



NetEye Conference 2026

AI & Human Insight: la coesistenza strategica per le IT Operations

Finding the Blind Spots: *analisi delle lacune di monitoraggio con AI, GLPI e NetEye*

Vladimir Mozharov & Alessandro Paoli



Agenda

01

GLPI come il fonte di verità

Inventario, naming e matching con NetEye

02

Lacune di monitoraggio

Asset in GLPI senza check in NetEye

03

Modulo AI Analysis

Suggerimenti di monitoraggio nella host view

04

Demo live

Il modulo in azione su NetEye

Observability

GLPI · NetEye · AI

NIS2

11 Settori ad alta criticità

Allegato I

- **Energia:** elettricità, teleriscaldamento, petrolio, gas, idrogeno
- **Trasporti:** aereo, ferroviario, per vie d'acqua, stradale
- **Banche e infrastrutture dei mercati finanziari**
- **Sanità:** strutture sanitarie, laboratori, produttori di farmaci e dispositivi critici
- **Acqua potabile e acque reflue**
- **Infrastrutture digitali:** IXP, DNS, registri TLD, cloud, data center, CDN, servizi fiduciari, reti e servizi di comunicazione elettronica
- **Gestione dei servizi ICT:** MSP e MSSP
- **Pubblica amministrazione**
- **Spazio**

7 Altri settori critici

Allegato II

- **Servizi postali e di corriere**
- **Gestione dei rifiuti**
- **Sostanze chimiche:** fabbricazione e distribuzione
- **Alimenti:** produzione, trasformazione e distribuzione
- **Manifattura** di dispositivi medici, computer ed elettronica, apparecchiature elettriche, macchinari, autoveicoli e altri mezzi di trasporto
- **Fornitori digitali:** marketplace online, motori di ricerca, social network
- **Ricerca**

Altri settori

Allegato III - IV

- **PA**
- **Trasporto pubblico**
- **Istituti di ricerca e istruzione**
- ...

Fonti: Dir. (UE) 2022/2555 art. 21(2)(i) · D.Lgs. 138/2024 art. 24 · Det. ACN 379907/2025 · Reg. (UE) 2024/2690 sez. 12



NIS2 – Asset management

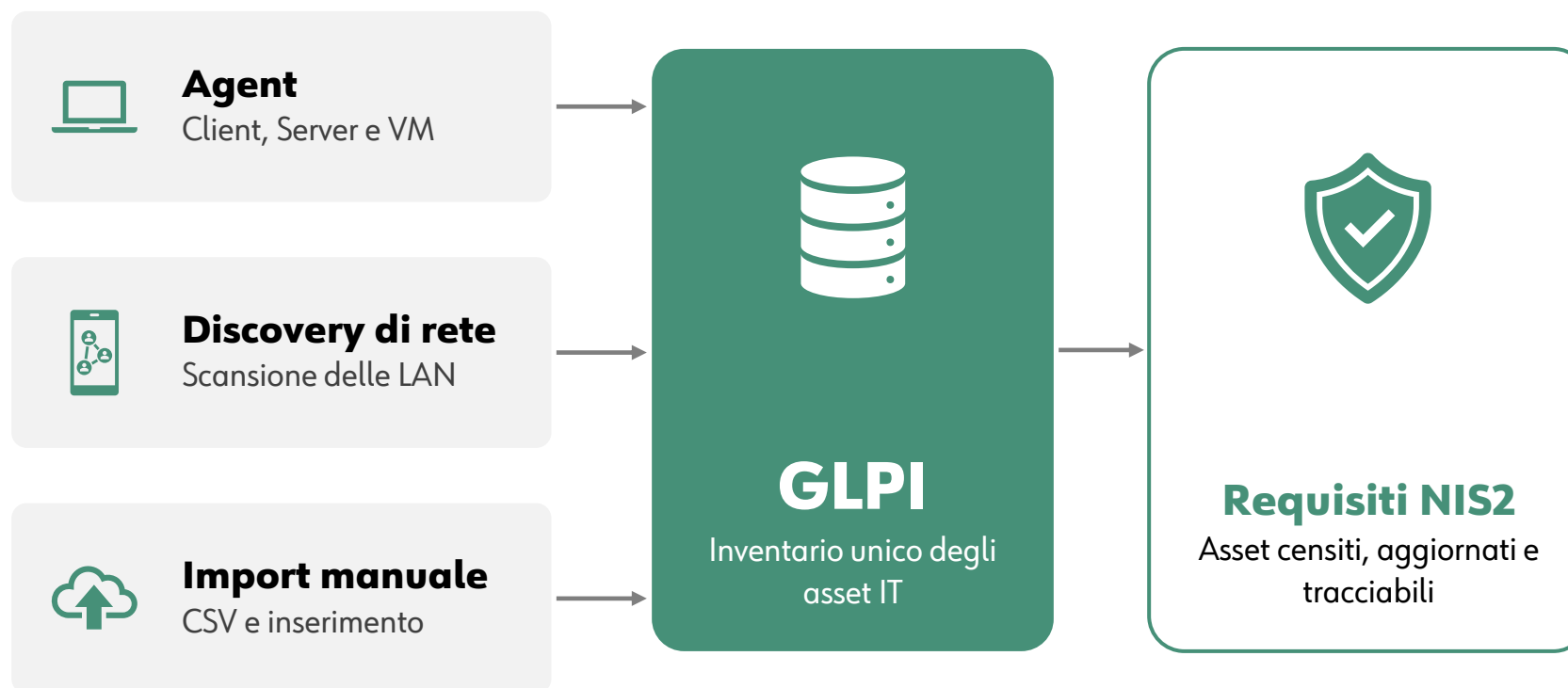
Requisito	Evidenza attesa NIS2	Fonte GLPI
ID.AM-01 Inventario hardware	Apparati con owner, ubicazione, criticità	Computer, apparati di rete, location, responsabile
ID.AM-02 Software e servizi	Software, versioni, servizi e sistemi	Inventario software da agente, licenze
ID.AM-03 Flussi di rete	Schema di rete e flussi autorizzati	Porte, connessioni, rack
ID.AM-04 Servizi dei fornitori	Fornitori e servizi esterni censiti	Fornitori, contratti, SLA
ID.AM-05 Criticità	Asset prioritizzati per impatto sui servizi NIS	Campo criticità, legame asset → servizio
Reg. 2024/2690 - 12.4 Inventario aggiornato	Riconciliazione periodica dichiarato vs reale	Data ultimo inventario per asset

