エグゼクティブサマリー

クラウドの検知と対応における5/5/5ベンチマーク：「5秒で検知・5分でトリアージ・5分で対応」を実現

クラウドへの攻撃は高速です。脅威アクターは、悪用できるIT資産を見つけた後、平均で10分もかからずに攻撃を開始します。クラウド環境ではIDおよびアクセス管理、脆弱性管理、そして、その他の予防的制御が一般的ですが、組織を安全に守るためにはゼロデイエクスプロイト、インサイダー脅威、その他の悪意ある振る舞いに対処するための脅威検知や対応プログラムが必須です。

クラウドをセキュアに運用するには、新しいマインドセットが求められます。クラウドネイティブの開発とリリースのプロセスには、脅威の検知と対応にクラウドネイティブ独自の課題があります。アプリケーションのコードのコミット、ビルド、デリバリーを含むDevOpsのワークフローには、セキュリティプログラムの主要なプレーヤーとしての新しいチームとロールが関与しています。クラウド攻撃は、従来型のリモートコード実行の脆弱性を悪用するのではなく、ソフトウェアのサプライチェーンへのハッキングや、ヒューマンIDおよびノンヒューマン（マシン）IDの悪用に重点を置いています。また、短命なワークロードには、インシデントレスポンスとフォレンジックに対応する 強化されたアプローチが 必要となります。

クラウドセキュリティプログラムには、新しいベンチマークが必要なのです。「5秒で検知・5分でトリアージ・5分で対応」を意味する「5/5/5ベンチマーク」は、最新の攻撃に関する現実を認識した上で、クラウドセキュリティプログラムを推進することを企業や組織に課すものです。このベンチマークは、クラウド環境が防御者にもたらす課題と機会という文脈で説明されています。5/5/5ベンチマークを達成するには、攻撃者が攻撃を完了するよりも早くクラウド攻撃を検知し、それに対応する能力が必要となります。

sysdig

5秒で脅威を検知するには

課題

クラウド攻撃の初期段階は、クラウドプロバイダーのAPIやアーキテクチャが統一されているため、高度に自動化されています。このレベルのスピードで検知を行うには、コンピュートインスタンス、オーケストレーター、およびその他のワークロードから収集したテレメトリーが必要となりますが、多くの場合そのようなテレメトリーは利用できないか、または不完全なものとなります。効果的な検知には、マルチクラウドのデプロイメント、接続されたSaaSアプリケーション、およびその他のデータソースなど、多くの環境におけるきめ細かな可視性が必要です。

課題への対策

クラウドプロバイダーのインフラが統一されており、APIエンドポイントのスキーマが既知であることも、クラウドからのデータ取得を容易にしています。eBPFのようなサードパーティのクラウド検知テクノロジーの普及により、IaaSインスタンス、コンテナ、クラスタ、サーバーレス機能を深くタイムリーに可視化することが可能となっています。

クラウドサービスプロバイダーとクラウドセキュリティツールからの検知シグナルを5秒以内に収集し、短命な資産に関する可視性を確保します。

5分で相互関連付けとトリアージを実施するには

課題

単一のクラウドサービスプロバイダー内であっても、複数のコンポーネントやサービス間で相互関連付けを行うのは困難です。クラウドで利用できる圧倒的な量のデータには、セキュリティ上のコンテキストが欠けていることが多く、分析を行う責任はユーザーにあります。単独では、与えられたシグナルが持つセキュリティ上の意味を完全に理解することは不可能です。クラウドのコントロールプレーン、オーケストレーションシステム、およびデプロイされたワークロードは密接に絡み合っているため、攻撃者はこれらの間を容易に行き来することができます。

課題への対策

環境内および環境間のデータポイントを組み合わせることで、脅威検知チームに実用的なインサイトを提供します。アイデンティティは、クラウドにおける重要なコントロールであり、環境の境界を越えた活動の属性を特定することができます。「シグナルに関するアラート」と「実際の攻撃の検知」の違いは、セキュリティオペレーションチームによる手作業を可能な限り減らしつつ、点と点を迅速に結びつける能力にあります。

最初に関連するアラートを受信してから5分以内に、相互に関連付けられているすべてのシグナルについて完全なコンテキストを収集することで、トリアージを自動化します。

5分で対応するには

課題

クラウドアプリケーションは、多くの場合、サーバーレス機能とコンテナを使用して設計されており、その寿命は平均で5分未満です。従来型のセキュリティツールは、フォレンジック調査のために、長寿命ですぐに使えるシステムを期待しています。一方、最新の環境はその複雑さから、影響を受けるシステムとデータの完全なスコープを特定した上で、クラウドサービスプロバイダー、SaaSプロバイダー、パートナーやサプライヤーの全体を通じて適切な対応策を決定することが困難になります。

課題への対策

クラウド・アーキテクチャーは自動化を可能にします。また、IT資産の定義と導入のためのAPIおよびIaC（Infrastructure-as-Code）ベースのメカニズムを活用することで、セキュリティ上の迅速な対応と修正が可能になります。さらに、ハッキングされたIT資産を迅速に破棄し、それをクリーンなバージョンと置き換えることができるため、ビジネスの中断を最小限に抑えることができます。通常、対応を自動化しフォレンジック調査を実行するために、追加のセキュリティツールが必要になります。

クラウドの持つ柔軟性を利用することで、高精度の検知から5分以内に、戦術的な対応 を開始でき ます。

結論

5/5/5ベンチマークは、クラウドにおける成熟した脅威検知機能に関するベンチマークです。このレベルのベンチマークを達成するには、クラウド向けに最適化された人のマインドセットとツールやプロセスが必要となります。セキュリティ部門に対して、主なユースケースで5/5/5ベンチマークを達成するよう課すことで、脅威の検知と対応プログラムを大幅に改善できます。

sysdig

PB-030-JA REV. A 2/24