DNP

クラウドワークロードセキュリティ
パート２：AWS のセキュリティ機能

本稿は、5 部構成となる今日のクラウドセキュリティシリーズのパート 2 です。パート 1 では、クラウドセキュリティ戦略を開発する際に何に注力する必要があるかを、考慮すべきセキュリティ管理策とそれを実装するための最善のアプローチと合わせて議論しました。パート 1 に続き、Azure、AWS、GCP の 3 つの主要なクラウドプラットフォームで提供されるセキュリティツールとサービスについて取扱っていきます。

パート 2 では、アマゾンウェブサービス（AWS）が提供するセキュリティソリューションの機能と制限に焦点を当てます。AWS がワークロードのクラウドセキュリティ確保のために提供する追加ツールに加え、ネットワークセキュリティ、クラウドセキュリティ態勢管理、クラウドワークロード保護プラットフォーム、脆弱性管理、コンテナセキュリティ、SIEM について説明します。

ネットワークセキュリティ

ネットワークセグメンテーション

AWS は、オンプレミスネットワークと非常に近いネットワークモデルを使用しています。オンサイトのサーバールームで通常見られるものに似た概念、用語、仮想ネットワークトポロジを使用します。ネットワークエンジニアは慣れ親しんだ環境にいることに気づき、すぐに作業に取り掛かることができます。

AWS は、ネットワークコンセプトの最上位として、オンプレミスネットワーク全体にほぼ相当する仮想プライベートクラウド（VPC）を実装しています。サブネットとルートテーブルがこれに続きます。サブネットは非オーバーラップの CIDR ブロックを使用する VPC のセグメントで、ルートテーブルはサブネットに関連付けられており、ネットワークトラフィックフローに指示したり拒否したりします。サブネットからサブネット、インターネットとサブネット間のルーティングを制御できます。したがって、ワークロードの厳密な分離を実施するようにルーティングテーブルを構成できます。

ネットワークレベルのファイアウォール

AWS は、ネットワークファイアウォールに似たツールも提供します。ネットワークインターフェース

のレベルで機能するセキュリティグループ（SG）と、サブネットレベルで機能するネットワークアクセスコントロールリスト（NACL）です。SG を使用すると、サブネット内のトラフィックをさらに制限し、宛先ポート番号と送信元（IP アドレスまたは別のセキュリティグループ）に基づいたトラフィックのみを許可します。一方、NACL はステートレスであり、SG では不可能なトラフィックの明示的拒否が可能です。すでに SG を使用している場合にこの追加機能を除けば、NACL はそれほど有用ではありません。

注：別の SG 宛に許可されたトラフィックの送信元として SG を指定できるという事実は、非常に強力であり、さまざまな CIDR ブロックを入念に処理する代わりに、認可されたトラフィックパスを意味論的に構築できます。

Web アプリケーションファイアウォール

AWS は、独自の Web アプリケーションファイアウォール （WAF）を提供しています。WAF は、（通常はインターネット上の）クライアントと Web サーバーとの間の HTTP トラフィックを検査します。SQL インジェクション、クロスサイトスクリプティングなどの特定の攻撃から Web アプリケーションを保護するために、このトラフィックを監視し、フィルタリングします。AWS WAF は、インターネットからの入力を提供する他の AWS サービス、つまり Elastic Load Balancing、Amazon API Gateway、CloudFront とシームレスに統合されます。しかし、EC2 インスタンスの前で AWS WAF を直接使用することはできません。

AWS WAF を使用すると、独自の WAF ルールを作成できますが、OWASP トップ 10 セキュリティリスク等の一般的な脅威に簡単に対処できるマネージドルールもいくつか提供されます。最後に、Firewall Manager は、AWS WAF および VPC セキュリティグループ（SG）の管理を簡素化し、複数の AWS アカウント間でも実行できます。

DDoS 保護

標準形式の AWS Shield はデフォルトで有効になっており、最もよく見られる DDoS 攻撃からほとんどの AWS コンポーネントを保護します。AWS Shield Advanced は、より高度な DDoS 攻撃の保護と軽減を提供します。たとえば、NACL にルールを自動的に設定し、インターネットに直接公開されている EC2 インスタンスを防御できるようにします。

