La guida definitiva alla protezione del runtime delle API

Sommario

Introduzione

Perché la sicurezza delle API è fondamentale

Facendo a gara nell'intento di soddisfare le esigenze dei clienti, le organizzazioni subiscono la pressione di dover sviluppare e produrre rapidamente, oltre che ottimizzare, applicazioni, servizi e strumenti basati sull'AI generativa. Questa esigenza di velocità, purtroppo, nasconde alcuni rischi: le API che lavorano "dietro le quinte" per tutte queste innovazioni, spesso, vengono create con errori di configurazione o di codifica, saltando i controlli di sicurezza. Quando poi queste API raggiungono la fase di produzione, si trovano a interagire non solo con gli utenti finali, ma anche con i criminali, costantemente alla ricerca di modi per violarle e accedere ai dati che custodiscono.

Le API compromesse e configurate in modo errato favoriscono violazioni di dati sempre più significative, tuttavia, solo poche organizzazioni riescono a tenere sotto controllo le migliaia di richieste ricevute dai loro ecosistemi digitali tramite le API e un numero ancora inferiore di aziende si può ritenere completamente protetto dalle minacce alle API di runtime.

Nel 2021, ad esempio, una società che opera nel settore del retail per il fitness, ha individuato un bug in un'API relativo ai dati degli account degli utenti, che consentiva di effettuare richieste non autenticate di dati, tra cui età, sesso, città, peso e data di nascita. Anche se questa vulnerabilità è stata fortunatamente rilevata e segnalata all'azienda da parte di un ricercatore della sicurezza, i bug di questo tipo possono passare inosservati e venire sfruttati per settimane o per mesi.

Se guardiamo alla sicurezza delle API, inoltre, va detto che gli strumenti tradizionali su cui, solitamente, si basano le organizzazioni, ad esempio gateway API e soluzioni WAF (Web Application Firewall), sono in grado di fornire una protezione di base. Ma i team addetti alla sicurezza richiedono ormai altri livelli di protezione perché gli attacchi alle API crescono in numero e complessità. Il segreto è aumentare i controlli esistenti con informazioni più dettagliate su vulnerabilità, potenziali percorsi di attacco, attività dannose e comportamenti delle API.

Le organizzazioni possono ottenere queste funzionalità tramite una soluzione completa per la sicurezza delle API, che comprende quattro aree:

1. Individuazione delle API
2. Gestione del sistema delle API
3. Protezione del runtime delle API
4. Esecuzione di test sulla sicurezza delle API

Argomenti trattati in questa guida

La protezione del runtime delle API è il processo che consente di proteggere le API nel momento in cui operano e gestiscono le richieste durante il loro normale funzionamento. Questa guida descrive i requisiti principali della protezione del runtime delle API, tra cui il monitoraggio delle API come difesa da errori di configurazione e tentativi di sfruttamento e la prevenzione degli attacchi alle API. Inoltre, la guida illustra le nozioni di base e le funzionalità di prevenzione del runtime offerte dalla soluzione Akamai API Security.

Perché è importante la protezione del runtime?

La protezione del runtime delle API consente di salvaguardare le API durante la fase di produzione del loro ciclo di vita quando sono operative e disponibili per interagire con gli utenti finali previsti (ma anche con i criminali). Aiutando le organizzazioni ad identificare e risolvere rapidamente le richieste delle API dannose, un efficace sistema di protezione del runtime può salvaguardare le API da una gamma di minacce post-implementazione, tra cui:

- Attacchi che acquisiscono elevati volumi di dati sensibili dalle API
- Attacchi di escalation dei privilegi in grado di sfruttare i bug di sicurezza
- Implementazione di API non autorizzate al di fuori dei normali processi

Il blocco delle minacce alle API di runtime richiede la comprensione del contesto delle operazioni di ciascuna API, tra cui l'accesso, l'utilizzo e il comportamento. Innanzitutto, dovete conoscere l'ambito di azione delle vostre API. La nostra guida definitiva all'individuazione delle API spiega l'importanza di stilare un inventario delle API. Con un inventario delle API completo, potete monitorare il traffico di tutte le vostre API e stabilire uno standard di comportamento "tipico" per ogni API da poter utilizzare per riconoscere eventuali anomalie. Una soluzione per la protezione del runtime delle API deve rilevare:

- Fuga di dati
- Violazioni delle policy relative ai dati
- Attacchi alla sicurezza delle API
- Manomissione di dati
- Comportamenti sospetti

Inoltre, una soluzione per la protezione del runtime deve registrare il traffico delle API, monitorare l'accesso ai dati sensibili, rilevare le minacce e bloccare o mitigare gli attacchi.

