INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

DNS Posture Management

El sistema de nombres de dominio (DNS) es un componente esencial de la infraestructura web de toda empresa, pero a menudo sigue siendo una vulnerabilidad que se pasa por alto. Los errores de configuración y los activos ocultos pueden provocar interrupciones del servicio, filtraciones de datos y fallos de cumplimiento, lo que afecta tanto a la seguridad como a la continuidad del negocio.

Un enfoque proactivo de la supervisión, la detección de riesgos y la aplicación de políticas es crucial para evitar interrupciones, mitigar las amenazas y garantizar el cumplimiento de las normativas del sector y de seguridad.

El desafío de la seguridad de DNS

Hoy en día, las organizaciones se enfrentan a una complejidad cada vez mayor a la hora de gestionar su estrategia de DNS debido a la evolución de las arquitecturas de red y las implementaciones híbridas y multinube que implican varios sistemas de DNS. Las empresas tienen dificultades para mantener la visibilidad en los entornos de red distribuidos, donde la TI en la sombra, las migraciones a la nube y las adquisiciones crean zonas de DNS no documentadas y registros que amplían la superficie de ataque. Desde el punto de vista técnico, los equipos se enfrentan a la detección y corrección de errores de configuración, transferencias de zonas no autorizadas y limpieza de registros obsoletos en plataformas de DNS dispares.

Sin una supervisión automatizada, los equipos de seguridad dependen de procesos manuales que introducen errores humanos y no aplican políticas de seguridad coherentes, lo que hace que la infraestructura esencial quede vulnerable a los ataques basados en DNS, como la suplantación de identidad de DNS, los túneles y la exfiltración de datos. Este enfoque fragmentado crea importantes riesgos de cumplimiento y, al mismo tiempo, aumenta el tiempo medio para detectar y corregir problemas, ya que los equipos de seguridad carecen de herramientas completas que se integren con los centros de operaciones de seguridad existentes.

Cómo ayuda Akamai DNS Posture Management

Akamai DNS Posture Management se ha diseñado para abordar estos desafíos de raíz al proporcionar visibilidad, automatización y mitigación de riesgos de forma integral para su infraestructura de DNS. Proporciona una vista unificada mediante la consolidación de zonas de DNS, dominios, subdominios y registros de todos los proveedores de DNS, lo que ayuda a eliminar las brechas de visibilidad y a mejorar la eficiencia. Este enfoque centralizado simplifica las complejidades de la gestión de la seguridad de DNS en entornos de varios proveedores, lo que permite a las organizaciones supervisar, proteger y optimizar su infraestructura de DNS desde una única plataforma.

Ventajas para su empresa

- **Realice un seguimiento del inventario de DNS**
  Localice y gestione los activos de DNS en todos los proveedores con un contexto completo de los activos para mejorar la supervisión
- **Obtenga una visibilidad eficaz**
  Obtenga una vista unificada de todos sus entornos de DNS, incluidos AWS Route 53, Akamai Edge DNS, Google Cloud DNS y muchos más
- **Detecte errores de configuración**
  Identifique y solucione rápidamente las vulnerabilidades basadas en la configuración y los cambios no autorizados que puedan poner en peligro la seguridad
- **Supervise la desviación del DNS**
  Realice un seguimiento de los cambios no autorizados o inesperados en los registros de DNS, y asegúrese de que la configuración de DNS se ajuste a las políticas de seguridad y las necesidades operativas de su organización
- **Integre los productos a la perfección**
  Las capacidades de API sin interfaz permiten la integración en sus plataformas SIEM, SOAR, GRC, ITSM y XDR favoritas
- **Proteja su marca**
  Identifique y gestione las amenazas de phishing y suplantación con supervisión continua de dominios similares
- **Mantenga el cumplimiento continuo**
  Ayude a cumplir los requisitos de cumplimiento de más de 15 marcos (CIS, NIST, ISO, HIPAA, PCI-DSS, y muchos otros)
- **Gestione los certificados**
  Supervise y evalúe los certificados digitales para evitar riesgos de seguridad derivados de certificados caducados, mal configurados o no autorizados
- **Implemente una seguridad preparada para los ataques cuánticos**
  Prepárese para las amenazas cuánticas con la supervisión de la criptografía poscuántica (PQC), que ayuda a garantizar que su infraestructura de certificados permanece protegida contra futuros ataques cuánticos antes de que se conviertan en realidad

Transforme la compleja seguridad de DNS en inteligencia útil

Una potente interfaz de usuario (IU) con paneles intuitivos permite a los usuarios buscar a la perfección problemas en los principales proveedores de DNS a través de la visualización de las relaciones y las amenazas potenciales (Figura 1). Las alertas se priorizan por gravedad, lo que garantiza que los problemas críticos reciban atención inmediata. Las capacidades de supervisión en tiempo real detectan riesgos emergentes, incluida la desviación del DNS que podría indicar que la configuración está en riesgo, al tiempo que identifican dominios similares y typosquatting que se dirigen a su marca.

