



ONE PLATFORM. ONE CONTEXT.

AI & Human Insight: the strategic coexistence for IT Operations

Georg Kostner

22 Ottobre 2026, Crowne Plaza Verona Fiera



SAME HOUR. FOUR SIGNALS.

ONE INCIDENT – FOUR PARTIAL VIEWS

OUTSIDE

08:57

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

MONITORING

09:02

vpn-gw-01: SNMP shows an outbound traffic surge - latency rises.

NETWORK

09:03

Large flows from the gateway to an ASN never seen before.

SECURITY

09:04

A privileged login from an unusual source.

Just load – or data leaving? • Whose asset is it? • What happens next?

FOUR TOOLS, FOUR TEAMS, FOUR PARTIAL VIEWS. The answer exists - spread across systems that do not share a key.

You are not lacking data. **You are lacking context.**

SIX CHALLENGES. ONE PATTERN.

THE ANSWER IS NEVER ANOTHER TOOL

01

Tool sprawl & data silos

One platform, one data layer

02

Cloud-native complexity

OpenTelemetry · Kubernetes · root cause

03

NIS2 · DORA · CRA

Evidence by design

04

A growing attack surface

SATAYO: the outside-in view - asset join in progress

05

Cloud & Kubernetes cost

FinOps with OpenCost - planned

06

AI on both sides

Agentic AI - human in the loop by default

Every one of them is answered **by context.**

MEET NETEYE.

FIVE MODULES · ONE DATA LAYER · ONE PLATFORM

CONTEXT FOR AI · AI & HUMAN INSIGHT

MONITORING

Infrastructure · Network status
Icinga 2 · Icinga DB · SLM

IT OPS · AIOPS

Network · storage · server
DB · apps · RUM · Alyvix
ML flags degradation → alert

OBSERVABILITY

Metrics · traces · logs
bottlenecks in code · queries
and between microservices

SECURITY

SIEM · XDR
SATAYO · Deep & Dark Web

ASSETS & ITSM

GLPI 11 · IT Service Mgmt
NIS2-relevant visibility

NETWORK – status · performance

INTEGRATED DATA LAYER

PostgreSQL · MySQL · MariaDB · ClickHouse (time series, NetFlow) · Elastic - shared keys: tenant · service.name · trace.id · entity · asset

PLATFORM

Kubernetes (RKE2) self-managed · NetEye.Cloud fully managed (AWS EKS) · vision: every service a microservice

BUILT WITH OUR TECHNOLOGY PARTNERS



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

INNOVATION WITH EVERY RELEASE.

NETEYE 4.45 – 4.50 · DECEMBER 2025 – OCTOBER 2026 · EVERY MODULE AND ITS VALUE FOR YOU

- AI capability

	4.45	4.46	4.47	4.48	4.49	4.50
MONITORING scales further · SLA to the ms	Icinga DB Web default UI		6 modules + history on Icinga DB	IDO decommissioned		Icinga 2.16 · metrics via OTLP
IT OPS · AIOPS the user experience in view				Alyvix Live Preview		Alyvix Core 3.8
OBSERVABILITY vendor-neutral OpenTelemetry	ECS-compliant data streams			PromQL for metrics	OTel Collector · tenant-aware	OTLP replaces legacy writer
SECURITY · AI alerts become attacks	• Elastic 9.2 · Agent Builder preview		• 9.3 · Workflows · Agent Builder GA	9.4 · Workflows GA · Enterprise default		• 9.5 · AI alert triage
ASSETS & ITSM one inventory · one login				OCS Inventory retired	GLPI 10 → 11	SSO via Keycloak
PLATFORM no big-bang upgrades		Backup & restore (S3)	No standby during updates	Clusters on AWS	Kubernetes (RKE2) begins	IN PROGRESS NetEye Operator

Every release moves the modules forward - **no big upgrade project needed.**

THE FOUNDATION IS MOVING.

THE TRANSFORMATION TO KUBERNETES AND CLOUD NATIVE HAS JUST BEGUN. **ROADMAP 2027**

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

LIVE

No standby during updates

4.47

Clusters on AWS · backup & restore

4.46 – 4.48

Kubernetes foundation (RKE2)

4.49 · OTel Collector, then Keycloak

IN PROGRESS

Services move to Kubernetes

release by release

NetEye Operator

coming for every service · tested on every PR

... until all services run on it

blueprint: SATAYO2 microservices

PLANNED

Zero-downtime upgrades

target: end of 2027

NetEye.Cloud Shared

from 2027 · SMB · tenants via RBAC

NetEye.Cloud Dedicated SaaS

from 2027 · own namespace per tenant

Self-managed or fully managed. **The same NetEye.**

ONE LOOP FOR EVERY TEAM.

