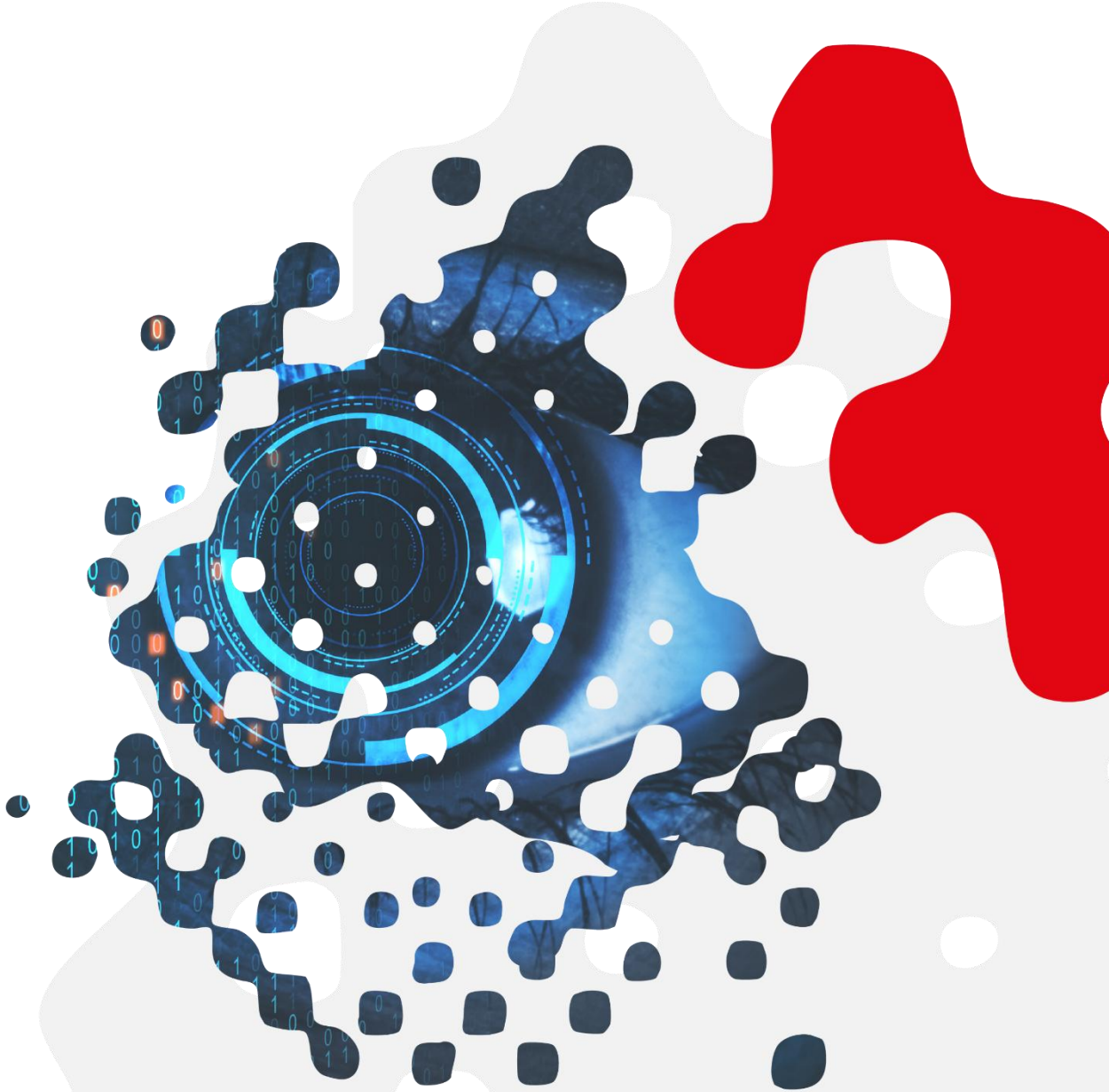
NetEye Conference DACH 2026

Next Generation Observability: Kubernetes & Data Platforms with NetEye

12 months of innovation towards one platform

NetEye Conference Nürnberg · October 2026

One platform. Inside and out. Before it happens.



WÜRTH | IT

GRAVITATE

SAME HOUR. FOUR SIGNALS.

ONE INCIDENT - OR FOUR?

A normal Tuesday morning. Four tools raise their hand within seven minutes.

OUTSIDE

08:57

Admin credentials for vpn-gw-01 are offered on a dark-web market.

MONITORING

09:02

vpn-gw-01: CPU at 100 %, check latency triples.

