NetEye

NETEYE CONFERENCE 2025

Intelligent Operations in Action

23 ottobre 2025

NetEye

NETEYE CONFERENCE 2025

Use Case–Driven UI for Threat Intelligence

Marco Berlanda – Pietro Melillo

Introduzione al contesto

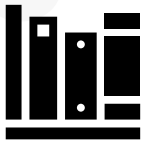
- **Panorama delle minacce complesso:** gli attacchi informatici odierni colpiscono infrastrutture critiche, aziende private e supply chain, con tecniche sempre più sofisticate;
- **Ruolo centrale della CTI:** in questo scenario, la Cyber Threat Intelligence diventa fondamentale per raccogliere dati da fonti eterogenee, interpretarli e trasformarli in azioni difensive concrete;
- **Difesa proattiva:** l'analisi di intelligence consente di agire tempestivamente sulle minacce emergenti, prima che colpiscano l'azienda.

Introduzione al contesto

Deep Dive

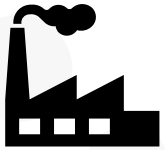
+42% credenziali rubate e **decine di mld** di exploit/anno

+70% aziende colpite da incidenti **supply chain**



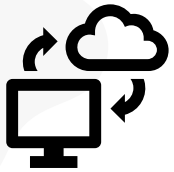
+ 22% settore manifatturiero come target principale