Monitoraggio del traffico delle API per il rilevamento degli attacchi

Esaminare il comportamento del traffico delle API è fondamentale per identificare i rischi implicati. Implementare una soluzione di monitoraggio senza disporre di un quadro preciso del patrimonio delle API fornisce solo una visibilità limitata. Dopo aver stilato un inventario delle API, la soluzione di protezione del runtime delle API deve monitorare continuamente il traffico e l'utilizzo delle API allo scopo di individuare le vulnerabilità e gli errori di configurazione.

Rilevamento dei comportamenti anomali

Stabilire uno standard per il comportamento normale delle API consente di identificare eventuali anomalie. Riesaminare i dati cronologici può aiutare ad identificare i comportamenti anomali, che potrebbero rivelare le intenzioni di un criminale.

È necessario indagare ulteriormente le potenziali anomalie nel contesto di altre azioni che si verificano all'interno dell'applicazione o della rete. Ad esempio, se le richieste di dati sono generalmente di una certa dimensione e una chiamata API richiede dati che non rientrano nelle richieste normali, siamo di fronte a un'anomalia che va segnalata. Anche se potrebbe non nascondere intenzioni dannose, un'anomalia simile va comunque esaminata ulteriormente.

Rilevamento dell'esposizione dei dati

Alcune delle vostre API potrebbero inviare e ricevere dati sensibili. Le informazioni sensibili che vengono rese visibili a causa di una vulnerabilità della sicurezza consentono ad un criminale di configurare in modo improprio privilegi o altre opzioni per il controllo degli accessi. Potete utilizzare l'AI e l'apprendimento automatico per analizzare il traffico in tempo reale e rilevare le anomalie, fornendo informazioni contestuali sulla fuga e sulla manomissione dei dati, sulle violazioni delle policy relative ai dati, sui comportamenti sospetti e sugli attacchi alla sicurezza delle API.

Un tipo di attacco che è diventato sempre più comune consiste nell'acquisire chiavi API valide da parte dei criminali informatici. In questo caso, l'unico modo per proteggersi dall'utilizzo improprio delle API e da potenziali violazioni di dati consiste nella capacità di rilevare e bloccare i comportamenti anomali e l'esposizione dei dati.

Verifica della sicurezza delle API

Gli strumenti di verifica della sicurezza delle API devono monitorare il traffico in tempo reale e avvisare l'utente in caso di attacchi e altre minacce. Una soluzione per la verifica della sicurezza delle API deve:

- Effettuare un monitoraggio continuo per identificare i criminali e le richieste dannose
- Eseguire una scansione passiva delle API, sia all'interno che all'esterno, per individuare errori di configurazione e vulnerabilità che potrebbero attivare o peggiorare una violazione oppure indebolire i sistemi di difesa
- Rafforzare le policy sui tipi di dati che le API possono o meno inviare o ricevere

La soluzione di protezione del runtime delle API deve anche includere un sistema di gestione della sicurezza delle API, che consente di identificare errori di configurazione e vulnerabilità note. Per ulteriori informazioni, consultate la nostra guida definitiva alla gestione del sistema di sicurezza delle API.

Le funzioni indispensabili per la protezione del runtime

Se la vostra organizzazione sta attivamente sviluppando e implementando le API, occorre includere nel vostro programma di sicurezza delle API una solida soluzione di protezione del runtime. Ecco alcune importanti funzioni che i vostri strumenti per la protezione del runtime devono prevedere:

Monitoraggio fuori banda in tempo reale

Il monitoraggio della sicurezza delle API non deve influire sul traffico delle API, rallentarlo o aggiungere problemi di latenza, ma deve essere eseguito completamente fuori banda senza richiedere modifiche alla rete né l'utilizzo di agenti complicati e difficili da installare. Gli strumenti per la protezione del runtime devono riflettere il traffico proveniente da fonti di dati identificate ed eseguire analisi di questi dati in background con la generazione di avvisi in tempo reale sugli eventuali problemi rilevati.

