AKAMAI 제품 설명서

DNS Posture Management

DNS(도메인 네임 시스템)는 모든 기업 인프라의 핵심 요소지만, 여전히 자주 간과되는 취약점입니다. 설정 오류나 숨겨진 자산은 서비스 중단, 데이터 유출, 컴플라이언스 위반으로 이어져 보안과 비즈니스 연속성에 영향을 줄 수 있습니다.

서비스 중단을 방지하고 위협을 방어하며 업계 및 보안 규정을 준수하려면 모니터링, 리스크 탐지, 정책 적용에 대한 선제적 접근이 필수입니다.

DNS 보안의 과제

오늘날 기업은 하이브리드 및 멀티클라우드 환경에서 다양한 DNS 시스템을 운영해야 하며, 복잡한 네트워크 아키텍처로 인해 DNS 보안 체계를 유지하는 데 어려움을 겪고 있습니다. 섀도 IT, 클라우드 전환, 인수합병 등으로 인해 문서화되지 않은 DNS 영역과 레코드가 생성되면서 공격 표면이 확대되고, 분산된 네트워크 환경 전반에 대한 가시성을 유지하는 것이 어려워지고 있습니다. 기술적으로는 서로 다른 플랫폼 간의 설정 오류, 무단 영역 전송, 오래된 레코드 처리 문제를 탐지하고 해결하는 데 어려움이 있습니다.

자동화된 모니터링이 부재한 환경에서 보안팀은 인적 오류가 발생할 수 있는 수동 프로세스에 의존하게 되고 일관된 보안 정책을 적용하지 못해 DNS 기반 공격(DNS 스푸핑, 터널링, 데이터 유출 등)에 취약한 핵심 인프라를 노출시킵니다. 이렇게 접근 방식이 세분화됨에 따라 보안팀에 기존 보안 운영 센터와 통합된 포괄적인 툴이 부족하게 되어 컴플라이언스 리스크가 커지고 문제 탐지 및 해결에 소요되는 평균 시간을 길어집니다.

Akamai DNS Posture Management가 지원하는 방법

Akamai DNS Posture Management는 DNS 인프라의 가시성, 자동화, 리스크 방어를 제공해 이러한 과제를 직접 해결하도록 설계되었습니다. 모든 DNS 공급업체의 DNS 영역, 도메인, 서브도메인, 레코드를 통합해 단일 창에서 관리할 수 있는 가시성을 제공함으로써 가시성의 격차를 제거하고 효율성을 높입니다. 이처럼 중앙 집중화된 접근 방식은 멀티 벤더 환경에서도 DNS 보안을 간편하게 관리할 수 있게 해 주며, 기업은 단일 플랫폼을 통해 DNS 인프라를 모니터링, 보호, 최적화할 수 있습니다.

기업이 누릴 수 있는 장점

DNS 인벤토리 추적
공급업체 전반에 걸쳐 DNS 자산을 파악하고 관리하며 자산의 전체 맥락을 기반으로 관리하여 통제력을 강화합니다

강력한 가시성 확보
AWS Route 53, Akamai Edge DNS, Google Cloud DNS 등 DNS 환경 전반에 걸쳐 단일 보기를 제공합니다

설정 오류 탐지
설정 기반 취약점 및 보안 위협을 초래할 수 있는 무단 변경을 신속하게 식별하고 대응합니다

DNS 드리프트 모니터링
무단 또는 예상치 못한 DNS 레코드 변경을 추적해 DNS 설정을 기업의 보안 정책 및 운영 요구사항과 일치시킵니다

원활한 통합
헤드리스 API 기능을 통해 SIEM, SOAR, GRC, ITSM, XDR 플랫폼과 원활하게 통합할 수 있습니다

브랜드 보호
유사 도메인에 대한 지속적인 모니터링을 통해 피싱 및 위조 위협을 식별하고 관리합니다

지속적인 컴플라이언스 유지
CIS, NIST, ISO, HIPAA, PCI-DSS 등 15개 이상의 프레임워크 컴플라이언스 요구사항을 준수하는 데 도움을 줍니다

인증서 관리
디지털 인증서를 모니터링하고 평가해 만료된 인증서, 잘못 설정된 인증서 또는 악성 인증서 같은 보안 리스크를 방지합니다

양자 준비 보안 배포
미래의 양자 공격으로부터 인증서 인프라를 보호하는 PQC(Post-Quantum Cryptography) 모니터링을 통해 양자 위협에 대비합니다

복잡한 DNS 보안을 실행 가능한 인텔리전스로 전환

사용자는 직관적인 대시보드를 갖춘 강력한 UI(User Interface)를 통해 주요 DNS 공급업체 전체를 원활하게 검색하고 관계 및 잠재적 위협을 시각화할 수 있습니다(그림 1). 심각도에 따라 알림에 우선순위가 지정되므로 중요한 문제를 즉시 처리할 수 있습니다. 실시간 모니터링 기능은 설정 손상의 징후일 수 있는 DNS 드리프트를 포함한 새로운 리스크를 탐지하며, 브랜드를 표적으로 삼는 유사 도메인과 타이포스쿼팅 도메인도 탐지합니다.

