NetEye CONFERENCE 2025

From Insight to Action:
NetEye Platform

Georg Kostner di Würth Phoenix

Agenda

- Le sfide dal punto di vista dei CIO, CTO e CISO
- La soluzione: NetEye Platform
- NetEye Vision

CIO – CTO – CISO – IT Manager Ops

Challenges

- Growing complexity from multi-cloud, SaaS, and legacy systems
- Uncontrolled use of SaaS and open-source software
- Many monitoring, logging, and security tools in different teams
- Supply chain and third-party security challenges
- Compliance with regulations like NIS2, GDPR, ISO, SOC2, EU CRA
- Larger attack surface requiring stronger security
- Need for 24/7 availability and fast delivery
- Data-driven IT investment decisions
- Alert fatigue from false positives
- Long root cause analysis and high MTTR
- Skilled staff shortages causing team strain

Requirements

- Integrated observability and security platform to establish a trusted single source of truth
- Complete visibility into IT service health and business impact
- Automation to minimize manual tasks, less error prune
- Scalable, future-ready architecture
- Use of open standards like OpenTelemetry and API-first design
- Transparency and reporting for leadership and regulators
- AI/ML to reduce noise and speed up troubleshooting
- Integration with ITSM and automation systems
- Clear SLA/SLO/SLI reporting to demonstrate reliability
- **IT as business enabler**

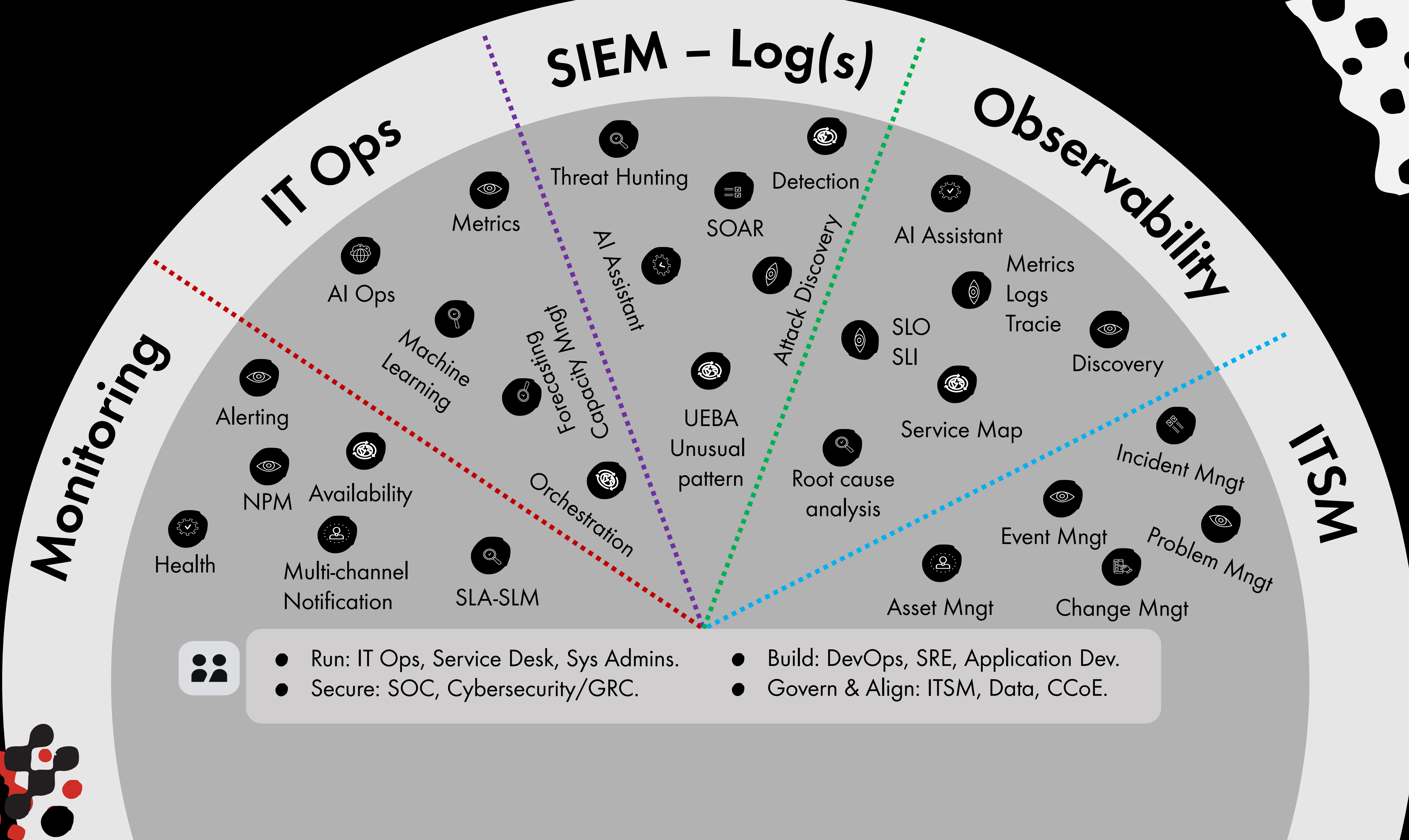
CIO – CTO – CISO – IT Manager Ops

Challenges Faced by IT Organizations

- Teams like Operations, Security, and Development often work separately, causing data silos.
- Different tools across teams hinder a unified source of truth.
- Manual processes can’t keep pace with business demands and cloud-native speed.
- Limited visibility makes it hard to pinpoint root causes of issues.