- Bitsight

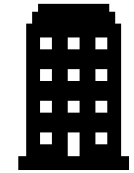


SAP nel mirino (2025): campagne globali su **infrastrutture critiche**

- Onapsis

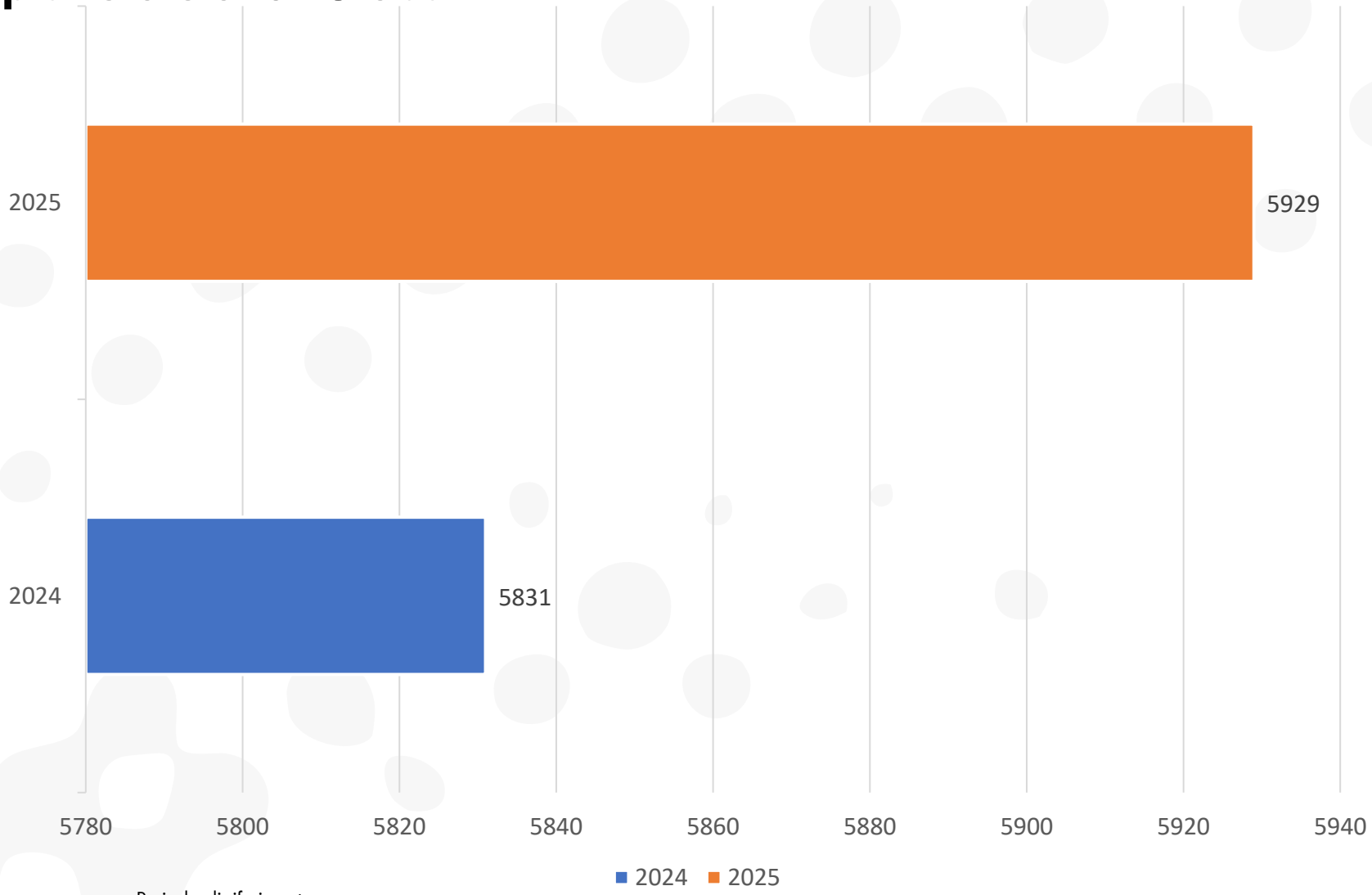


OT/SCADA esposti: exploit **diretti** al cuore delle infrastrutture, **alto impatto** sulla continuità operativa.



