DNP

クラウドワークロードセキュリティ
パート４：GCP のセキュリティ機能

クラウド上のワークロードのセキュリティを確保する上で、適切な制御を備えた明確なセキュリティ戦略を持つことは、戦いの半分しか勝てないことを意味します。本シリーズでは、強力なクラウドセキュリティ戦略の構築に役立つ重要なセキュリティ管理とカテゴリ、およびそれをクラウドプラットフォームに実装する方法について説明します。

攻撃対象領域を減らし、侵入を検知し、攻撃にタイムリーに対応することは、セキュリティ戦略を支える 3 つの大きな柱となります。クラウド上のアプリケーションやコードを、モニタリングやログ記録によって可視化することが重要です。VM、Kubernetes、CaaS、FaaS のためのクラウドネイティブな(Born In The Cloud)全体的なセキュリティは、Linux の脅威検知機能の統合とともに、クラウドセキュリティ戦略を設計する際に考慮すべき点となっています。本シリーズのパート 1 では、これらの重点分野に沿ったコントロールとカテゴリを探り、その詳細を説明しました。

本シリーズの他の記事では、AWS や Azure のサービスやツールを使ってコントロールを実装する方法を紹介しました。本稿では、Google Cloud Platform(GCP)に組み込まれたセキュリティサービスと、それらがクラウドセキュリティ戦略とどのように統合されるかを探ります。

GCP クラウドセキュリティコントロール

AWS や Azure と同様に、GCP もお客様がクラウドセキュリティ戦略を実装するために活用できる幾つもの組込サービスを提供しています。セキュリティ制御を実装するサービスがすぐに利用できない場合は、必要に応じてサードパーティのソリューションを使用してギャップに対処できます。

ネットワーク

仮想プライベートクラウド（VPC）を使用したプライベート展開

GCP では、仮想プライベートクラウド（VPC）により、ワークロードの安全なプライベート展開を可能になり、第 1 レベルのセグメンテーションが実現します。 ポート、プロトコル、送信元、宛先に基づいてトラフィックを制御できるファイアウォール・ルールを使用して、VPC 内で追加のマイクロセグメンテーションを設定できます。Google Kubernetes Engine（GKE）クラスタ内のコンテナ化されたワーク

ロードに対しては、ネットワークポリシーを使用して、多層防御を実装できます。

ポッドとサービス間のトラフィックは、ポッドレベルのファイアウォール・ルールによって制御されるため、攻撃が発生しても、影響は侵害されたコンテナに限定されます。GKE ワークロード用の Istio ベースのマイクロセグメンテーションは、相互の TLS 認証(authentication)、Istio の認可(authorization)、およびネットワークアクセスロギングを通じて、さらなるセキュリティレイヤーを提供します。

Cloud Armor

Google Cloud Armor は、Web アプリケーションファイアウォール（WAF）として設計されており、HTTP(s)ロードバランサーの背後にあるワークロードを不正なアクセスや攻撃から保護します。これは 、レイヤー3.4 および 7 の属性に基づいてトラフィックを制限または許可するセキュリティルールによって行われます。このサービスには、クロスサイトスクリプティング（XSS）、SQL インジェクション、リモートファイルインジェクション、リモートコード実行などの一般的なタイプの攻撃からワークロードを保護するルールがあらかじめ設定されています。

HTTP(s)、SSL プロキシ、TCP プロキシロードバランサーの背後に配置されたサービスは、自動的に DDoS 攻撃から保護されます。ロードバランサーは防御の最前線として機能し、SYN フラッド、IP フラグメントフラッド、ポートの枯渇などの一般的な DDoS 攻撃からの保護を提供します。

クラウドセキュリティのポスチャ管理

GCP は、Security Command Center を通じて包括的なクラウドセキュリティポスチャ管理（CSPM）を提供します。これは、クラウドアセットセキュリティの状態を俯瞰できるネイティブ GCP サービスです。包括的な脅威防止機能が組み込まれており、レガシーアプリケーションライブラリ、リバースシェル、疑わしいバイナリなどの弱点を明らかにします。

クラウド資産は自動検出され、Security Command Center に登録され、継続的に監視されます。設定ミスやクラウドのコンプライアンス違反があった場合には、修復を開始するための実行可能な推奨事項とともにフラグが立てられます。GCP Security Health Analytics は、コンテナランタイム攻撃の検出など、さまざまなサービスの脆弱性評価スキャンを提供します。Cloud Console 上で脆弱性を検出しますが、サードパーティのサービスを利用して、アプリやリソースレベルで実行時の脆弱性を検出することをお勧めします。

