DESCRIZIONE DEL PRODOTTO AKAMAI

DNS Posture Management

Il DNS (Domain Name System) è un componente fondamentale dell'infrastruttura di ogni organizzazione, eppure spesso rimane una vulnerabilità trascurata. Errori di configurazione e risorse nascoste possono causare interruzioni dei servizi, violazioni dei dati e problemi di conformità, con conseguenze sia sulla sicurezza che sulla continuità aziendale.

Un approccio proattivo al monitoraggio, al rilevamento dei rischi e all'applicazione delle policy è fondamentale per prevenire interruzioni, mitigare le minacce e garantire la conformità alle normative di settore e di sicurezza.

Le sfide legate alla sicurezza del DNS

Oggi le organizzazioni devono affrontare una crescente complessità nella gestione del DNS a causa dell'evoluzione delle architetture di rete e delle implementazioni ibride e multicloud che coinvolgono più sistemi DNS. Le aziende hanno difficoltà a mantenere la visibilità negli ambienti di rete distribuiti in cui le attività IT nascoste, le migrazioni nel cloud e le acquisizioni creano record e zone DNS non documentati che espandono la superficie di attacco. Dal punto di vista tecnico, i team si trovano ad affrontare il rilevamento e la correzione di configurazioni errate, trasferimenti di zona non autorizzati e una gestione obsoleta dei record su diverse piattaforme DNS.

Senza un monitoraggio automatizzato, i team addetti alla sicurezza si affidano a processi manuali che introducono errori umani e non riescono ad applicare policy di sicurezza coerenti, rendendo le infrastrutture critiche vulnerabili agli attacchi basati su DNS, tra cui spoofing DNS, tunneling ed esfiltrazione dei dati. Questo approccio frammentato crea rischi significativi per la conformità, aumentando al contempo il tempo medio necessario per rilevare e risolvere i problemi, poiché i team addetti alla sicurezza non dispongono di strumenti completi che si integrino con i centri operativi di sicurezza esistenti.

Come Akamai DNS Posture Management può aiutare

Akamai DNS Posture Management è progettata per affrontare queste sfide direttamente, offrendo visibilità end-to-end, automazione e mitigazione dei rischi per la vostra infrastruttura DNS. Fornisce un'unica visione centralizzata consolidando zone, domini, sottodomini DNS e record di tutti i provider di servizi DNS, contribuendo a eliminare le lacune di visibilità e a migliorare l'efficienza. Questo approccio centralizzato semplifica le complessità legate alla gestione della sicurezza del DNS in ambienti multi-vendor, consentendo alle organizzazioni di monitorare, proteggere e ottimizzare la propria infrastruttura DNS da un'unica piattaforma.

Vantaggi per le aziende

Tracciamento dell'inventario DNS
Individuate e gestite le risorse del DNS tra i provider con un contesto completo delle risorse per una migliore supervisione

Maggior livello di visibilità
Ottenete un'unica visione centralizzata dei vostri ambienti DNS, tra cui AWS Route 53, Akamai Edge DNS, Google Cloud DNS e molti altri

Rilevamento delle configurazioni errate
Identificate e affrontate rapidamente le vulnerabilità basate sulla configurazione e le modifiche non autorizzate che potrebbero compromettere la sicurezza

Monitoraggio delle variazioni del DNS
Tenete traccia delle modifiche non autorizzate o inattese ai record del DNS, garantendo che le impostazioni del DNS siano in linea con le policy di sicurezza e le esigenze operative dell'organizzazione

Integrazione perfetta
Le funzionalità API headless consentono l'integrazione con le vostre piattaforme SIEM, SOAR, GRC, ITSM e XDR preferite

Protezione del proprio marchio
Identificate e gestite le minacce di phishing e impersonificazione con un monitoraggio continuo di domini analoghi falsificati

Mantenimento della conformità nel tempo
Contribuite a soddisfare i requisiti di conformità di oltre 15 quadri normativi (CIS, NIST, ISO, HIPAA, PCI-DSS e molti altri)

Gestione dei certificati
Monitorate e valutate i certificati digitali per prevenire rischi per la sicurezza quali certificati scaduti, configurati in modo errato o non autorizzati

Implementazione di una sicurezza pronta per il quantum
Preparatevi alle minacce quantistiche con il monitoraggio della crittografia post-quantistica (PQC, post-quantum criptography), che aiuta a garantire che la tua infrastruttura di certificati rimanga protetta da futuri attacchi quantistici prima che diventino realtà

Trasformare la complessa sicurezza del DNS in informazioni fruibili

Una potente interfaccia utente con dashboard intuitive consente agli utenti di effettuare ricerche senza problemi tra tutti i principali provider DNS, visualizzando relazioni e potenziali minacce (Figura 1). Gli avvisi sono classificati in base alla gravità, per garantire che i problemi critici ricevano attenzione immediata. Le funzionalità di monitoraggio in tempo reale rilevano i rischi emergenti, tra cui le variazioni del DNS che potrebbero indicare una compromissione della configurazione, identificando al contempo domini analoghi falsificati e di typosquatting che prendono di mira il vostro marchio.