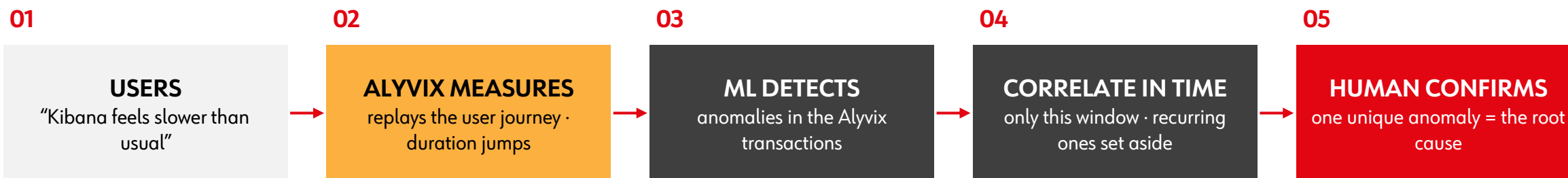
AI & HUMAN IN THE LOOP - THE SAME PRINCIPLE FOR SOC, NOC & SRE, DEVOPS & APP TEAMS

	01 DETECT	02 INVESTIGATE	03 RESPOND	04 PROVE
SOC security analysts	SIEM · XDR network risk flags · SATAYO	AI alert triage (4.50) Agent Builder GA (4.47)	Workflows GA (4.48) native SOAR	NIS2 · DORA · CRA evidence by design
NOC · SRE system · network · storage	Icinga · SNMP · ntopng AIOps: ML flags degradation	correlate on asset and service · GLPI	Tornado · Workflows automation · ticket	SLA reports Service Level Management
DEVOPS · APP TEAMS dev · application mgmt	traces · logs · metrics OpenTelemetry · APM	root-cause investigation code · queries · services · 2027	Workflows the owner gets the case	root-cause report severity vs. SLO
AI WITH CONTEXT	correlates every signal	trriages and enriches	runs the playbook	records every step
HUMAN IN THE LOOP	decides what matters	judges the case	approves the action	stays accountable
HUMAN INSIGHT TEACHES	feedback on detections	runbooks · past incidents	playbooks · release	postmortems · lessons learned

Coexistence: AI brings ever more context - **how far and how deep stays a human call.**

PROOF: FROM "SLOWER" TO ROOT CAUSE.

A REAL CASE FROM OUR OWN NETEYE ENVIRONMENT · ALYVIX + ELASTIC ML



WHAT THE MACHINE DID

measured · detected anomalies · lined them up in time

WHAT PEOPLE DID

set up the ML jobs · judged the correlations · named the cause

"This synergy between automated analysis and human insight can significantly reduce the root cause investigation time."

NetEye Blog, December 2025

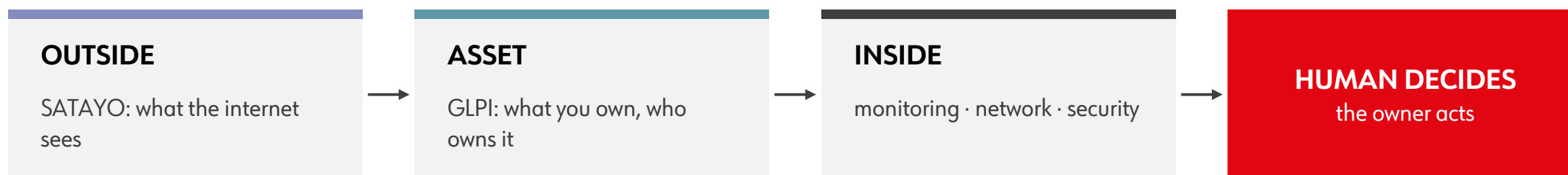
LIVE

Alyvix in IT Ops · AIOps · Elastic ML anomaly detection - in NetEye today

The machine narrows the search - **human insight names the cause.**

ASSET MANAGEMENT NAMES THE OWNER.

