La quantificazione del rischio cyber tramite dati operativi e modelli predittivi

Stefano Giovanni Romano - Senior Partner Head of GRC competence line

Paolo De Pietro - Principal Data Science

Milano 09 giugno 2026

Un approccio data-driven alla quantificazione del cyber risk

Framework per la quantificazione del rischio cyber

Stima della distribuzione di probabilità delle perdite attese legate al rischio cyber tramite dati operativi e modelli predittivi

Caratteristiche

Data-driven, basata su dati osservati del SOC, con assunzioni esplicite e calibrate statisticamente

Probabilistica, capace di modellare il rischio come distribuzione di probabilità delle perdite, stimata tramite simulazioni Monte Carlo

Scenario-based, le perdite derivano da scenari di attacco coerenti con le minacce rilevanti, gli asset critici e i controlli di sicurezza in essere

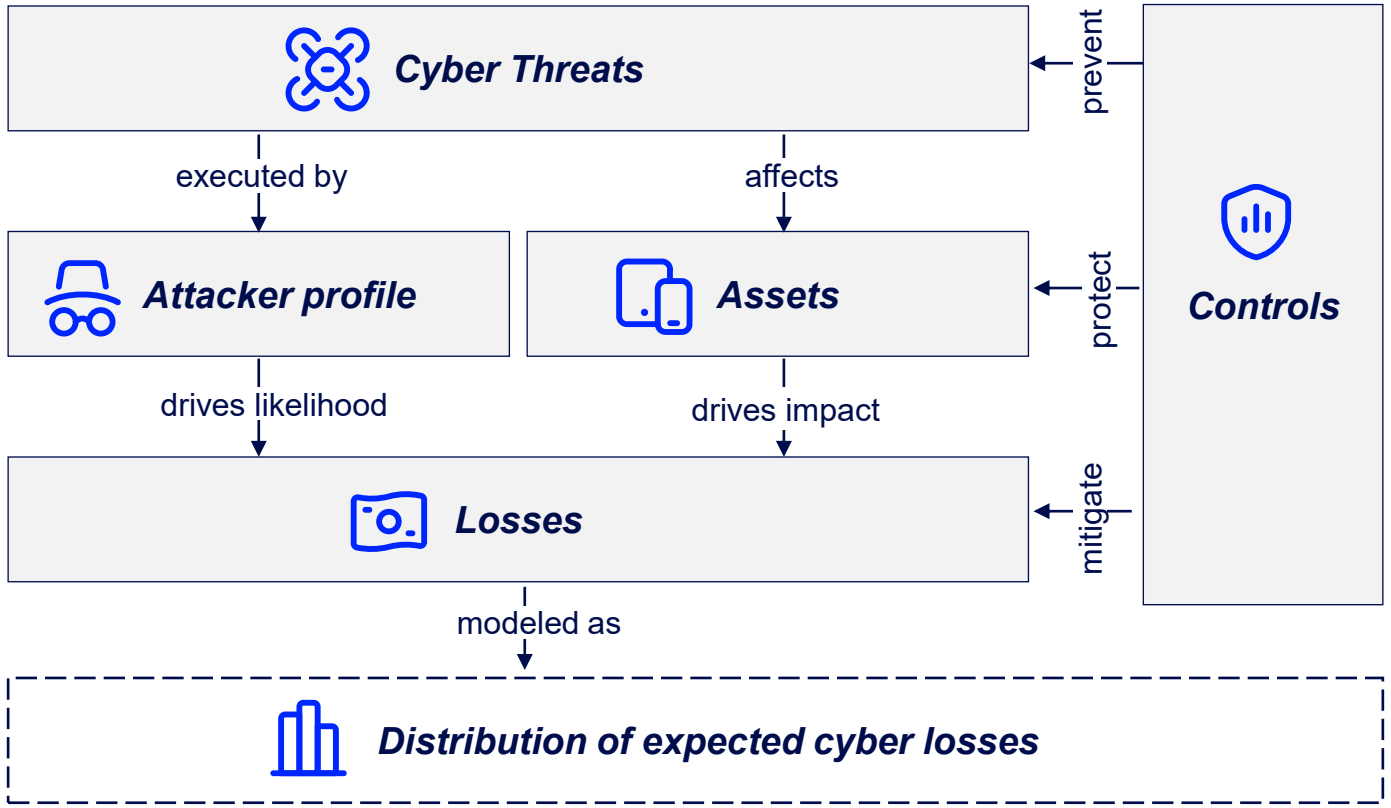
Actionable, in grado di scomporre le perdite lungo le fasi dell'attacco e dei controlli, rendendo chiari i driver di rischio su cui è possibile intervenire

