



NetEye Conference 2026

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

Il Threat Modeling in modo semplice:

*capire il contesto dell'organizzazione
prima ancora di cercare le minacce*

Libero Chianello



Agenda

- Il vero problema
- Una nuova prospettiva
- Partiamo dal contesto
- Il contributo dell'AI
- Un nuovo approccio
- Un esempio concreto
- PIRs
- Limiti e uso responsabile
- Elementi chiave

Cybersecurity

Il vero problema

Lunghe liste di minacce e tecniche di attacco che non mostrano dove sta davvero il rischio



Segnali generici

Phishing, Malware, DDoS, furto di dati, attacchi alla Supply Chain, Vulnerabilità

Cosa manca?

Il collegamento con i servizi, l'impatto sul business, le dipendenze e le figure di riferimento

La conseguenza

Tanti alert, prioritizzazione carente, responsabilità non definite

Non più "cosa potrebbe attaccarci?" ma "cosa dobbiamo **realmente** proteggere, garantire ed essere in grado di ripristinare?"



Il contesto rende le minacce rilevanti

La stessa minaccia può risultare critica per un servizio ma irrilevante per un altro



Prima delle minacce, costruiamo il contesto

Creare una visione completa e condivisa dei servizi che supportano il business



AMBITO ED ESITO

Cosa deve continuare a funzionare per i clienti e l'organizzazione?

DIPENDENZE

Dati, applicazioni, identità, pagamenti, fornitori e logistica

RESPONSABILITÀ

Chi convalida le ipotesi e decide cosa succede dopo?

UNA MINACCIA HA SIGNIFICATO SOLO SE ASSOCIABILE A QUALCOSA DI REALE



Il contributo dell'AI

Il valore non è il giudizio autonomo. È una sintesi più rapida che porta a domande mirate.

01

COLLEGA

Riunire frammenti approvati: servizi, asset, dati, dipendenze, proprietari.

02

CHIARISCE

Fa da strumento di conversione tra il linguaggio business e quello tecnico. Fa emergere le relazioni e le scoperture.

03

METTE ALLA PROVA

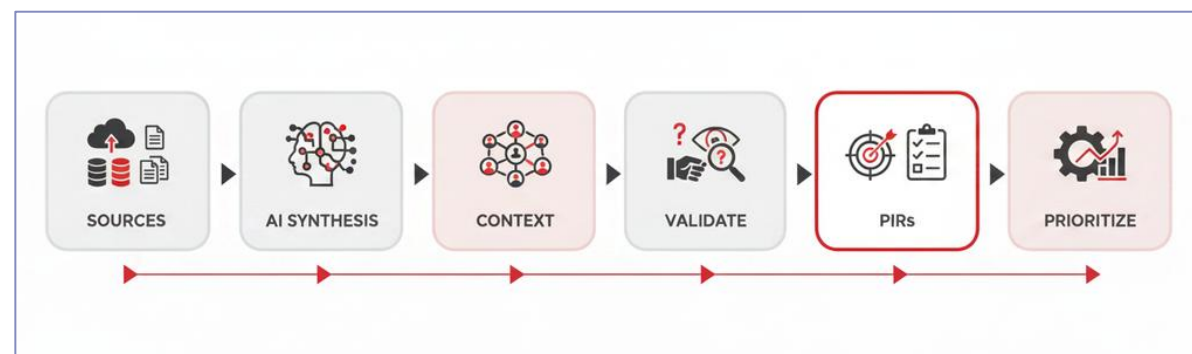
Suggerisce domande di validazione e assunzioni da verificare prima di classificare le minacce.

L'AI ACCELERA L'ANALISI E MIGLIORA LE CAPACITÀ DI SINTESI: LE PERSONE RESPONSABILI SUPERVISIONANO E CONVALIDANO IL RISULTATO.