NETWORK

09:03

Unusual flows towards the gateway from an ASN never seen before.

SECURITY

09:04

A privileged login from an unusual source.

Is it load, an attack - or both? · Whose asset is it? · What happens next?

Four tools, four teams, four partial **truths**. The answer exists - spread across systems that do not share a key.

UNDER THE HOOD SATAYO · Icinga · ntopng · Elastic Security — the same gateway, seen four times

You’re not lacking data. You are lacking context.

SIX CHALLENGES.

ONE PATTERN BEHIND THEM.

CHALLENGE	WHAT IT MEANS	THE NETEYE ANSWER
Tool sprawl & data silos	Every team its own tool, every tool its own truth.	One platform: monitoring, observability, SIEM/XDR, assets and network on one data layer.
A growing attack surface	Cloud, SaaS, shadow IT, leaked credentials.	ESAM with SATAYO on NetEye.Cloud driven by your PIRs, mapped to the inside.
NIS2 · DORA · CRA	Asset inventory, detection, incident handling - with evidence.	Evidence by design: the platform that collects the data produces the proof.
Hybrid & cloud-native complexity	Kubernetes, microservices, ephemeral workloads.	OpenTelemetry end to end, the network as fourth signal - and NetEye itself on Kubernetes.
Cloud & Kubernetes cost	Spend grows with every workload - nobody sees who causes it.	FinOps in NetEye: OpenCost allocates cost per namespace, service and tenant in Elastic.
AI on both sides	Attackers automate. Defenders have to do as well.	Agentic AI on linked data - with a human in the loop.

Six challenges, one pattern: the answer is never another tool. It is context.

MONITORING AND SECURITY GROW TOGETHER.

NEXT GENERATION OBSERVABILITY — INSIDE AND OUT.

YESTERDAY: SEPARATE WORLDS

NOC	is it up?
SRE / DevOps	is it fast?
SOC	is it an attack?
CISO	what can the internet see?
FinOps	what does it cost?

NEXT GENERATION OBSERVABILITY: ONE CONTEXT

metrics | logs & traces | network | security signals

assets & owners | external exposure | cost (FinOps)

The same incident, explained from every angle at once - from the host to the dark web, and what it costs, on one data layer.

THE REST OF THIS TALK — THREE LINKS, EACH ONE ENABLES THE NEXT

1 FOUNDATION
Kubernetes & microservices - secure, reliable, zero-downtime

→

2 LINKED DATA
modules share identity: host · asset · service · flow · finding · cost

→

3 CONTEXT FOR AI
correlation becomes the context for agentic analysis

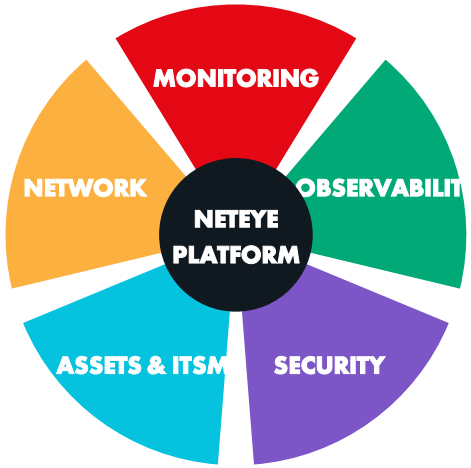
UNDER THE HOOD Icinga DB · OpenTelemetry/EDOT · ntopng · Elastic Security · GLPI 11 · SATAYO · OpenCost (coming)

Observability no longer stops at the firewall - or at your own perimeter.

MEET NETEYE.

One platform for holistic IT visibility across operations, security and service management

Five capabilities, one data layer - **each module is a data source** for the same context.



one data layer · one tenancy

- **MONITORING**
  Icinga 2 · Icinga DB · Director · Tornado · Service Level Management
- **NETWORK**
  ntopng 7 - IMEdge
- **OBSERVABILITY**
  Elastic APM · RUM · OpenTelemetry/EDOT · Alyvix · FinOps with OpenCost (coming)
- **SECURITY**
  Elastic Security SIEM · XDR · SOAR · SATAYO on NetEye.Cloud — PIR-driven CTI + ESAM
- **ASSETS & ITSM**
  GLPI 11 · CloudInventory · IT Service Management · Service Context

ASSET MANAGEMENT — THE JOIN BETWEEN OUTSIDE AND INSIDE
With NetEye.Cloud, **every external finding knows its internal owner**

CONTEXT FOR AGENTIC AI
built up module by module — so **NOC, SRE, SOC, CISO and FinOps** reach the same insight faster

UNDER THE HOOD Elastic 9.5 · Icinga 2.16 · GLPI 11 with Keycloak SSO · NetEye 4.50 · coming: ntopng 7 · IMEdge · OpenCost

Not a bundle of tools - five data sources for one context.