クラウドセキュリティ態勢マネジメント（CSPM）

セキュリティポリシーと構成の実施

AWS Config は非常に便利なツールであり、少なくとも CSPM 戦略の一部として評価すべきです。AWS リソース全体を継続的にスキャンし、AWS リソースの構成の変更を記録します。

このツールは、検出されたリソース構成をルールと比較し、アラートを送信したり、自動化された修復アクションを実行したりできます。AWS によって作成された事前定義されたルール（たとえば、公開されているポート 22 [SSH]がない）を使用することも、独自のカスタムルールを定義することもできます。AWS Config は、AWS ワークロードが特定の標準（HIPAA や PCI など）に準拠していることを確認するのにも役立ちます。

ランタイムセキュリティ評価

AWS Inspector は、EC2 インスタンスで実行時にセキュリティ評価を実行します。この評価は、CSPM の観点から役立ち、潜在的なセキュリティ問題を検出し、開発者と DevOps エンジニアが迅速に修正できるようにします。

さらに、AWS Security Hub は CSPM にも役立ちます。実際、継続的なセキュリティチェックとリソース構成チェックを自動化することができます。これは通常、特定のワークロードを PCI や CIS などの標準に準拠させるコンプライアンスプログラムの一部として実行されますが、このようなチェックは CSPM 戦略の一部として実行することもできます。

脆弱性管理

パッチ適用

AWS Systems Manager Patch Manager を使用すると、Linux および Windows インスタンスに存在する必要のあるパッチを定義できます。構成が完了すると、Patch Manager はバックグラウンドで動作し、選択したインスタンスに正しいパッチが適用されるようにします。適切に構成された Patch Manager は、インスタンスのオペレーティングシステムに既知の脆弱性がないことを確認します。そうは言っても、パッチと宛先マシンは手動で選択する必要があるため、パッチマネージャーの操作は非常に面倒な場合があります。事前定義された構成を提供しますが、特定のユースケースをカバーしていない可能性があります。

クラウドワークロード保護プラットフォーム（CWPP）

攻撃対象領域と攻撃を受ける可能性を減らす試みとして、環境をより安全にするためにさまざまな方法を適用できますが、必要なのは、攻撃が発生したときにそれを検出する機能です。CWPP はこの管理策を提供し、不正な悪意のあるコードやその他の悪意のあるアクティビティを警告することで、攻撃が未検出のままにならないようにします。CWPP は、コンピューティングリソースレベルに焦点を当て、ランタイム環境に関連する多数のパラメーターを監視して、疑わしいコードの実行をチェックします。これに

より、ソフトウェアとデータの保護の重要なレイヤーとして機能します。

AWS は CWPP を提供していないため、AWS ワークロードと完全に統合できるサードパーティのソリューションを探す必要があります。サーバーを適切に CWPP で保護するために、Intezer Protect などの外部プロバイダーがあります。Intezer は、ワークロード中心のアプローチを使用して、ハイブリッド環境とマルチクラウド環境の両方で、セキュリティ態勢の包括的な概要を一枚のウィンドウ画面で提供します。

コンテナセキュリティ

オープンソースプロジェクト Clair から提供されている Elastic Container Registry（ECR）は、Common Vulnerabilities and Exposures（CVE）データベースを使用して、保存されている Docker イメージをスキャンして既知の脆弱性を検出できます。このほかには、AWS は、少なくともこの記事の執筆時点（2020 年 11 月）では、追加の脆弱性管理ツールを提供していません。

Elastic Container Service（ECS）でコンテナを実行する場合、IAM ロールやセキュリティグループなど、EC2 インスタンスと同様のセキュリティ面があります。Elastic Kubernetes Service（EKS）でコンテナを実行する場合、AWS は RBAC やネットワークポリシーなどの標準の Kubernetes セキュリティ要素を提供します。

セキュリティ情報およびイベント管理（SIEM）

AWS は有名なサードパーティプロバイダーと接続しますが、自身に適切な SIEM ツールはありません。

AWS アカウントすべてのセキュリティステータスの包括的な概要については、Security Hub を使用できます。これにより、優先度の高いすべてのセキュリティアラートを確実に受信し、自動か手動かに関係なく、救済措置を講じることができます。

Security Hub はそれ自体が SIEM ソリューションではありませんが、集約等いくつか重要な SIEM のような機能を提供します。実際、すべての AWS サービスとサブスクリプションからのすべての結果を 1 か所で包括的に表示します。

