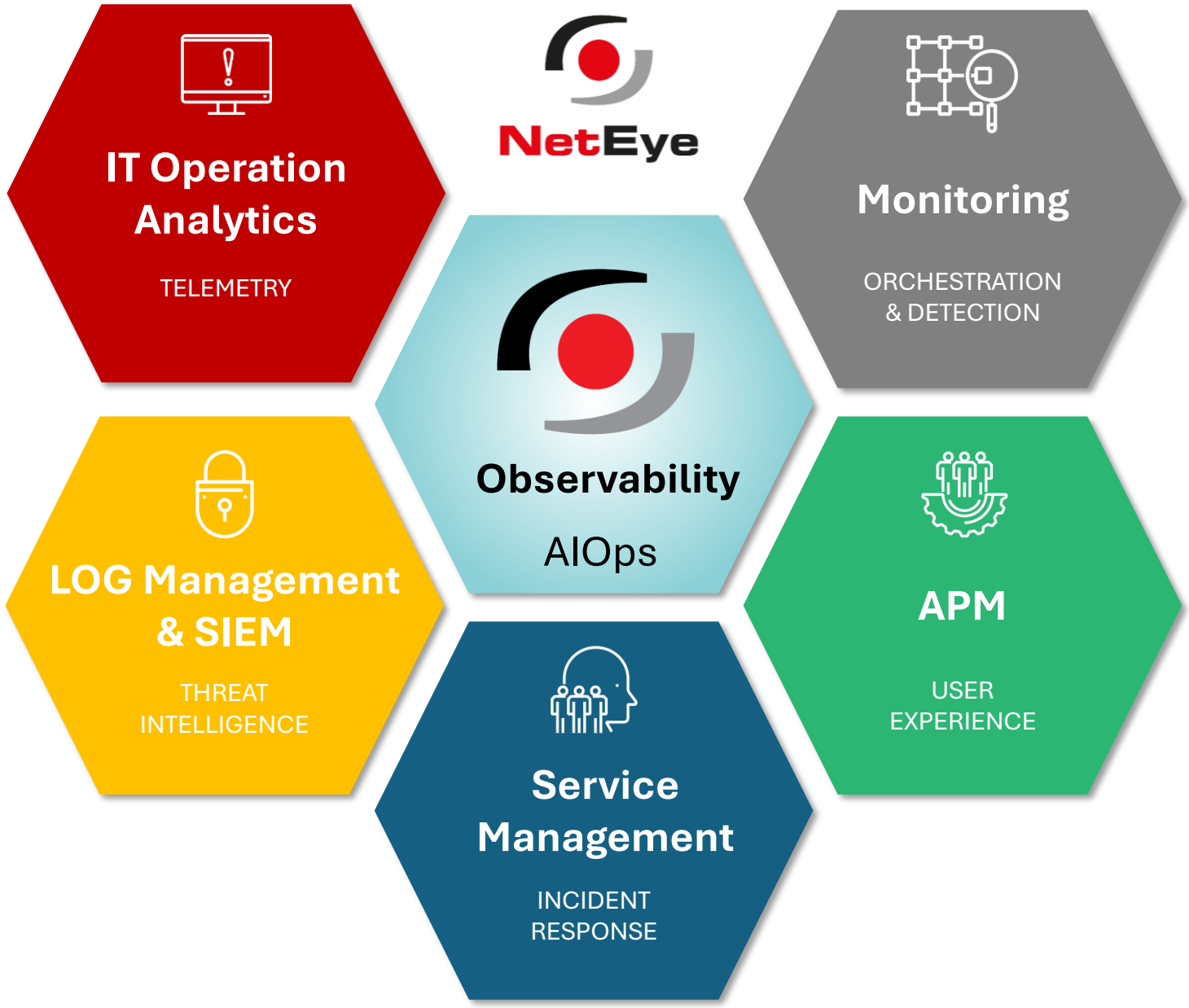
SOC

Security

NetEye

NetEye Conference DACH 2024

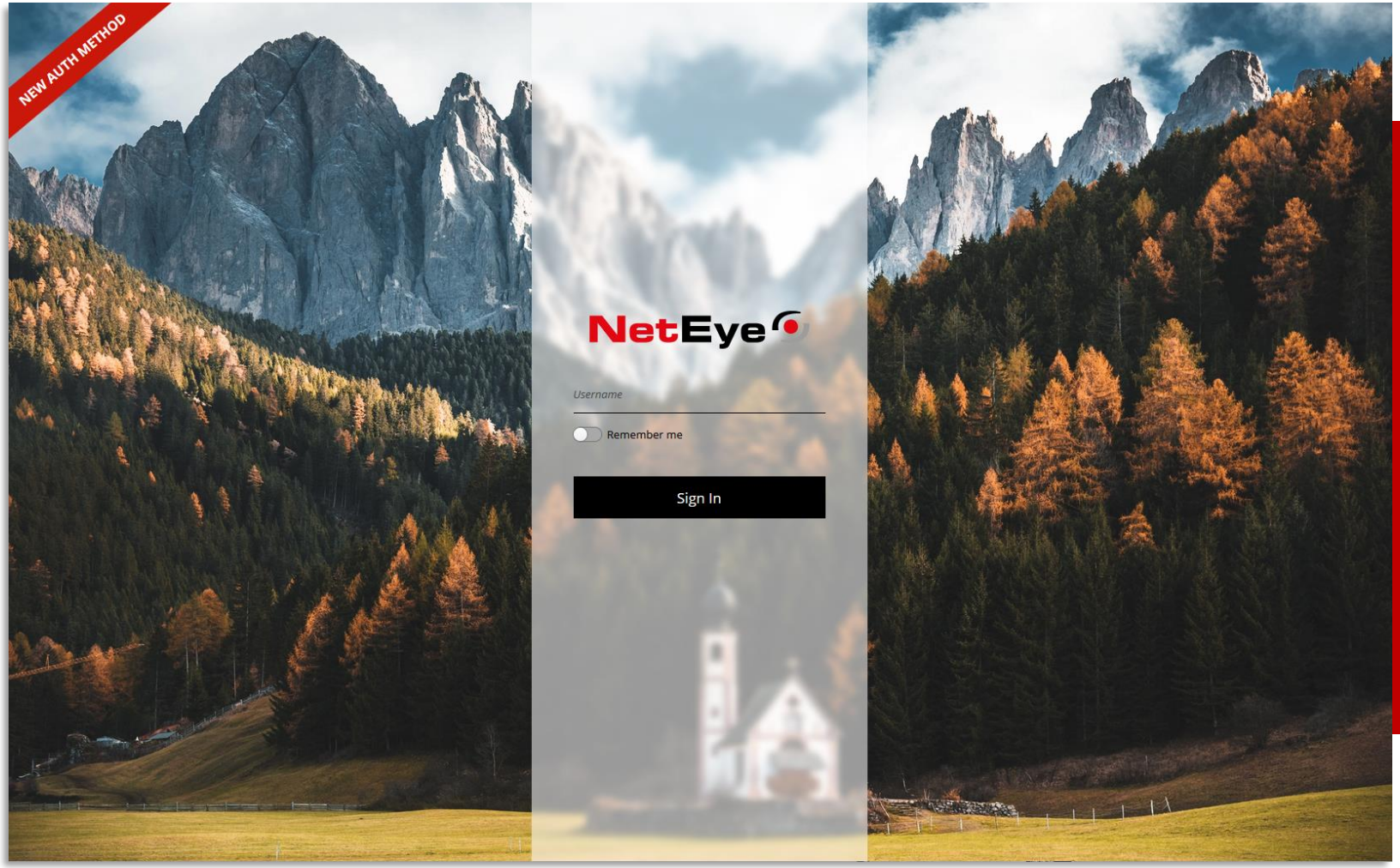
UNIFIED MONITORING PLATFORM



NetEye: SSO Authentifizierung

Keycloak zur Integration mit Identity Provider