THE FOUNDATION IS MOVING.

FROM A TRADITIONAL RED HAT CLUSTER TO KUBERNETES — THE JOURNEY HAS BEGUN.

Every one of you plans an outage to upgrade the system that is supposed to tell you when you have an outage.

WHERE WE COME FROM

Traditional Red Hat cluster

Active / standby nodes, resources fail over

Packages on a mutable OS - drift, half-states

A maintenance window: the platform is blind

→

TODAY

4.47 standby period eliminated - nodes stay operational during updates

4.49 Kubernetes foundation on RKE2

First service on it: the tenant-aware OpenTelemetry Collector

→

NEXT

More NetEye services as microservices

Every layer an application cluster

One operator per layer - shard health, config sync, catch-up rules

→

TARGET

Zero-downtime update and upgrade

Immutable, signed OS image with atomic rollback

OS and services stop sharing a release cycle

Kubernetes gives generic primitives. Our operators add what each layer needs.

an upgrade becomes a declarative state change the operator reconciles, not a runbook executed by a human at 02:00.

UNDER THE HOOD RKE2 since 4.49 · standby-free updates since 4.47 · existing deployments keep working · plan cluster networking before 4.49

Secure, reliable operations - and no more planned outage for the system that reports your outages.

YOUR ENVIRONMENT. YOUR CHOICE.

SAME PLATFORM POWER. DIFFERENT OPERATING MODEL.

One Kubernetes foundation - two ways to run NetEye.

SELF-MANAGED

Kubernetes (RKE2) in your own environment

Operated in your own environment.

Keep full control over operations and data handling.

Manage updates and security.

For local operation, direct control and infrastructure resilience.

FULLY MANAGED

NetEye.Cloud - SaaS on AWS EKS

Managed by Würth IT experts.

Reduced operational overhead.

Contractually defined service model.

For faster adoption, operational relief and innovation.

Both models deliver the same NetEye platform. The difference lies in how operation, responsibility and control are allocated.

UNDER THE HOOD self-managed: RKE2 on your infrastructure · fully managed: NetEye.Cloud on AWS EKS, operated by Würth IT

Run it yourself or let us run it - the platform, the data model and the innovation are the same.

A NEW SIGNAL BASE.

ICINGA DB AT THE CORE. OPENTELEMETRY END TO END.

THE MONITORING CORE WAS REPLACED

- **4.44** Icinga DB introduced alongside IDO
- **4.45** Icinga DB Web becomes the default UI
- **4.47** six modules migrated transparently
- **4.48** **migration complete - IDO decommissioned**

Higher throughput, a faster UI, millisecond-precision SLA figures the largest migration in years is behind us.

OPENTELEMETRY BECAME THE STANDARD

- **4.44** EDOT GA - OpenTelemetry-native schemas across all signals
- **4.49** **tenant-aware OTel Collector - the first NetEye service on Kubernetes**
- **4.50** Icinga 2.16 ships its metrics over OTLP
- **NEXT** OpenCost - Kubernetes and cloud cost through the same Collector into Elastic

Instrument once - every signal, and soon its cost, arrives with the same schema and the same tenant.

LINKED TODAY **Every signal now carries the keys that let it be joined.**

tenant
OIDC identity through the OTel Collector

trace.id
logs, traces and spans of one request

service.name
APM, Icinga DB, SLM - and cost - on one service

entity
host, user, account - resolved in Elastic

UNDER THE HOOD OTLPMetricsWriter replaces ElasticsearchWriter (4.50) · Elastic Entity Analytics GA (4.48) · OpenCost: roadmap

Shared keys are what turn a set of modules into a data platform.

WHAT DOES IT COST?

FINOPS BECOMES PART OF OBSERVABILITY - OPENCOST IN ELASTIC.

COMING TO NETEYE

Kubernetes made infrastructure elastic — and the bill opaque. Cost becomes one more signal on the same data layer.

SOURCES
Kubernetes clusters · AWS · Azure · GCP · on-prem pricing

→

OPENCOST
cost allocation per cluster, namespace, pod and service

→

OTEL COLLECTOR
tenant-aware - scrapes OpenCost's metrics

→

ELASTIC
cost next to metrics, logs and traces - same tenant, same service

→

NETEYE
dashboards, SLM and reports: cost per service, tenant and team

WHO PAYS FOR WHAT

Cost per namespace, workload, service and tenant - showback and chargeback for your clusters and for NetEye.Cloud.