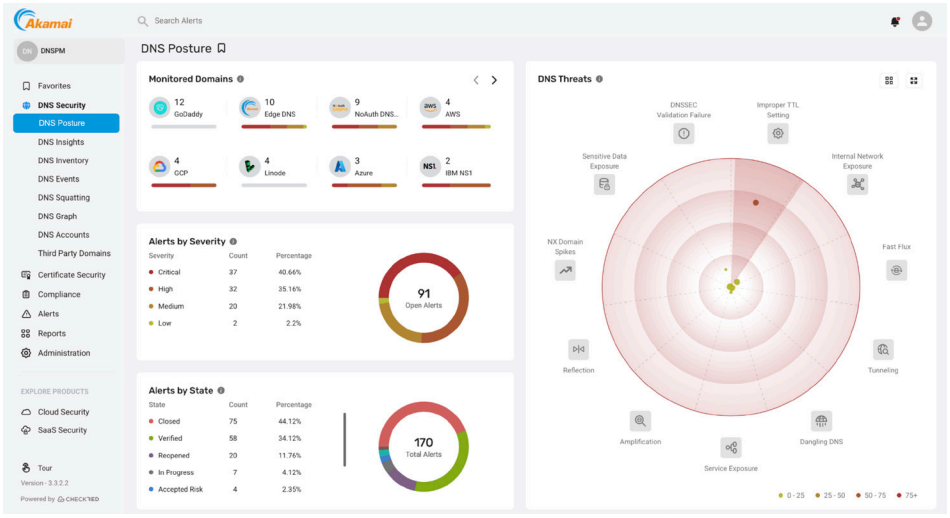

Fig. 1: Una dashboard potente offre visibilità e controllo completi sulle risorse DNS per rilevare e mitigare minacce e configurazioni errate

L'interfaccia utente offre inoltre una preziosa funzionalità di benchmarking del settore che fornisce un punteggio di rischio comparativo rispetto ai dati anonimizzati di aziende simili, aiutando le aziende a quantificare il proprio livello di sicurezza DNS rispetto alle altre aziende del settore (Figura 2).

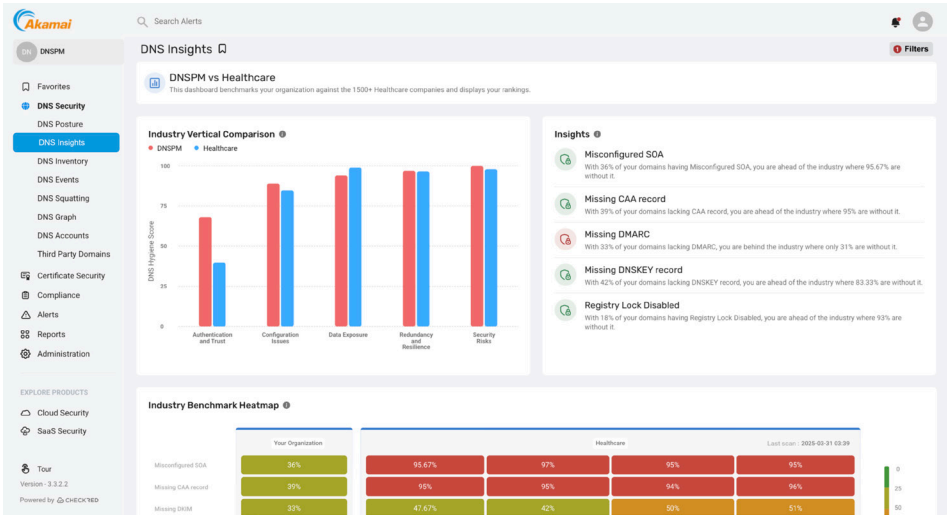

Fig. 2: Le organizzazioni possono operare un confronto del proprio livello di sicurezza rispetto a quello delle altre aziende del settore

Funzionalità principali

Copertura multi-provider

- Si integra perfettamente con tutti i principali provider DNS, tra cui Akamai Edge DNS, AWS Route 53, Azure DNS, Infoblox, Google Cloud DNS e molti altri, per una sicurezza coerente e un controllo centralizzato

Visibilità unificata in tutti gli ambienti

- Offre un'unica visione centralizzata di tutte le risorse del DNS (domini, sottodomini e record) che coprono più provider di servizi cloud e infrastrutture on-premise

Controlli approfondati delle policy

- Eseguite controlli e configurazioni completi delle policy nell'intera infrastruttura DNS, incluso il rilevamento di vulnerabilità CNAME, per scoprire le vulnerabilità prima che possano essere sfruttate; applicate regole estensibili per adattare i controlli di sicurezza DNS alle policy specifiche della vostra organizzazione e alle esigenze di conformità in continua evoluzione

Rilevamento e prevenzione proattivi dei rischi

- Non richiede alcuna installazione su endpoint o server, offrendo un'implementazione rapida, costi di gestione minimi e informazioni immediate sulle vulnerabilità

Reportistica e flussi di lavoro di mitigazione dinamici

- Fornisce assistenza con la mitigazione passo dopo passo con flussi di lavoro manuali, semiautomatizzati e completamente automatizzati, semplificando la risoluzione dei problemi in modo rapido ed efficace

Abilitazione della conformità

- Aiuta le organizzazioni a mantenere la conformità (seguendo i benchmark Center of Internet Security [CIS]), a ridurre i rischi normativi e a mantenere la fiducia dei clienti attraverso controlli continui delle policy e report completi

Gestione del sistema dei certificati

- Identificate i certificati TLS/SSL configurati in modo errato o scaduti per ridurre l'esposizione e supportare la prontezza degli audit

Akamai Managed Service (opzionale)

- Gli specialisti del Security Operations Command Center monitorano attivamente la vostra infrastruttura DNS per fornire suggerimenti proattivi sulle vulnerabilità e garantire supporto di emergenza per le minacce rilevate

Per ulteriori informazioni, visitate il sito akamai.com/it o contattate il team di vendita di Akamai.