Le soluzioni di Akamai vengono eseguite fuori banda e senza agenti per impostazione predefinita, tuttavia, se necessario, consentono di eseguire il rilevamento basato su agenti e il blocco online.

Rilevamento dello sfruttamento e delle anomalie nelle API

La raccolta passiva di dati non è sufficiente, specialmente considerando il fatto che il numero di API e il volume totale del traffico delle API continuano ad aumentare. Le attività delle API devono essere analizzate di continuo per rilevare eventi anomali e per avvisare i team addetti alla sicurezza e alle operazioni. Gli strumenti della piattaforma all'avanguardia integrano funzionalità basate sull'AI e sull'apprendimento automatico per analizzare il traffico in tempo reale e per fornire informazioni contestuali sulla fuga e sulla manomissione di dati, sulle violazioni delle policy relative ai dati, su comportamenti sospetti e attacchi alla sicurezza delle API.

Prevenzione degli attacchi alle API e mitigazione dei rischi correlati

Una volta identificata un'anomalia o un altro problema e generato un avviso, la tempistica è essenziale. Eventuali spostamenti non autorizzati di dati sensibili tramite le API o altri abusi sospetti delle API devono essere rilevati e mitigati. La protezione del runtime deve non solo bloccare eventuali abusi delle API tramite l'integrazione con i firewall e i gateway API esistenti, ma anche consentire di eseguire la mitigazione, se possibile, in modo automatizzato. Cercate funzionalità che includono una valutazione dei criminali per aiutare il vostro team a stabilire se i segnali di abusi, attacchi o violazioni sono legittimi o richiedono una segnalazione.

Integrazioni per la risposta agli incidenti

Come regola generale, gli strumenti per la protezione del runtime devono integrarsi facilmente con gli altri strumenti di sicurezza, monitoraggio e gestione utilizzati dall'organizzazione. Ad esempio, quando si verifica un incidente, gli strumenti per la protezione del runtime devono includere le integrazioni necessarie per garantire che le attività di mitigazione vengano assegnate ai team appropriati. Una volta rilevati, eventuali errori di configurazione, violazioni delle policy relative ai dati o comportamenti sospetti devono essere segnalati al gateway API, al sistema SIEM e ad altri motori per la sicurezza delle informazioni allo scopo di garantire che vengano informate le persone giuste. Disporre di una funzionalità in grado di fornire una valutazione dell'affidabilità dei criminali può consentire ai team di escludere ciò che ritengono inappropriato e focalizzare la loro attenzione sulle reali priorità in termini di sicurezza delle API.

Rapyd

Rapyd, una società di elaborazione dei pagamenti a livello globale che opera nel settore della tecnofinanza, gestisce i suoi sistemi di pagamento in più di 100 paesi. Non disponendo di una visibilità granulare sull'utilizzo e sul comportamento delle API, la società aveva bisogno di un modo migliore per proteggere le API pubbliche e le centinaia di API interne in un sistema altamente complesso, che opera dal cloud AWS su scala globale. Rapyd aveva bisogno di un inventario granulare di tutte le sue API, di una visibilità su errori di configurazione e vulnerabilità e di avvisi con assegnazione intelligente delle priorità per un approccio alla mitigazione più logico.

Akamai API Security ha soddisfatto le esigenze di Rapyd offrendo una visibilità completa e la protezione del runtime che utilizza l'apprendimento automatico allo scopo di creare uno standard del traffico per ogni API, con operazioni automatizzate di rilevamento e mitigazione delle anomalie.

Leggete la storia completa del cliente

> Ora possiamo valutare i nostri rischi nel modo più corretto scientificamente e controllare il nostro destino.

- Nir Rothenberg
CISO, Rapyd

La protezione del runtime offerta da Akamai API Security

La capacità di identificare e contrastare tempestivamente gli attacchi alle API deve essere parte integrante del vostro programma di conformità e valutazione dei rischi. Potete pensare a questa capacità come l'ultima linea di difesa quando gli altri controlli di sicurezza si sono rivelati insufficienti.