COST NEXT TO PERFORMANCE

The same service.name links cost to latency, errors and SLA. Idle capacity becomes visible, right-sizing a decision with evidence.

CONTEXT FOR AI

OpenCost ships an MCP server: cost becomes context for agentic analysis - is this peak worth scaling for?

UNDER THE HOOD OpenCost (open source, CNCF incubating) · /metrics → OTel Collector → Elasticsearch · cloud billing APIs

Observability asks "is it healthy?" FinOps adds "is it worth it?", on the same data layer.

THE FOURTH SIGNAL: THE NETWORK.

TWO MODULES, TWO QUESTIONS.

Kubernetes and data platforms live on the network - traffic and dependencies show what the other signals can't.

NetEye — ONE PLATFORM

IMEdge	→ RRD →	IMEdge graphs	load, errors, trends, capacity - "how loaded is it?"
ntopng	→ ClickHouse →	ntopng dashboards	flows, Layer 7, security analysis - "where does it come from?"

A peak in SNMP → which flow caused it? · A suspicious flow → which port carried it?

COMING TO NETEYE

ntopng 7 — THE FLOW AND SECURITY VIEW

Layer 7 on encrypted traffic: TLS metadata, fingerprints, behaviour - no decryption, risk flags on suspicious flows.

"Is it the network?" with proof: RTT, application delay, jitter, retransmissions, top talkers.

Crypto & AI inventory: TLS ciphers per host, quantum-safe or not, AI services in use.

What changed since Monday: new hosts, services, dependencies - incl. IoT.

COMING TO NETEYE

IMEdge - THE DEVICE AND PORT VIEW

SNMP at scale: traffic every 15 s, errors every 60 s, configuration every 10 min with reboot detection.

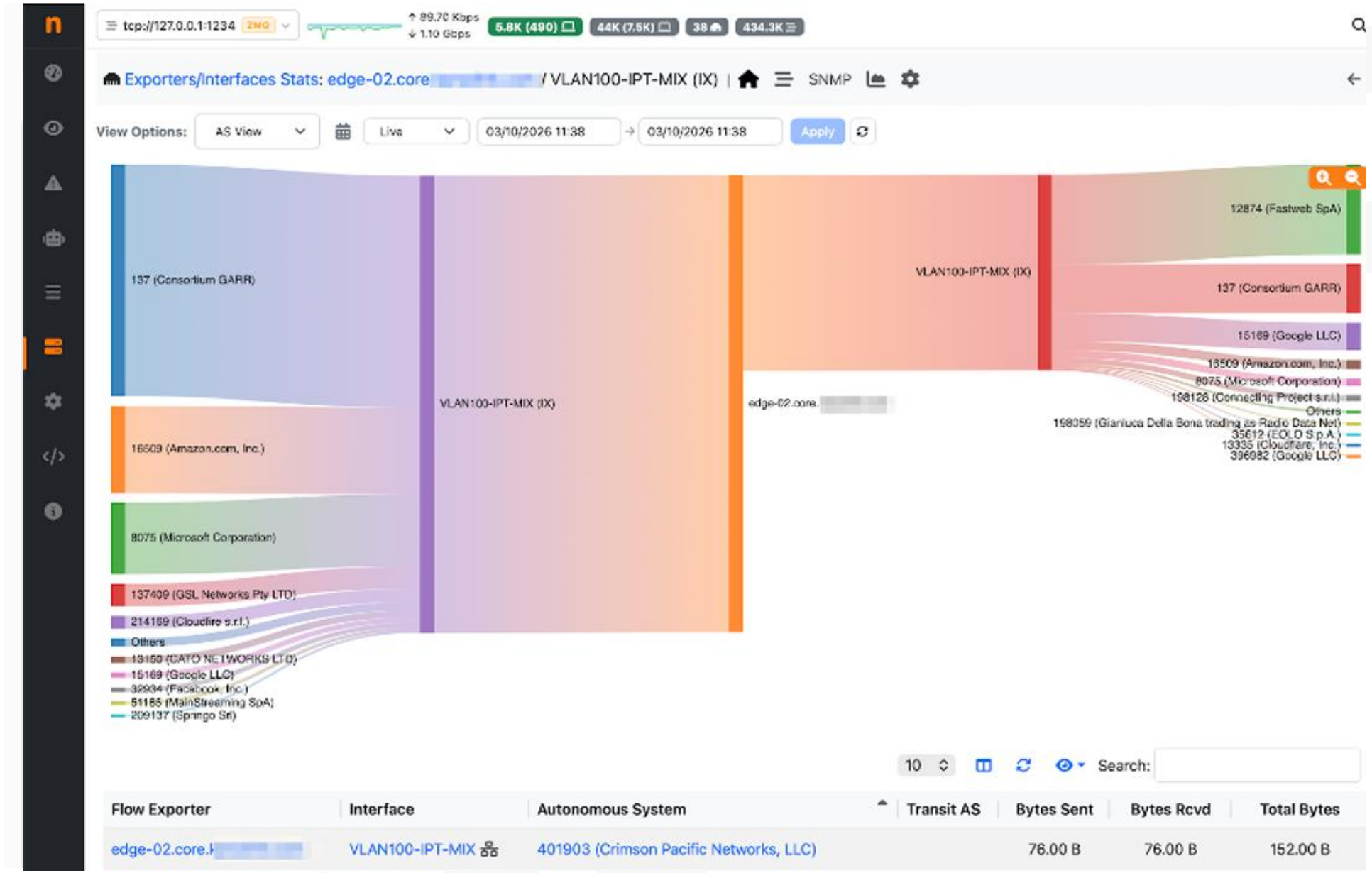
Collection on the edge node: a WAN outage degrades reporting, not collection; scale by adding nodes.

