WHITE PAPER

# Rilevamento delle anomalie con Akamai API Security

Le API sono un componente essenziale delle organizzazioni poiché consentono di offrire servizi ai clienti, generare profitti e operare in modo efficiente. Tuttavia, la crescita continua, la vicinanza ai dati sensibili e la mancanza di controlli di sicurezza delle API le rendono un bersaglio allettante per i criminali moderni. Acquisire informazioni in tempo reale sui comportamenti degli utenti è fondamentale per identificare in modo proattivo i segnali che indicano un potenziale attacco o abuso delle API.

Le funzionalità di rilevamento delle anomalie disponibili nella soluzione Akamai API Security sono progettate per identificare i comportamenti anomali degli utenti che indicano tentativi potenzialmente dannosi di sfruttare le API della vostra organizzazione. Stabilendo uno standard per il traffico normale, le funzionalità di rilevamento delle anomalie di Akamai possono confrontare le richieste in entrata con questo riferimento e determinare se il traffico è stato generato da un criminale.

Il nostro algoritmo di rilevamento delle anomalie identifica eventuali comportamenti sospetti, come:

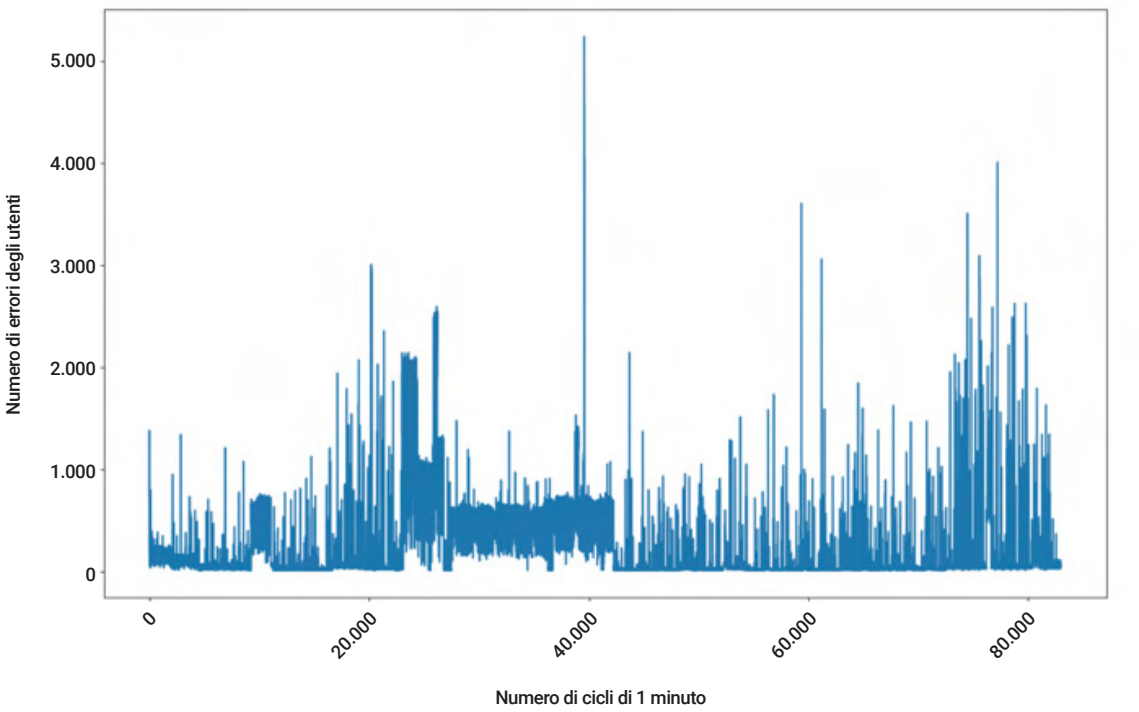
- Utilizzare un campo imprevisto nella richiesta di un'API
- Acquisire dal server una quantità di dati superiore a quella di un utente regolare
- Tentare di utilizzare altre risorse dell'utente/amministratore
- Richiamare le API in un ordine imprevisto

L'algoritmo è basato su un modello di intelligenza artificiale e apprendimento automatico (AI/ML) online e non controllato, che è in grado di apprendere le varie caratteristiche di un comportamento statistico del traffico e di rilevare eventuali anomalie dopo un periodo di apprendimento stabilito. Il nostro modello si adatta ai cambiamenti del traffico nel corso del tempo e alle anomalie classificate come falsi positivi da parte degli utenti.