NetEye Solutions Overview

- Unified platform combining monitoring, observability, SIEM, and IT automation to break down data silos.
- Uses correlation and AI Ops to reduce noise, analyze root causes, and speed up MTTR.
- Merges security and operations views to manage uptime and compliance effectively.
- Integrates with ITSM, SOAR, and DevOps for seamless workflow alignment.
- Offers SLA dashboards and business process monitoring to showcase IT’s value.
- Supports data-driven decisions with SLI and SLO metrics.



Monitoring

Alerting

NPM

Availability

Health

Multi-channel Notification

SLA-SLM

IT Ops

Metrics

AI Ops

Machine Learning

Forecasting

Capacity Mngt

Orchestration

SIEM – Log(s)

Threat Hunting

Detection

SOAR

AI Assistant

Attack Discovery

UEBA Unusual pattern

Observability

AI Assistant

Metrics
Logs
Tracie

SLO
SLI

Discovery

Service Map

Root cause analysis

ITSM

Incident Mngt

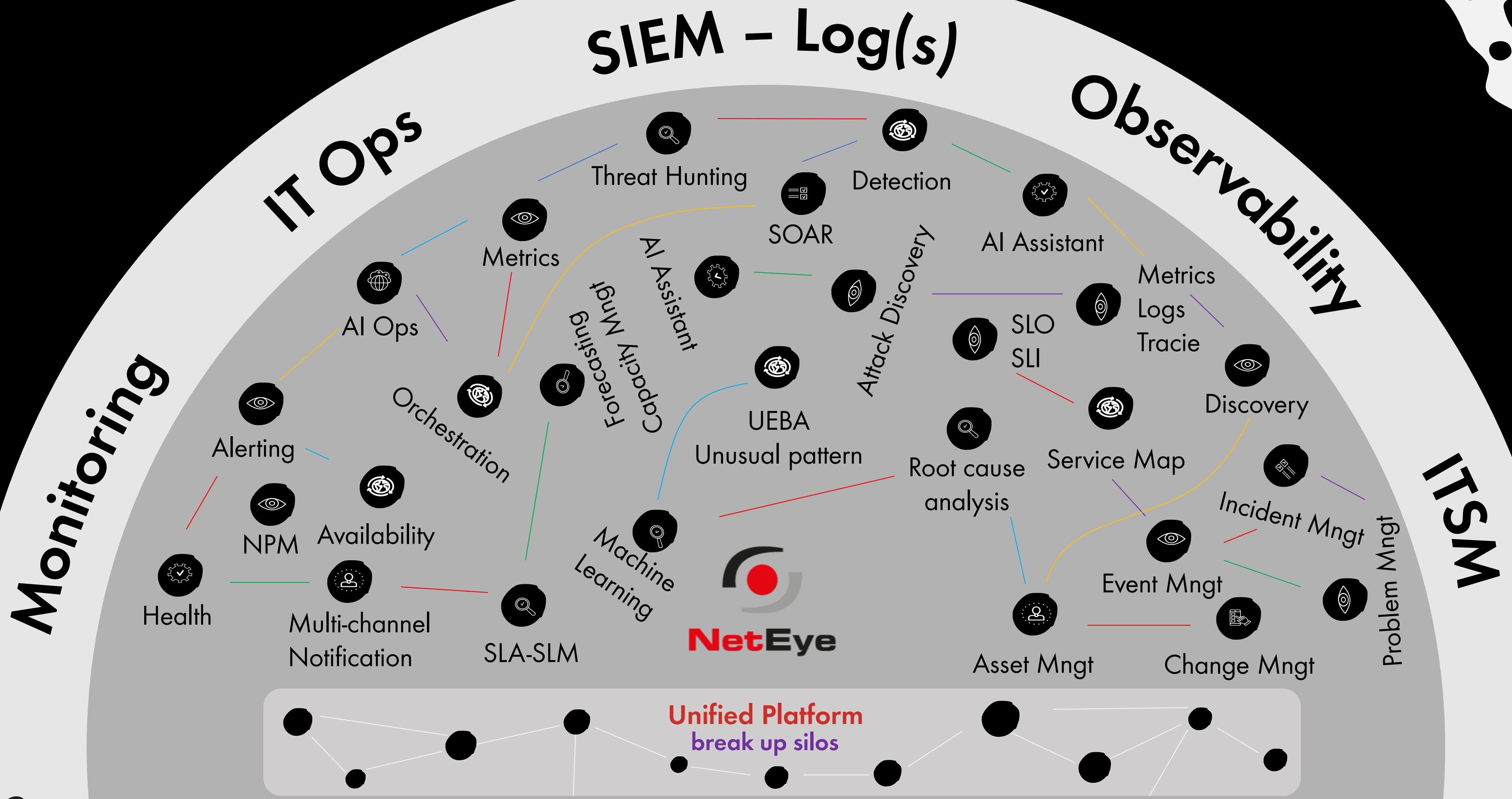
Event Mngt

Problem Mngt

Asset Mngt

Change Mngt

- Run: IT Ops, Service Desk, Sys Admins.
- Secure: SOC, Cybersecurity/GRC.
- Build: DevOps, SRE, Application Dev.
- Govern & Align: ITSM, Data, CCoE.



