AKAMAI データシート

API Security ShadowHunt

API Security ShadowHunt は、Akamai のマネージド型脅威ハンティングサービスです。API 脅威ハンティングに熟達した Akamai のエキスパートアナリストが貴社のセキュリティチームを支援します。スタッフが不足しているチームや API セキュリティの専門知識がないチームにとって、リスクを軽減するために役立つアウトソーシングソリューションです。脅威ハンターは、お客様のチームの一部として機能し、API トラフィックに隠れている極めて見つけづらい難読化された攻撃を検知して報告します。

API Security ShadowHunt の仕組み

ShadowHunt のオペレーションは、API Security プラットフォームの API アクティビティデータから始まります。この自動分析により、異常なふるまいや脆弱性の悪用が検知され、機械学習からの信号が ShadowHunt アナリストに送信されて調査が行われます。ここからは、専門知識を備えた人間の出番です。

お客様の API 資産に精通したアナリストがアクティブな脅威を迅速に特定し、ShadowHunt Alert を作成して送信します。調査結果にあいまいな点がある場合は、アナリストが ShadowHunt のサービス加入者に連絡して確認します。アナリストと API Security 調査チームは、脅威インテリジェンス情報を利用して、すべてのサービスをご利用のお客様に定期的に新しい脅威に関するレポートを提供します。

API Security + 人間の専門知識

API Security プラットフォームは、次のような総合的な API セキュリティ機能を提供します。

- **API ディスカバリー：**広範かつ継続的な API ディスカバリー
- **リスク状況：**API のリスクを把握
- **ふるまい分析による脅威検知：**Akamai のクラウドベースのビッグデータ分析エンジンが、時間の経過にあわせてすべての API アクティビティを検査し、API の悪用を継続的に検知
- **予防と対応:**カスタマイズされた条件付き対応プレイブックにより、セキュリティと API DevSecOps プロセスを強化
- **調査と脅威ハンティング：**強力な調査機能により、API トラフィックに隠れている脅威を検出することが可能

脅威ハンティングは、API Security プラットフォームの最も高度な機能の 1 つです。API Security ShadowHunt サービスは、脅威ハンティングのためのツール、専門知識、時間のいずれかがないお客様を対象としています。

ビジネス上のメリット

- エキスパートが API アクティビティを調査しているという安心感
- API データに潜むセキュリティ上の脅威の検知
- Akamai が API セキュリティに集中的に取り組み、お客様のチームは時間的余裕を獲得
- ソフトウェア開発と IT 運用の実用的なインサイト
- 追加の厳格な精査により、API のふるまいに対する可視性を向上

頼りになる API Security ShadowHunt サービス

アラート：API 資産内の脅威を通知します。アラートは API Security ShadowHunt サービスの最も重要な要素であり、アクティブなインシデントが確認されると直ちに送信されます。アラートには以下が含まれます。

- インシデントの調査結果と分析
- インシデントに関する脅威インテリジェンスの概要
- 改善提案

脅威レポート：API セキュリティインテリジェンスを早い段階で得られます。API Security ShadowHunt Emerging Threat Report は、チームがアクセスできるグローバルな脅威インテリジェンス、API Security 調査チームからのインプット、継続的な脅威ハンティング活動に基づいています。Emerging Threat Report には次のものが含まれます。

- チームが特定した新しい API の脆弱性、脅威、攻撃の詳細
- API 資産への影響
- 改善提案（必要な場合）

月次レビュー：API 環境を完全に可視化します。ShadowHunt Monthly Threat Report は、毎月第 1 週に API Security を利用しているすべてのお客様に配信されます。レポートの内容は次のとおりです。

- 前月に送信された ShadowHunt Alert と Emerging Threat Report の概要
- お客様の API 資産の概要
- 過去 2 か月間の API アクティビティの比較
- API 業界のセキュリティに関するニュース

専門家に尋ねる：サービス加入者は、API Security ShadowHunt チームに連絡して、Alert と Emerging Threat Report の両方に関する質問や話し合いを行うことができます。

API Security を利用する理由

API Security は、脆弱性や API の悪用から API のセキュリティを確保するという課題に対し、広範な検知と対応（XDR）の原則を適用します。API アクティビティをクラウドベースのビッグデータ環境に集約して、複雑なデータエンリッチメントとオーガニゼーションを行うのは、API Security だけです。この独自のアーキテクチャにより、継続的な API ディスカバリー、リスクスコアリング、コンテキスト認識型のふるまい分析による API の悪用や脅威の検知、脅威ハンティングが可能になります。API Security アーキテクチャは、設計にプライバシーが組み込まれており、データレイクに向かうあらゆる API アクティビティをトークン化できます。

脅威ハンティングの専門知識で API を保護

API の導入が拡大すると、組織の IT セキュリティ部門に負担がかかる可能性があります。API Security ShadowHunt サービスがセキュリティ担当者を今すぐサポートします。

エキスパートによるコンサルティングで詳細をご確認ください。