Google Developer Groups

DevFest Mediterranean 2025

AI al servizio della cybersecurity

..sicurezza con l'AI

Vincenzo Agrillo

Lorenzo Deodato

Sant'Agata di Militello, 13 Dicembre 2025

ids Unitelm

Lorenzo Deodato

CISO - IDS & Unitelm

Vincenzo Agrillo

CTO Infrastruttura Data Center

IDS & Unitelm

CSP ACN – ISO 2700x – operativa dal 1987

Governance della Cyber Security

Il Chief Information Security Officer è il garante della sicurezza informatica aziendale, con responsabilità strategiche e operative che spaziano dalla compliance normativa alla gestione del rischio cyber.
Il CTO..... erogazione dei servizi....garanzia di prestazioni/uptime.. rispetto degli sla

Service Management

Gestione del Service Value Chain in linea con *ITILv4*: gestione di CMDB , Change/Incident Mgmt e SLA monit.

Compliance Normativa

Garantire l'aderenza a GDPR, **NIS2**, ISO 27001 e framework di sicurezza settoriali.

Sicurezza Operativa

Progettare e implementare strategie di difesa, gestione degli incidenti e business continuity.

Risk Management

Identificare, valutare e mitigare i rischi informatici attraverso assessment continui e strategie di resilienza.

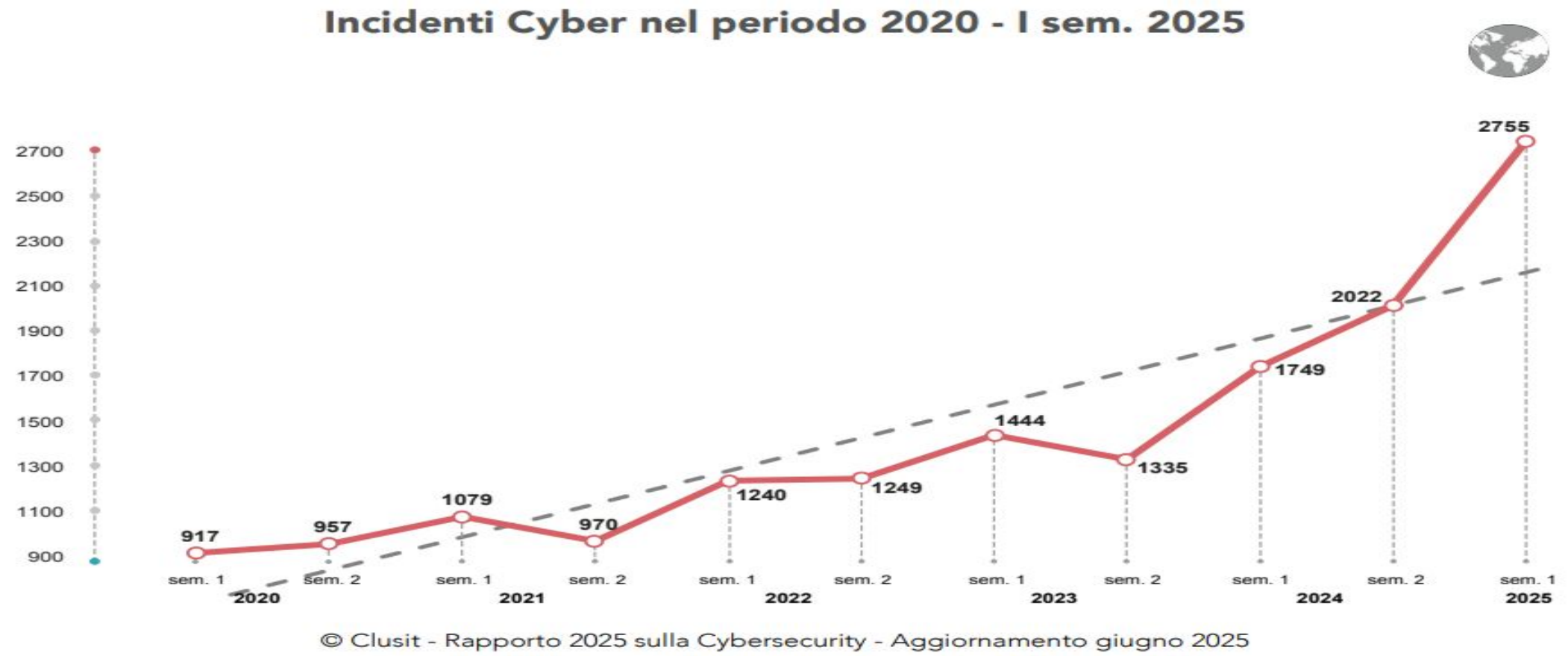


Fig. 1 - Andamento degli incidenti cyber nel periodo 2020 - I semestre 2025

Il panorama delle minacce cyber è in costante evoluzione, e con esso devono evolvere anche le strategie di difesa.