THE JOIN BETWEEN OUTSIDE AND INSIDE



Monitoring says something is wrong. The inventory says what it is, who looks after it and what it is worth.

LIVE

GLPI 11 (4.49) · Keycloak SSO & CloudInventory (4.50) · OCS Inventory retired (4.48)

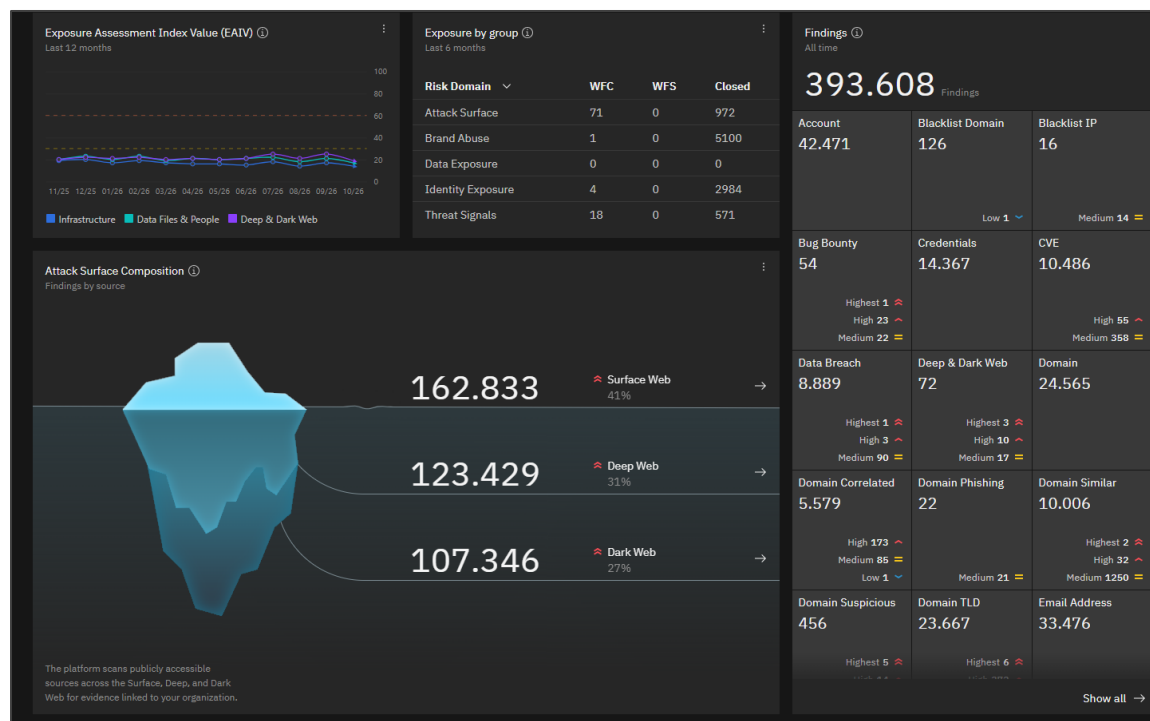
IN PROGRESS

SATAYO ↔ GLPI first, visible to analysts in both modules · then the network context on the same asset

Asset context tells AI whose system it is. **The owner decides.**

SATAYO2 – COMING TO NETEYE.CLOUD.

THE NEW GENERATION OF SATAYO – THE BLUEPRINT FOR ALL OF NETEYE



SATAYO2 dashboard – demo data

MACHINE-SCALE OSINT, HUMAN-VERIFIED: EASM · Impersonation · Deep & Dark Web - EPSS-prioritised, verified by CTI analysts, a ticket not a feed

