AKAMAI 製品概要

DNS Posture Management

Domain Name System（DNS）は、あらゆる組織のインフラの重要なコンポーネントですが、見過ごされがちな脆弱性でもあります。設定ミスや隠れたアセットは、サービスの中断、データ漏えい、コンプライアンスの障害につながり、セキュリティとビジネス継続性の両方に影響を与える可能性があります。

サービス障害を防止し、脅威を緩和し、業界やセキュリティ規制へのコンプライアンスを確保するためには、監視、リスク検知、ポリシー適用に対するプロアクティブなアプローチが不可欠です。

DNS のセキュリティにおける課題

今日の組織では、ネットワークアーキテクチャの進化や、複数の DNS システムが関与するハイブリッドおよびマルチクラウドの展開により、DNS ポスチャの管理がますます複雑化しています。企業は、シャドー IT、クラウド移行、買収によって、文書化されていない DNS ゾーンやレコードが作成され、アタックサーフェスが拡大する分散ネットワーク環境全体の可視性をどう維持していくかに苦慮しています。技術面では、チームはさまざまな DNS プラットフォーム間で、設定ミス、不正なゾーン転送、古いレコードの健全性の検知と修正に取り組んでいます。

自動監視がない場合、セキュリティチームは、人為的ミスを招きがちで、一貫したセキュリティポリシーを適用できず、手作業によるプロセスに依存することになるため、重要なインフラは DNS スプーフィング、トンネリング、データ窃取などの DNS ベースの攻撃に対して脆弱なままになります。このように断片化されたアプローチでは、セキュリティチームが既存のセキュリティ運用センターと統合する包括的なツールを欠いているため、重大なコンプライアンスリスクを生み出し、問題の検知と修復にかかる平均時間を増加させます。

Akamai DNS Posture Management がどう役立つのか

Akamai DNS Posture Management は、前述の課題に正面から取り組むために設計されており、DNS インフラにおけるエンドツーエンドの可視性、自動化、リスク緩和を提供します。すべての DNS プロバイダーの DNS ゾーン、ドメイン、サブドメイン、レコードを 1 つの画面で表示できるため、可視性のギャップをなくし、効率性を向上させることができます。この一元化されたアプローチにより、マルチベンダー環境における DNS セキュリティ管理の複雑さが軽減され、組織は単一のプラットフォームから DNS インフラの監視、セキュリティの保護、最適化を行うことができます。

ビジネス上のメリット

DNS インベントリの追跡
完全な資産コンテキストにより、プロバイダー全体で DNS 資産を特定して管理し、監視を強化

強力な可視性
AWS Route 53、Akamai Edge DNS、Google Cloud DNS を含む DNS 環境全体を、1 つの画面で一元的に把握

設定ミスを検知
セキュリティを侵害する可能性のある設定ベースの脆弱性や不正な変更を迅速に特定して対処

DNS ドリフトの監視
DNS レコードに対する不正な変更や予期せぬ変更を追跡し、DNS 設定が組織のセキュリティポリシーや運用ニーズと一致していることを確認

シームレスな統合
ヘッドレス API 機能の統合により、お気に入りの SIEM、SOAR、GRC、ITSM、XDR プラットフォームへの統合が可能

ブランドを保護
類似ドメインの継続的な監視により、フィッシングやなりすましの脅威を特定して管理

継続的なコンプライアンスの維持
CIS、NIST、ISO、HIPAA、PCI-DSS など、15以上のフレームワークのコンプライアンス要件に対応

証明書の管理
デジタル証明書を監視および評価して、期限切れ、誤設定、不正な証明書などのセキュリティリスクを防止

量子に対応したセキュリティを展開
耐量子計算機暗号（PQC）監視により、将来の量子攻撃が現実になる前に、証明書インフラを確実に保護し脅威に備えます

複雑なDNSセキュリティを
実用的なインテリジェンスに変換

直感的なダッシュボードを備えた強力なユーザーインターフェース（UI）により、ユーザーは主要なすべての DNS プロバイダーをシームレスに検索し、関係性と潜在的な脅威を可視化できます（図1）。アラートは重大度別に優先されるため、重大な問題に即座に注意が向けられます。リアルタイム監視機能が、設定の侵害を示す可能性のある DNS ドリフトなどの新たなリスクを検知すると同時に、ブランドを標的とする類似ドメインやタイポスクワッティングドメインを特定します。

