2023 年 8 月 4 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai、ビジネス悪用やデータ窃盗から API を守る API Security を発表

※本リリースは 2023 年 8 月 2 日 (現地時間) マサチューセッツ州ケンブリッジで発表されたプレスリリースの抄訳版です。

オンラインライフの力となり、守るクラウド企業、Akamai Technologies, Inc.（NASDAQ：AKAM）は、API Security の提供開始を発表しました。これは、アプリケーション・プログラミング・インターフェース（API）への攻撃を阻止し、API 内部に潜む実装の脆弱性とビジネスロジックの悪用を検知する製品です。Akamai の API Security には、ふるまい分析を使用して API アクティビティを探索、監査、監視する機能があり、脅威や悪用を予防し、速やかに対処できます。

API への攻撃が増え続ける今日、API のセキュリティは組織にとって重大な懸念材料となっています。Akamai が最近発行したインターネットの現状レポートによると、2022 年には、アプリケーションと API への攻撃数が過去最多となりました。Web Application and API Protection（WAAP）製品を使用していても、なりすましなどで認可されてしまった API のふるまいや、データセンターやクラウド内部での API の利用状況まで可視化することはできません。攻撃者はこの盲点に気づき、広範な API アタックサーフェスの悪用へとシフトしています。

Akamai が独立したソリューションとして提供する API Security は、今年 4 月に発表された Akamai による Neosec の買収がもたらした成果です。この製品は、あらゆる API ゲートウェイ、WAAP、クラウド実装と併用できます。さらに、Akamai のお客様は、エッジサーバーに統合されたエッジコネクターを活用することも可能です。これにより、クリックするだけで、インテグレーションとモニタリングの開始にかかる時間、労力、コストを節約できます。

API Security は、API アクティビティを完全に可視化し、ふるまい分析を用いて複雑な脅威を検知するとともに、データレイクに独自に保存されている履歴データの分析を通じて検知能力をさらに高めます。また、API ディスカバリー、可視化、リスク監査の機能に加え、検知と対処を支援する広範な調査と脅威ハンティングを提供します。API Security の差別化要因ともいえる Shadow Hunt 脅威ハンティングのマネージドサービスでは、調査のために機械学習からのシグナルが人間のアナリストに提供されます。自社の API を把握できるということは、API アクティビティを記録し、侵害の可能性があればそれを検知し、顧客データの安全を維持できるということです。

金融テクノロジー企業、Earnin 社の CISO である Stan Lee 氏は「Akamai の API Security は、すべてのアプリケーションの重要な API を検出し監視するためにとても役立っています。当社は、この製品のおかげで、ビジネスプロセスのアジリティと成果を実現しながら、コンプライアンスとリスク管理を向上させることができます」と、述べています。

Akamai の Application Security 部門で Senior Vice President と General Manager を兼務する Rupesh Chokshi は「最近発生した情報漏えい事件から、API セキュリティソリューションが不可欠であることが痛いほど明らかとなりました。今や、API ベースの攻撃を防御するためにエンドポイントのガードと認証情報のチェックだけではもはや十分ではありません。また、Akamai の API Security を使用することで、組織はあらゆるプラットフォームやゲートウェイで API のふるまいを監視し、ビジネスプロセスが円滑かつ安全に機能していることを確認できます」と、述べています。

Forrester Research は、最近の攻撃を踏まえ、次のように API セキュリティの重要性を指摘しました。「API セキュリティは 2023 年注目のアプリケーション・セキュリティ・ツールです。API は 2022 年に何度かトップニュースに登場しました。たとえば、Optus は 980 万人の顧客の個人情報を盗まれ、身代金を要求されましたが、これは認証を求めることなく API が公開されていたためでした。被害にあったのは Optus だけではありません。Twitter、T-Mobile、そして法執行機関のアプリケーションまでもが、API の脆弱性によってデータを流出させました。一方で良いニュースもあります。グローバルセキュリティの意思決定者らが、2020 年から 2022 年までの期間に API セキュリティの採用が増加し、減速する兆しがないと報告しています。増加したセキュリティ予算は、API のインベントリとセキュリティ確保に充てるべきです」（State of Application Security,2023、Forrester Research,Inc.、2023 年 6 月 7 日）

API Security は、Akamai の既存製品である App & API Protector（AAP）ソリューションを補完するものです。これらを併用することで、最大限に包括的なグローバル防御が実現し、エンタープライズ規模の可視性、API アクティビティのふるまい分析、攻撃および悪用の防御を結びつけることができます。このジョイント戦略によって、以下のことが可能となります。

- 広範なディスカバリー：Akamai のコンテンツ・デリバリー・ネットワーク上および、それ以外のインフラ上の API を把握
- 複層型の検知：シグネチャーベースの検知とふるまい検知の両方を利用
- 個々の脅威にあわせた対処：インラインでの脅威ブロックや問題箇所の発見と修正を支援
- これらの防御機能すべてを 1 か所のコントロールセンターから簡単に導入。さらに、OWASP Top 10 および、API Security Top10 脆弱性の両方のリストに対応し、API 脅威ハンティングの専門知識への確実なアクセスを提供

Akamai について：

Akamai はオンラインライフの力となり、守っています。世界中の先進企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、世界中の人々の生活、仕事、娯楽をサポートしています。超分散型のエッジおよびクラウドプラットフォームである Akamai Connected Cloud は、アプリと体験をユーザーに近づけ、脅威を遠ざけます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。