Ransomware

Attacchi Doppia Estorsione - Globali



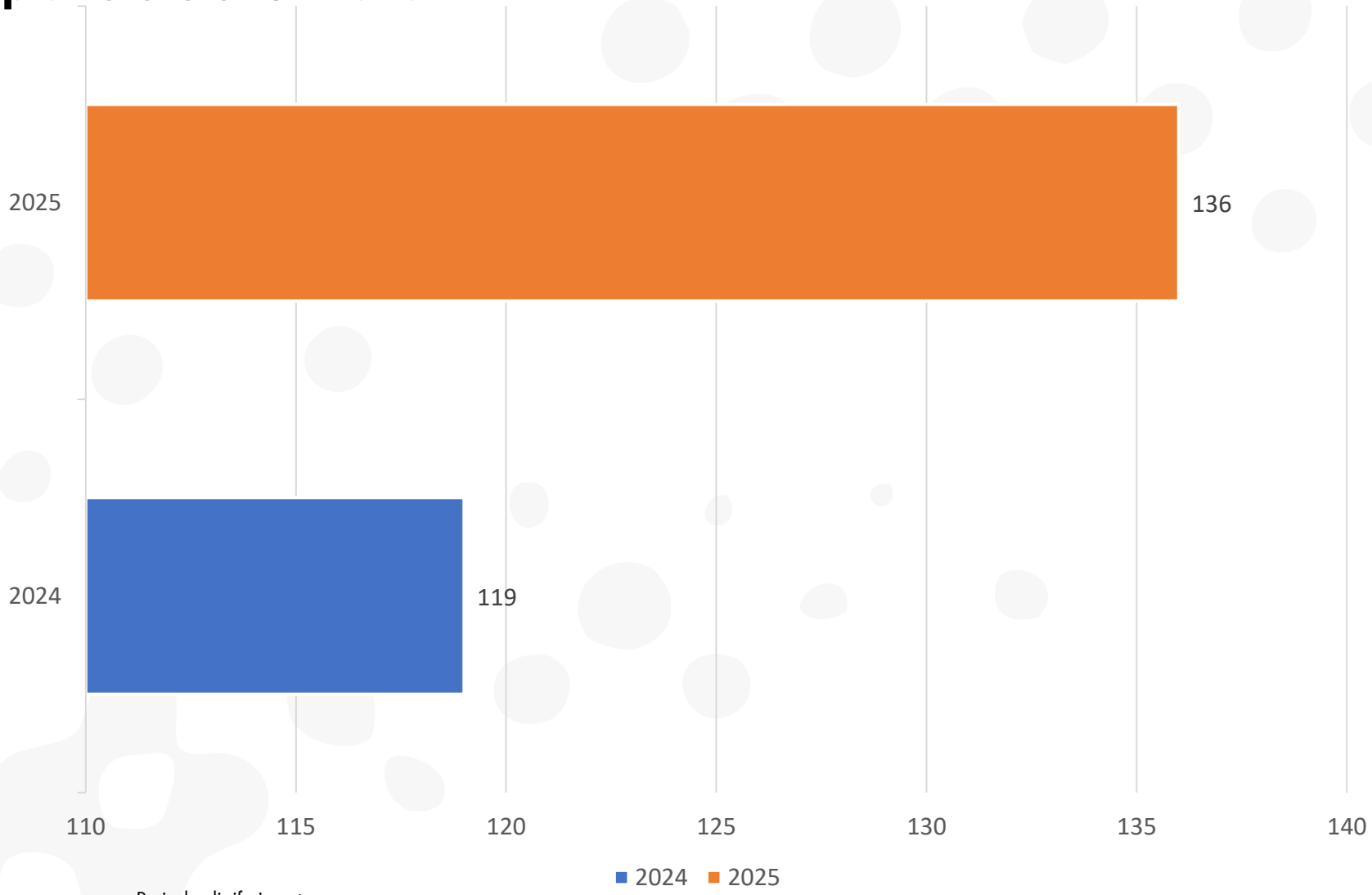
+98

Periodo di riferimento:
Gennaio –Dicembre 24
Gennaio – Ottobre 25

Source: SATAYO, October 2025

Ransomware

Attacchi Doppia Estorsione - Italia



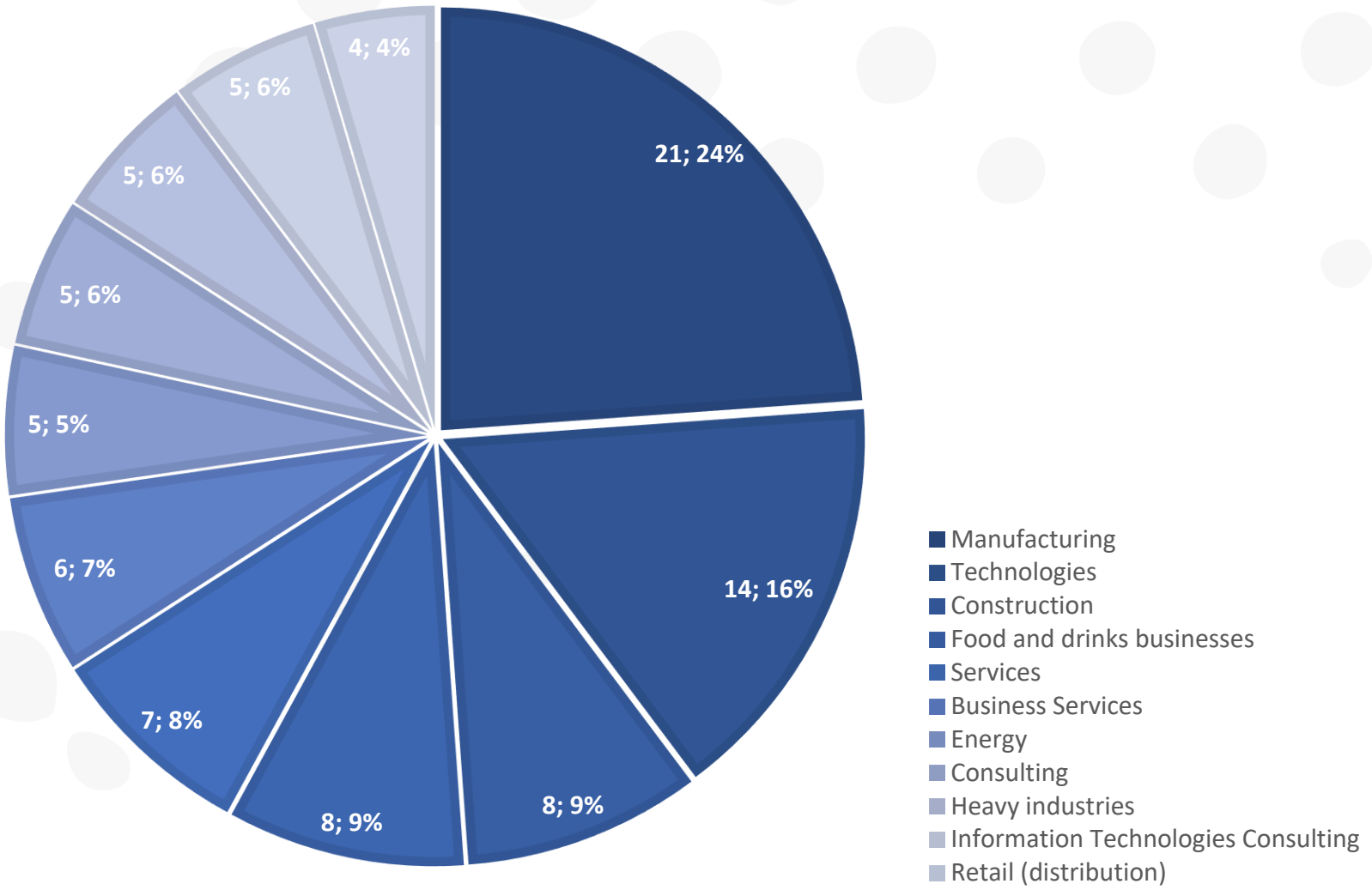
+17

Periodo di riferimento:
Gennaio –Ottobre 24
Gennaio – Ottobre 25

Source: SATAYO, October 2025

Ransomware in Italia

Sectors - Italia



Source: SATAYO, October 2025

NetEye

Cyber Threat Intelligence

Introduzione

