FONDAZIONE BRUNO KESSLER
MAGAZINE

Quando l’AI aiuta a distinguere il rumore dalle vere minacce

21 Aprile 2026

ARES-AI: un nuovo approccio alla sicurezza delle reti

Nel mondo della cybersecurity, uno dei problemi più difficili da affrontare non è solo individuare gli attacchi informatici, ma distinguere quelli reali dal cosiddetto “rumore di fondo”. In molte infrastrutture di rete, infatti, i sistemi di sicurezza generano migliaia di allarmi, molti dei quali si rivelano falsi positivi, ossia segnalazioni di attività sospette che, dopo verifica, risultano essere del tutto legittime.

Il progetto ARES-AI si concentra proprio su questo problema. È stato sviluppato dal Centro Cybersecurity della Fondazione Bruno Kessler (FBK) in collaborazione con l’azienda Nubee, nell’ambito del programma InnovAction, un’iniziativa co-finanziata dal Ministero delle Imprese e del Made in Italy (MIMIT). L’obiettivo del programma è costruire un Polo Europeo di Innovazione Digitale per supportare la trasformazione digitale e green delle aziende.

L’intento è chiaro nella formulazione ma complesso nell’implementazione: **rendere più intelligente una sonda di sicurezza di rete già esistente**, integrando tecniche di Machine Learning capaci di filtrare gli allarmi e supportare gli analisti nel loro lavoro quotidiano.

Dalle firme statiche all’intelligenza artificiale

Il punto di partenza del progetto è **ARES**, una sonda di sicurezza progettata e sviluppata da Manuel Roccon, per monitorare il traffico di rete aziendale e individuare attività potenzialmente malevole. Il sistema si basa su un approccio tradizionale molto diffuso nella sicurezza informatica: l’analisi tramite **firme statiche**.

In questo modello il traffico viene confrontato con un insieme di regole che descrivono comportamenti noti di attacco. Quando una regola viene soddisfatta, il sistema genera un alert. Questo approccio ha il vantaggio di essere deterministico e facilmente interpretabile, ma presenta alcuni limiti strutturali: riesce a identificare con precisione minacce già conosciute, ma fatica a individuare nuove varianti o comportamenti anomali non ancora catalogati.

Un altro problema riguarda il volume degli alert generati. In molti casi, gli analisti devono verificare manualmente centinaia di segnalazioni, la maggior parte delle quali si rivela innocua. Questo processo richiede tempo e risorse, aumentando il carico operativo dei team di sicurezza.

ARES-AI nasce proprio per affrontare questa criticità: **affiancare al motore di rilevamento tradizionale un componente intelligente capace di analizzare il traffico e migliorare la qualità degli alert generati.**

Imparare il comportamento “normale” della rete

Per realizzare questo obiettivo, il team di ricerca ha sviluppato un modello di Machine Learning basato su un’architettura chiamata **autoencoder**, utilizzata frequentemente nei sistemi di rilevamento delle anomalie.
Invece di cercare direttamente gli attacchi, il modello impara a riconoscere il comportamento normale della rete. Quando osserva un flusso di traffico che si discosta da questo comportamento, lo segnala come potenzialmente anomalo. Questo approccio si è rivelato particolarmente adatto al contesto del progetto. Durante la raccolta dei dati, infatti, è emerso che la maggior parte del traffico osservato è legittimo, mentre gli attacchi reali sono relativamente rari. In queste condizioni, addestrare un classificatore supervisionato, cioè un modello che impara a distinguere tra traffico benigno e malevolo a partire da esempi già etichettati, risulta difficile perché richiede un numero sufficiente di attacchi correttamente identificati. **Le tecniche di anomaly detection permettono di sfruttare la grande quantità di traffico benigno disponibile**.

In pratica, il sistema costruisce un modello del comportamento normale della rete aziendale. Quando osserva nuove comunicazioni tra i dispositivi, le confronta con ciò che ha imparato. Se il comportamento è molto diverso da quello abituale, il sistema lo segnala come potenzialmente anomalo.

Un’architettura flessibile per la sicurezza di rete

Uno degli aspetti più interessanti del progetto riguarda l’integrazione tra il sistema esistente e il nuovo componente di Machine Learning, per cui il team ha proposto ed esplorato due possibili approcci. Il sistema esistente è la sonda di rete ARES, che analizza il traffico della rete aziendale e genera alert utilizzando un motore di rilevamento basato su firme, cioè regole che identificano pattern di attacco già noti.

Nel primo approccio, chiamato **sequenziale**, il modello di Machine Learning analizza solo le possibili anomalie già identificate dal sistema tradizionale. In questo modo può verificare se si tratta di veri attacchi o di falsi positivi, riducendo significativamente il numero di segnalazioni da controllare manualmente.