OpenID + KEYCLOAK



IdP Integration

OpenID - OAUTH

SAML

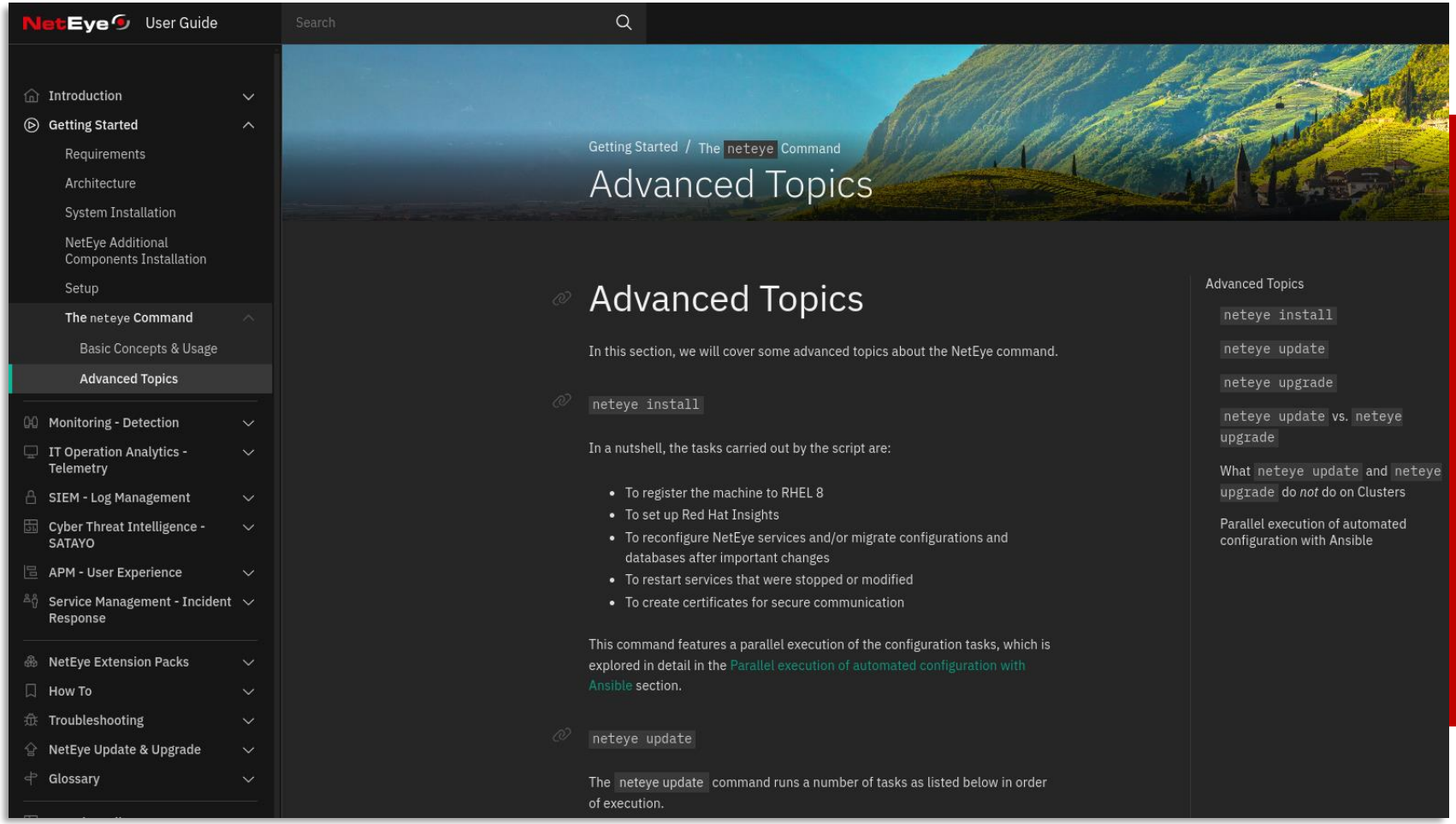
LDAP - AD

https://www.keycloak.org/

NetEye Conference DACH 2024

NetEye: User Guide

Neue Suche – neue Struktur