Fonti: Dir. (UE) 2022/2555 art. 21(2)(i) · D.Lgs. 138/2024 art. 24 · Det. ACN 379907/2025 · Reg. (UE) 2024/2690 sez. 12



GLPI come il fonte di verità

GLPI tramite il deploy di agent su client e VM, Discovery network o import manuali copre le richieste di NIS2



Cosa importa GLPI per ogni tipo di asset



Client

Agent GLPI su PC e server

- Hardware: CPU, RAM, dischi, schede di rete
- Sistema operativo e versione
- Utente e data dell'ultimo inventario

Software installato

Ogni pacchetto con la sua versione: base per vulnerabilità, licenze e **monitoraggio**



Network device

Discovery e inventario SNMP

- Modello, firmware e numero di serie
- Porte: stato, velocità, VLAN, MAC
- Indirizzi IP

Porte e LLDP

Ogni porta viene collegata all'asset vicino: GLPI sa chi è connesso dove



Unmanaged asset

LLDP e scansioni SNMP rivelano dispositivi mai censiti: GLPI li importa da classificare



Printer

Discovery e inventario SNMP

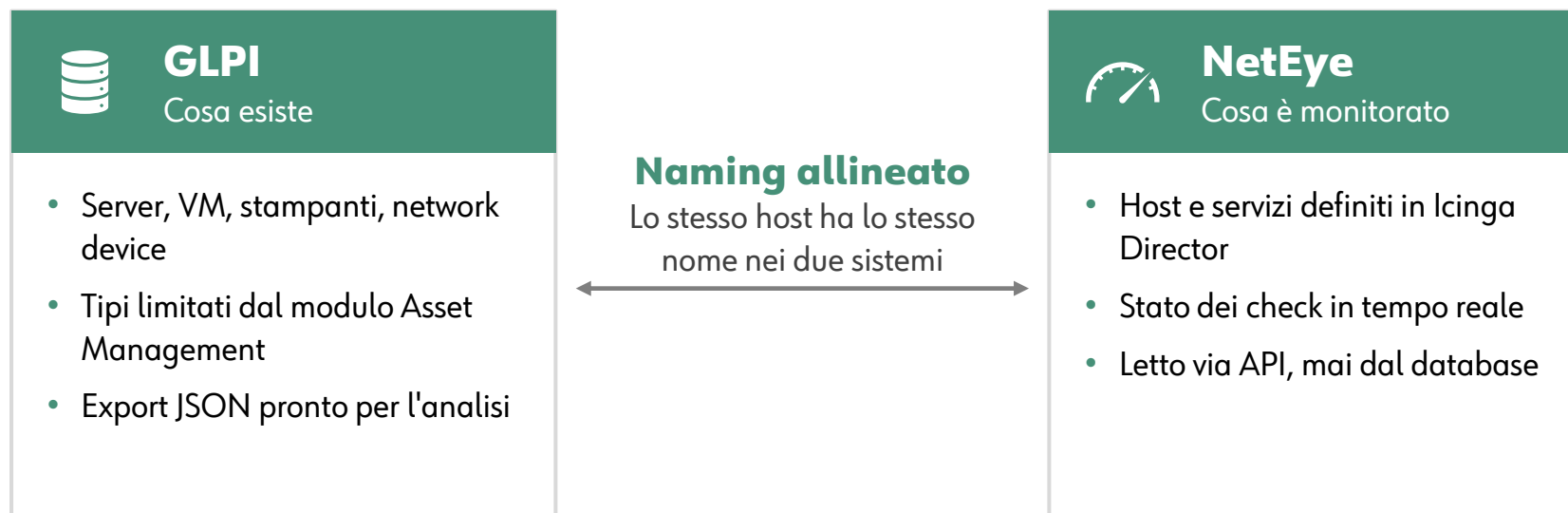
- Modello, numero di serie e IP
- Contatori pagine stampate
- Porta di rete e posizione