Monitoring

IT Ops

SIEM – Log(s)

Observability

ITSM

Health

Alerting

NPM

Availability

AI Ops

Metrics

Multi-channel Notification

SLA-SLM

Orchestration

Forecasting

Capacity Mngt

AI Assistant

Threat Hunting

SOAR

Detection

Attack Discovery

UEBA Unusual pattern

Machine Learning

AI Assistant

Metrics Logs Tracie

SLO SLI

Discovery

Service Map

Root cause analysis

Incident Mngt

Event Mngt

Problem Mngt

Asset Mngt

Change Mngt

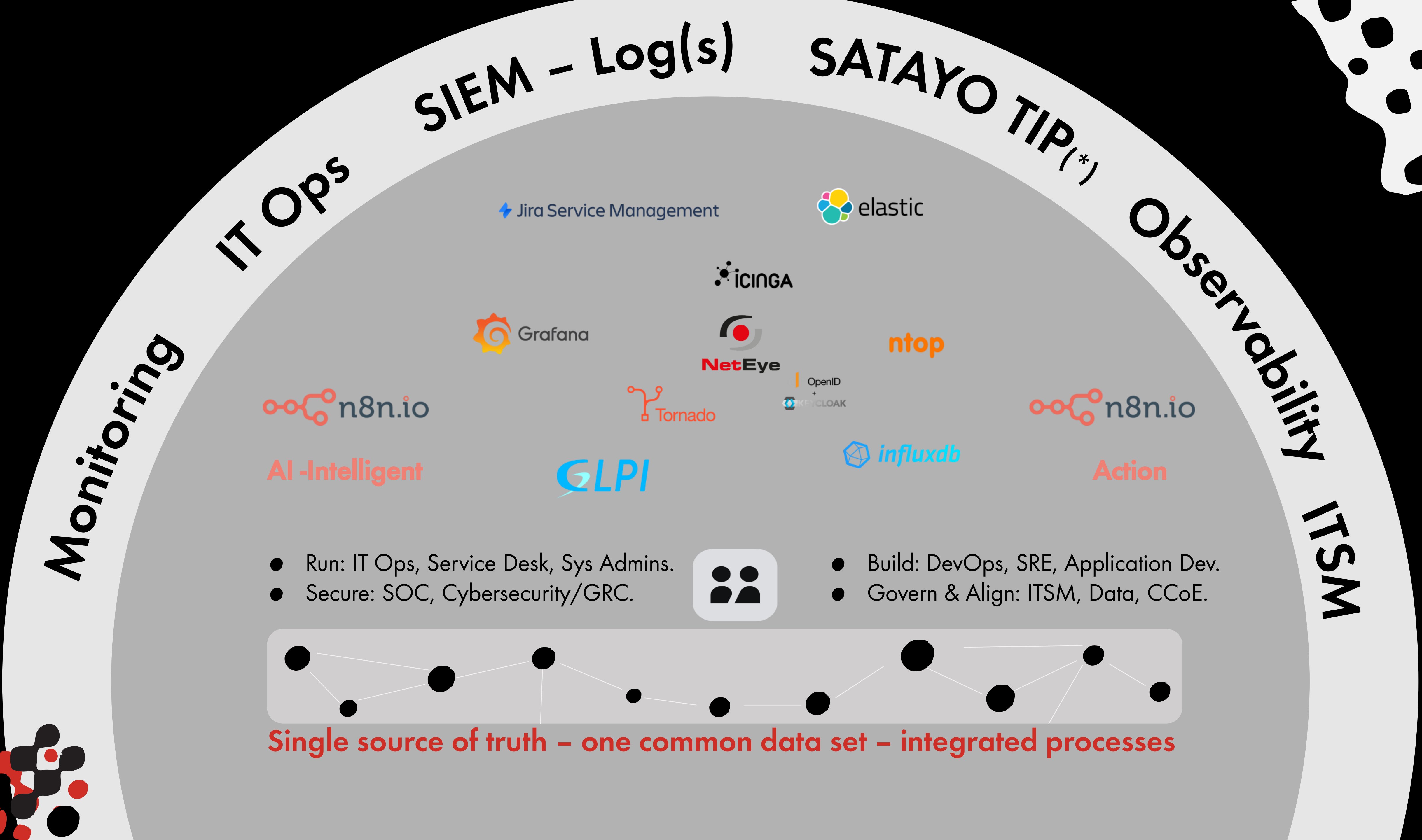
NetEye

Unified Platform

break up silos

- Run: IT Ops, Service Desk, Sys Admins.
- Secure: SOC, Cybersecurity/GRC.

- Build: DevOps, SRE, Application Dev.
- Govern & Align: ITSM, Data, CCoE.



- Run: IT Ops, Service Desk, Sys Admins.
- Secure: SOC, Cybersecurity/GRC.

- Build: DevOps, SRE, Application Dev.
- Govern & Align: ITSM, Data, CCoE.

Single source of truth – one common data set – integrated processes

SOC – Threat Intelligence

- Monitoring
- Detection

- SOAR
- IR

SOC
Threat Intelligence

NetEye

Unified Platform

NetEye

SIEM - Security

NetEye Monitoring - ITOA

IcingaDB – IcingaDBWeb - Tornado

- Scalability 1.000.000/min Service Checks
- Improved filtering, visualization, and performance
- Content Security Policy (CSP) to strengthen security
- Asset GLPI Data integration in Icinga Views

IMEdge – Icinga edge monitoring SNMP

- Scalability 100.000 and more SNMP monitoring
- Distributed Architecture, edge metrics storage
- SNMPv3 ready

Mariadb Galera Cluster

- MariaDB Galera Cluster ensures high availability, data consistency and better performance
- Native Observability dashboards for Galera