Suche

Inhalt

Struktur

https://neteye.guide/

NetEye: Core

Update – Upgrade – Install mit Ansible

Parallelisiert

Vereinfacht

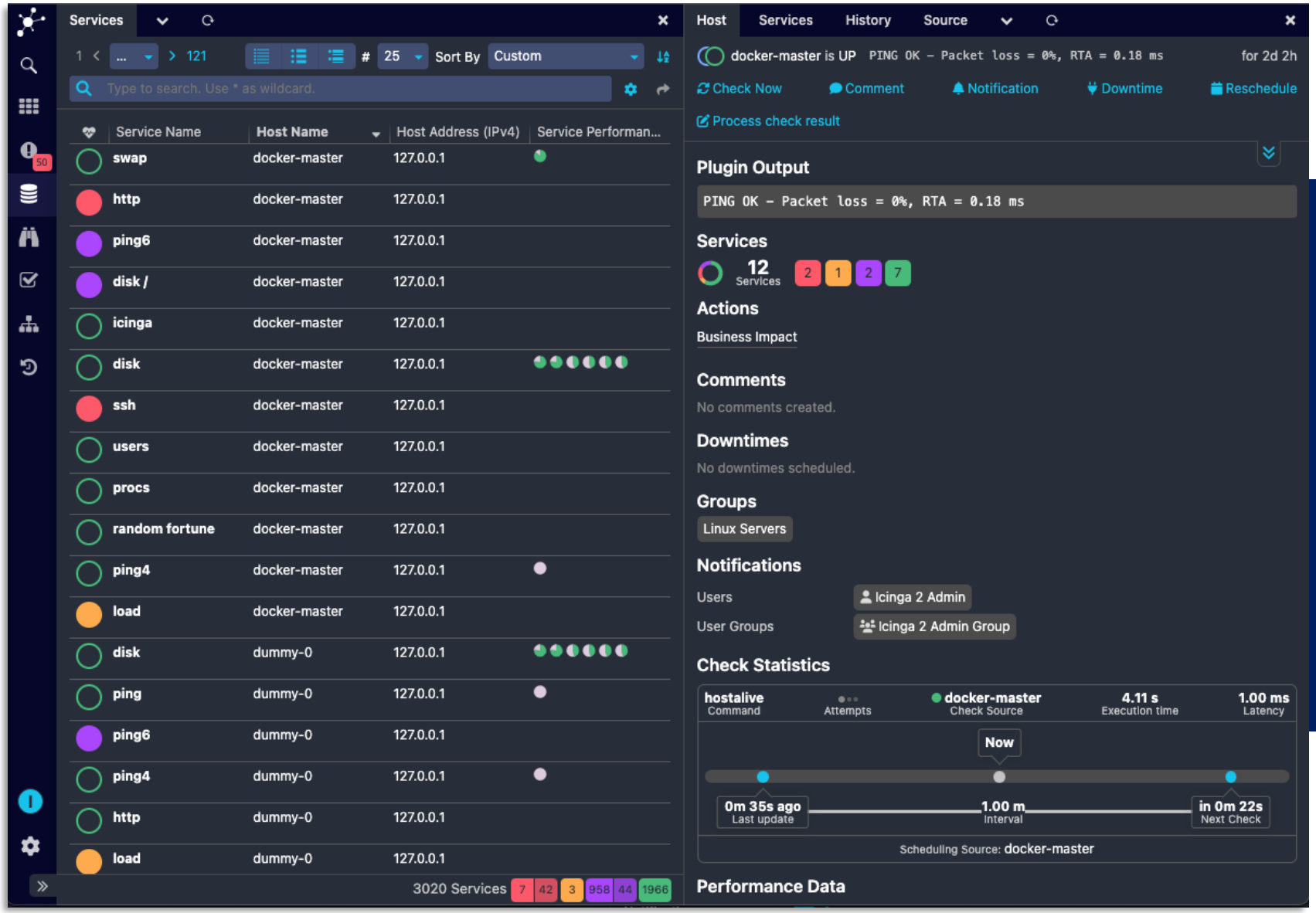
Pflegbarer

OS Upgrade

https://github.com/ansible/ansible