Un workflow basato sul contesto

Il ruolo dei PIRs collocati tra contesto convalidato e la definizione delle azioni



FONTI	SINTESI AI	CONTESTO	CONVALIDA	PIRS	DEFINISCE LE PRIORITÀ
Raccolta informazioni affidabili	Relazioni e pattern	Vista globale del servizio	Validazione con i responsabili	Domande decisionali	Azioni prioritzate

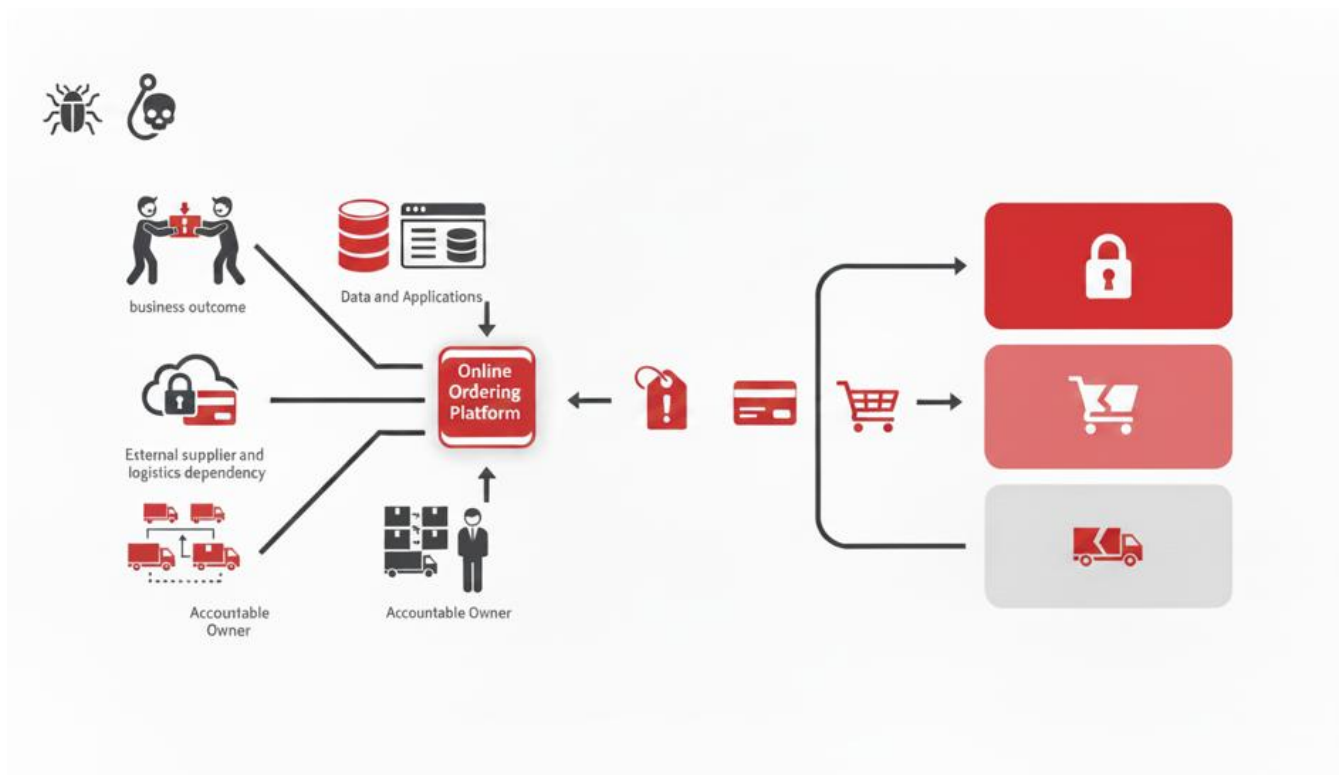
I **Priority Intelligence Requirements (PIRs)** convertono il contesto aziendale in domande mirate e requisiti orientati alle decisioni:

- Cosa potrebbe compromettere questo servizio?
- Quali sue dipendenze sono più esposte?
- Quali indicatori potrebbero rivelare una compromissione?
- Chi deve essere informato e in che fase?