Inventory, not just counters: MAC vendor, a new device on a port is a security event.

The budget question on its own: utilization and capacity trends, without flow data.

UNDER THE HOOD ntopng 7.0 (Sept 2026) on ClickHouse · nDPI · IMEdge: distributed SNMP edge nodes, open source - both coming to NetEye

One platform, both directions: the load question and the cause question answered on the same asset.


tcp://127.0.0.1:1234
89.70 Kbps
1.10 Gbps
5.8K (490)
44K (7.5K)
38
434.3K
Exporters/Interfaces Stats: edge-02.core / VLAN100-IPT-MIX (IX)
SNMP
View Options:
AS View
Live
03/10/2026 11:38
03/10/2026 11:38
Apply
137 (Consortium GARR)
16509 (Amazon.com, Inc.)
8075 (Microsoft Corporation)
137409 (GSL Networks Pty LTD)
214189 (Cloudfire s.r.l.)
Others
13150 (CATO NETWORKS LTD)
15169 (Google LLC)
32934 (Facebook, Inc.)
51185 (MainStreaming SpA)
209137 (Sprango Srl)
VLAN100-IPT-MIX (IX)
edge-02.core
VLAN100-IPT-MIX (IX)
12874 (Fastweb SpA)
137 (Consortium GARR)
15169 (Google LLC)
16509 (Amazon.com, Inc.)
8075 (Microsoft Corporation)
198128 (Connecting Project s.r.l.)
Others
198059 (Gianluca Della Bona trading as Radio Data Net)
35612 (EOLO S.p.A.)
13335 (Cloudflare, Inc.)
396982 (Google LLC)
10
Search:
Flow Exporter
Interface
Autonomous System
Transit AS
Bytes Sent
Bytes Rcvd
Total Bytes
edge-02.core.
VLAN100-IPT-MIX
401903 (Crimson Pacific Networks, LLC)
76.00 B
76.00 B
152.00 B

FROM SIEM TO XDR.

AND COMPLIANCE AS A TARGET BY PLATFORM.

NETEYE	ELASTIC	WHAT ARRIVED IN SECURITY
4.44	9.0	**Attack Discovery GA** - AI-driven security analytics · rule migration from legacy SIEMs
4.45	9.2	**Device Control** - storage-device enforcement on the endpoint
4.47	9.3	**Threat Hunting Agent** · Entity AI Summary GA · Memory Dump response action
4.48	9.4	**Workflows GA** - native SOAR · **Entity Analytics GA** · SIEM Readiness · endpoint forensics
4.50	9.5	**AlertZero** · AI-driven alert triage · agentic SOAR · **human-in-the-loop approvals**

DETECT

Rules, Attack Discovery and the Threat Hunting Agent correlating alerts and entity risk - across domains.