Icinga: Icinga DB Web

Roadmap



Performance

Skalierbarkeit

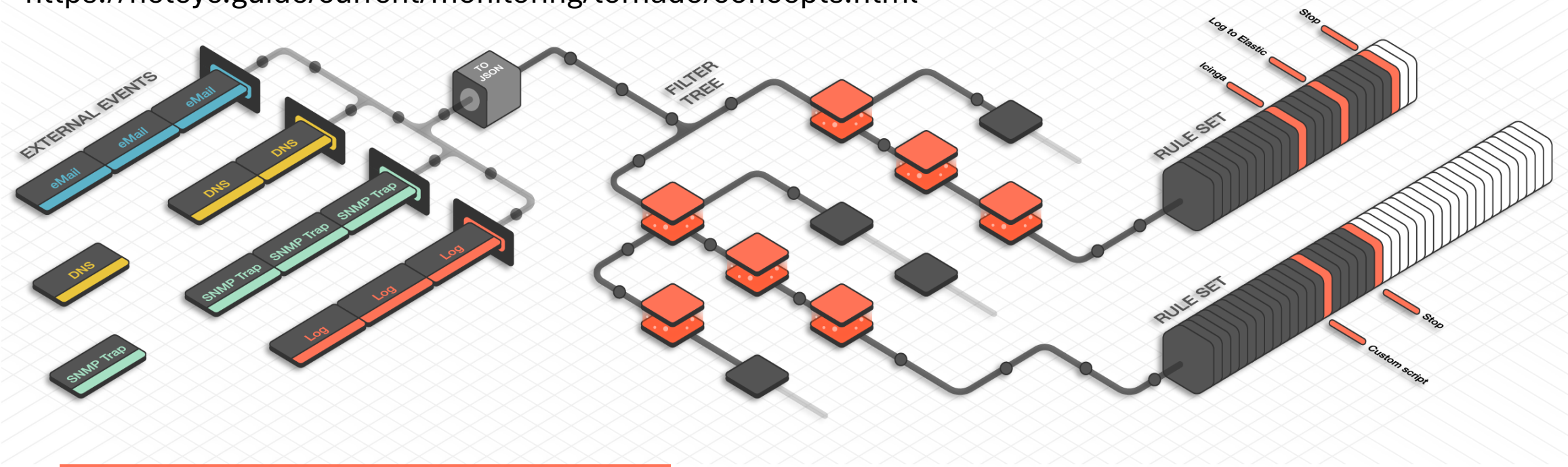
Darstellung

Filter

Tornado

Complex Event Processing

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