Grafana 12

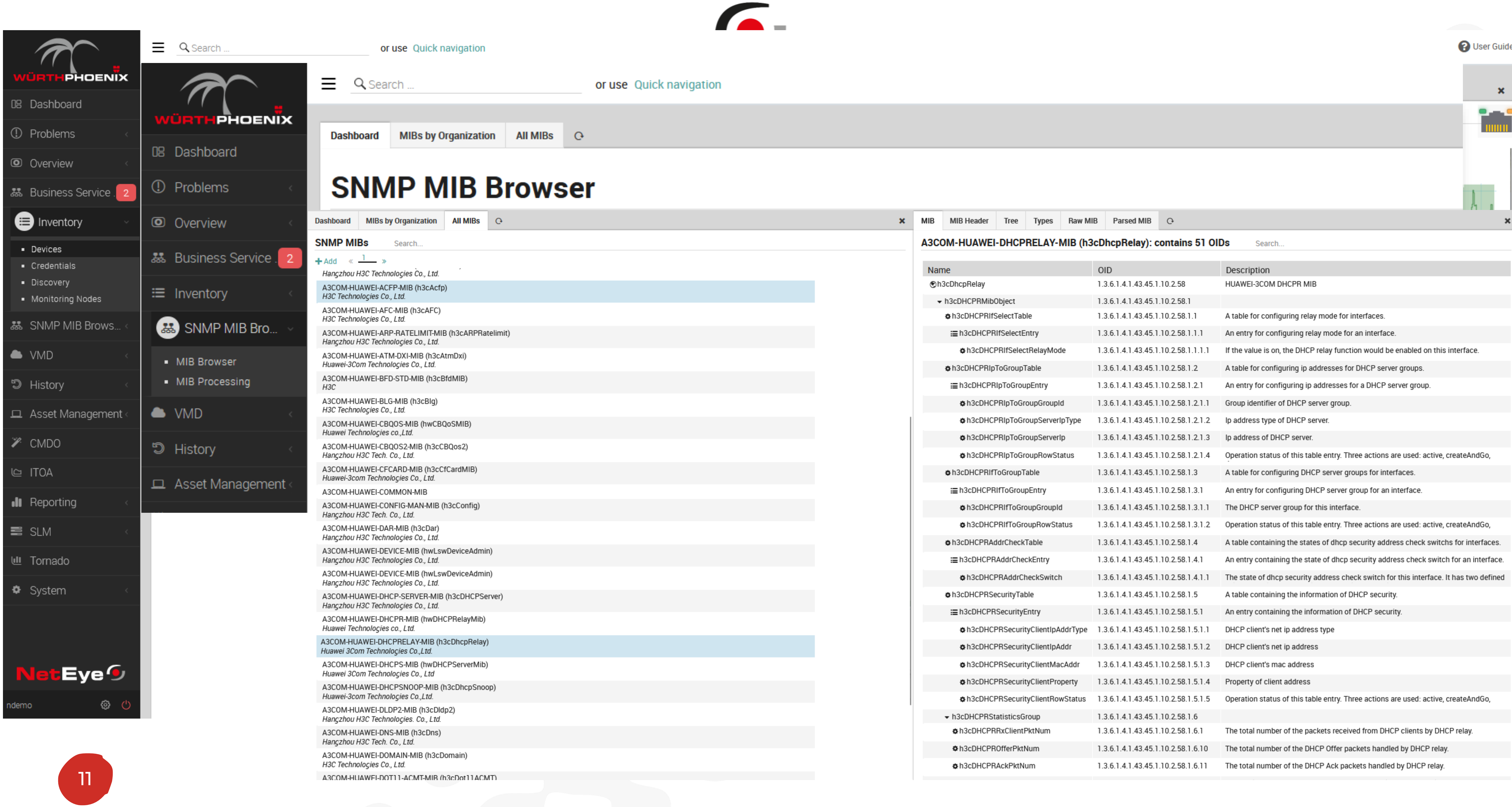
- Canvas
- Gitsync
- New GUI for an enhanced UX

NetEye Master on Azure – GLPI 11 (coming soon)

- Standard deployment of NetEye Master on Azure
- GLPI 11 introduces custom assets and group access rights for assets

User Guide

- Redesigned and restructured UG to deliver a clearer, use-case-oriented user experience



SNMP MIB Browser

SNMP MIBs

Hangzhou H3C Technologies Co., Ltd.

A3COM-HUAWEI-ACFP-MIB (h3cAcfp)
H3C Technologies Co., Ltd.

A3COM-HUAWEI-AFC-MIB (h3cAFC)
H3C Technologies Co., Ltd.

A3COM-HUAWEI-ARP-RATELIMIT-MIB (h3cARPRatelimit)
Hangzhou H3C Technologies Co., Ltd.

A3COM-HUAWEI-ATM-DXI-MIB (h3cAtmDxi)
Huawei-3Com Technologies Co., Ltd.

A3COM-HUAWEI-BFD-STD-MIB (h3cBfdMIB)
H3C

A3COM-HUAWEI-BLG-MIB (h3cBlg)
H3C Technologies Co., Ltd.

A3COM-HUAWEI-CBQOS-MIB (hwCBQoSMIB)
Huawei Technologies co.,Ltd.

A3COM-HUAWEI-CBQOS2-MIB (h3cCBQos2)
Hangzhou H3C Tech. Co., Ltd.

A3COM-HUAWEI-CFCARD-MIB (h3cCfCardMIB)
Huawei-3com Technologies Co., Ltd.

A3COM-HUAWEI-COMMON-MIB

A3COM-HUAWEI-CONFIG-MAN-MIB (h3cConfig)
Hangzhou H3C Tech. Co., Ltd.

A3COM-HUAWEI-DAR-MIB (h3cDar)
Hangzhou H3C Technologies Co., Ltd.

A3COM-HUAWEI-DEVICE-MIB (hwLswDeviceAdmin)
Hangzhou H3C Technologies Co., Ltd.

A3COM-HUAWEI-DEVICE-MIB (hwLswDeviceAdmin)
Hangzhou H3C Technologies Co., Ltd.

A3COM-HUAWEI-DHCP-SERVER-MIB (h3cDHCPServer)
Hangzhou H3C Technologies Co., Ltd.

