DNP

クラウドワークロードセキュリティ
パート３：Azure のセキュリティ機能

脅威は常に進化しており、企業はクラウドセキュリティ戦略を常に更新する必要があるため、クラウドセキュリティ管理は常に継続的な課題となります。クラウドプラットフォームの種類にかかわらず、セキュリティコントロールとカテゴリを明確に定義することで、クラウドセキュリティ管理のベースラインを確立することができます。本シリーズは、クラウドセキュリティの重点分野と、この戦略を構築するために考慮すべき最も重要なコントロールとカテゴリを理解するのに役立ちます。

本シリーズのパート１では、このフレームワークについて、クラウドセキュリティ戦略を策定する際に考慮すべき重点分野（攻撃対象領域の削減、攻撃や違反の検知、攻撃への対応など）を紹介しました。

また、これらの重点分野に沿ったコントロールとカテゴリについても説明しました。選択したクラウドプラットフォームにこれらのコントロールを実装することが次のステップです。この記事では 、クラウド上のワークロードにセキュリティ管理を実装するために使用できるさまざまな Microsoft Azure サービスとツールについて解説します。

Azure クラウドセキュリティコントロール

クラウドセキュリティ管理を実装する際の経験則として、クラウドプラットフォームでネイティブに利用可能なサービスやツールを活用することが挙げられます。ネイティブで利用できない機能については、サードパーティのサービスを検討することができます。ここでは、Azure に関連するセキュリティ管理とカテゴリを実装するためのオプションを検討してみましょう。

ネットワーク

VNet マイクロセグメンテーションのアプリケーションセキュリティグループ

アプリケーションセキュリティグループは、Azure VNet に配備されたアプリケーションコンポーネントのマイクロセグメンテーション[i]に役立ちます。これらは、きめ細かいセキュリティポリシーをビジネスロジックと整合させることにより、IP の設定と管理を抽象化します。NSG でアプリケーションセキュリティグループ[ii]を使用すると、「North-South」トラフィック（基幹から末端へと流れる通信）と「East-West」トラフィック（末端間の通信）のフィルタリングを管理できます。Azure VNet にネットワーク

マイクロセグメンテーションを実装する最も簡単な方法を探している場合は、アプリケーションセキュリティグループがソリューションとなります。

Azure Firewall 脅威インテリジェンスベースのフィルタリング

Azure Firewall は、既知の悪意のあるソースとの間のトラフィックを拒否する脅威インテリジェンスベースのフィルタリングを提供することにより、ワークロードを保護します。悪意のあるソースに関する情報は、Azure Security Center を含む Azure の複数のセキュリティサービスで使用される Microsoft の Intelligent Security Graph サービスを利用した Microsoft 脅威情報フィードから取得されます。

Azure Web アプリケーションファイアウォール

Azure Web アプリケーションファイアウォール （WAF）は、Azure に配備された Web アプリケーションを一般的な脅威や既知の脆弱性から保護します。WAF は、SQL インジェクションやクロスサイトスクリプティングなどの既知のエクスプロイトだけでなく、進化するエクスプロイトに対する自動保護を提供します。WAF は、包括的なワークロード保護のために、Azure Application Gateway、Azure Front Door、Azure Content Delivery Network（CDN）（パブリックプレビュー）の Azure サービスと統合できます。

WAF は Azure Application Gateway との併用が一般的で、Open Web Application Security Project（OWASP）の ModSecurity コアルールセットに基づく保護機能を提供します。

Azure DDoS Protection

Azure は、ベーシックとスタンダードの DDoS Protection を提供します。デフォルトでは、すべての Azure リソースでベーシックな保護を利用できます。一方、お客さまは、AzureVNet に接続されているワークロードのセキュリティを強化するためにスタンダード DDoS Protection を設定することができます。標準サービスでは、攻撃ベクトルの監視と分析のためのリアルタイム遠隔測定によって、ボリューム攻撃、プロトコルを狙った攻撃、アプリケーション層（レイヤ 7）の攻撃[iii]に対する保護と自動軽減が提供されます。

組込の「攻撃状況測定ツール(attack metrics)」を活用して、進行中の攻撃について関係者に通知するアラートを設定できます。WAF やサードパーティ製アプリケーションファイアウォールなどのレイヤー7 保護サービスと統合することで、Azure の DDoS Protection は、Azure ワークロードのレイヤー3 からレイヤー7 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

Azure Security Center のポリシーと推奨事項

Azure Security Center は、組込のクラウドセキュリティポスチャ管理ソリューションで、設定ミスの

可能性や Azure セキュリティベンチマークとの整合性について Azure の展開を監視します。Azure Security Center は、定義されたセキュリティコントロールに対してリソースの継続的な評価を行い、是正措置の優先順位付けに役立つセキュリティスコアを割り当てます。