SATAYO2 shows the way - **every NetEye service a microservice on Kubernetes.**

THE BLUEPRINT: CLOUD-NATIVE FROM THE GROUND UP

UX

one consistent UX - every view through the REST API

REST API

OpenAPI / Swagger - the whole architecture

SATAYO2 SDK

generated from OpenAPI

MICROSERVICES ON AWS EKS

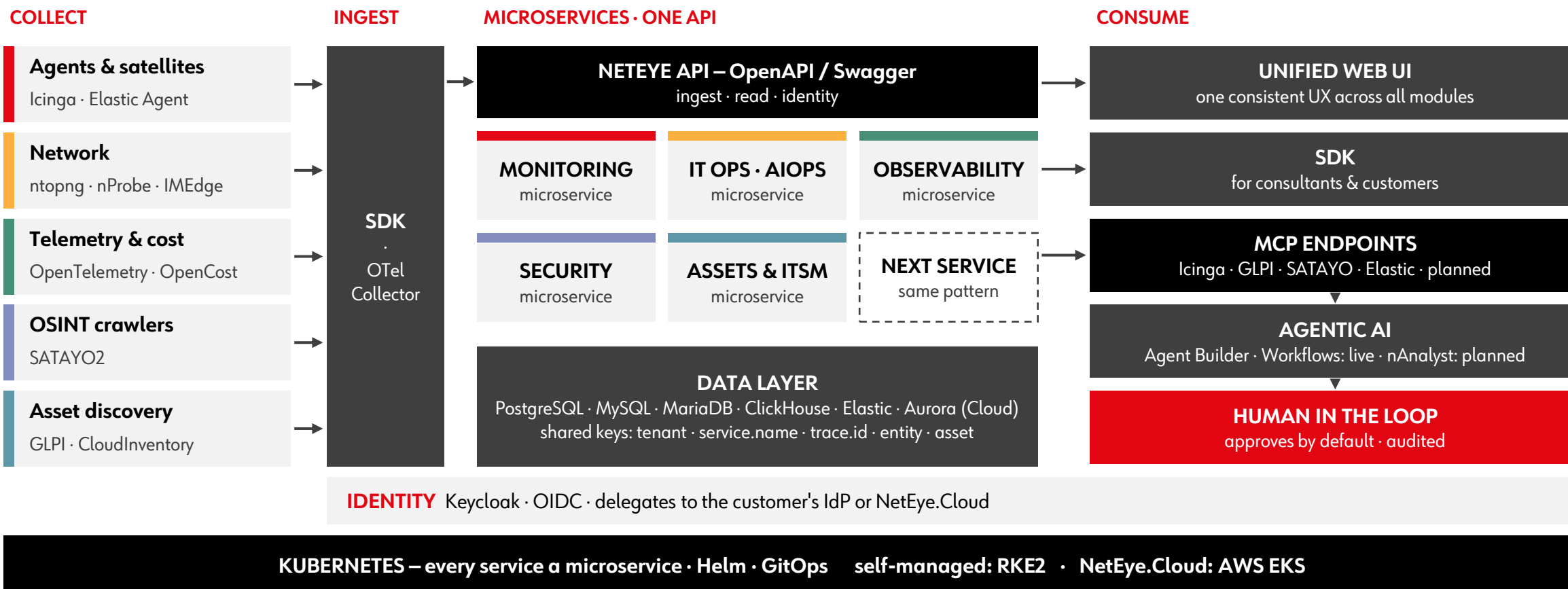
Rust API · Keycloak SSO · OpenTelemetry

DATABASE

AWS Aurora MySQL Serverless

THE NETEYE TARGET ARCHITECTURE.

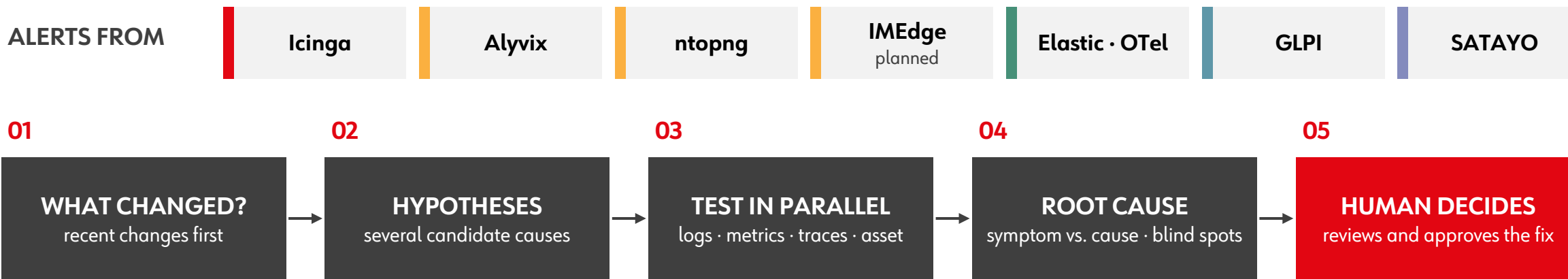
VISION · BUILT LIKE SATAYO2 · SELF-MANAGED OR SAAS



One pattern for every service - **and every service is context for AI.**

FROM ALERT TO ROOT CAUSE.

