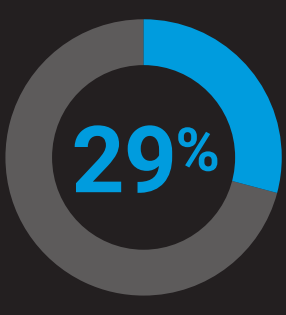
10 YEARS OF SECURITY INSIGHT

影に潜む脅威

攻撃トレンドで API の脅威を解き明かす

API の普及は、現代のエンタープライズにイノベーションの促進と効率化をもたらしました。しかし、セキュリティチームはこれらの API がもたらすリスクの規模と複雑さを把握することに苦労しています。ほとんどの組織は、文書化されていない API やシャドー API についてすべて説明することさえできず、境界内に侵入口を作っています。Akamai の最新の調査レポートでは、API 攻撃の最新トレンドに光を当てています。

API の課題が浮き彫りに



2023 年のすべての Web 攻撃のうち API を標的とした攻撃の割合

API 攻撃ベクトルトップ 3

44%
HTTP 攻撃

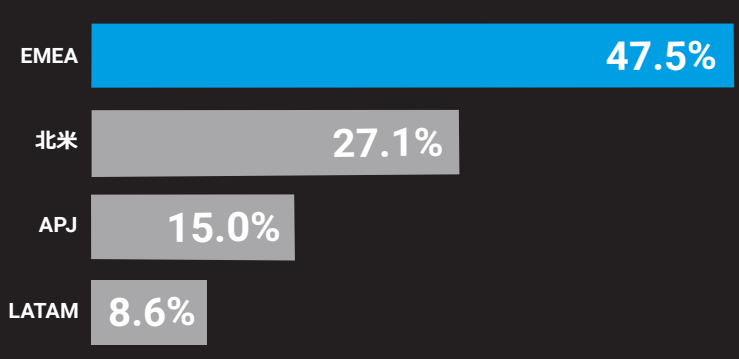
25%
アクティブセッション

14%
SQL インジェクション

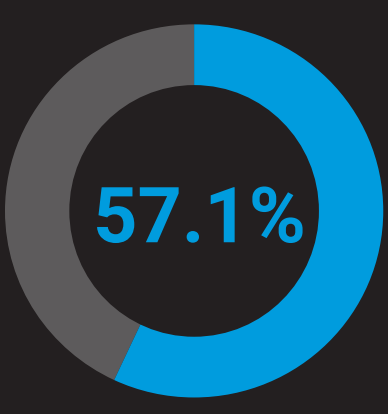
数字で見る API の情勢

地域別の API 攻撃の割合

2023 年 1 月 1 日～2023 年 12 月 31 日



欧州・中東・アフリカ（EMEA）地域は API を標的とした攻撃の割合が全世界で最も多く、47.5% でした。



自社の API インベントリーの精度が 25% ～ 75% であると推定した回答者の割合

2023 年度版 API セキュリティに関する SANS の調査に基づく

API 攻撃を受けることの多い業界トップ 3

- コマース
- ビジネスサービス
- その他のデジタルメディア

組織に対する 3 つの質問

API の悪用と窃取は、OWASP API Security Top 10 で説明されている脆弱性以外にも拡大する可能性があります。自社に包括的なセキュリティ戦略があることを確認するために、次の項目にチェックを入れてください。

- ☐ **脆弱性**：API を使用した開発のためのベストプラクティスを実践していますか？
- ☐ **可視性**：プログラムがすべての API を保護していることを確認するためのプロセスと技術的な制御を備えていますか？
- ☐ **ビジネスロジックの悪用**：不審なアクティビティを特定するために、通常の API トラフィックのベースラインを把握していますか？

なぜ可視性が重要か

API の脆弱性は組織の環境への侵入口です。攻撃者に悪用される前に、脆弱性を見つける必要があります。

API の世界を守る

API を保護する方法

- ✔ すべての API が文書化され API セキュリティコントロールに組み込まれていることを確認し、可視性を強化する
- ✔ API の誤設定の問題に対処し、将来の脆弱性の発生を防止するプロセスを実施する
- ✔ 攻撃者に利用される前にセキュリティギャップを埋めるため、API のモニタリングと脅威ハンティングの原則を確立する
- ✔ OWASP API Security Top 10 のリスクから従来の Web 攻撃まで、あらゆる脅威を緩和できるソリューションを選択する
- ✔ 最も一般的な攻撃を防ぐためのコーディングプラクティスに関する OWASP のガイダンスを活用する
- ✔ ビジネスロジックの悪用やその他の異常を検知するための、ふるまい分析を提供するセキュリティソリューションを使用する

身近な API にコンプライアンスが求められるように

PCI DSS v4.0 には、データ侵害リスクの低減を目的とする、システムやソフトウェアの開発と保守における API 使用方法に関する新しい基準が含まれています。

シフトレフトによる攻撃の防止

コーディングのベストプラクティスには、本番環境前に API をテストすることや、API ライフサイクル全体を通してセキュリティを強化することが含まれます。

レポート全文では API 攻撃のトレンドと対策についてより詳しく説明しています。ぜひお読みください。

レポート（英文）をダウンロード

| 公開日 2024 年 3 月