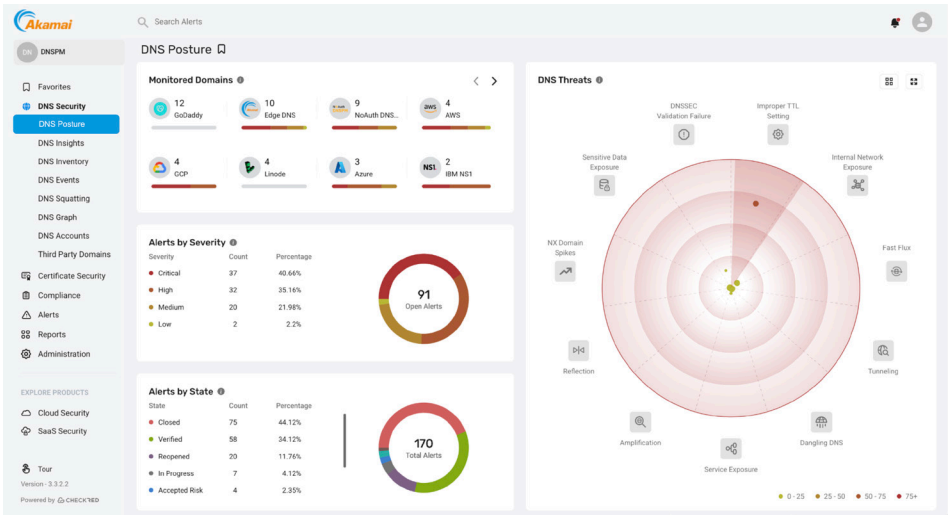

図 1：強力なダッシュボードによってDNS 資産を完全に可視化して制御し、脅威や設定ミスを検知して修正

また、このUIは、同業他社からの匿名化されたデータとリスクを比較評価する、業界の重要なベンチマーク機能も備えており、企業は同業他社と比べて自社の DNS セキュリティポスチャを定量的に評価することができます（図2）。

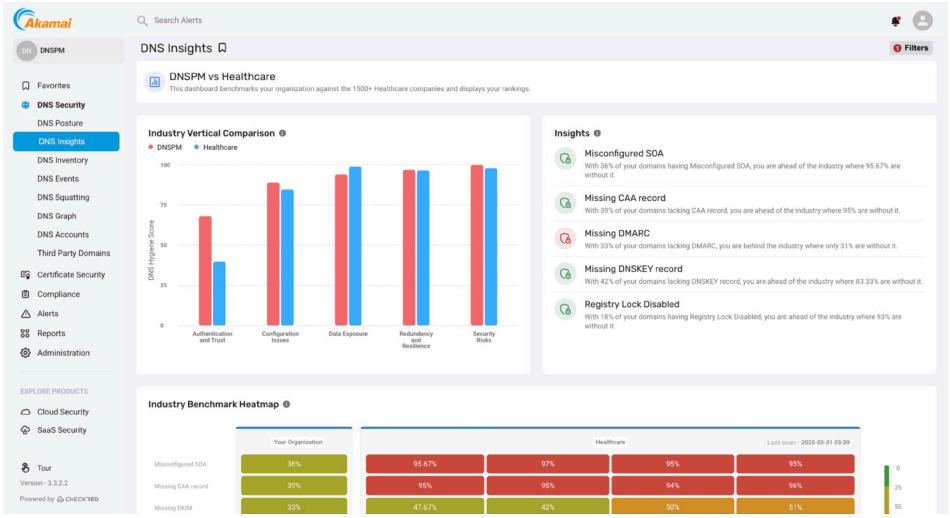

図 2：組織はセキュリティ態勢を同業他社と比較して評価できる

主な機能

マルチプロバイダー対応

- Akamai Edge DNS、AWS Route 53、Azure DNS、Infoblox、Google Cloud DNS など、すべての主要な DNS プロバイダーをシームレスに統合し、一貫したセキュリティと一元管理を実現します。

環境全体で統一された可視性

- 複数のクラウドプロバイダーおよびオンプレミスインフラ全体で、すべての DNS 資産を一元的に表示します。

詳細なポリシーチェック

- DNS インフラ全体で広範なポリシーチェックと設定（ダングリングになっている CNAME レコードの検知など）を実施して、脆弱性が悪用される前に発見します。また、拡張可能なルールを適用して、組織固有のポリシーや進化するコンプライアンスニーズに合わせて DNS セキュリティチェックをカスタマイズします。

プロアクティブなリスク検知と防止

- エンドポイントやサーバーにインストールする必要がないため、迅速な展開、最小限のオーバーヘッド、脆弱性に関する即座の知見を提供できます。

動的な修復ワークフローとレポート

- 手動、半自動、完全自動のワークフローにより、段階的な修正ガイダンスを提供し、問題を迅速かつ効果的に解決します。

コンプライアンスの実現

- 継続的なポリシーチェックと包括的なレポート作成により、組織がコンプライアンスを維持し（Center of Internet Security（CIS）ベンチマークに準拠）、規制によるリスクを軽減し、お客様の信頼を維持できるよう支援します。

証明書のポスチャ管理

- TLS／SSL 証明書の誤設定や有効期限切れを特定し、リスクの軽減と、監査対応の強化を支援します。

Akamai Managed Service（オプション）

- Security Operations Command Center のスペシャリストがお客様の DNS インフラを積極的に監視し、脆弱性に関する予防的な推奨事項を提供し、検知された脅威に対する緊急サポートを提供します。

詳細については、www.akamai.com/ja または Akamai の営業担当チームにお問い合わせください。