La **Cyber Threat Intelligence (CTI)** è il processo di raccolta, analisi e condivisione di informazioni relative a minacce informatiche attuali o potenziali, con l'obiettivo di **trasformare dati grezzi in conoscenza azionabile**.

Cyber Threat Intelligence

Introduzione

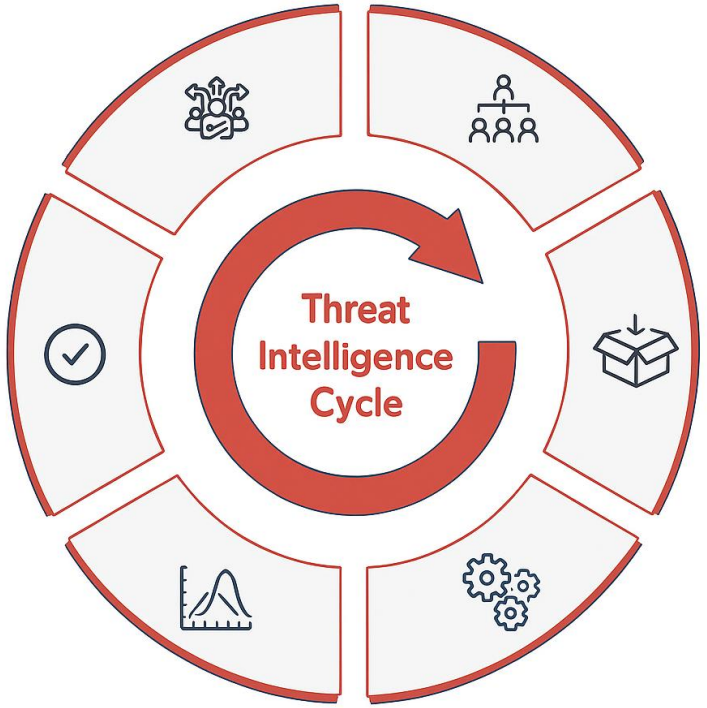
La CTI consente alle organizzazioni di:

- **comprendere** attori e tecniche di attacco (TTPs);
- **anticipare** le minacce emergenti;
- **supportare** decisioni strategiche, tattiche e operative in materia di sicurezza;
- **rafforzare** la resilienza e la conformità normativa (e.g NIS2).