Per un Cloud Service Provider, questa trasformazione è ancora più critica.

Il nuovo paradigma per i Cloud Service Provider

Sfide specifiche

- Infrastrutture multi-tenant
- Superfici di attacco ampliate
- Compliance rigorosa (GDPR, NIS2, ISO 27001/17/18)
- Responsabilità condivisa con i clienti
- Volumi di traffico massivi da analizzare

+36%

È la crescita degli incidenti rispetto al II semestre 2024

Aumento attacchi
I semestre 2025

+143%

è l'aumento degli incidenti con impatto Critico o Alto negli ultimi 5 anni

Fonte: Rapporto Clusit 2025

Dal perimetro alla Zero Trust

Sicurezza Perimetrale

Firewall, DMZ, VPN: un castello con fossato. Efficace fino agli anni 2010, quando il perimetro era definito e controllabile.

Zero Trust Architecture

"Never trust, always verify": verifica continua dell'identità e del contesto. Nessuna fiducia implicita, nemmeno all'interno del perimetro.

1

2

Pattern Recognition

EDR, IPS, antivirus: riconoscimento di firme note e comportamenti sospetti. Reattivo ma limitato alle minacce conosciute.

3

Behavioral Analysis

Machine learning per identificare anomalie e deviazioni dal comportamento normale. Proattivo e adattivo alle nuove minacce.

4

AI-Driven Threat Intelligence

01

Raccolta dati

Log di reverse proxy classificati: traffico malevolo vs autorizzato. Dataset storico per training del modello.

> *"Il valore aggiunto è nei dati!"*
>
> La qualità del dataset di training è fondamentale per l'accuratezza del modello

02

Training del modello

Machine learning supervisionato per identificare pattern di attacco e comportamenti anomali nei flussi di traffico.

03

Generazione threat intelligence

Il modello produce liste dinamiche di sorgenti malevole aggiornate in tempo reale.

04

Integrazione con security stack

Le liste *(opendata)* alimentano firewall , WAF e altri strumenti di sicurezza classici, potenziandoli con intelligenza predittiva.

Tecniche e tecnologie

Caratteristiche del Modello

Aspetto	Descrizione
Architettura	Embedding → LSTM → Dense Layers
Scalabilità	738K parametri
Specificità	Addestrato su log web server
Output	Classificazione binaria con probabilità

Cos'è LSTM?

LSTM è una particolare architettura di rete neurale ricorrente (RNN) progettata per:

- Elaborare sequenze temporali di dati
- Memorizzare dipendenze a lungo termine
- Riconoscere pattern complessi nel tempo

Perché LSTM per i Log?

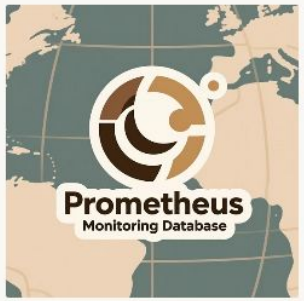
I log sono sequenze temporali: LSTM eccelle nell'identificare comportamenti anomali analizzando la sequenza delle richieste.

Python 3

Linguaggio principale per sviluppo del sistema di analisi e orchestrazione dei componenti

TensorFlow

Framework Google per implementazione e training del modello LSTM di deep learning