A3COM-HUAWEI-DHCPR-MIB (hwDHCPRelayMib)
Huawei Technologies co., Ltd.

A3COM-HUAWEI-DHCPRELAY-MIB (h3cDhcpRelay)
Huawei 3Com Technologies Co.,Ltd.

A3COM-HUAWEI-DHCPS-MIB (hwDHCPServerMib)
Huawei 3Com Technologies Co., Ltd

A3COM-HUAWEI-DHCPSNOOP-MIB (h3cDhcpSnoop)
Huawei-3com Technologies Co.,Ltd.

A3COM-HUAWEI-DLDP2-MIB (h3cDldp2)
Hangzhou H3C Technologies. Co., Ltd.

A3COM-HUAWEI-DNS-MIB (h3cDns)
Hangzhou H3C Tech. Co., Ltd.

A3COM-HUAWEI-DOMAIN-MIB (h3cDomain)
H3C Technologies Co., Ltd.

A3COM-HUAWEI-DOT11-ACMT-MIB (h3cDot11ACMT)

A3COM-HUAWEI-DHCPRELAY-MIB (h3cDhcpRelay): contains 51 OIDs

Name	OID	Description
h3cDhcpRelay	1.3.6.1.4.1.43.45.1.10.2.58	HUAWEI-3COM DHCPR MIB
h3cDHCPRMibObject	1.3.6.1.4.1.43.45.1.10.2.58.1	
h3cDHCPRIfSelectTable	1.3.6.1.4.1.43.45.1.10.2.58.1.1	A table for configuring relay mode for interfaces.
h3cDHCPRIfSelectEntry	1.3.6.1.4.1.43.45.1.10.2.58.1.1.1	An entry for configuring relay mode for an interface.
h3cDHCPRIfSelectRelayMode	1.3.6.1.4.1.43.45.1.10.2.58.1.1.1.1	If the value is on, the DHCP relay function would be enabled on this interface.
h3cDHCPRIpToGroupTable	1.3.6.1.4.1.43.45.1.10.2.58.1.2	A table for configuring ip addresses for DHCP server groups.
h3cDHCPRIpToGroupEntry	1.3.6.1.4.1.43.45.1.10.2.58.1.2.1	An entry for configuring ip addresses for a DHCP server group.
h3cDHCPRIpToGroupGroupId	1.3.6.1.4.1.43.45.1.10.2.58.1.2.1.1	Group identifier of DHCP server group.
h3cDHCPRIpToGroupServerIpType	1.3.6.1.4.1.43.45.1.10.2.58.1.2.1.2	Ip address type of DHCP server.
h3cDHCPRIpToGroupServerIp	1.3.6.1.4.1.43.45.1.10.2.58.1.2.1.3	Ip address of DHCP server.
h3cDHCPRIpToGroupRowStatus	1.3.6.1.4.1.43.45.1.10.2.58.1.2.1.4	Operation status of this table entry. Three actions are used: active, createAndGo,
h3cDHCPRIfToGroupTable	1.3.6.1.4.1.43.45.1.10.2.58.1.3	A table for configuring DHCP server groups for interfaces.
h3cDHCPRIfToGroupEntry	1.3.6.1.4.1.43.45.1.10.2.58.1.3.1	An entry for configuring DHCP server group for an interface.
h3cDHCPRIfToGroupGroupId	1.3.6.1.4.1.43.45.1.10.2.58.1.3.1.1	The DHCP server group for this interface.
h3cDHCPRIfToGroupRowStatus	1.3.6.1.4.1.43.45.1.10.2.58.1.3.1.2	Operation status of this table entry. Three actions are used: active, createAndGo,
h3cDHCPRAddrCheckTable	1.3.6.1.4.1.43.45.1.10.2.58.1.4	A table containing the states of dhcp security address check switchs for interfaces.
h3cDHCPRAddrCheckEntry	1.3.6.1.4.1.43.45.1.10.2.58.1.4.1	An entry containing the state of dhcp security address check switch for an interface.
h3cDHCPRAddrCheckSwitch	1.3.6.1.4.1.43.45.1.10.2.58.1.4.1.1	The state of dhcp security address check switch for this interface. It has two defined
h3cDHCPRSecurityTable	1.3.6.1.4.1.43.45.1.10.2.58.1.5	A table containing the information of DHCP security.
h3cDHCPRSecurityEntry	1.3.6.1.4.1.43.45.1.10.2.58.1.5.1	An entry containing the information of DHCP security.
h3cDHCPRSecurityClientIpAddrType	1.3.6.1.4.1.43.45.1.10.2.58.1.5.1.1	DHCP client's net ip address type
h3cDHCPRSecurityClientIpAddr	1.3.6.1.4.1.43.45.1.10.2.58.1.5.1.2	DHCP client's net ip address
h3cDHCPRSecurityClientMacAddr	1.3.6.1.4.1.43.45.1.10.2.58.1.5.1.3	DHCP client's mac address
h3cDHCPRSecurityClientProperty	1.3.6.1.4.1.43.45.1.10.2.58.1.5.1.4	Property of client address
h3cDHCPRSecurityClientRowStatus	1.3.6.1.4.1.43.45.1.10.2.58.1.5.1.5	Operation status of this table entry. Three actions are used: active, createAndGo,
h3cDHCPRStatisticsGroup	1.3.6.1.4.1.43.45.1.10.2.58.1.6	
h3cDHCPRRxClientPktNum	1.3.6.1.4.1.43.45.1.10.2.58.1.6.1	The total number of the packets received from DHCP clients by DHCP relay.
h3cDHCPROfferPktNum	1.3.6.1.4.1.43.45.1.10.2.58.1.6.10	The total number of the DHCP Offer packets handled by DHCP relay.
h3cDHCPRAckPktNum	1.3.6.1.4.1.43.45.1.10.2.58.1.6.11	The total number of the DHCP Ack packets handled by DHCP relay.