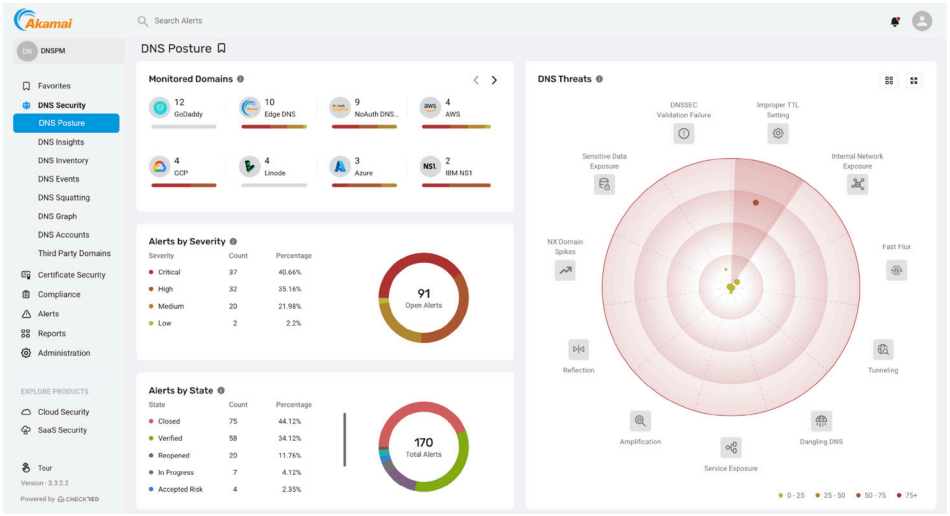

그림 1: 강력한 대시보드는 DNS 자산에 대한 완전한 가시성과 제어를 제공해 위협 및 설정 오류를 탐지하고 해결합니다.

UI가 유사한 기업으로부터 수집된 익명화된 데이터와 비교해 리스크 점수를 제공하는 가치 있는 업계 벤치마킹 기능을 제공하기 때문에 기업은 업계 동료와 비교해 DNS 보안 체계를 정량화할 수 있습니다(그림 2).

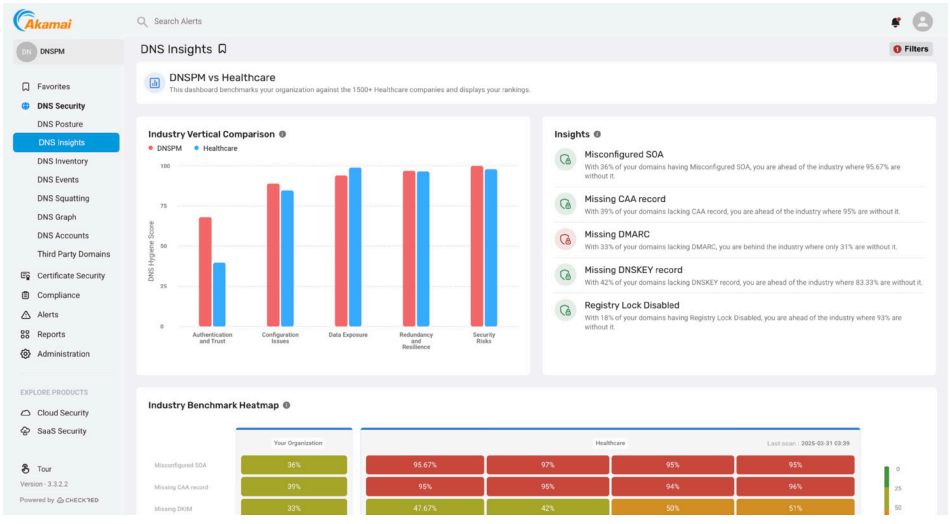

그림 2: 기업은 업계 동료와 비교해 보안 체계를 벤치마킹할 수 있습니다.

핵심 기능

다양한 공급업체 지원

- Akamai Edge DNS, AWS Route 53, Azure DNS, Infoblox, Google Cloud DNS 등을 포함한 주요 DNS 공급업체와 원활하게 통합되어 일관된 보안 및 중앙 집중식 제어를 제공합니다

환경 전반의 가시성 통합

- 다수의 클라우드 공급업체 및 온프레미스 인프라를 아우르는 모든 DNS 자산(도메인, 서브도메인, 레코드)에 대한 단일 보기를 제공합니다

심층 정책 검사

- DNS 인프라 전반에 걸쳐 광범위한 정책 검사 및 설정(CNAME 댕글러 탐지 포함)을 수행해 취약점이 악용되기 전에 발견합니다. 따라서 확장 가능한 룰을 적용해 기업의 고유한 정책 및 변화하는 컴플라이언스 요구사항에 맞춰 DNS 보안 검사를 실시할 수 있습니다

선제적 리스크 탐지 및 방지

- 엔드포인트나 서버에 설치가 필요 없어 빠른 배포, 최소한의 오버헤드, 취약점 발견 시 즉시 인사이트를 제공합니다

동적 복구 워크플로우 및 보고

- 수동, 반자동, 완전 자동화된 워크플로우를 통해 단계별 복구 지침을 제공해 문제를 신속하고 효과적으로 해결할 수 있습니다

컴플라이언스 지원

- 지속적인 정책 점검 및 포괄적인 보고서를 통해 기업이 CIS(Center of Internet Security)에 따라 컴플라이언스를 유지하고, 규제 리스크를 줄이고, 고객 신뢰를 유지하는 데 도움을 줍니다

인증서 체계 관리

- 잘못 설정되거나 만료된 TLS/SSL 인증서를 식별해 노출을 줄이고 감사 준비를 지원합니다

Akamai Managed Service(옵션)

- SOCC(Security Operations Command Center) 전문가들이 DNS 인프라를 실시간으로 모니터링해 취약점에 대한 사전 대응 권장 사항을 제공하고 탐지된 위협에 대한 긴급 지원을 제공합니다

자세한 내용은 akamai.com를 방문하거나 Akamai 영업 담당자에게 문의하시기 바랍니다.