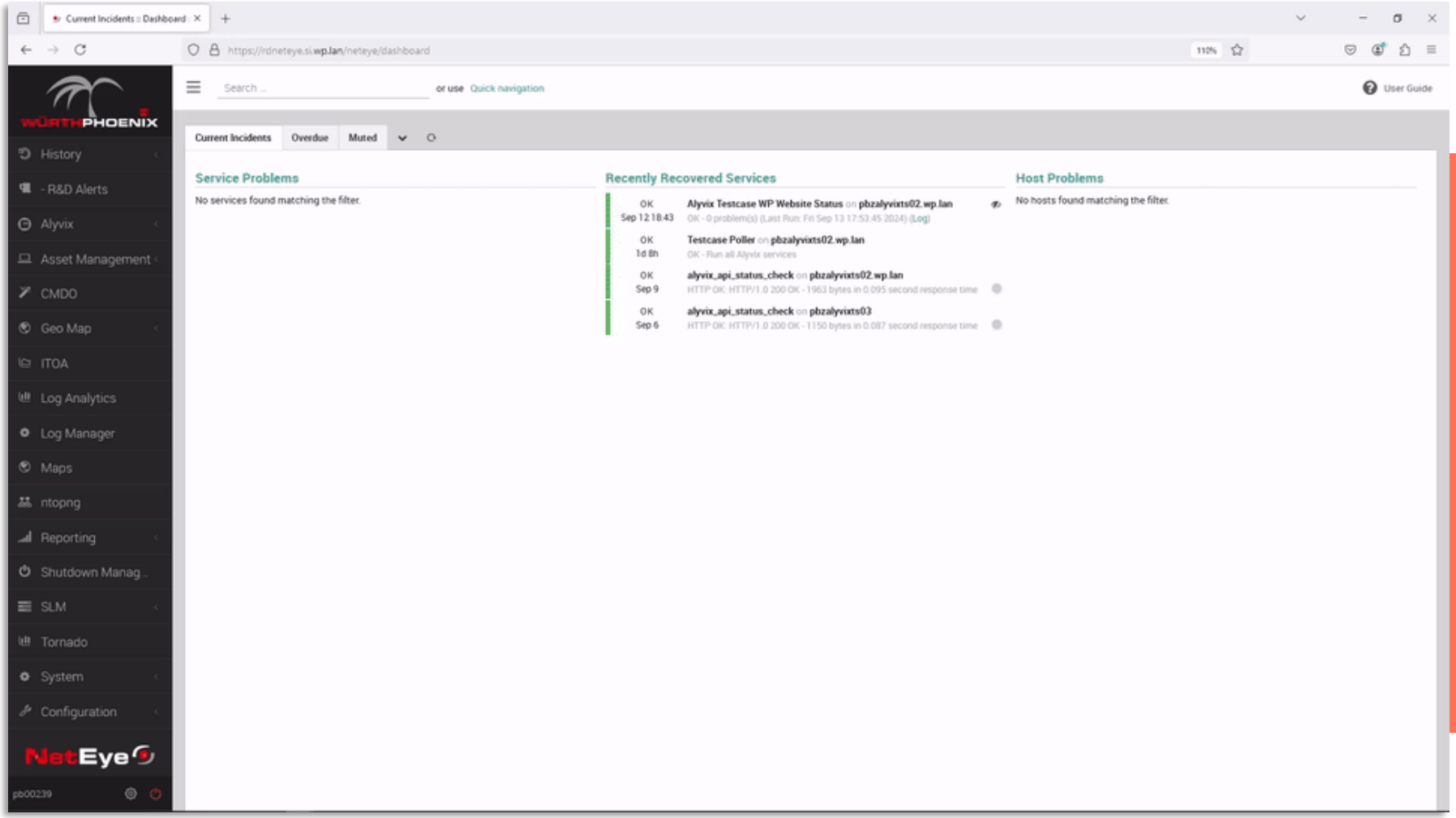


External Event Integration

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

Tornado

Evolution



Usability

Event Test

Iterator

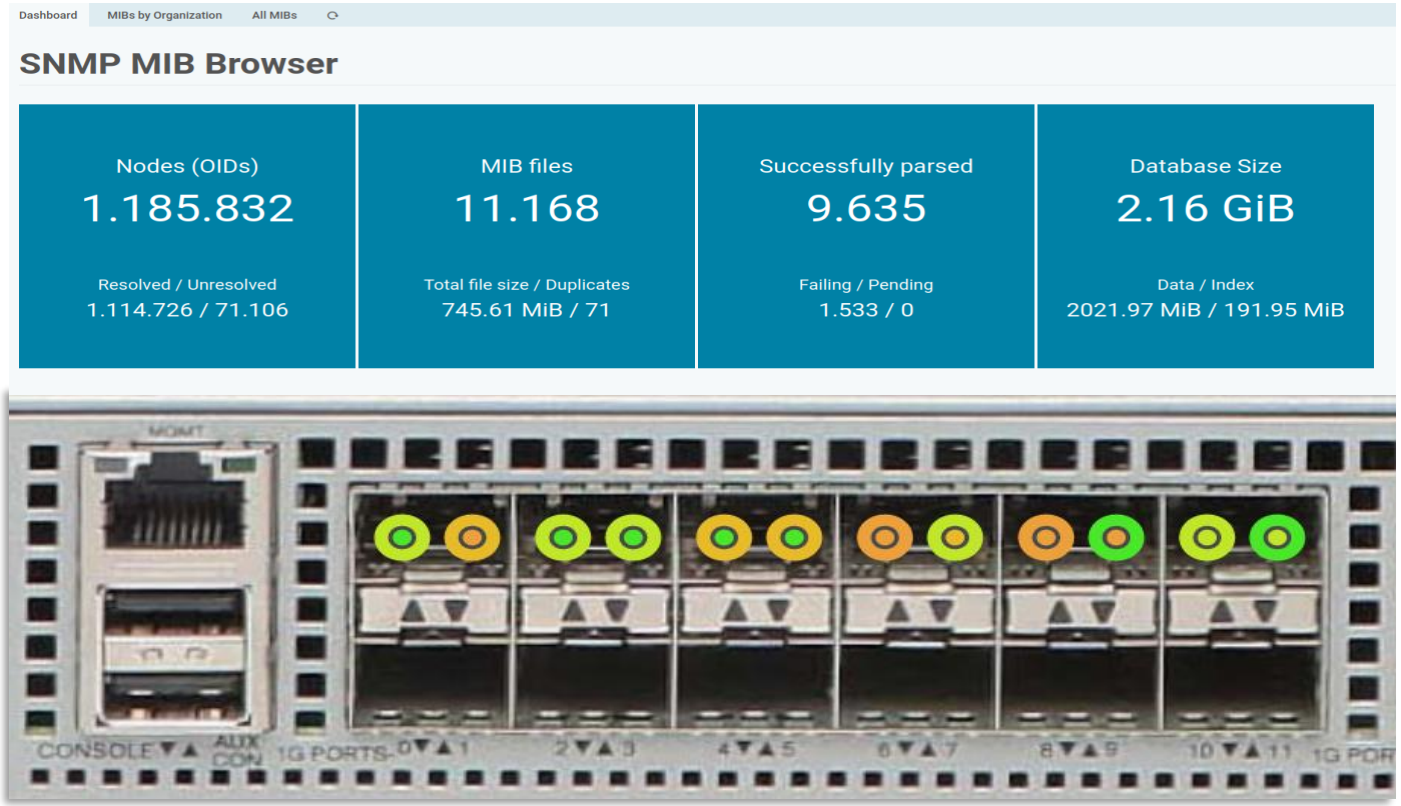
...