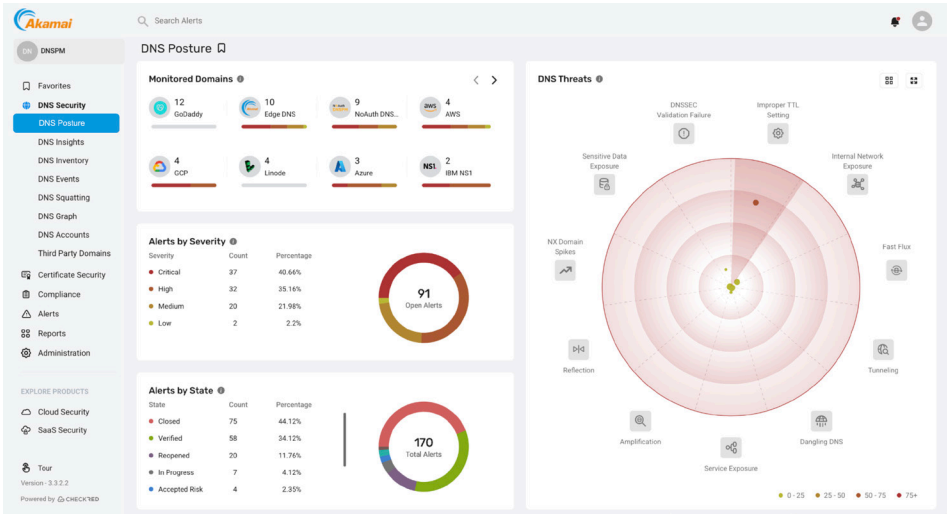

Fig. 1: El potente panel proporciona visibilidad y control completos de los activos de DNS para detectar y corregir amenazas y configuraciones erróneas

La interfaz de usuario también proporciona una valiosa función de evaluación comparativa del sector que proporciona una puntuación de riesgo comparativa con respecto a datos anónimos de empresas similares, lo que ayuda a las empresas a cuantificar su estrategia de seguridad de DNS con respecto a sus homólogos del sector (Figura 2).

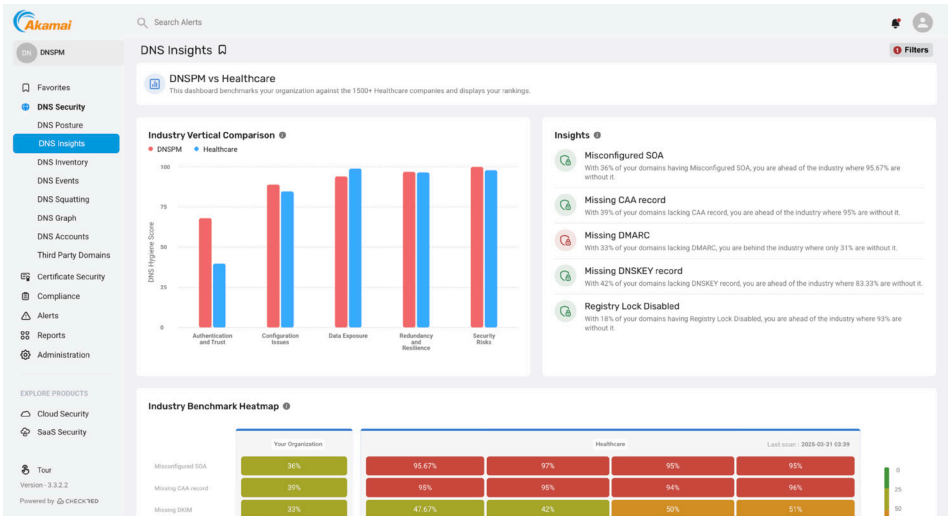

Fig. 2: Las organizaciones pueden comparar su estrategia de seguridad con la de otras empresas del sector

Capacidades clave

Cobertura de varios proveedores

- Se integra a la perfección en los principales proveedores de DNS, incluidos Akamai Edge DNS, AWS Route 53, Azure DNS, Infoblox, Google Cloud DNS, y muchos otros, para una seguridad coherente y un control centralizado.

Visibilidad unificada en todos los entornos

- Ofrece una vista unificada de todos los activos de DNS (dominios, subdominios y registros) de los diversos proveedores de nube y de la infraestructura local.

Comprobaciones exhaustivas de políticas

- Lleve a cabo comprobaciones y configuraciones de políticas exhaustivas en toda su infraestructura de DNS, incluida la detección de dispositivos CNAME colgantes, para descubrir vulnerabilidades antes de que se puedan explotar; aplique reglas extensibles para adaptar las comprobaciones de seguridad de DNS a las políticas únicas y a las necesidades cambiantes en materia de cumplimiento de su organización.

Detección y prevención de riesgos proactivas

- No requiere instalación en terminales ni servidores, lo que permite una implementación rápida, una inversión mínima e información inmediata sobre las vulnerabilidades.

Informes y flujos de trabajo de corrección dinámicos

- Proporciona orientación paso a paso sobre la corrección con flujos de trabajo manuales, semiautomatizados y totalmente automatizados, lo que facilita la resolución de problemas de forma rápida y eficaz.

Habilitación del cumplimiento

- Ayuda a las organizaciones a mantener el cumplimiento (siguiendo los puntos de referencia del Center of Internet Security [CIS]), reducir el riesgo de incumplimiento de normativas y mantener la confianza del cliente mediante comprobaciones continuas de políticas y elaboración de informes exhaustivos.

Gestión de la situación de los certificados

- Identifique certificados TLS/SSL mal configurados o caducados para reducir la exposición y respaldar la preparación para auditorías.

Akamai Managed Service (opcional)

- Los especialistas de Security Operations Command Center supervisan activamente su infraestructura de DNS para proporcionar recomendaciones proactivas para las vulnerabilidades y ofrecer asistencia de emergencia para las amenazas detectadas.

Para obtener más información, visite akamai.com/es o póngase en contacto con su equipo de ventas de Akamai.