NetEye

SIEM - Security

NetEye SIEM - Security

Elastic 9

- Attack Discovery – AI Assistent
- SecOps with AI-driven security analytics, accelerating threat detection, investigation, and response
- Built on Lucene 10 to gain major performance improvements
- ES|QL LOOKUP JOIN
- **Kibana Multi-instance** for scalability on execution of rule detection

SATAYO 2 TIP (next generation)

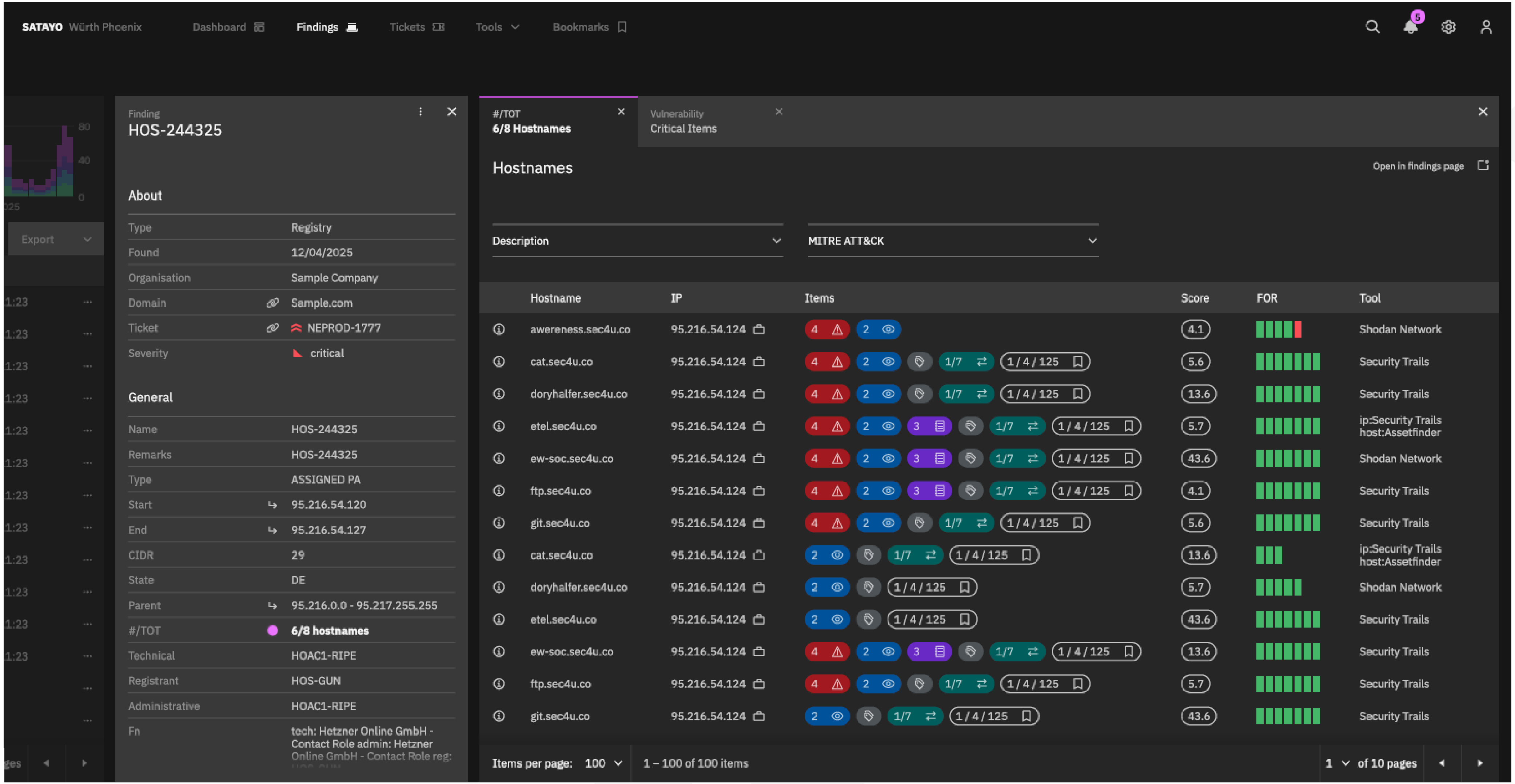
- External Attack Surface Management
- Natively integrated in NetEye.Cloud

NIS2

ISO 27001 – 27017 - 27018

EU Cyber Resilience Act

SATAYO 2 TIP



Finding
HOS-244325

About

Type	Registry
Found	12/04/2025
Organisation	Sample Company
Domain	Sample.com
Ticket	NEPROD-1777
Severity	critical

General

Name	HOS-244325
Remarks	HOS-244325
Type	ASSIGNED PA
Start	↳ 95.216.54.120
End	↳ 95.216.54.127
CIDR	29
State	DE
Parent	↳ 95.216.0.0 - 95.217.255.255
#/TOT	● **6/8 hostnames**
Technical	HOAC1-RIPE
Registrant	HOS-GUN
Administrative	HOAC1-RIPE
Fn	tech: Hetzner Online GmbH - Contact Role admin: Hetzner Online GmbH - Contact Role reg: HOS-GUN