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

NetEye Conference DACH 2024

SNMP: Monitoring at scale

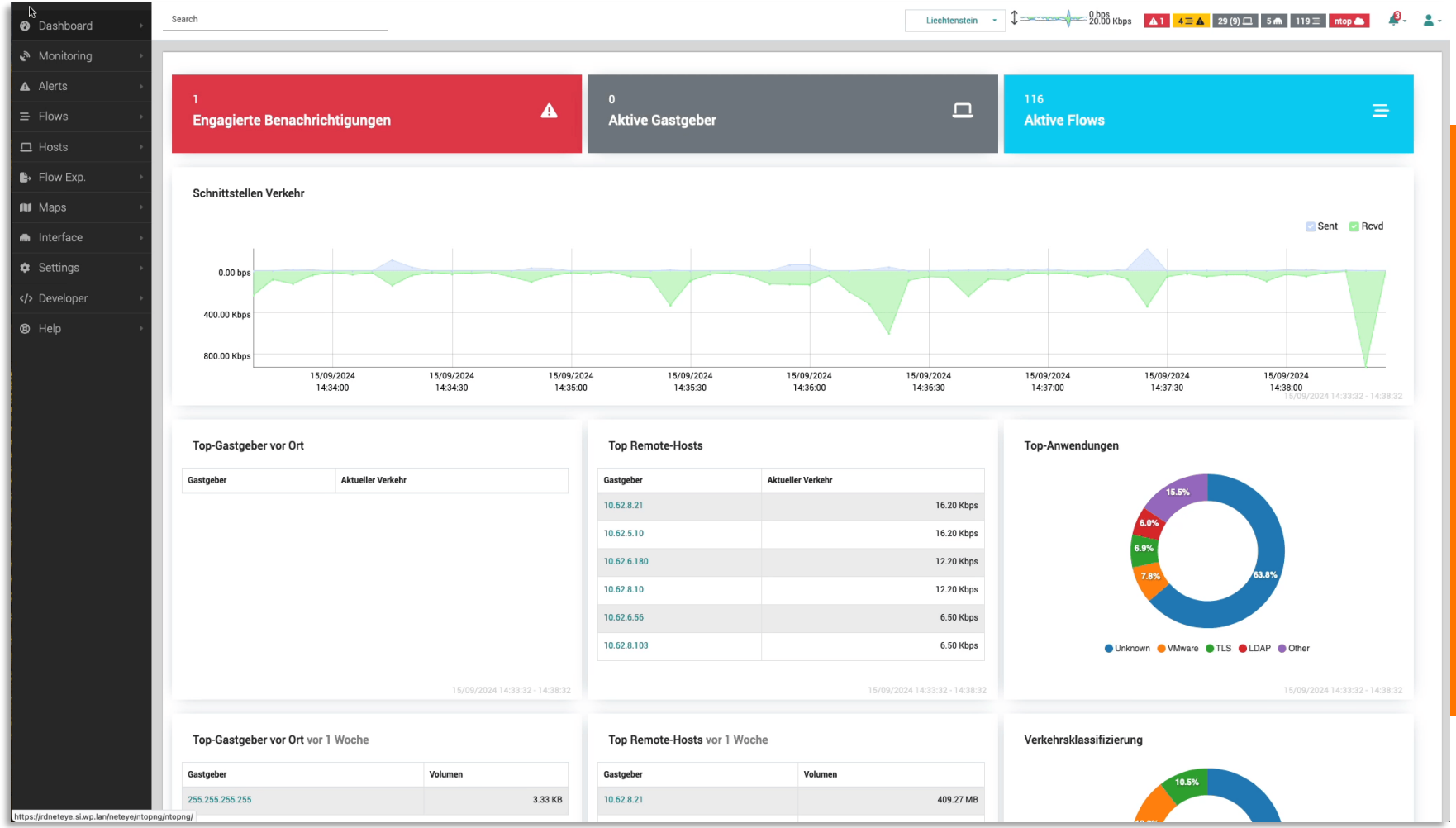
Roadmap (neues Modul)