OBSERVABILITY · WORKFLOW + AGENT · VISION 2027 · CLOUD OR ON-PREM



WORKFLOW known failure modes - deterministic queries, AI only classifies and summarises

AGENT open incidents - test and refute hypotheses, cite every claim, name the blind spots

LIVE

Building blocks in NetEye: Agent Builder GA (4.47) · Workflows GA (4.48)

VISION

2027: root-cause workflows and agents across all NetEye sources · Elastic AI SRE: private preview

Correlation is not causation - **every conclusion shows its evidence.**

WHAT DOES IT COST?

FINOPS BECOMES PART OF OBSERVABILITY – COMING TO NETEYE



WHO PAYS FOR WHAT

Showback and chargeback per namespace, service and tenant

COST NEXT TO PERFORMANCE

service.name links cost to latency, errors and SLA

CONTEXT FOR AI

“Is this peak worth scaling for?” - the human decides

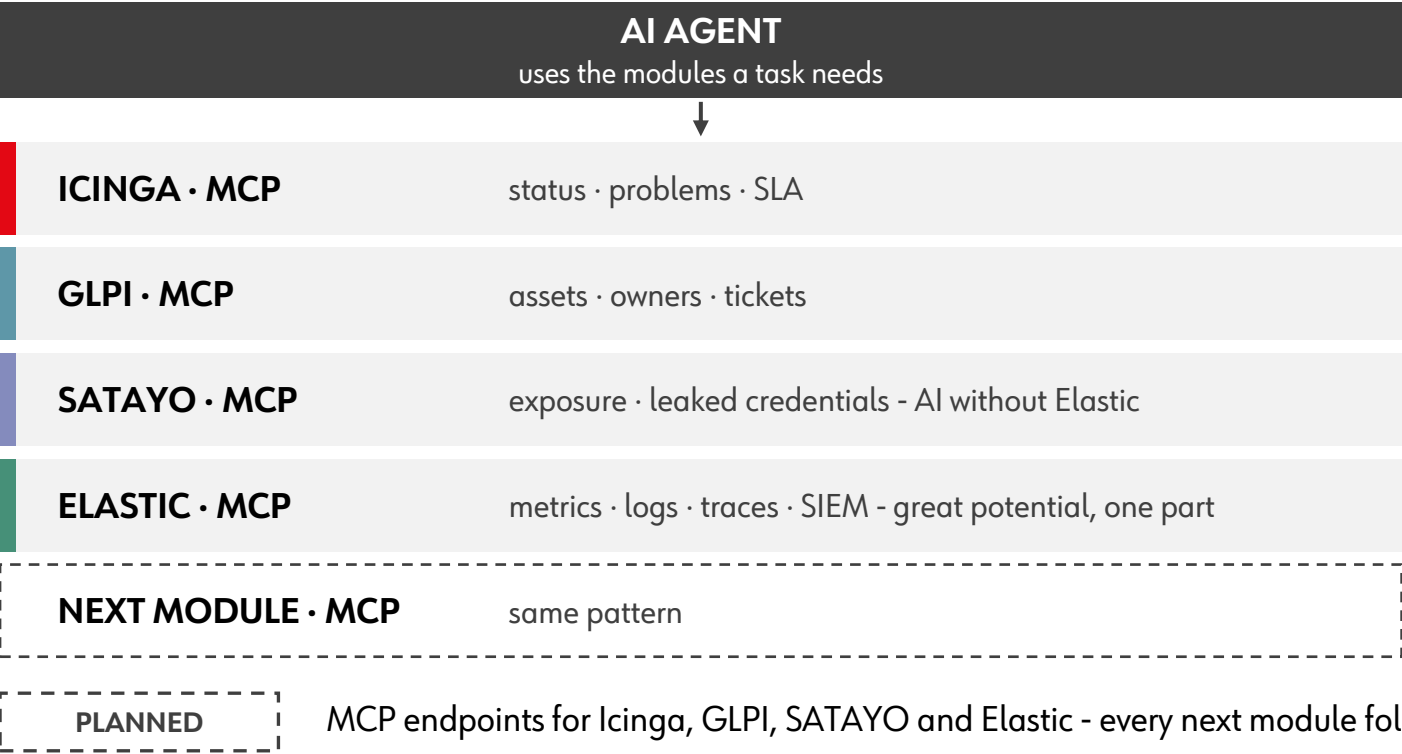
PLANNED

Coming to NetEye: OpenCost - open source, CNCF incubating

Observability asks “is it healthy?” - **FinOps adds “is it worth it?”**

EVERY MODULE SPEAKS TO AI.