RESPOND

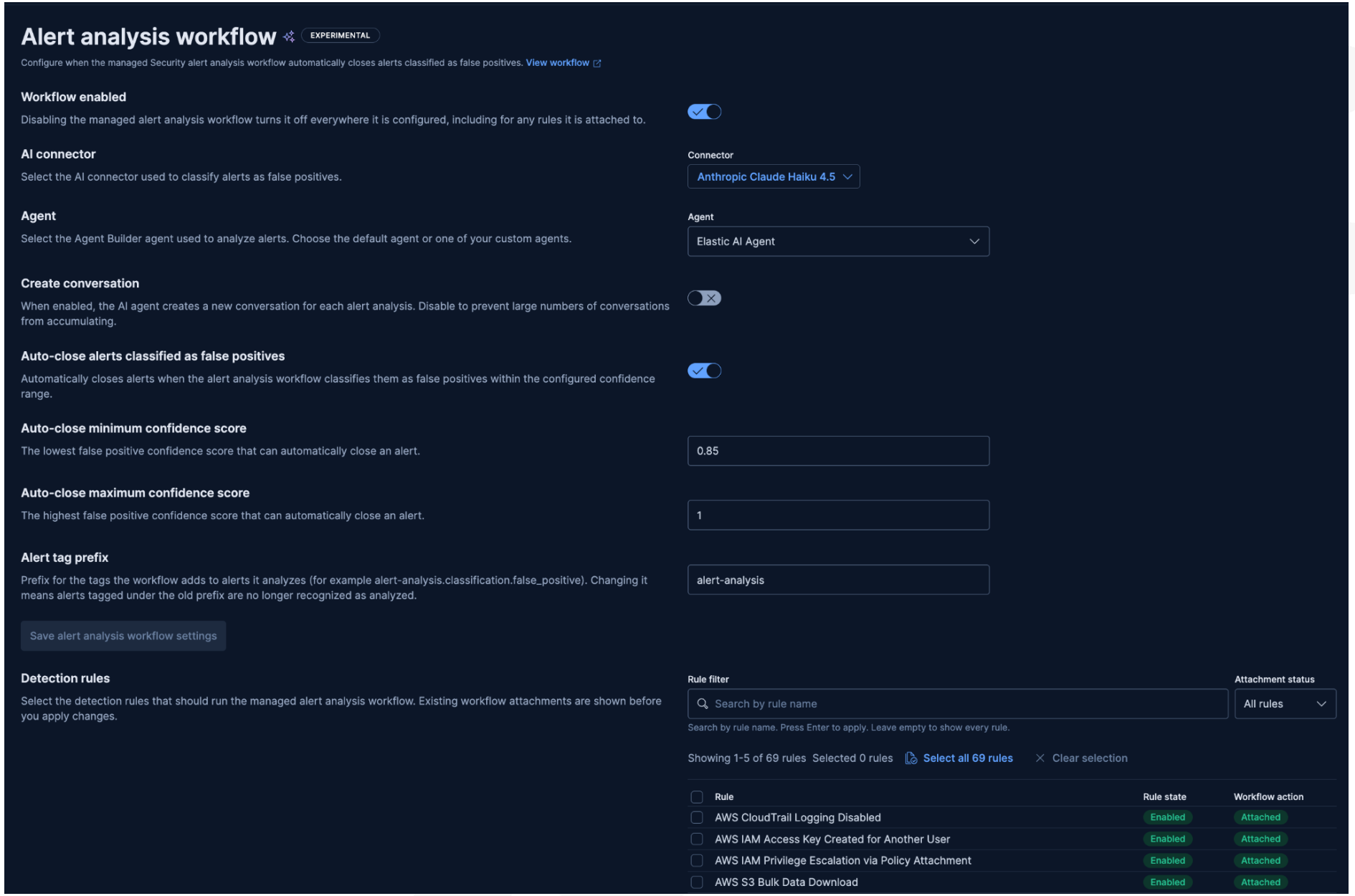
Endpoint response, Workflows and agentic SOAR - with human approval gates and an audit trail for every action.

EVIDENCE BY DESIGN

Asset inventory (GLPI), detection and response records (SIEM/XDR) and documented external exposure (ESAM) sit in the platform that already collects them. NIS2-, DORA- and CRA-relevant visibility comes out as a report, not a project.