La protezione del runtime offerta da Akamai API Security include tutte le qualità descritte nella sezione precedente. La sua funzione principale è rilevare e bloccare gli attacchi alle API in tempo reale. Il monitoraggio automatizzato con l'apprendimento automatico viene utilizzato per condurre un'analisi del traffico e per fornire informazioni contestuali sulla fuga e sulla manomissione dei dati, sulle violazioni delle policy relative ai dati, sui comportamenti sospetti e sugli attacchi alla sicurezza delle API. La protezione del runtime rileva le anomalie e le potenziali minacce nel traffico delle API e semplifica la mitigazione basandosi su policy di risposta agli incidenti predefinite.

La protezione del runtime si integra con soluzioni WAF, gateway API, ITSM, SIEM e altri strumenti di workflow per fornire una difesa olistica dagli attacchi. Potete scegliere di automatizzare totalmente la mitigazione delle minacce o richiedere diversi livelli di intervento manuale per migliorare le caratteristiche di visibilità e controllo. La soluzione Akamai API Security offre anche un'integrazione nativa con la piattaforma di Akamai che ci consente di bloccare gli indirizzi IP dei criminali direttamente sull'edge.

Generazione di ticket

Tramite l'apprendimento automatico, Akamai crea un modello per ogni API. Questo standard di riferimento del comportamento normale viene poi utilizzato per rilevare gli attacchi alla logica aziendale delle API, come le violazioni dell'autorizzazione a livello di

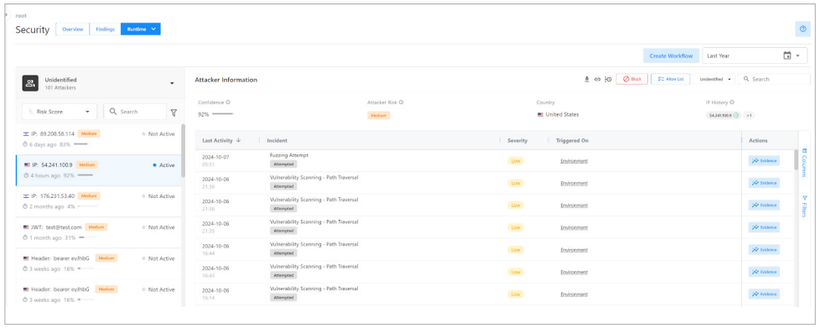
oggetto (BOLA, Broken Object Level Authorization), in cui i criminali riescono ad esfiltrare dati a cui non dovrebbero accedere. Akamai genera quindi un ticket in tempo reale ogni volta che il traffico delle API devia dal comportamento normale. Un ticket è molto simile ad un avviso e viene generato quando vengono rilevati errori di configurazione o comportamenti anomali delle API. Quando viene generato un ticket, il relativo avviso viene inviato automaticamente ad un sistema SIEM, come Splunk o QRadar, oppure ad un sistema di creazione di ticket, come ServiceNow o Jira.

Informazioni sui ticket

Ogni ticket generato dal modulo di protezione del runtime offerto dalla soluzione Akamai API Security include informazioni su gravità, stato, associazione con le 10 principali vulnerabilità della sicurezza delle API riportate nell'elenco OWASP e dettagli sui criminali, se disponibili.

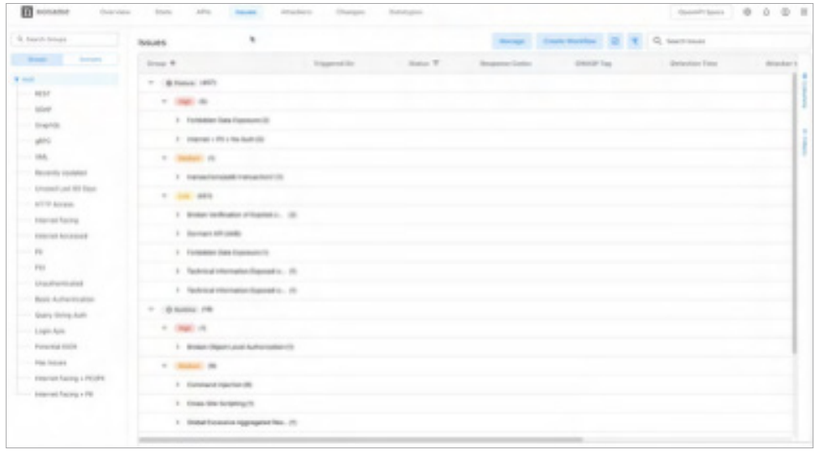
Le pagine delle informazioni sui ticket includono una descrizione del problema e del suo potenziale impatto sulla vostra organizzazione, oltre a fornire consigli per la sua risoluzione. Akamai API Security offre anche alle organizzazioni una visibilità sui tipi di azioni eseguite dai criminali in uno specifico periodo di tempo, con un record cronologico di ogni attacco, e la possibilità di intraprendere un'azione contro i criminali.