Output

- Stima della **distribuzione di frequenza** delle principali minacce cyber e delle **perdite associate**, con calcolo delle metriche economico-finanziarie rilevanti (es. es. **Expected Loss, VaR, Expected Shortfall** ...)
- Identificazione e quantificazione dei **principali driver di rischio** (minacce, asset, vulnerabilità, efficacia dei controlli), con **simulazione di scenari specifici** per valutarne l'impatto

Framework modulare

La quantificazione del cyber risk richiede un framework modulare e che tenga conto di minacce, asset, profilo degli attaccanti, controlli e impatti economici



- ***Cyber Threats***: Valutazione delle minacce rilevanti, caratterizzate per frequenza, vettori di attacco e tipologia
- ***Assets***: Esposizione degli asset aziendali critici (hardware, software, network, processi)
- ***Controls***: Efficacia delle misure di sicurezza tecniche e organizzative implementate per prevenire o mitigare gli attacchi.
- ***Attacker profile***: Caratterizzazione degli attaccanti per capacità, risorse e comportamento.
- ***Losses***: Quantificazione delle perdite economiche associate agli incidenti cyber, dirette e indirette

Processo analitico di quantificazione del rischio cyber

Il processo analitico si basa su un approccio simulativo che, a partire dalla frequenza degli eventi, costruisce scenari di attacco coerenti con asset e minacce, incorpora l'efficacia dei controlli e stima le perdite economiche

Simulazione Monte Carlo e calcolo metriche

Frequenza e tipologia eventi cyber

La frequenza degli eventi è stimata a partire dai dati SOC e le altre fonti informative e gli eventi caratterizzati sulla base della loro tipologia

Definizione scenario di attacco

A partire da questa frequenza, ad ogni evento si associano scenari di attacco, che specificano minaccia, asset e profilo dell'attaccante

Verifica controlli di prevenzione

Si simula l'efficacia dei controlli nel bloccare l'attacco prima che generi impatti economici, tenendo conto di eventuali costi operativi

Stima perdita economica

Per gli eventi non bloccati dal sistema di controlli si stima la perdita lorda e si applicano i controlli di mitigazione, ottenendo la perdita netta

Security Operation Center e dati operativi

Il SOC integra persone, processi e tecnologie per rilevare eventi di sicurezza e gestire gli incidenti cyber, producendo dati operativi essenziali per analizzare e quantificare la frequenza degli attacchi cyber

Principali componenti tecnologiche

EDR/XDR (*Endpoint/Extended Detection and Response*): monitora endpoint (e altri domini in XDR) per rilevare e rispondere alle minacce.

NDR (*Network Detection and Response*): analizza il traffico di rete per individuare anomalie e attacchi.

IAM/UEBA (*Identity Security*): gestisce accessi e analizza i comportamenti degli utenti per rilevare compromissioni e abusi.

SIEM (*Security Information and Event Management*): raccoglie e correla log da diverse fonti per identificare eventi di sicurezza sospetti

SOAR (*Security Orchestration, Automation and Response*): automatizza e orchestra i processi di risposta agli incidenti.