L'**obiettivo** è identificare e dare priorità alle minacce reali per focalizzare la modellizzazione e la threat intelligence su decisioni concrete.

Un esempio reale – servizio ordini online

Dal servizio alle azioni, un filo continuo



CONTESTO DEL SERVIZIO

- Risultato** Ordini evasi in tempo
- Dati** Dati di clienti, ordini e prodotti
- Accesso** Dipendenze di accesso e pagamento
- Partners** Fornitori di magazzino e consegna
- Owner** Responsabile del servizio e obiettivo di ripristino

Domanda: Quale relazione va convalidata per prima?

Dalle minacce alle domande decisionali

Tramite i PIRs si concentra l'attenzione su ciò che l'organizzazione necessita davvero

01

Compromissione identità / informazioni di pagamento

Può la compromissione di un provider avere impatti sui dati degli utenti o delle transazioni?

Decisione: monitorare, restringere gli accessi o attivare misure di emergenza

02

Interruzione logistica / partner

La temporanea interruzione operativa di un partner può impattare gli ordini e le consegne?

Decisione: definire più vettori e mantenere ridondanza con più fornitori distinti, definire un piano di continuità operativa

03

Alterazione dati ordini / prodotti

Ci sono stati impatti sull'integrità dei dati degli ordini o dei prodotti?

Decisione: investigare, eventualmente contenere, correggere, o sospendere.

I PIRs non sono più solo minacce

Sono domande focalizzate che indicano quali informazioni sono realmente necessarie

Contesto -> Domande -> Evidenze -> Azioni

Uso responsabile e limiti

L'uso responsabile è un modello operativo, non una dichiarazione di principio o la spunta di una casella

L'output dell'AI è fatto di ipotesi – non decisioni

01 Sorgenti approvate

Utilizzare fonti approvate e pertinenti. Proteggere i dati sensibili ed evitare le informazioni non controllate.

02 Validazione umana

I responsabili dei servizi, dell'area aziendale e dell'area tecnica verificano le relazioni, le ipotesi fatte e l'impatto.

03 Decisioni tracciabili

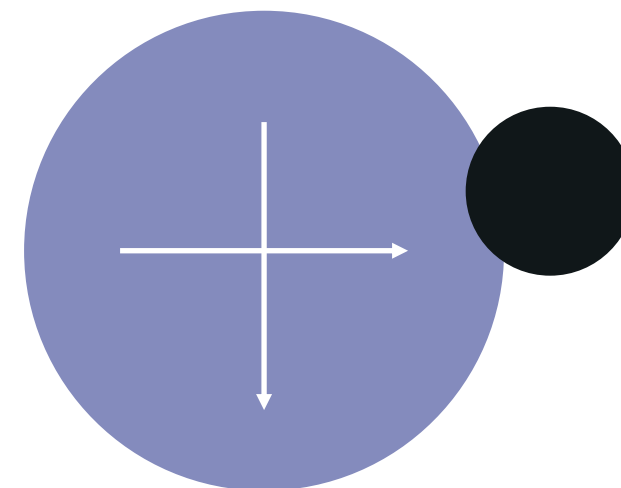
Tenere traccia di evidenze, ipotesi, PIR, responsabili, decisioni prese e azioni successive.

L'AI propone, gli esperti validano. I leader decidono

Conclusioni

Il contesto converte liste di minacce in decisioni operative guidate dal reale rischio associato.

- Comprendi e mappa il servizio
- Usa l'AI per collegare e chiarire
- Convalida con i responsabili
- Definisci i Priority Intelligence Requirements
- Assegna le priorità



AVVIA UN PROGETTO PILOTA SU UN SERVIZIO CRITICO

Inizia in piccolo, rendi visibile il contesto. *Lascia che siano le decisioni a seguire.*





Perchè ciò che sfugge oggi può diventare parte della killchain di domani.

Grazie per l'attenzione.

Domande?