Toner e consumabili

Livello di ogni cartuccia: sostituzione pianificata prima del fermo



GLPI e NetEye: due fonti di verità



Si crede a GLPI: ogni asset in GLPI, di cui voglio il monitoring, senza host in NetEye è una lacuna di monitoraggio.



Lacune di monitoraggio

Anche l'host più critico del sistema può avere lacune banali, se nessuno le ha mai riviste a mano.

Monitoriamo l'applicazione A, ma non sappiamo che dipende da un servizio B che nessuno ci ha chiesto di guardare

Esempio: un'applicazione JobScheduler è monitorata.

Quell'applicazione si appoggia a MySQL installato sullo stesso host – ma MySQL non era mai aggiunta a Director.

GLPI come source of truth non serve solo per l'inventario asset in ottica NIS2 – diventa anche il modo per scoprire cosa stiamo monitorando "a metà"



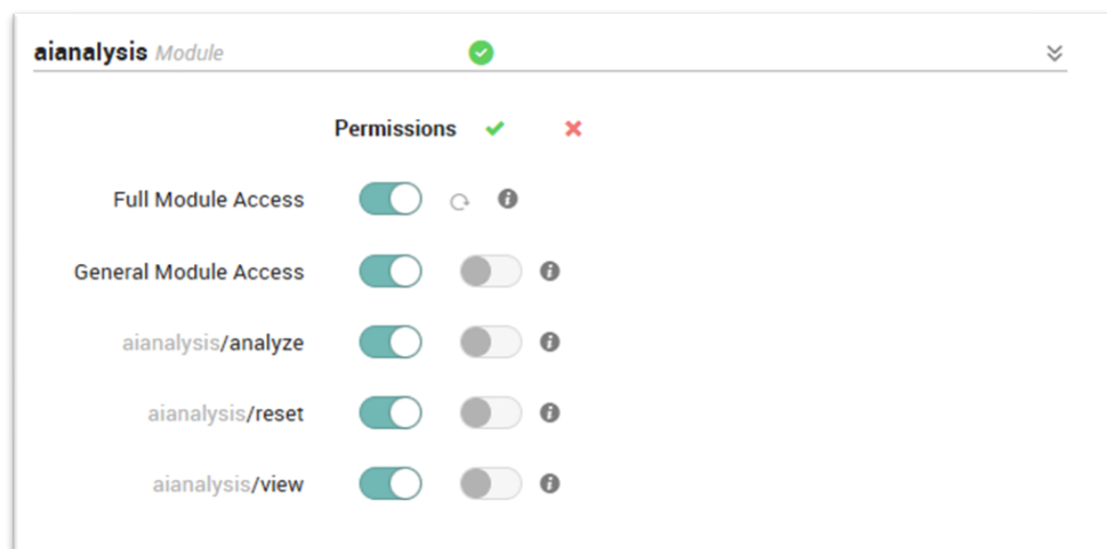
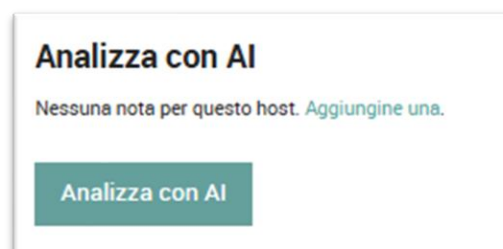
Architettura: dove si inserisce l'AI

GLPI resta source of truth per l'inventario.

NetEye/Icinga resta source of truth per lo stato del monitoraggio.