Cyber Threat Intelligence

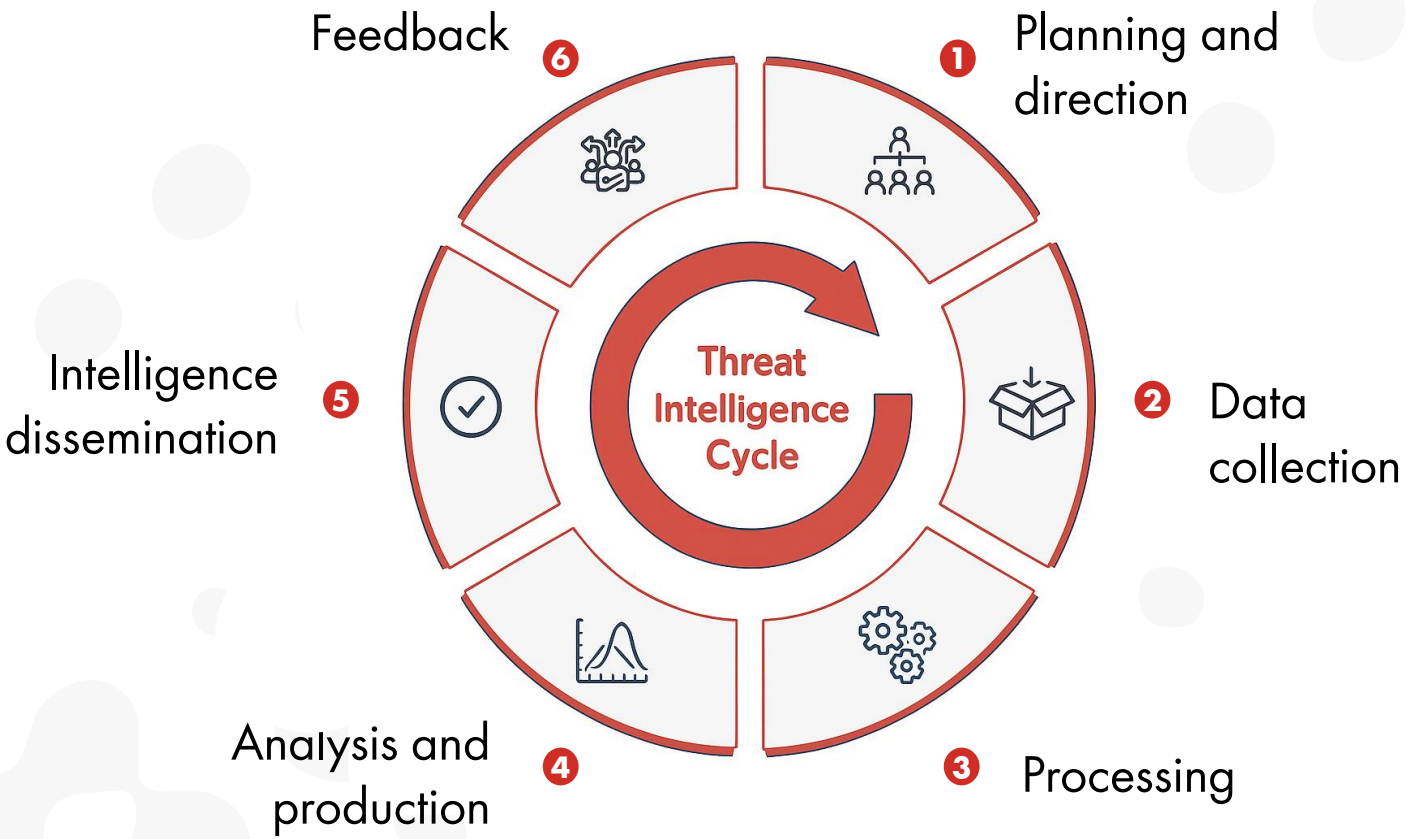
Ciclo di vita

Il ciclo di vita della **Cyber Threat Intelligence** segue una sequenza di fasi iterative, basata su framework come **intelligence cycle** e **intelligence requirements management.**



Cyber Threat Intelligence

Ciclo di vita



Cyber Threat Intelligence

CTI manuale VS TIP (Threat Intelligence Platform)

satayo
SEARCH ALL THINGS ABOUT YOUR ORG

- Fonti eterogenee e non normalizzate
- Aggiornamento tardivo delle minacce
- Prioritizzazione soggettiva e rumorosa
- Elevato effort su attività ripetitive a basso valore