脆弱性管理

パッチの展開

GCP の OS パッチ管理サービスは、Windows および Linux VM を最新のパッチで更新するのに役立ち

ます。コンプライアンスレポートを通じて、VM のパッチステータスを一元的に確認できます。また、自動パッチ展開オプションを使用して、指定されたメンテナンスウィンドウ中に不足しているパッチをシステムに展開できます。

Web アプリケーションの脆弱性スキャン

Cloud Security Scanner サービスは、Compute Engine、GKE、App Engine に実装された Web アプリケーションをスキャンして、セキュリティの抜け穴と脆弱性を特定します。このサービスは、Flash インジェクション、混合コンテンツ検出、クロスサイトスクリプティング、セキュリティで保護されていないパスワード送信など、一般的な脆弱性を特定して警告することができます Cloud Security Scanner は Security Command Center と統合されており、結果は一元化されたダッシュボードに表示されます。

クラウドワークロード保護プラットフォーム（CWPP）

セキュリティ制御で強化された Shielded VM

標準のセキュリティベストプラクティスを使用して VM を強化すると、複数の既知の脆弱性や攻撃から VM を保護することができます。GCP の Shielded VM は、ルートキットとブートキットの脅威から保護されています。この高度な保護は、セキュアブートプロセス、仮想トラステッドプラットフォームモジュール（vTPM）対応のメジャーブート、UEFI ファームウェア、および整合性監視によって実現されます。

vTPM は、システムへのアクセスの認証に使用される鍵と証明書を保護します。Shielded VM のセキュアブートプロセスは、ブートシグネチャを検証し、信頼できるソフトウェアのみの実行を許可します。したがって、悪意のあるインサイダー攻撃、ゲストファームウェア、カーネルやユーザーモードの脆弱性などの高度な脅威に対する保護を実現します。

すべてのランタイムの脆弱性から保護するのに VM の強化だけでは不十分です。クラウドエコシステムは、VM に加えて、K8、CaaS、FaaS などのソリューションで構成される可能性があります。したがって、これらすべてのサービスの全体的な保護を可能にする Intezer Protect などのサードパーティソリューションを組み込んで、セキュリティ体制を強化することができます。

注：ワークロード中心の適応型アプリケーション制御とメモリ内保護機能により、信頼できるコードとアプリケーションのみをクラウド環境で実行できます。GCP には、これを有効にすることができるネイティブサービスがありません。Intezer Protect のような CWPP は 、アプリケーション制御とメモリ内保護機能により、ワークロードのセキュリティステータスを高度に可視化します。これを活用して、クラウド資産のセキュリティを強化し、不正なコードやコマンドから保護するのに役立つアプローチを GCP に実装できます。

コンテナセキュリティ

コンテナの脆弱性スキャン

GCP の Container Analysis サービス は、コンテナレジストリにアップロードされた新しいコンテナイメージをスキャンしてセキュリティの脆弱性を検出します。また、脆弱性データベースから受け取った更新情報に基づいて、進化する脅威に対してスキャンしたコンテナメタデータを継続的に分析します。

この実行前のイメージスキャンは、継続的な分析とともに、コンテナ内のワークロードのエンドツーエンドのライフサイクルセキュリティを確保することができます。コンテナ CI / CD パイプラインを Kristis Signer と統合し、コンテナ分析の脆弱性スキャン結果に基づいて証明書を作成することもできます。

信頼できるイメージの展開

Binary Authorization サービスに基づく展開時のセキュリティ制御を使用して、信頼できる検証済みのイメージのみが展開されるようにすることができます。DevOps のビルドやリリースプロセスと統合すると、検証済みのコンテナのみがクラウド環境に実装され、コンテナで実行されている悪意のあるコードによる潜在的な脅威から保護されます。

Binary Authorization は、プロアクティブな CSPM に役立ち、コンテナのリリース方法の標準化を支援します。展開ポリシーを定義することが GKE コントロールパネルとネイティブに統合されているため、導入プロセスがはるかに簡単になります。

セキュリティ情報およびイベント管理（SIEM）

セキュリティ情報およびイベント管理（SIEM）のツールは、複数のソースからログを集約し、高度な分析を通じて脅威と脆弱性のインテリジェンスを導き出すのに役立ちます。GCP ユーザーは、セキュリティテレメトリデータを Chronicle 社に送信し、新しく発表された Chronicle Detect の機能を活用して、高度な脅威を検出できます。また、 REST API 統合を利用して、Security Command Center から既存のセキュリティシステムに情報を送信することもできます。追加の分析のために、Splunk などの SIEM ツールを使用して Security Command Center からデータをエクスポートできます。