Esempio: visibilità sulle azioni dei criminali

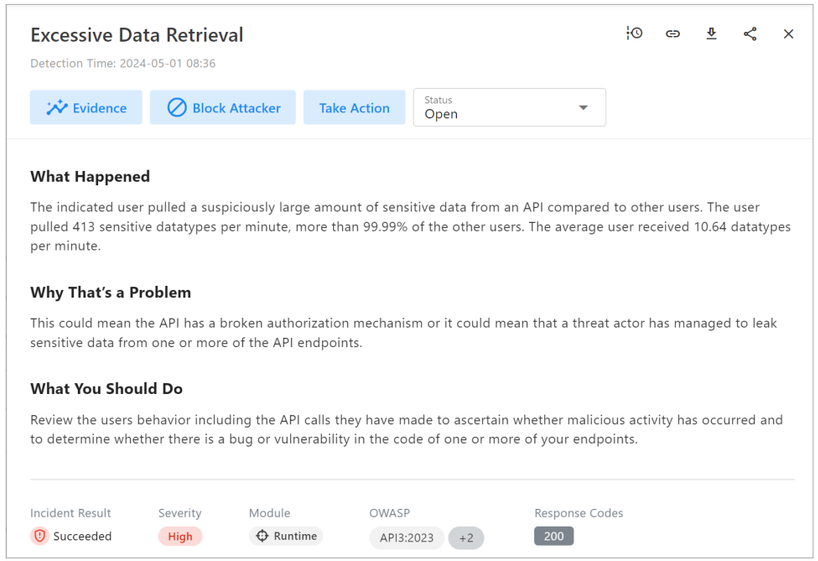


Ogni problema riscontrato include una relativa prova con i dettagli sulla sessione del criminale che ha fatto generare il ticket, nonché una copia della richiesta e della risposta delle API (intestazione e corpo della richiesta/risposta) per assistere nell'individuazione e nella risoluzione dei problemi in modo rapido. Con dashboard intuitive, funzioni di filtraggio, avvisi e funzionalità di generazione di rapporti, il modulo di protezione del runtime offerto dalla soluzione Akamai API Security può aiutare le organizzazioni a stabilire cosa è successo e perché, oltre a precisare cosa bisogna fare ora esattamente.

Esempio: generazione di ticket sulle API con prove



Esempio: informazioni sul recupero di una quantità eccessiva di dati



Azioni delle policy

Akamai API Security consente di eseguire un'azione per applicare una policy in modo semiautomatico per ogni ticket generato, ad esempio l'apertura di un ticket, l'invio di informazioni ad un sistema SIEM o l'invio di un webhook ad un sistema di terze parti oppure anche il blocco di un criminale. I tipi di azioni disponibili sono stabiliti in base alle integrazioni configurate nella piattaforma di Akamai.

La soluzione include numerose policy predefinite immediatamente disponibili per il rilevamento di errori di configurazione e attacchi alle API. Akamai API Security include anche più di 20 tipi di dati preconfigurati per aiutarvi a creare le policy di dati desiderati allo scopo di rilevare e intraprendere le azioni appropriate quando i dati sensibili attraversano le API.