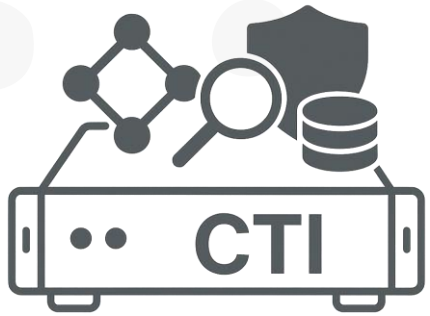
- Ingest unificato e tracciabile delle fonti informative
- Enrichment e scoring per contesto
- Pubblicazione di IoC/TTP su SIEM/SOAR/EDR
- Playbook e ticket automatici

SATAYO

Architettura e Integrazione

NetEye

- Telemetria Server, Firewall, Endpoint, App
- Raccolta, correlazione e detection
- Alerting e triage centralizzato
- Integrazione SOAR/response



satayo
SEARCH ALL THINGS ABOUT YOUR ORG

- Dark Web & Data Leak Sites monitoring
- CVE/Exploit prioritization (KEV/EPSS)
- Ransomware: campagne, TTP, IoC curati
- Enrichment e scoring per contesto

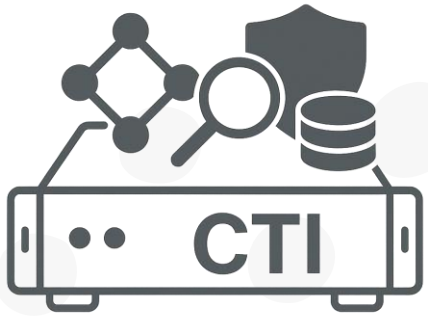
NetEye

Funzionalità

Funzione	**SIEM (NetEye)**
Raccolta dati	✅ Log ed eventi interni (server, firewall, endpoint, app)
Correlazione eventi	✅ Anomalie e incidenti interni
Rilevamento minacce	✅ Comportamenti sospetti già avvenuti
Contestualizzazione	❌ Limitata a dati aziendali
Proattività	⚠ Reattivo (incidenti già avvenuti)
Supply Chain	❌ Non monitorata
Gestione allarmi	✅ Allarmi interni (molti, rischio overload)
Benefit	Visione interna (“cosa succede dentro”)

SATAYO

Funzionalità



satayo
SEARCH ALL THINGS ABOUT YOUR ORG

Funzione	**SATAYO TIP**
Raccolta dati	✅ Fonti esterne (dark web, CVE, ransomware, DLS)
Correlazione eventi	❌ Nessuna correlazione con log interni
Rilevamento minacce	✅ Minacce emergenti prima che colpiscano
Contestualizzazione	✅ Ampio contesto (campagne, gruppi criminali, TTPs)
Proattività	✅ Proattivo (anticipa attacchi)
Supply Chain	✅ Esposizione fornitori e partner
Gestione allarmi	⚠ Feed esterni da integrare
Benefit	Visione esterna (“cosa succede fuori”)

SATAYO e NetEye

Integrazione

NetEye

Full Protection 360

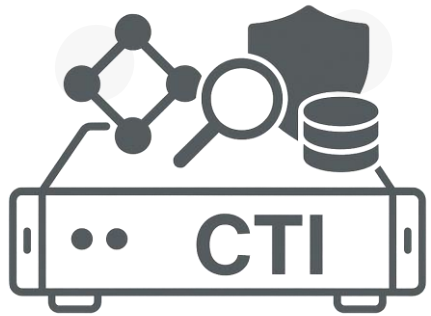
satayo
SEARCH ALL THINGS ABOUT YOUR ORG

SATAYO e NetEye

Integrazione

NetEye

Funzione	**Integrazione SIEM + SATAYO**
Raccolta dati	✅ Entrambi: interno + esterno → visione a 360°
Correlazione eventi	✅ Correlazione avanzata interno ↔ esterno
Rilevamento minacce	✅ Rilevamento combinato → tempi di risposta ridotti
Contestualizzazione	✅ Arricchimento automatico dei log con intelligence
Proattività	✅ Mix reattivo + proattivo → difesa predittiva
Supply Chain	✅ Monitoraggio integrato con impatto diretto sugli asset aziendali
Gestione allarmi	✅ Prioritizzazione intelligente (riduce falsi positivi)
Benefit	Visione unificata + decisioni più rapide e consapevoli