脅威の検出とセキュリティ分析

Security Command Center のプレミアム層の Event Threat Detection 機能は、クラウドログストリームから収集されたログを監視し、事前構成された脅威ルールに基づいて一般的な脅威を検知します。Event Threat Detection 機能は、ブルートフォース攻撃やフィッシングなどを識別します。ログデータを BigQuery に保存し、脅威モデルに基づいて SQL クエリを実行することで、カスタム検出ルールを作

成することもできます。

セキュリティ操作と脅威検知の成功は、セキュリティテレメトリデータから受信したインテリジェンスに依存します。Chronicle を利用したセキュリティテレメトリ分析サービスは、ペタバイトのテレメトリデータを分析し、その情報を既知の脅威データと関連付けることができます。このサービスはまた、主要なファイルや UR の分析サービスである VirusTotal を活用して、テレメトリデータから洞察を導き出します。サービスで使用されているインテリジェントな識別プロセスは、ユーザーとマシンの ID を関連づけて、攻撃ベクトルを効率的に追跡します。ただし、VirusTotal の脅威検出エンジンは、シグネチャまたはアノマリベースの検出に依存しているため、Linux の脅威の検出には効果的ではありません。Intezer Protect など、Linux の脅威を検出するための実証済みの機能を備えたサードパーティツールを活用することをお勧めします。

GCP でのログとセキュリティの監視

不正なユーザーからクラウド資産を守るためには、管理者やデータへのアクセス活動を監視し、不審なイベントが発生していないかを確認することが不可欠です。GCP では、プラットフォーム内のすべての管理アクティビティ、データアクセス、システムイベントの強力な監査証跡をほぼリアルタイムで提供し、ログデータは高度に保護された不変の暗号化されたストレージに保存され、整合性を確保します。

このプロセスによって実装されるアクセスの透明性は、内部監査ログの「手の届かない」ログを対象とします。たとえば、サポートやエンジニアリングで必要とされるターゲットアクセスの場合です。これを、YARA-L 検出を使用して重大な侵入の痕跡（IOC）を定義し、高度なハンティングスタイルの検索を実行するセキュリティ脅威分析と組み合わせると、GCP でのクラウド資産の使用状況を包括的にセキュリティ監視できます。

まとめ

GCP は、Gmail や GSuite などの Google 製品を保護するために使用されるのと同じセキュリティサービスを使用しています。これは、革新的であるだけでなく、十分にテストが重ねられていることを意味します。Google は、進化するセキュリティの脅威からワークロードを保護するために、GCP のセキュリティ機能とプライバシー機能の強化に多額の投資を行ってきました。

このブログで説明されている GCP サービスは比較的成熟していますが、クラウド管理者は設定がかなり複雑であると感じるかもしれません。オンプレミス管理者や、他のクラウドプラットフォームに精通している専門家にとっては、ハードルが高いと感じる可能性があります。App Control やメモリ内保護など、ネイティブサービスでカバーされていない制御がいくつかあるため、セキュリティを強化するには、Intezer などのサードパーティソリューションと統合する必要があります。Intezer は、Linux の脅威に対する効果的な保護にも役立ちます。これは、ワークロードに Linux を活用することを好む多くの組織

にとって重要な機能です。

AWS や Azure などの他のクラウドサービスプロバイダーがこれらのセキュリティ制御をどのようにサポートしているかを理解するには 、このブログシリーズの他のパートを参照してください。このシリーズの最終回となるパート５では､ビッグ３クラウドプロバイダのセキュリティ制御機能を比較します。

■原文

Intezer Blog

Cloud Workload Security: Part 4 - Explaining the Security Features of GCP (January 21 2021)

https://www.intezer.com/blog/cloud-security/cloud-workload-security-part-4-explaining-the-security-features-of-gcp/

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 9 月

■免責事項

本稿は原文にできるだけ忠実に翻訳するよう努めていますが、完全性や正確性を保証するものではありません。翻訳監修主体は、本翻訳物に記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。原文の内容を理解する必要がある場合、上記の原文をお読み下さい。

翻訳監修主体：大日本印刷株式会社　AB センターDX 事業開発本部サイバーセキュリティ事業推進ユニット

■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 (https://www.dnp.co.jp/cka/column/column-vol06.html)

パート２：AWS のセキュリティ機能 (https://www.dnp.co.jp/cka/column/column-vol07.html)

パート３ ：Azure のセキュリティ機能 (https:/www.dnp.co.jp/cka/column/column-vol09.html)

パート４ ：GCP のセキュリティ機能 <本稿>

パート５：三大クラウドプロバイダのセキュリティ機能 <準備中>