Durante la fase di apprendimento, il nostro sistema analizza i dati dei clienti e identifica i diversi metodi di autenticazione, i vari tipi di API, utenti e dati, ecc. Come per ogni API, il modello genera un elenco di elementi che caratterizzano un traffico regolare, tra cui il numero di attacchi alle API e di errori generati, la percentuale di richieste autenticate, la quantità di dati recuperati dal server e molto altro. Il nostro algoritmo rileva eventuali comportamenti anomali degli utenti confrontando le loro caratteristiche e quelle delle API con i risultati previsti da parte del modello statistico appreso dall'algoritmo.

# Come funziona il rilevamento delle anomalie di Akamai API Security

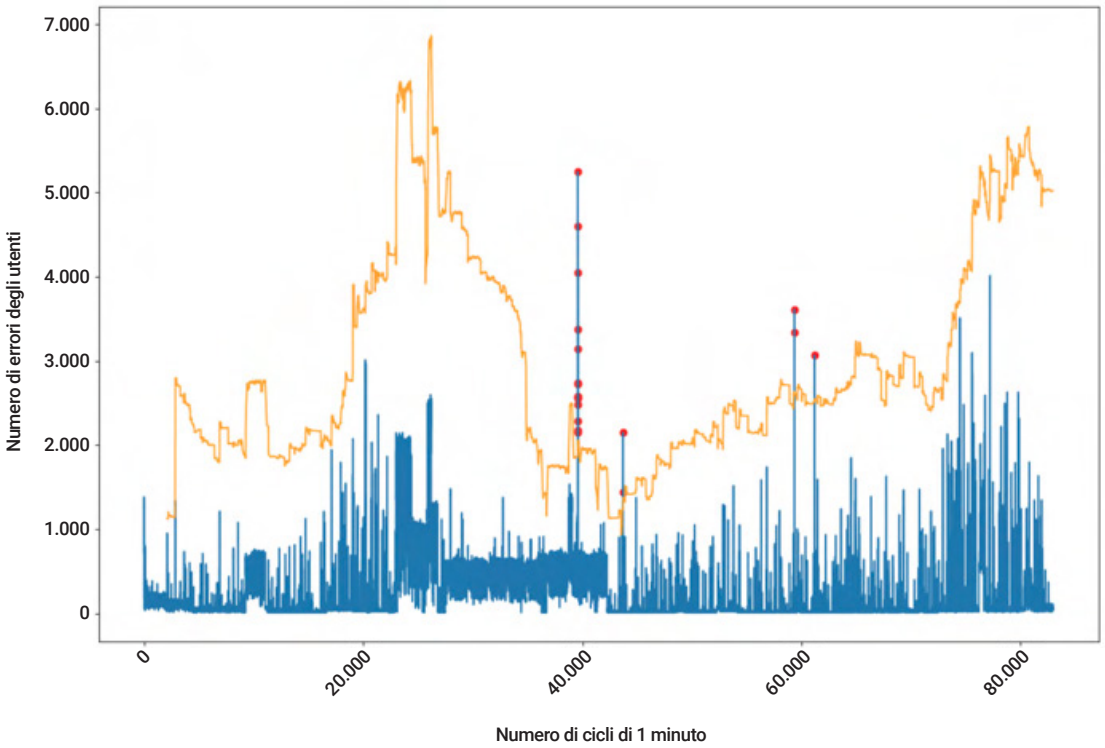
Le funzionalità di rilevamento delle anomalie disponibili in Akamai API Security identificano gli utenti che creano un numero molto più elevato di errori rispetto ad altri utenti per consentire di identificare vari tipi di attacchi, come quelli di forza bruta, di scansione dei percorsi e di scraping. Nel seguente grafico, viene mostrata la quantità massima di errori generati da un utente ogni minuto in un ambiente.