Un backend Python dedicato fa da ponte: legge entrambe le fonti via API (mai il database, mai file di inventario grezzi che possono essere parziali), incrocia i dati, e orchestra l'analisi.

Il modulo Icinga Web 2 (aianalysis) espone il risultato nella host view, con un pulsante "Analizza con AI"



Come lavora l'AI: regole prima, modello dopo

Tutto ciò che si può decidere con regole deterministiche (noise reduction sul software installato, matching host vs asset, rilevazione di check già esistenti) si fa con regole, non con l'LLM.

L'analisi è divisa in 5 passaggi mirati: sistema/risorse, storage, servizi, rete, e una sintesi finale che deduplica e priorizza: mai più di 10 suggerimenti per host, per restare utile e non diventare rumore.

Ogni suggerimento cita l'evidenza esatta su cui si basa: niente affermazioni senza un dato a supporto.

Regole deterministiche effettivamente implementate:

1. Matching host Icinga ↔ asset GLPI (matching.py) Gerarchia di 7 chiavi in ordine di affidabilità (glpiid+glpiassettype → UUID → serial → IP → MAC → FQDN → hostname breve).
2. Rilevazione discrepanze GLPI↔NetEye (reconcile.py) Sette controlli puramente a regole, zero LLM: glpiassettype_missing, glpiid_type_mismatch, glpiid_dangling, glpiid_deleted, ip_mismatch (con severità calcolata, non fissa), not_monitored, not_in_glpi, ambiguous_match.
3. Classificazione monitor_yes/monitor_no/to_evaluate (classify.py). Se più regole applicabili danno esiti diversi: niente tie-break silenzioso, va a to_evaluate con entrambe le motivazioni.
4. MAC address → vendor (mac_lookup.py) Lookup su database IEEE locale (54mila voci, nessun download a runtime), longest-prefix-match su 24/28/36 bit.
5. Pre-elaborazione dati per l'AI (preprocess.py) Filtro software per pattern monitorabili + esclusione di pattern noti + deduplica dei sotto-pacchetti di uno stesso servizio logico.



Trasparenza e controllo umano

L'AI suggerisce, non applica: nessuna scrittura automatica su Director o GLPI.

Una nota operatore per host permette di correggere in linguaggio naturale casi che i soli dati non possono spiegare (es. "non è possibile aggiungere un check del toner su questa stampante: il firmware non lo espone via SNMP") – l'AI la rispetta con priorità sulle proprie inferenze.

Ogni analisi è completamente ispezionabile: un link mostra, passaggio per passaggio, esattamente cosa è stato mandato al modello e cosa ha risposto: nessuna "scatola nera".

Analizza con AI

Nota per l'IA: non è possibile aggiungere un check del toner su questa stampante: il firmware non lo espone via SNMP – [modifica](#)

+ Risultato (0 suggerimenti)

– Vedi i dati inviati all'IA (5 passaggi)

+ Passaggio: os_resources

+ Passaggio: storage

+ Passaggio: services

+ Passaggio: network

+ Passaggio: synthesis

Ri-analizza

Reset dati analisi per questo host



Esecuzione asincrona e sovranità del dato

L'analisi può richiedere minuti: parte in background, la pagina mostra l'avanzamento in tempo reale e si aggiorna da sola: nessun JavaScript custom, solo meccanismi nativi di Icinga Web 2.

Si può abbandonare la pagina e tornare ad analizzare i risultati più tardi. Finché non viene richiesta una nuova analisi, i risultati persistono

Il modello è pensato per girare in locale (Qwen open-weight, su hardware dedicato): nessun dato del cliente esce verso il cloud per impostazione predefinita: requisito non negoziabile per un'integrazione pensata in ottica NIS2.



Live Demo



Prossimi passi

Dalla demo al prodotto:

- Modello locale in produzione: completare il deployment di Qwen su hardware dedicato, eliminando ogni dipendenza residua da servizi esterni.
- Campo di esclusione esplicito in GLPI: un campo dedicato per dichiarare "questo asset non va monitorato" invece di dedurlo implicitamente: elimina ambiguità alla radice.
- Identificazione automatica degli asset non gestiti: estendere il riconoscimento a dispositivi di rete privi di agent (stampanti, apparati, IoT) tramite fingerprinting di rete, con la stessa logica di cross-check già costruita.
- Allineamento naming: proporre (mai applicare in automatico) una convenzione di naming coerente tra i due sistemi, con GLPI come autorità.
- Valutazione comparativa strutturata: un set di casi reali con output atteso, per misurare oggettivamente modelli e quantizzazioni diverse nel tempo, non solo "a sensazione".





Grazie per l'attenzione!

Domande?