#/TOT
6/8 Hostnames

Vulnerability
Critical Items

Hostnames

Open in findings page

Description

MITRE ATT&CK

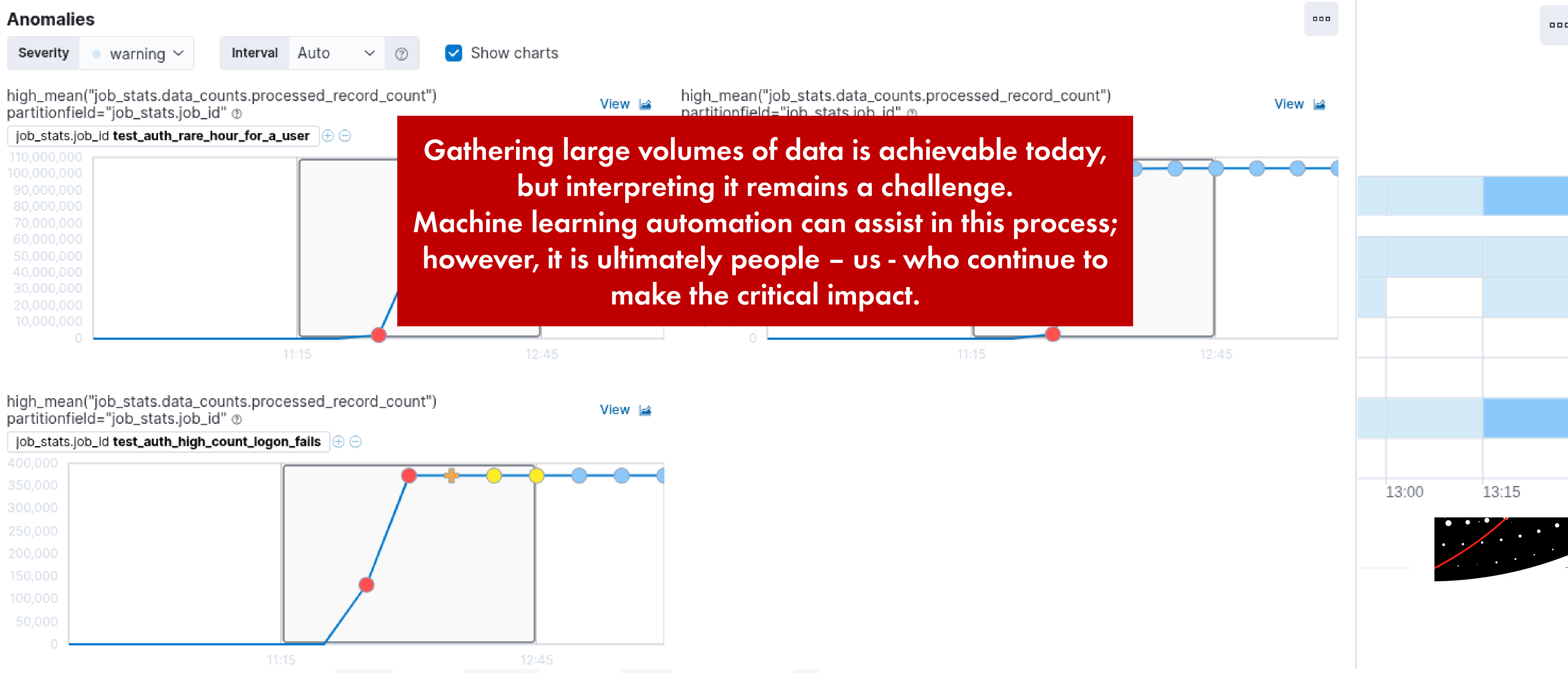
Hostname	IP	Items	Score	FOR	Tool
awereness.sec4u.co	95.216.54.124	4 ⚠ 2 👁	4.1	🟩🟩🟩🟩🟥	Shodan Network
cat.sec4u.co	95.216.54.124	4 ⚠ 2 👁 🏷 1/7 ⇄ 1 / 4 / 125 🔖	5.6	🟩🟩🟩🟩🟩🟩🟩	Security Trails
doryhalfer.sec4u.co	95.216.54.124	4 ⚠ 2 👁 🏷 1/7 ⇄ 1 / 4 / 125 🔖	13.6	🟩🟩🟩🟩🟩🟩🟩	Security Trails
etel.sec4u.co	95.216.54.124	4 ⚠ 2 👁 3 ☰ 🏷 1/7 ⇄ 1 / 4 / 125 🔖	5.7	🟩🟩🟩🟩🟩🟩🟩	ip:Security Trails host:Assetfinder
ew-soc.sec4u.co	95.216.54.124	4 ⚠ 2 👁 3 ☰ 🏷 1/7 ⇄ 1 / 4 / 125 🔖	43.6	🟩🟩🟩🟩🟩🟩🟩	Shodan Network
ftp.sec4u.co	95.216.54.124	4 ⚠ 2 👁 3 ☰ 🏷 1/7 ⇄ 1 / 4 / 125 🔖	4.1	🟩🟩🟩🟩🟩🟩🟩	Security Trails
git.sec4u.co	95.216.54.124	4 ⚠ 2 👁 🏷 1/7 ⇄ 1 / 4 / 125 🔖	5.6	🟩🟩🟩🟩🟩🟩🟩	Security Trails
cat.sec4u.co	95.216.54.124	2 👁 🏷 1/7 ⇄ 1 / 4 / 125 🔖	13.6	🟩🟩🟩	ip:Security Trails host:Assetfinder
doryhalfer.sec4u.co	95.216.54.124	2 👁 🏷 1 / 4 / 125 🔖	5.7	🟩🟩🟩🟩🟩	Shodan Network
etel.sec4u.co	95.216.54.124	2 👁 🏷 1 / 4 / 125 🔖	43.6	🟩🟩🟩🟩🟩🟩🟩	Security Trails
ew-soc.sec4u.co	95.216.54.124	4 ⚠ 2 👁 3 ☰ 🏷 1/7 ⇄ 1 / 4 / 125 🔖	13.6	🟩🟩🟩🟩🟩🟩🟩	Security Trails
ftp.sec4u.co	95.216.54.124	4 ⚠ 2 👁 🏷 1/7 ⇄ 1 / 4 / 125 🔖	5.7	🟩🟩🟩🟩🟩🟩🟩	Security Trails
git.sec4u.co	95.216.54.124	2 👁 🏷 1/7 ⇄ 1 / 4 / 125 🔖	43.6	🟩🟩🟩🟩🟩🟩🟩	Security Trails