satayo
SEARCH ALL THINGS ABOUT YOUR ORG

SATAYO e NetEye

Funzionalità principali e vantaggi operativi

- **Correlazione interna/esterna:** SATAYO correla eventi interni con dati di minaccia esterni, identificando attacchi che un SIEM tradizionale potrebbe non rilevare (unione di evidenze interne + esterne);
- **Monitoraggio continuo:** rileva in tempo reale nuove minacce (CVE critiche come Log4j, malware, IOC, domini sospetti) e attività sul dark web (credenziali rubate, annunci ransomware);
- **Ricerca & community**: integra risultati e metodologia del progetto ***DEEPDARKCTI*** come riferimento di analisi su dark/deep web, una raccolta curata di fonti dal deep & dark web che la community CTI usa ogni giorno da **Massimo Giaimo**;
- **Coverage infostealer**: include feed/integrazione HUDSON ROCK con il modulo di infostealer della piattaforma Cavalier per attribuzione e arricchimento delle evidenze.

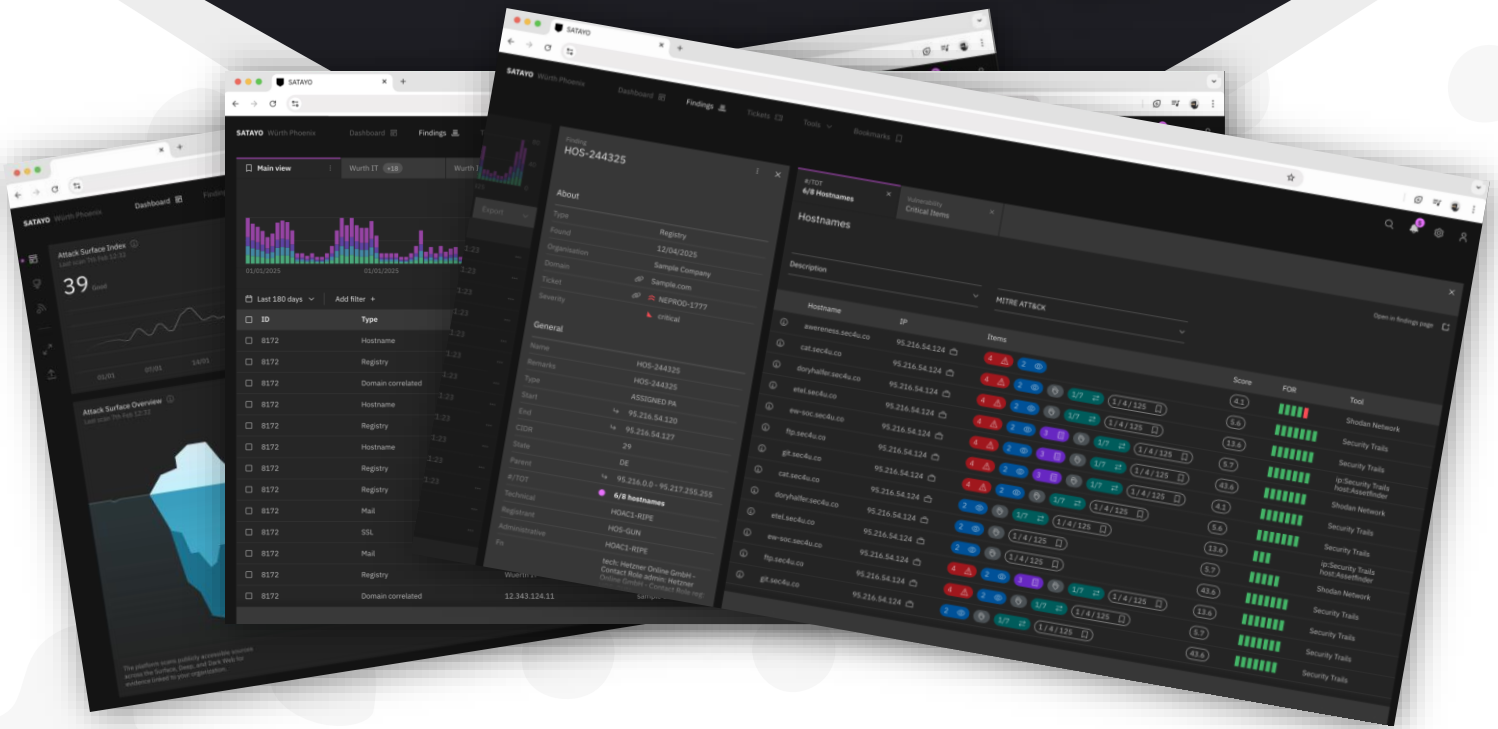
satayo
SEARCH ALL THINGS ABOUT YOUR ORG

WÜRTH

satayo

SEARCH ALL THINGS ABOUT YOUR ORG

NEW



L'evoluzione della **Threat Intelligence**

NetEye

SATAYO

Nuove funzionalità

- **Nuova UI e UX:**
  Interfaccia ed esperienza ridisegnate intorno a **use-case** emersi da interviste con **utenti reali**, con l'obiettivo di rendere più intuitiva e rapida la navigazione e la comprensione delle informazioni.

- **Nuove Dashboard per "Persona"**
  Sarà possibile **monitorare lo stato generale** della superficie di attacco (e di tutte le sue parti) da un'unica pagina, progettata per rispondere alle **diverse esigenze** di **diversi tipi di utenti**.

- **Funzionalità collaborative:**
  Interfacce pensate per consentire uno **scambio di informazioni fluido** e semplice tra team di lavoro, anche da remoto, **rimuovendo attriti** e possibili **incomprensioni**.

- **Nuovi tool ed integrazioni:**
  Verranno introdotti **nuovi tool specifici** per ottenere insight mirati, e Satayo si **integrerà sempre di più con NetEye** per automatizzare e incrementare il suo potenziale di azione.

Use case

Vulnerabilità critica Log4j

Scenario:
Un portale web aziendale presenta la vulnerabilità Log4j (CVE-2021-44228), tuttora sfruttata da attaccanti anche nel 2025