- 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

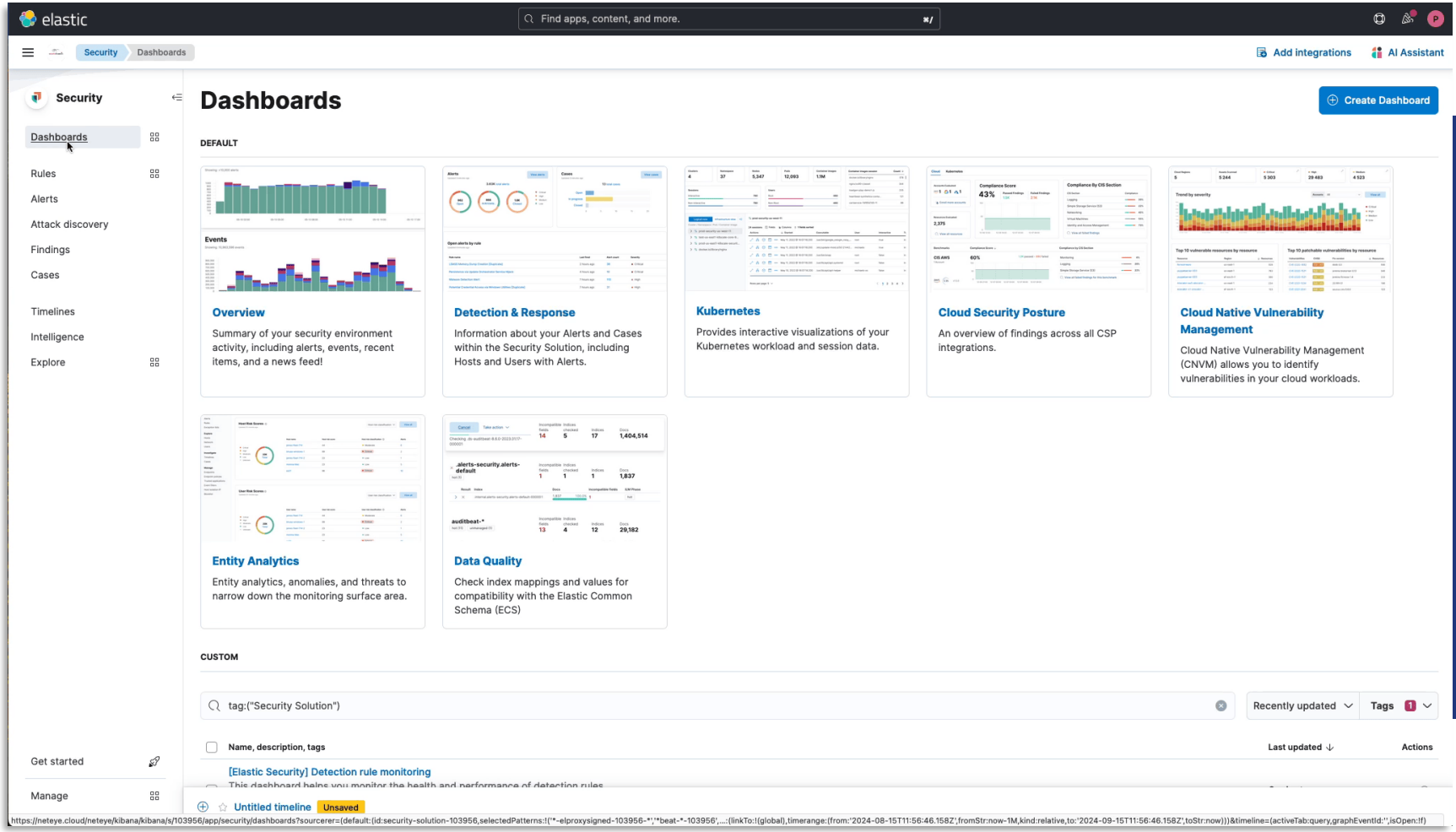
Periodic Reports

-60% Memory

https://ntop.org/

Elastic: Release 8.15 News

Release 8.15



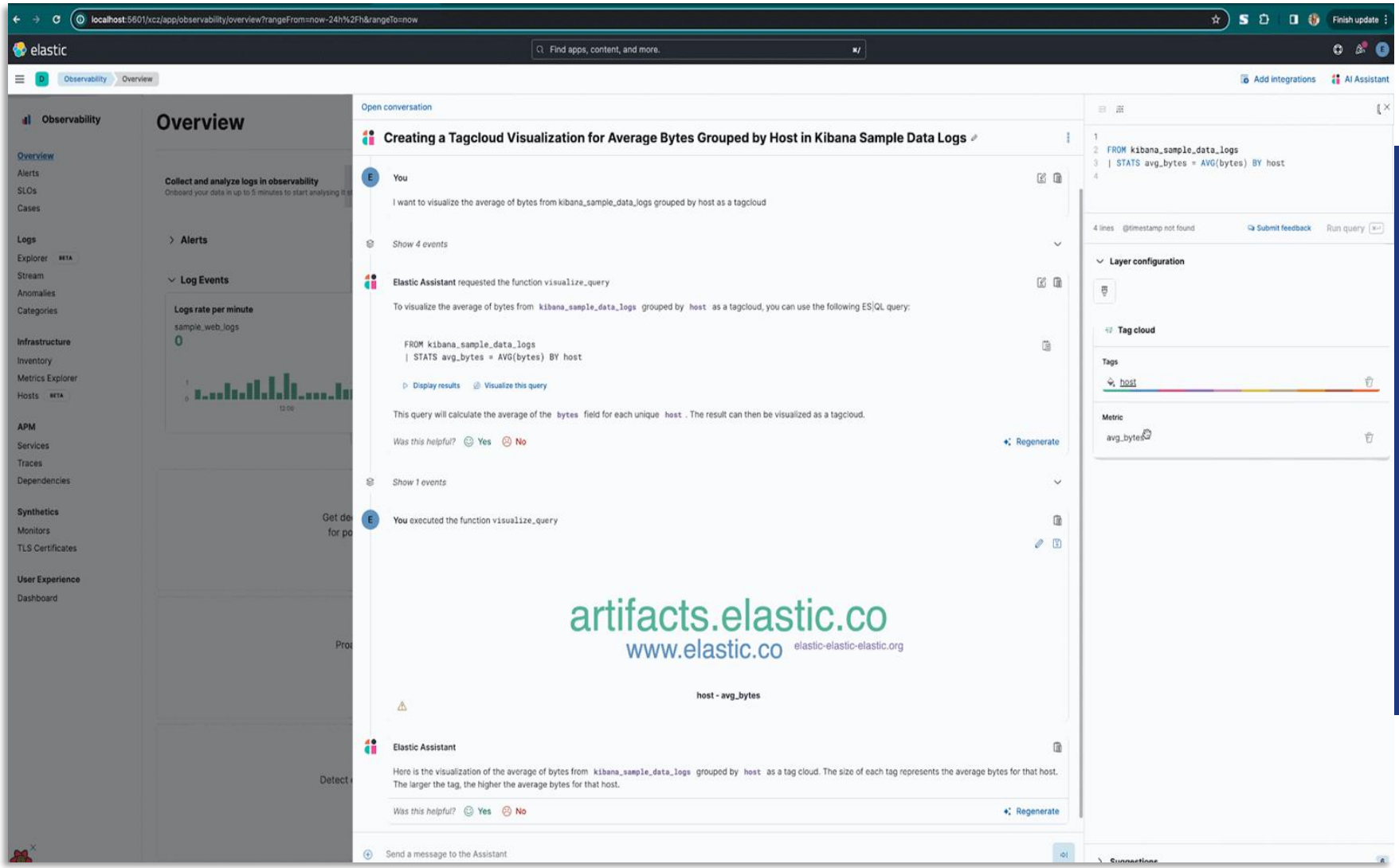
- Dashboards
- Detection Response
- Entity Analysis
- Data Quality ECS
- Mitre Att&ck