In questo caso, si possono verificare vari problemi durante l'identificazione delle anomalie:

1. Il modello deve considerare i cambiamenti dei dati durante il calcolo della soglia di riferimento.
2. È necessario evitare che l'algoritmo apprenda le anomalie durante la fase di apprendimento del modello.
3. L'apprendimento viene condotto in modo da impedire al modello di vedere tutti i dati e da dover regolare ogni fase temporale.
4. Gli avvisi devono avvenire in tempo reale, pertanto il nostro algoritmo non può basarsi sui dati futuri per prevedere un'anomalia.
5. Per evitare lo spamming degli utenti, il nostro modello deve apprendere una soglia statisticamente garantita dei dati.

Nel grafico riportato di seguito, possiamo vedere come il nostro modello riesca a soddisfare questi requisiti adattando le soglie in base ai dati in entrata.




La linea arancione mostra la funzione della soglia calcolata da parte del modello, mentre i puntini rossi indicano le anomalie rilevate in base a questa funzione.

# Domande frequenti

### Qual è il periodo di apprendimento necessario per l'algoritmo di rilevamento delle anomalie di Akamai?

La maggior parte dei nostri algoritmi richiede un periodo di apprendimento che varia dai due ai sette giorni. Inoltre, il periodo di apprendimento dell'algoritmo è anche influenzato dal numero dei diversi comportamenti degli utenti osservati in questo intervallo di tempo.

### Se viene rilevato un comportamento anomalo, quanto tempo ci vuole per generare il relativo avviso?

Il nostro algoritmo crea il relativo avviso da inviare al client nella maggior parte dei casi, dopo 30 - 60 secondi dal momento in cui riceve il traffico anomalo.

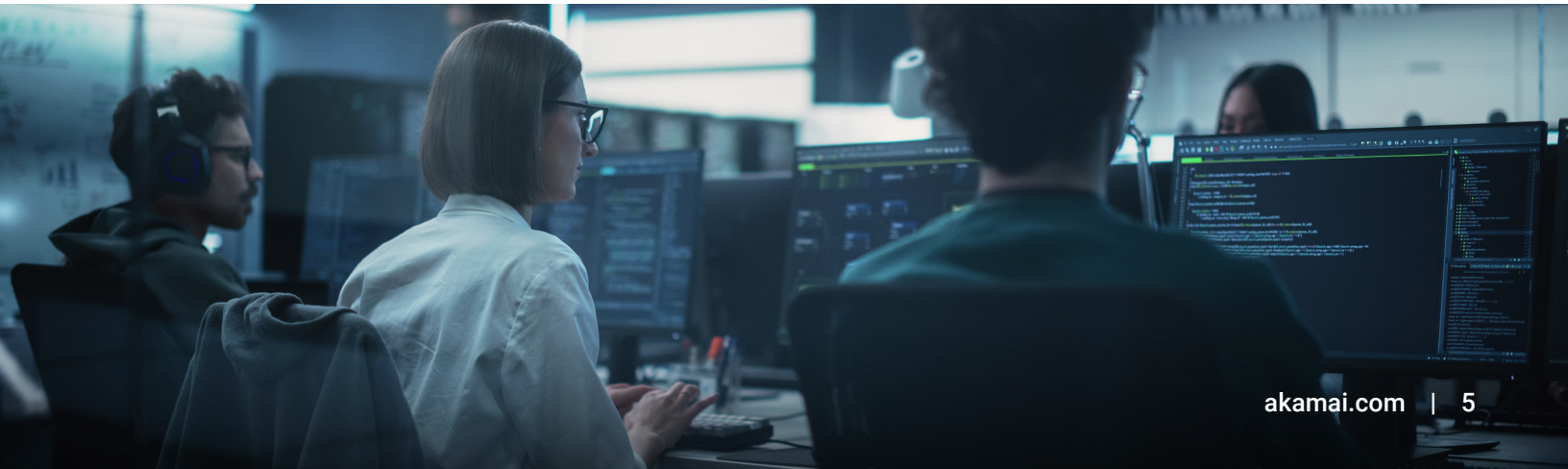
### L'algoritmo utilizza un modello controllato o non controllato?