Items per page: 100 1 – 100 of 100 items 1 of 10 pages

NetEye

SIEM - Security

NetEye Observability APM - Alyvix



Anomalies

Severity ● warning

Interval Auto

☑ Show charts

high_mean("job_stats.data_counts.processed_record_count") partitionfield="job_stats.job_id"

job_stats.job_id **test_auth_rare_hour_for_a_user**

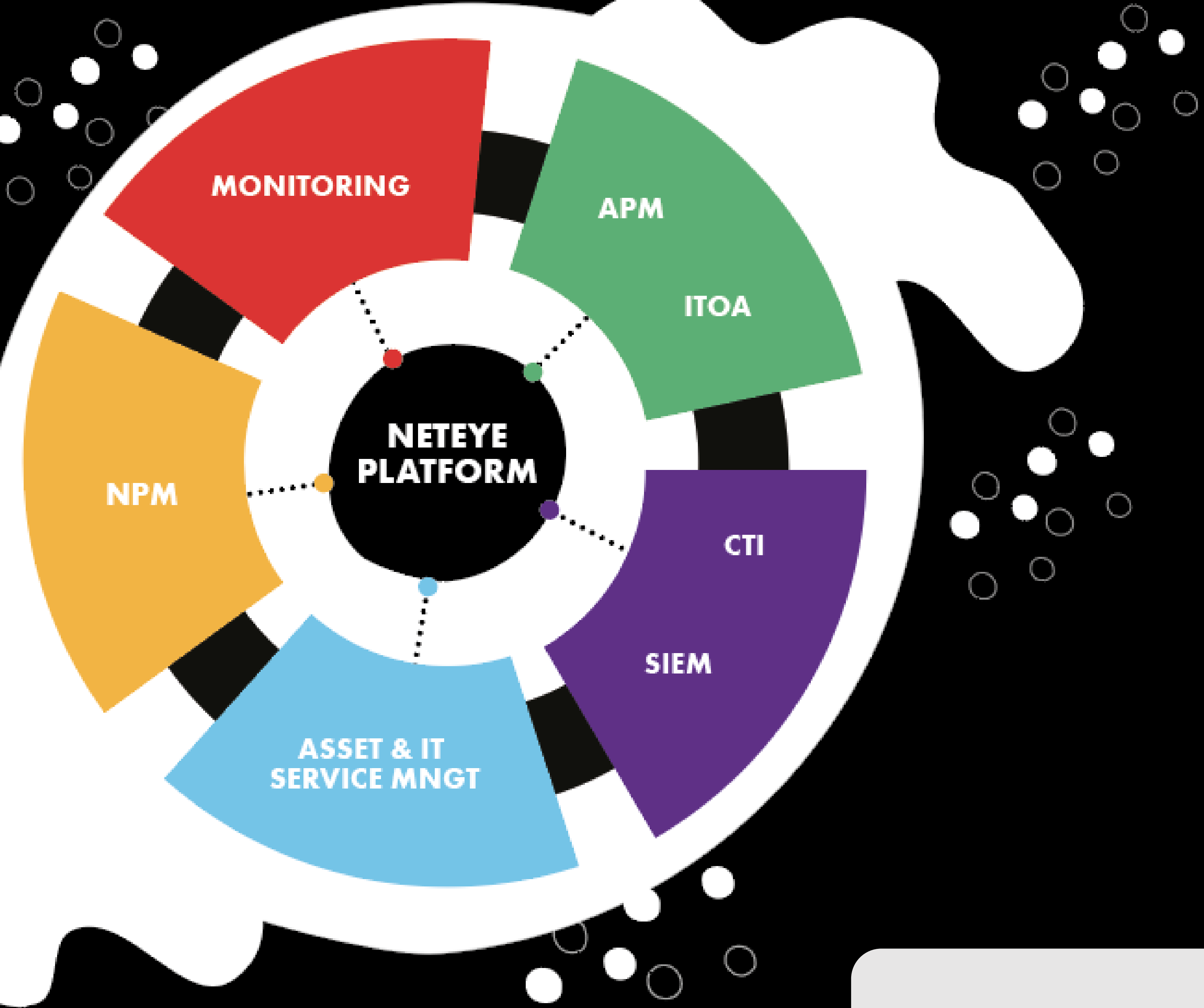
high_mean("job_stats.data_counts.processed_record_count") partitionfield="job_stats.job_id"

high_mean("job_stats.data_counts.processed_record_count") partitionfield="job_stats.job_id"

job_stats.job_id **test_auth_high_count_logon_fails**

Gathering large volumes of data is achievable today, but interpreting it remains a challenge.
Machine learning automation can assist in this process; however, it is ultimately people – us - who continue to make the critical impact.

FROM TODAY TO the FUTURE



Self Managed

- OpenShift – on-prem
- MS Azure
- AWS
- GCP

Full Managed – SaaS(*)

- OpenShift
- MS Azure
- AWS
- GCP

Cloud Native Architecture

- Container
- Kubernetes
- Mesh
- CI/CD

NetEye