https://demo.elastic.co/

NetEye Conference DACH 2024

Elastic: ES|QL – Security - Observability AI assistant

Release 8.15

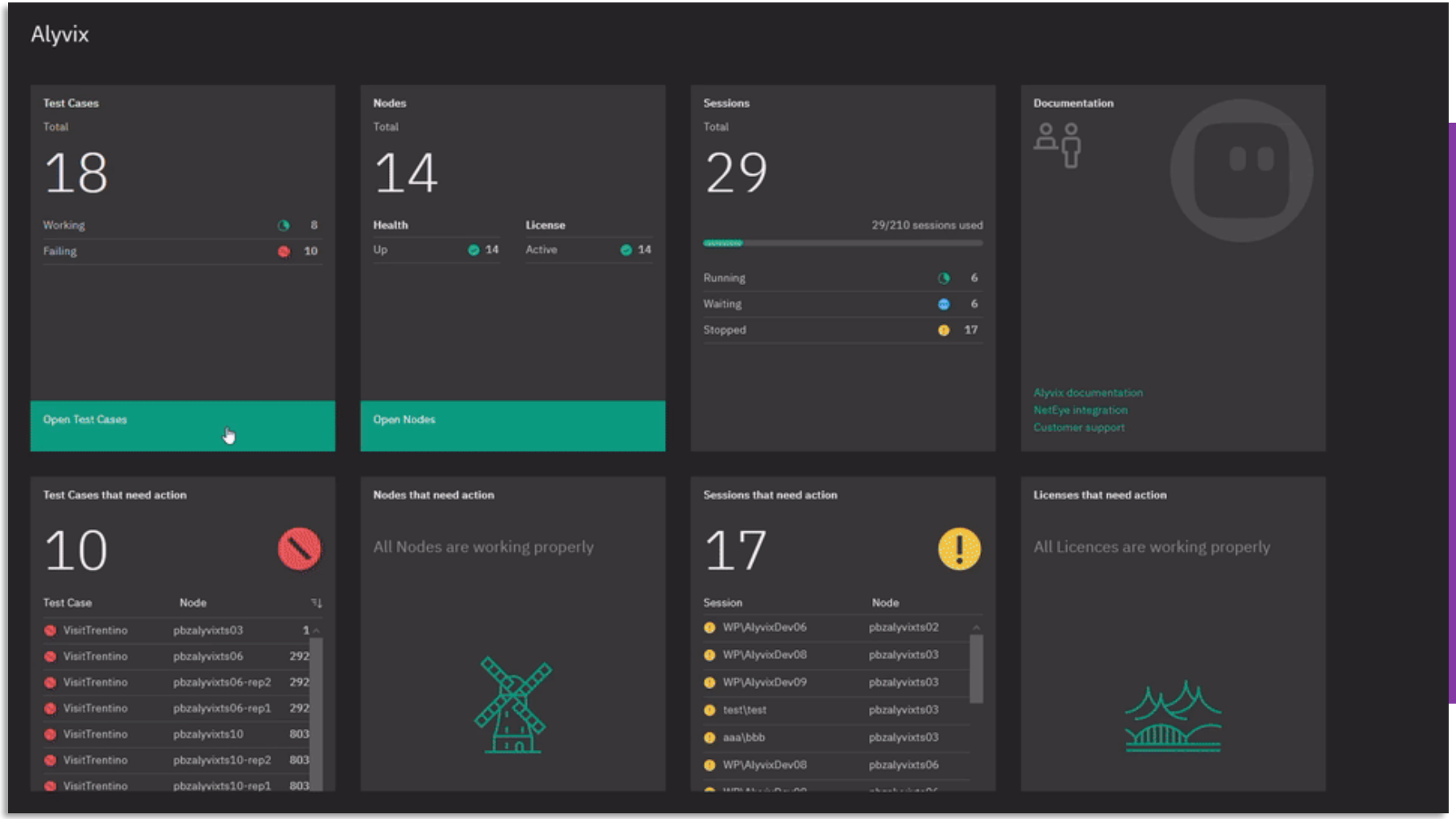


Verkürzung des Arbeitsablaufs für User bei der Verwendung des Observability KI-Assistenten

https://demo.elastic.co/

Alyvix: Synthetic monitoring

Quantifizieren Sie Ihre User Experience



Workflow Test case
Run Bots

Analyse - Insights

Aktionen

https://alyvix.com/

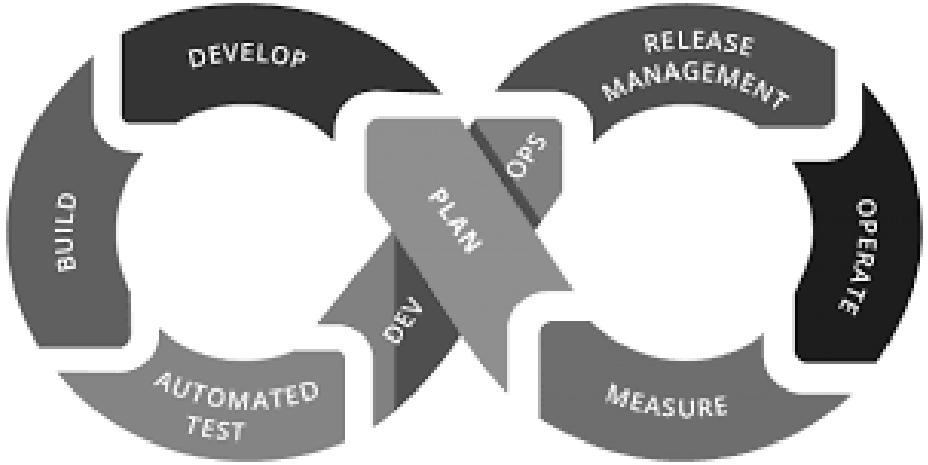
NetEye Conference DACH 2024

NetEye

Ausblick - Schwerpunkte

- 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