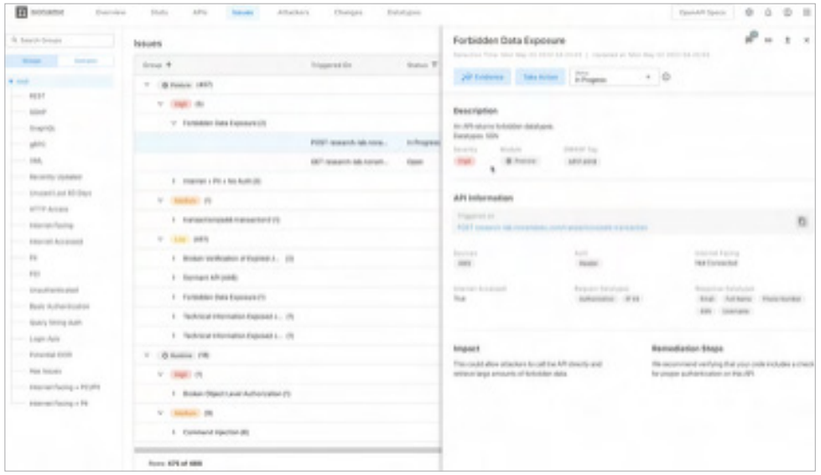
Riepilogando, il modulo di protezione del runtime offerto dalla soluzione Akamai API Security include funzioni di rilevamento e prevenzione degli attacchi alle API in tempo reale insieme ad un continuo rilevamento degli errori di configurazione delle API, in aggiunta alle integrazioni dei workflow più comuni che semplificano le operazioni e la mitigazione.

Anatomia di un problema di sicurezza delle API

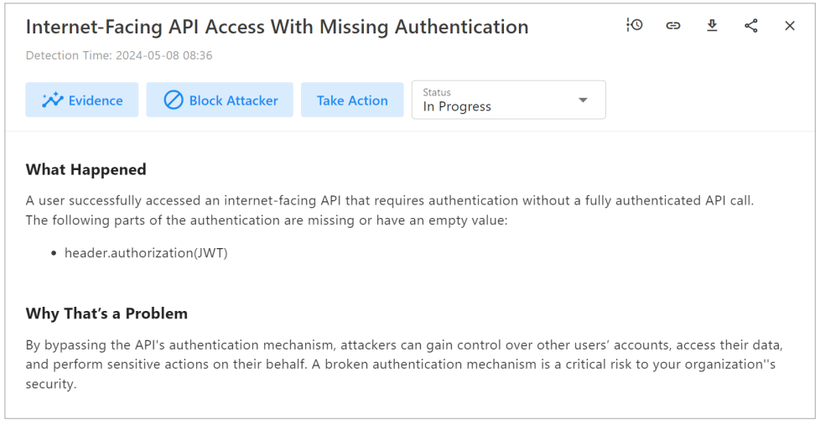
Esaminiamo più da vicino l'esempio di un'esposizione di dati riservati, che, in questo caso, si riferisce ad un problema di sicurezza interno ad un'API. La piattaforma di Akamai conosce il contesto dei tipi di dati e dei valori associati ad ogni API.

Nella figura seguente, i dati riservati sono resi visibili da un'API. La piattaforma di Akamai ha rilevato il tipo di dati trasmessi, in questo caso, un codice fiscale, e ha capito che questi dati, in precedenza, erano stati contrassegnati come riservati. Akamai, inoltre, consente di rilevare errori di configurazione esterni alle API, come API accessibili da Internet, ma non registrate con un gateway API.

Esempio: informazioni sull'esposizione di dati riservati



Esempio: identificazione di API non autenticate



Altre operazioni da eseguire per un'efficace protezione del runtime delle API

Ogni volta che un cliente, un partner o un vendor interagiscono con la vostra organizzazione in modo digitale, c'è un'API "dietro le quinte" che facilita un rapido scambio dei dati (spesso sensibili). Implementare le principali funzionalità di protezione del runtime delle API (ad esempio, il monitoraggio delle API per difendersi dagli errori di configurazione e dallo sfruttamento, nonché la prevenzione degli attacchi alle API) può aiutarvi a proteggere la vostra organizzazione da un vettore di attacco in rapida crescita.

Scoprite come valutare i vendor di soluzioni per la sicurezza delle API che offrono le principali funzionalità di protezione del runtime.

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

Akamai Security protegge le applicazioni che danno impulso alle vostre attività aziendali e rafforzano le interazioni, senza compromettere le performance o le customer experience. Tramite la scalabilità della nostra piattaforma globale e la visibilità delle minacce, possiamo unire le nostre forze per prevenire, rilevare e mitigare le minacce affinché voi possiate rafforzare la fiducia nel brand e realizzare la vostra visione. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito **akamai.com** o **akamai.com/blog** e seguite Akamai Technologies su **X** (in precedenza Twitter) e **LinkedIn**. Data di pubblicazione: 12/24.

Akamai