Il nostro algoritmo si basa su un modello non controllato per adattarsi all'ambiente di ciascun cliente senza richiedere una precedente conoscenza delle sue caratteristiche. Inoltre, il nostro algoritmo utilizza l'apprendimento online per adattarsi ai cambiamenti dell'ambiente nel corso del tempo.

### Quali sono i diversi tipi di anomalie rilevati da Akamai API Security?

Akamai API Security rileva due tipi di anomalie:

- Anomalie basate sui modelli: queste anomalie sono basate sull'identificazione dei modelli dannosi presenti nel traffico, come le tecniche di sfruttamento del web e l'utilizzo di noti user agent dannosi, tra cui comandi di tipo injection, path traversal.e user agent sospetti.
- Anomalie basate sui comportamenti: queste anomalie sono basate sui modelli di apprendimento degli utenti e sull'identificazione di comportamenti anomali, come l'eccessivo utilizzo delle API, la violazione dei limiti stabiliti e la violazione dell'autorizzazione a livello di oggetto (BOLA, Broken Object Level Authorization).



### Quali parametri considera Akamai API Security per identificare un'anomalia?

I nostri algoritmi sono basati su diverse funzioni progettate in modo da condurre un'analisi statistica del traffico, che rileva, ad esempio:

- Il numero dei diversi utenti che utilizzano un'API
- Lo stato di autenticazione dell'API
- Il codice di risposta del server
- La quantità dei dati acquisiti dall'utente
- La geolocalizzazione dell'indirizzo IP dell'utente
- Le informazioni user agent dell'utente, ecc.

### È possibile controllare la sensibilità dell'algoritmo?

Sì, è possibile controllare la sensibilità di ciascuna anomalia modificando il valore della policy corrispondente. La sensibilità della policy si esprime con un numero compreso tra 1 (bassa) e 5 (alta); il valore più elevato corrisponde alla policy delle anomalie più sensibile che è possibile configurare in Akamai API Security. Il nostro algoritmo considera questo parametro come parte del modello.

### È possibile contrassegnare un problema segnalato da Akamai come falso positivo e influenzare l'algoritmo in tal modo?

Sì, per migliorare la funzione di rilevamento del nostro algoritmo, è possibile contrassegnare i problemi desiderati come "falsi positivi". Il nostro algoritmo tiene conto di questa valutazione e adatta il modello in base all'input fornito.

### In che modo Akamai evita lo "spamming" del client nel caso di un utente che continua ad inviare lo stesso scenario di attacco?

Il nostro algoritmo identifica i problemi simili che utenti e API continuano ad inviare e, in questi casi, li ignora per un periodo di tempo specifico.

### In che modo Akamai riesce a gestire i cambiamenti e/o la stagionalità dei dati?

Akamai API Security utilizza vari algoritmi diversi per rilevare le anomalie presenti nei dati. A seconda della complessità dell'algoritmo e della pre-elaborazione dei dati sottostanti, è possibile "allentare" l'adeguamento della soglia o applicare i cambiamenti desiderati ad ogni ciclo allo scopo di garantire l'adozione di soglie statistiche per il rilevamento delle anomalie. Insieme con il controllo dei messaggi spam, è possibile utilizzare una semplice interfaccia persino quando uno specifico algoritmo richiede altri cicli per regolare le soglie stabilite.

### In che modo Akamai riesce a gestire il data poisoning?

Poiché si basa su un algoritmo di apprendimento online, Akamai API Security si trova ad affrontare vari problemi, tra cui:

- Nuove API
- Nuovi campi presenti nelle API esistenti
- Modifica del tipo/intervallo dei valori presenti in un campo
- Problemi di disponibilità del server
- Bug presenti nelle API che possono causare errori (404, 500, ecc.) e altri problemi legati alla difficoltà di stabilire cosa l'algoritmo deve apprendere o meno (Akamai evita che l'algoritmo apprenda le anomalie richiedendo una combinazione di vari fattori, come numero minimo di utenti, periodo di tempo e persistenza prima di attivare l'apprendimento)

## Scoprite come possiamo aiutarvi programmando una **demo personalizzata su Akamai API Security**.