ONE MCP ENDPOINT PER MODULE · ELASTIC IS ONE OF THEM · SECURED BY DESIGN



SECURED BY DESIGN

- AI WORKS INSIDE THE TENANT**
the AI reads and acts only within the customer's tenant
- ROLES & PERMISSIONS**
the AI sees and does only what the user may
- EVERY ACTION AUDITED**
every query · every step · every approval
- HUMAN IN THE LOOP**
approves by default

Every module speaks to AI - **Elastic is a strong part, not the whole.**

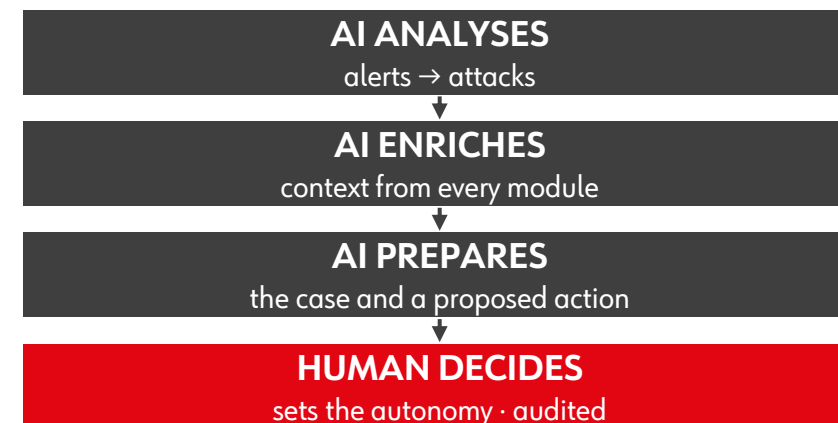
CONTEXT FOR AGENTIC AI.

HUMAN IN THE LOOP BY DEFAULT – AI & HUMAN INSIGHT

vpn-gw-01 – asked as one question

ASSET		business-critical gateway, owner: network team
OUTSIDE	08:57	credentials on a dark-web market - analyst-verified
MONITORING	09:02	outbound surge: likely exfiltration, not load
NETWORK	09:03	flows to an unknown ASN - same case
SECURITY	09:04	privileged login, unusual source - same case

PROPOSED ACTION Block the outbound transfer, rotate the credentials, open a ticket for the owner – waiting for human approval.



AUTONOMY – SET BY THE HUMAN

SUGGEST

AI proposes

APPROVE

default

AUTO-RUN

trusted playbook

on the loop only for released playbooks · audited

IN NETEYE TODAY Agent Builder GA (4.47) · Workflows GA (4.48) · AI alert triage (4.50)

AI prepares. **Humans decide.**

WHERE WE ARE HEADING.

EVERY STEP ADDS ONE MORE SOURCE TO THE SAME CONTEXT

COMING TO NETEYE

SATAYO2 on NetEye.Cloud cloud-native blueprint · API-first · SDK	PLANNED
FinOps with OpenCost cost as a signal	PLANNED
nAnalyst · IMEdge network layer · ntopng 7 already in NetEye	PLANNED
ClickHouse replaces InfluxDB InfluxDB still in use today	PLANNED
MCP endpoint per module Icinga · GLPI · SATAYO · Elastic	PLANNED

TOWARDS 2027

NetEye.Cloud Shared & Dedicated SaaS models from 2027	PLANNED
Zero-downtime upgrades target: end of 2027	PLANNED
Outside-in view joined on the asset SATAYO ↔ GLPI first	IN PROGRESS
Root-cause workflows across all sources from 2027 in NetEye projects	VISION

One platform today. One context tomorrow - **for AI and for the people who decide.**

ONE PLATFORM. ONE CONTEXT.

AI & HUMAN INSIGHT – THE STRATEGIC COEXISTENCE

1

WHERE WE COME FROM

Separate tools, partial truths.

2

WHAT WE BUILT

Six releases: innovation in every module, on a renewed foundation.

3

WHERE WE ARE HEADING

Ever more AI with context - how far and how deep stays human.



THANK YOU.

Questions?