UNDER THE HOOD Elastic Security 9.5 in NetEye 4.50 · Enterprise is the default licence for new installations since 4.48

Compliance is a target provided by a data integrated platform


Alert analysis workflow
EXPERIMENTAL
Configure when the managed Security alert analysis workflow automatically closes alerts classified as false positives. View workflow
Workflow enabled
Disabling the managed alert analysis workflow turns it off everywhere it is configured, including for any rules it is attached to.
AI connector
Select the AI connector used to classify alerts as false positives.
Connector
Anthropic Claude Haiku 4.5
Agent
Select the Agent Builder agent used to analyze alerts. Choose the default agent or one of your custom agents.
Agent
Elastic AI Agent
Create conversation
When enabled, the AI agent creates a new conversation for each alert analysis. Disable to prevent large numbers of conversations from accumulating.
Auto-close alerts classified as false positives
Automatically closes alerts when the alert analysis workflow classifies them as false positives within the configured confidence range.
Auto-close minimum confidence score
The lowest false positive confidence score that can automatically close an alert.
0.85
Auto-close maximum confidence score
The highest false positive confidence score that can automatically close an alert.
1
Alert tag prefix
Prefix for the tags the workflow adds to alerts it analyzes (for example alert-analysis.classification.false_positive). Changing it means alerts tagged under the old prefix are no longer recognized as analyzed.
alert-analysis
Save alert analysis workflow settings
Detection rules
Select the detection rules that should run the managed alert analysis workflow. Existing workflow attachments are shown before you apply changes.
Rule filter
Search by rule name
Attachment status
All rules
Search by rule name. Press Enter to apply. Leave empty to show every rule.
Showing 1-5 of 69 rules Selected 0 rules
Select all 69 rules
Clear selection
Rule
Rule state
Workflow action
AWS CloudTrail Logging Disabled
Enabled
Attached
AWS IAM Access Key Created for Another User
Enabled
Attached
AWS IAM Privilege Escalation via Policy Attachment
Enabled
Attached
AWS S3 Bulk Data Download
Enabled
Attached

SAME HOUR. FOUR SIGNALS. ONE ASSET.

LINKED DATA IS THE BRIDGE.

OUTSIDE 08:57
credentials on a dark-web market

MONITORING 09:02
CPU at 100 %, latency x3

NETWORK 09:03
flows from an unknown ASN

SECURITY 09:04
privileged login, unusual source

vpn-gw-01 — the same asset, the same owner, the same hour

LINKED TODAY

Monitoring, observability and security meet on service and entity.

tenant · trace.id · service.name · Elastic entity resolution

NEXT

Network, asset, cost and outside-in view join on the same key.

IP / MAC / switch port → GLPI asset & owner → cost (OpenCost) → external exposure

Correlation makes it right. Linked data gives AI the context to make it fast.

ESAM IS A BEST PRACTICE.

PIRS SET THE FOCUS. SATAYO ON NETEYE.CLOUD MAKES IT A DAILY ROUTINE.

1 PLAN · PIR
decision questions agreed with your stakeholders

→

2 DISCOVER
your external exposure — continuously, OSINT only

→

3 ALERT
exposed services, leaked credentials, dark-web findings

→

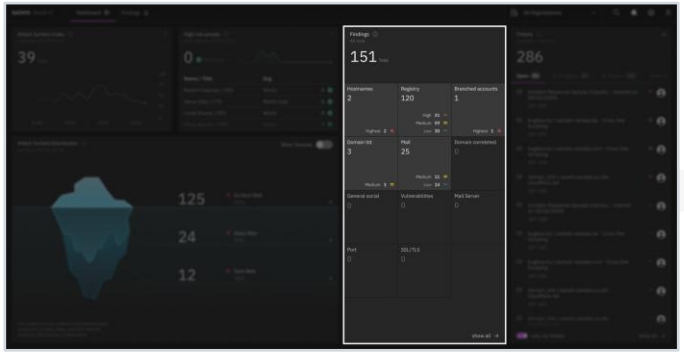
4 VERIFY
confirmed by Würth IT CTI analysts - included in the subscription

→

5 TICKET
a verified finding becomes a ticket - the owner acts

↺ **FEEDBACK** every ticket tests the PIR — relevant, timely, acted on? The next cycle gets sharper.

With NetEye.Cloud, every external finding knows its internal owner — linked to the GLPI asset.



SATAYO on NetEye.Cloud — demo tenant

ATTACK SURFACE INDEX — one tracked number with a trend — exposure becomes a metric, a reduction becomes provable.

SURFACE · DEEP · DARK — most exposure is public; the part that hurts is not indexed at all. Both are watched continuously.