追加の脅威検出機能

トラフィックを監視して異常を検出するには、Amazon GuardDuty が最適なツールです。これは、ネットワークトラフィック、S3 アクセス、AWS API コールなどの幅広いデータを分析するだけでなく、

機械学習と振る舞いモデルを使用して、暗号通貨マイニング、資格情報の侵害、異常なデータアクセス、既知の悪意のあるエンティティとの間の通信などの、悪意のあるアクティビティを特定するエージェントレスサービスです。

GuardDuty は、疑わしいアクティビティが検出されると、自動化された軽減を促進します。それ自体はクラウドワークロード保護プラットフォームの一部ではありませんが、Amazon GuardDuty は、エージェントベースの CWPP ソリューションへの便利な補完機能です。

利用可能なセキュリティログと監視

ログの取込と処理はパブリッククラウドの基本的な機能であるため、AWS は明確にデータプレーンロギングを提供し、このための独自のツールも備えています。CloudWatch Logs は、アプリケーション、サービス、およびオペレーティングシステムからログを取込み、処理し、保持することができます。付属のユーティリティである CloudWatch Logs Insights は、多数のログから情報をフィルタリングして、諺にあるように干し草の山から針を簡単に見つけるのにも役立ちます。

コントロールプレーンロギング用に提供されているさらに別のツールは CloudTrail です。これにより、誰が、何が呼び出しを行ったか、呼び出しの日時、呼び出したエンティティが呼び出しを許可されたまたは拒否されたかどうかなど、すべての AWS API コールをログに記録できます。CloudTrail にはいくつかのユースケースがあります。

・フォレンジックツールとして
・異常な活動を検出目的として
・監査可能性を要求する標準規格類へのコンプライアンス目的として

最後に、AWS は、VPC に出入りするネットワークトラフィックのログ記録とモニタリングを支援します。フローログを有効にして、これらの VPC に関連するすべてのネットワークトラフィックをログに記録することもできます。これには、ネットワークパケットの IP ヘッダから、パケットがアクセス許可または拒否されたかどうかまでのフィールドがいくつか含まれます。

注 : GuardDuty を使用したい場合は、VPC フローログを有効にする必要があります。GuardDuty はこれらのログを使用して疑わしいトラフィックを検出するためです。また、フォレンジック分析や特定の標準（HIPAA など）に準拠するために使用することもできます。

まとめ

結論として、AWS にはさまざまなセキュリティツールがあり、使用するソリューションを評価する際には、これらを最初に検討する必要があります。それでも、いくつかの例外を除けば、これらのツールを正しく理解して構成するのは非常に難しいかもしれません。AWS が（提供するソリューションが）不足している分野では、サードパーティのソリューションの使用が賢明な方法です。

重要なのは、「クラウドのセキュリティ」に関して、 AWS が常にセキュリティを最優先することは称賛に値することです。Amazon は、クラウドプラットフォームのセキュリティを危険にさらすようなことは絶対にしません。それによって、エキサイティングな新製品をリリースできなくなったり、よりユーザーフレンドリーな製品にする要求に応えられなくなったりしてもです。

サードパーティのソフトウェアは AWS Marketplace から、または直接ベンダーから入手できますが、AWS のセキュリティ製品は CWPP の面で特に不足しています。Intezer Protect は、特にリアルタイムでワークロードを保護するのに役立ちます。

全体として、AWS は、自社のインフラストラクチャ内のセキュリティを非常に厳しく把握していることで、当然のふさわしい評判を得ています。これは、提供するすべての製品で保証されているセキュリティを介してユーザーに受け継がれるものです。

■原文
Intezer Blog
Crowd Workload Security: Part 2 - Security Features of AWS (November 18 2020)
https://www.intezer.com/blog/cloud-workload-security-part-2-security-features-of-aws/
本稿は Intezer 社の許可を得て、同社のブログを翻訳したものです。翻訳を許諾いただいた Intezer 社に感謝します。
日本語版作成：2021 年 5 月

■権利帰属

■関連コンテンツ

クラウドワークロードセキュリティ

パート１： 知っておくべきこと

パート２： AWS のセキュリティ機能　<本稿>

パート３：Azure のセキュリティ機能の説明　<準備中>

パート４：GCP のセキュリティ機能説明　<準備中>

パート５：<準備中>