Dati operativi SOC

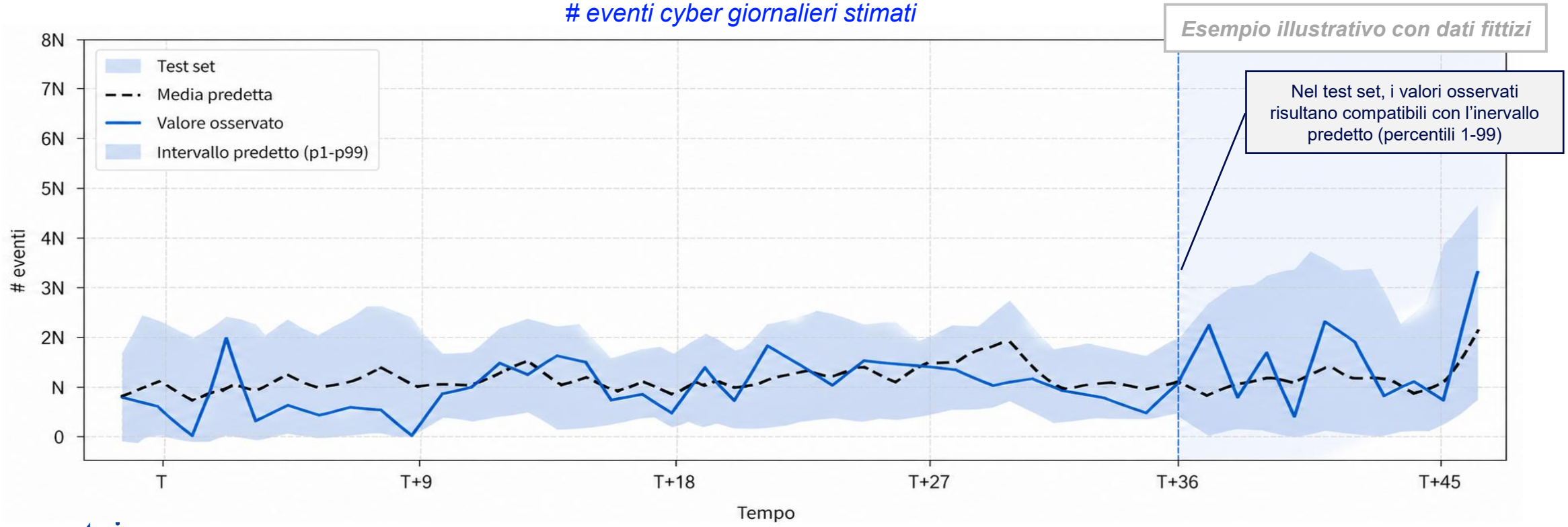
- **Data e ora dell'attacco**: timestamp dell'evento di sicurezza rilevato
- **Tipologia di minaccia**: secondo standard interni SOC o framework riconosciuti (es. MITRE ATT&CK)
- **Modalità di detection**: strumento o sistema che ha identificato l'evento e dettaglio della regola di detection
- **Severity score**: livello di gravità attribuito dagli strumenti di sicurezza
- **IP e geolocalizzazione**: indirizzi IP sorgente/destinazione e localizzazione geografica
- **Asset target**: sistema o applicazione coinvolta, se identificabile (server, endpoint, ambiente cloud, ecc.)
- **Utente coinvolto**: account target o compromesso, se applicabile
- **Eventi correlati**: alert o eventi associati allo stesso incidente
- **Esito della minaccia**: valutazione finale (falso positivo, attività legittima, minaccia bloccata, incidente con impatto)

L’affidabilità dell’approccio e l’aderenza con i dati reali

- La distribuzione giornaliera stimata è stata **valutata** tramite **CRPS** e tramite **test di Kolmogorov–Smirnov sui percentili osservati**.I risultati mostrano **forte aderenza ai dati reali**, inclusi i percentili più elevati, coerentemente con quanto si osserva anche nel confronto tra le serie temporali.

Il modello fornisce stime ben calibrate lungo tutta la distribuzione, incluse le code, aspetto essenziale per analizzare correttamente gli scenari di rischio più estremi.

 # eventi cyber giornalieri stimati



CONFIDENTIALITY

Sedi

BOLOGNA

Piazza Trento e Trieste, 3
+39 051 6480911

info@prometeia.com

MILANO

Via Brera, 18
+39 02 80505845

info@prometeia.com

ROMA

Viale Regina Margherita, 279
+39 06 45441350

info@prometeia.com

Uffici di rappresentanza

FRANCOFORTE

Messeturm, 9th floor,
Friederich-Ebert-Anlage, 49

info@prometeia.com

Branch

ISTANBUL

River Plaza, 19th floor
Büyükdere Cad. Bahar Sk., 13

turkey@prometeia.com

IL CAIRO

The GrEEK Campus
171, El Tahrir

egypt@prometeia.com

LONDRA

One Canada Square, 37th floor
Canary Wharf

uk@prometeia.com

LUSSEMBURGO

2, Rue Edward Steichen

info@prometeia.com

VIENNA

Wiedner Gürtel, 13

info@prometeia.com

ZURIGO

Technoparkstrasse, 1

switzerland@prometeia.com

Prometeia

Prometeiagroup

Prometeia

www.prometeia.com

prometeia