Valore di SATAYO:

- Identifica l'asset impattato con precisione (es. portale clienti);
- Contestualizza con severità (CVSS, EPSS, exploit attivi);
- Suggerisce remediation operative (patch, controlli configurazioni);

Beneficio:
Riduzione immediata del rischio con azioni chiare, anche per team non altamente tecnici;

Vulnerability Demo

Use case

Furto Credenziali da Infostealer

Scenario:
Un **malware infostealer** ruba le credenziali di un dipendente e le mette in vendita su un mercato del dark web;

Valore di SATAYO:

- Intercetta il dump di credenziali su forum/market.
- Notifica mirata con il nome dell'utente compromesso e la fonte del leak.
- Consente un playbook di risposta (reset password, blocco account, controlli aggiuntivi).

Beneficio:
Trasforma un incidente silenzioso in **un allarme immediatamente gestibile**, limitando i danni all'organizzazione.

Infostealer Demo

Use case

Monitoraggio Ransomware & DLS

Scenario:
I gruppi ransomware pubblicano vittime nei Data Leak Site (DLS). Un partner o fornitore critico dell'azienda appare in un DLS.

Valore di SATAYO:

- Ransomware Monitor rileva nuovi inserimenti nei DLS.
- Filtri avanzati per settore, paese, singolo gruppo criminale, etc.
- Correlazione con la supply chain aziendale.

Beneficio:
Permette decisioni rapide: sospendere accesso al fornitore compromesso, chiedere chiarimenti o rafforzare controlli interni. **Supporta la conformità a NIS2**, che richiede attenzione al rischio di filiera.

Ransomware e DLS Demo

Conclusioni & Call to Action

Conclusioni:

- Il panorama delle minacce è complesso: serve una **visione integrata** (interno + esterno);
- L'approccio **use case–driven** di SATAYO riduce falsi positivi e accelera la risposta;
- L'integrazione **NetEye SIEM + SATAYO TIP** trasforma i dati in intelligence **azionabile e prioritaria**.

Call to Action:

- Richiedi un **Preview Report personalizzato** per la tua azienda (stile Hudson Rock).
- Scopri come SATAYO può supportarti nel percorso di compliance (NIS2, ISO).
- Contattaci per un **Proof of Concept (PoC)** e testare i benefici concreti.