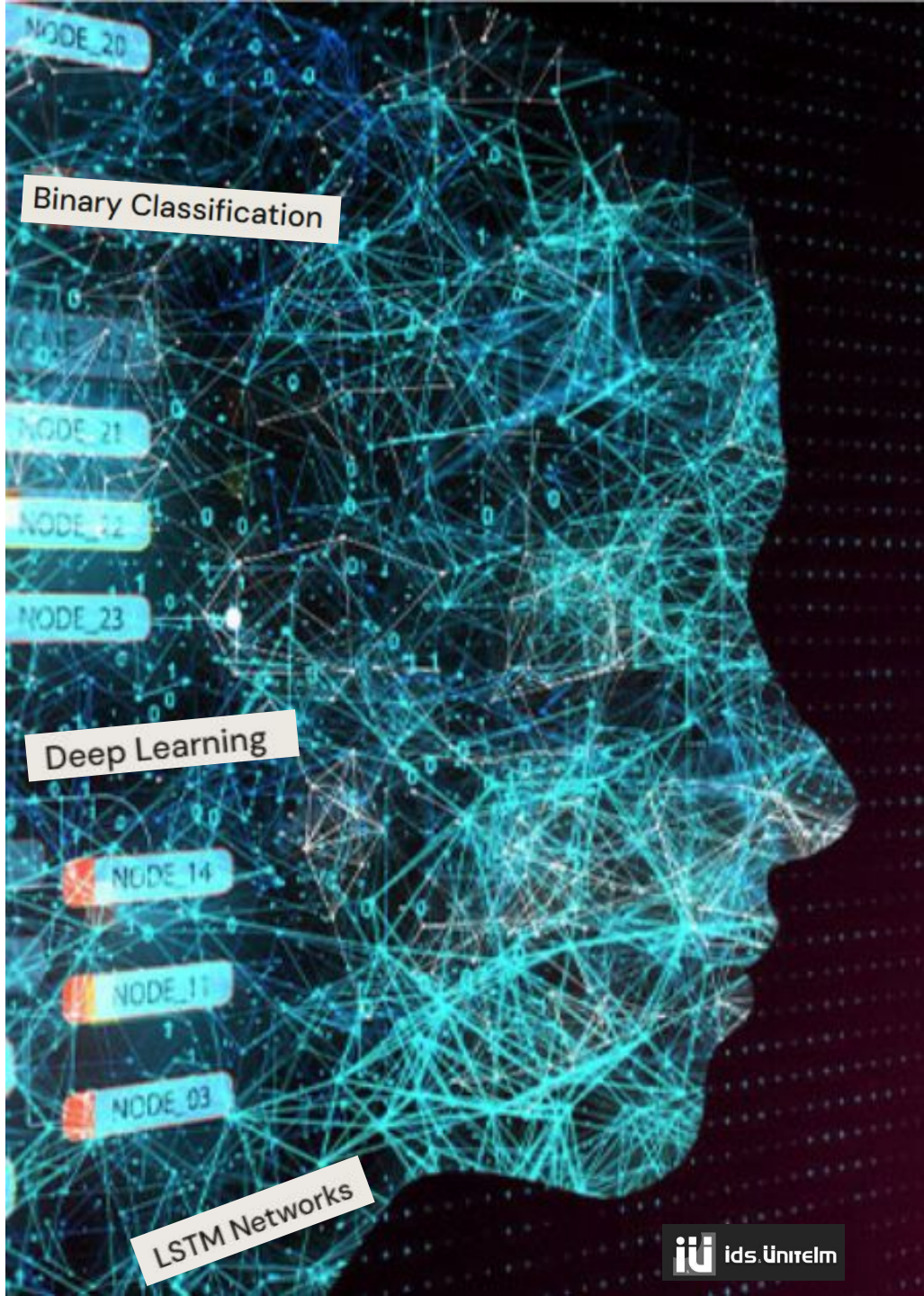
Prometheus

Time-series database per storage metriche e risultati delle analisi

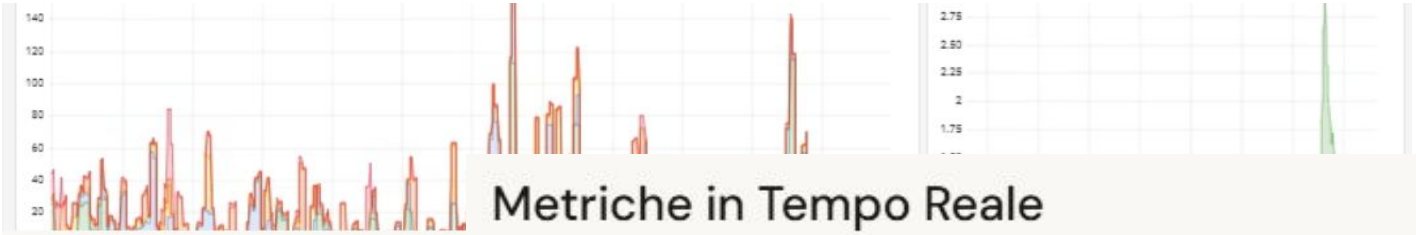
Grafana

Piattaforma di visualizzazione per dashboard real-time e reportistica avanzata

La scelta di tecnologie open-source garantisce flessibilità, scalabilità e integrazione con l'ecosistema esistente.



Risultati del modello



Metriche in Tempo Reale

- Visualizzazione continua delle anomalie rilevate
- Aggregazione per sede (Roma, Messina)
- Trend storici e pattern ricorrenti
- Alert automatici su soglie critiche

Performance Sistema

- Elaborazione su CPU con latenza accettabile
- Analisi di 50.000+ log ogni 10 minuti
- Tasso di **falsi positivi < 5%**
- Disponibilità dashboard 99.9%

Machine Learning Supervisionato: Il modello è stato addestrato con 200.000 righe di log già etichettate come "normali" o "anomale", permettendo di apprendere i pattern distintivi delle minacce.

Il valore dell'approccio ibrido

AI come motore di intelligence

Analisi predittiva, identificazione di minacce zero-day e adattamento continuo ai nuovi vettori di attacco attraverso apprendimento automatico.

Strumenti classici come enforcement

Firewall, IPS e WAF mantengono il loro ruolo di enforcement, ma potenziati da threat intelligence generata dall'AI in tempo reale.

Risultati misurabili

Riduzione dei falsi positivi del 60%, detection time ridotto da ore a minuti, e copertura estesa alle minacce emergenti.

L'AI non sostituisce gli strumenti esistenti: li potenzia, trasformando difese reattive in sistemi proattivi e intelligenti.