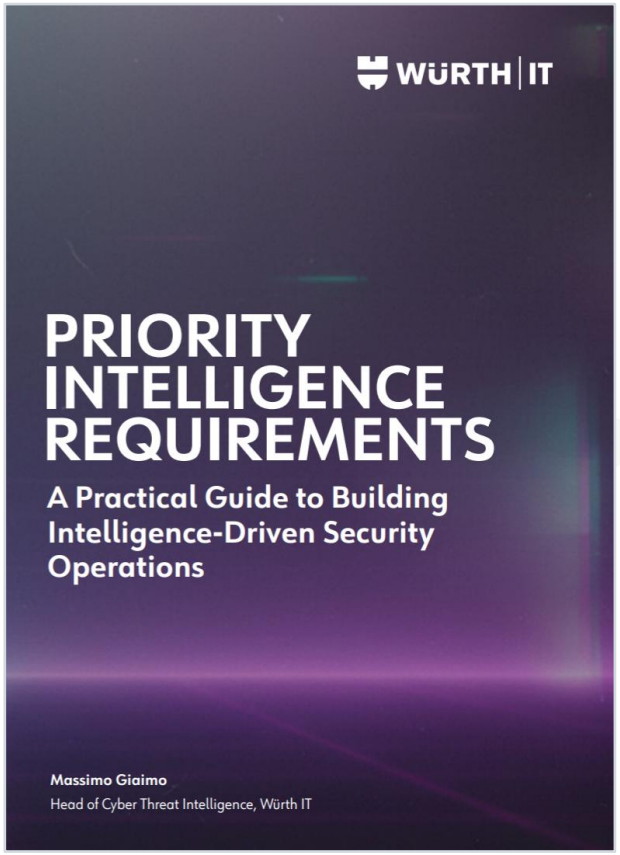
FINDINGS, PRIORITISED BY YOUR PIRS — domains, mail, ports, TLS, breached accounts, VIP people — graded by severity and EPSS.

UNDER THE HOOD PIR-driven CTI · ESAM with SATAYO on NetEye.Cloud · CTI analysis included · asset mapping to GLPI 11

GLPI tells you what you own. SATAYO tells you what the internet can see - and what is already being traded.

THE METHOD BEHIND IT.

PRIORITY INTELLIGENCE REQUIREMENTS - THE FIELD MANUAL BY WÜRTH IT.



More data is not the same as more intelligence.

A PIR is not a watchlist. It is a decision question: what must we know to make the next good decision?

01 REFRAME
turn collection into purposeful questions

02 FOCUS
prioritise what maps to your assets, risks and stakeholders

03 PROVE VALUE
review relevance, timeliness and outcomes — then tune

PLAN | COLLECT | PROCESS | ANALYZE | DISSEMINATE | FEEDBACK ↺

PIRs sit at planning - and steer every stage after it.

17 chapters plus case studies & templates — from threat model and stakeholders to SOC integration, metrics, a 12-week roadmap, AI and the SATAYO community.

For CTI analysts, SOC managers and security leaders

Make your intelligence matter: start with the question, not the feed.

NetEye Conference DACH 2026

CONTEXT FOR AGENTIC AI.

BEFORE IT HAPPENS.

TARGET vpn-gw-01 - asked as one question

ASSET	business-critical gateway, owner: network team
OUTSIDE	credentials offered on a dark-web market - analyst-verified
INSIDE	privileged login + flows from an unknown ASN - same source
LOAD	the CPU peak is the attack, not a capacity problem

PROPOSED ACTION

Rotate the credentials, block the source, open a ticket for the owner - waiting for human approval, with an audit trail.

SHIPPED BUILDING BLOCKS

- 4.44 Attack Discovery GA
- 4.47 Agent Builder GA · Threat Hunting Agent
- 4.48 agent skills · Workflows GA · agentic Kubernetes root cause analysis
- 4.50 AlertZero · AI triage · human-in-the-loop approvals

COMING TO NETEYE

- ntopng 7 nAnalyst - ask the network
- OpenCost MCP server - cost as context

Agentic operations & SOC

Outside-in security

Cloud-native platform

UNDER THE HOOD Elastic Agent Builder & Workflows inside NetEye · every agent action approved and audited

The building blocks shipped. Linked data turns them into answers - before it happens.

ONE PLATFORM. INSIDE AND OUT.

BEFORE IT HAPPENS.

1

FOUNDATION

The journey to Kubernetes has begun — secure, reliable, heading for zero downtime. Self-managed or fully managed on NetEye.Cloud.

→

2

LINKED DATA

Icinga DB, OpenTelemetry, the network, SIEM/XDR, GLPI, SATAYO — and soon cost with OpenCost — joined on shared keys.

→

3

CONTEXT FOR AI

Agentic analysis on correlated data, with a human in the loop — so you act before the incident becomes an outage.

UNDER THE HOOD NetEye 4.50 · RKE2 · NetEye.Cloud on AWS EKS · Elastic 9.5 · GLPI 11 · SATAYO · coming: ntopng 7, IMEdge, OpenCost

One platform. Inside and out. Before it happens.

NetEye