Nel secondo approccio, definito **parallelo**, il modello analizza direttamente tutto il traffico di rete, in parallelo con il sistema a firme statiche. Questo permette non solo di filtrare i falsi positivi, ma anche di individuare eventuali attacchi che il sistema tradizionale non è riuscito a rilevare.

Per coordinare le informazioni provenienti da queste diverse componenti, è stato sviluppato anche un modulo software dedicato, chiamato **Prediction Collector**, che aggrega le decisioni dei vari sistemi e produce una visione unificata degli eventi di sicurezza osservati.

Un dataset costruito a partire dal traffico reale

Un elemento fondamentale del progetto è stata la costruzione di un **dataset rappresentativo del traffico reale**, raccolto direttamente dalla sonda installata presso l'infrastruttura di Nubee.

Durante una settimana di osservazione sono stati registrati oltre 500 alert. L'analisi ha mostrato che la grande maggioranza di queste segnalazioni era legata a semplici controlli di reputazione degli indirizzi IP, mentre solo una piccola parte corrispondeva a veri tentativi di attacco o scansione.

Questa distribuzione conferma una realtà ben nota agli operatori della sicurezza: gran parte degli alert generati dai sistemi automatici è dovuta al cosiddetto **background noise di Internet**, ovvero traffico generico e spesso innocuo proveniente dalla rete globale.

Per addestrare il modello, il team ha utilizzato sia dataset pubblici di ricerca sia traffico reale raccolto dalla sonda, prestando particolare attenzione agli aspetti di privacy e protezione dei dati.

Ridurre gli alert fino al 99%

I risultati ottenuti durante la fase sperimentale sono incoraggianti. Infatti, nei test effettuati su dataset di riferimento, il modello è riuscito a **ridurre drasticamente il numero di falsi positivi** rispetto al sistema tradizionale: in alcune configurazioni, la riduzione ha raggiunto il **99% degli alert generati**, mantenendo comunque la capacità di individuare anomalie rilevanti nel traffico di rete.
Anche sui dati raccolti nell'ambiente reale di Nubee il sistema ha mostrato miglioramenti significativi, con una riduzione dei falsi positivi fino al 53%.

Questi risultati indicano che l'integrazione tra approcci tradizionali e Machine Learning può rappresentare una strada promettente per migliorare l'efficacia dei sistemi di sicurezza di rete.

Verso sistemi di difesa sempre più adattivi

Il progetto ARES-AI rappresenta un primo passo verso una nuova generazione di sonde di sicurezza capaci di **adattarsi dinamicamente al contesto operativo in cui vengono utilizzate**.

Uno degli elementi chiave è l'introduzione di un meccanismo **human-in-the-loop**, che permette agli analisti di validare gli alert e utilizzare queste informazioni per migliorare progressivamente il modello di Machine Learning. In questo modo il sistema può essere addestrato ripetutamente nel tempo ed adattarsi progressivamente alle caratteristiche specifiche dell'ambiente in cui opera.

Il prototipo sviluppato nel progetto ha raggiunto un livello di maturità tecnologica intermedio (TRL 4) ed è stato validato in un ambiente sperimentale realistico. L'architettura modulare e gli strumenti sviluppati, dal modello di Machine Learning all'infrastruttura di test automatizzata, costituiscono una base solida per futuri sviluppi industriali.

Una collaborazione tra ricerca e industria

ARES-AI dimostra come la collaborazione tra ricerca accademica e industria possa portare a soluzioni concrete per affrontare le sfide della cybersecurity.

Unendo l’esperienza scientifica di FBK nel campo dell’analisi del traffico di rete e del Machine Learning con la conoscenza operativa di Nubee nel monitoraggio delle infrastrutture aziendali, il progetto ha sviluppato un prototipo capace di migliorare significativamente l’efficienza dei sistemi di rilevamento delle minacce.

In un panorama in cui gli attacchi informatici diventano sempre più sofisticati e dinamici, strumenti capaci di apprendere dal comportamento della rete e adattarsi nel tempo rappresentano un tassello fondamentale per costruire sistemi di difesa più intelligenti e proattivi.

LINK

https://magazine.fbk.eu/it/news/quando-lai-aiuta-a-distinguere-il-rumore-dalle-vere-minacce/

TAG

- #alert
- #anomaly detection
- #ARES-AI
- #attacchi informatici
- #autoencoder
- #aziende
- #cybersicurezza
- #human-in-the-loop
- #industria
- #industriadigitale
- #innovaction
- #innovazione digitale
- #intelligenzaartificiale
- #Machine learning
- #malevolo
- #mimit
- #Nubee
- #prediction collector
- #trasformazione digitale
- #trasformazione green

AUTORI

- Martina Cicaloni