Azure Security Center には 、幅広いサービスのセキュリティ、コンプライアンス、およびコストと管理制御に関するポリシーと推奨事項が組込まれています。これらには、データ保護、ストレージ、コンピューティング、アプリサービス、VMSS、コンテナが含まれています。以下いくつか示します。

・トラフィックパターン分析に基づく適応型ネットワーク強化要件
・Kubernetes クラスタ内のポッドの相互アクセスを制限するポッドセキュリティポリシー
・推奨されるベストプラクティスに基づく Azure サブスクリプションの所有権の調整
・管理対象および非管理対象のデータベースインスタンスに対する高度なデータセキュリティ設定
・ストレージアカウントの高度な脅威保護
・インターネットトラフィックの保護
・ジャストインタイムのネットワークアクセス制御の実装
・重要なサービスの診断ログの設定
・データベースとストレージサービスの暗号化

脆弱性管理

Azure Update Management

Azure は、Azure Automation サービスの一部である Azure Update Management を通じて、ハイブリッドなパッチ展開オプションを提供しています。Azure Update Management は、Windows および Linux マシンのパッチレベルを評価し、デプロイメントプロセスを開始するために使用することができます。評価とデプロイメントプロセスは、Windows/Linux 用の Log Analytics エージェントと、Hybrid Runbook Worker、DSC（Linux マシン用）、WSUS（Windows マシン用）を利用します。マシンを Log Analytics のワークスペースに接続することは、アップデート管理の前提条件となります。

Azure Security Center の脆弱性評価

Azure Security Center は、Qualys 社が提供する仮想マシンのリアルタイムの統合された脆弱性スキャンを行い、その結果をレビュー用に提示します。Azure Resource Graph を利用して、脆弱性スキャンの結果をエクスポートし、さらにクエリ、分析、フィルタリングを行うこともできます。

サードパーティの脆弱性評価ソリューションのライセンスをすでに購入している場合は、それをセキュリティセンターと統合することができます。

クラウドワークロード保護プラットフォーム（CWPP）

Azure Security Center の脅威保護

Azure Security Center は 、Microsoft Defender Advanced Threat Protection（ATP）との統合を通じて、エンドポイントの検出と応答を提供します。

Azure Security Center の脅威保護は、ビッグデータ、高度な分析、インテリジェントなセキュリティグラフを利用しており、急速に進化する脅威に適応し、修復への実用的なアラートを提供します。Microsoft Defender ATP と Azure Security Center の統合により、Azure サーバ管理サービスのオンボードを支援し、すべてのマシンのセキュリティステータスをシングルペインで表示します。

Azure Defender Service は、Windows サーバに対して広範な保護機能を提供しますが、Linux サーバに対するカバー率はそれほど高くありません。このサービスは、監査ログを使用し、行動ルールを適用して脅威を検出します。データの照合・集約を支援する Log Analytics エージェントによって有効になり、Linux のシグナルに基づいて不審な活動を検出します。

最新の Linux の脅威を検知するには、行動指標や異常検知ではなく、実行されたコードを監視／検査する脅威検知アプローチの方が効果的であることが実証されています。そのため、お客さまは、クラウド上の高度な脅威から Linux システムを保護するために特別に設計された Intezer Protect のようなサードパーティソリューションを利用して、Linux ワークロードの保護を強化することを検討できます。

Azure Security Center の適応型アプリケーション制御

クラス最高のセキュリティを実装するには、クラウド環境を綿密に監視し、正当なソフトウェアとプロセスのみを実行できるようにすることが重要です。適応型アプリケーション制御は、高度な機械学習によるアプリケーションの分析と分類を用いてお客さまのマシンを分析し、安全なアプリケーションのリストを定義します。

許可リストにあるもの以外のアプリケーションをお客さまのマシンで実行すると、アラートが発生します。しかし、これにより、動的環境ではノイズが発生し、オーバーヘッドの増加に加えて、高い確率で誤検知が発生する可能性があります。アプリケーション制御はディスクレベルで動作しるため、システムメモリに注入された脅威に対しては効果がありません。従って、実行時に未承認で悪意のあるコードから保護するためには、動的環境でインメモリ保護を実装することが重要です。ここではサードパーティのツールを検討できます。

コンテナセキュリティ

コンテナレジストリ用 Azure Defender

サブスクリプションレベルでオプションの Azure Defender for container registry サービスを有効にすると、Linux をホストする Azure Container Registry イメージにプッシュされた Linux コンテナイメ

ージの自動スキャンが開始されます。このスキャンプロセスは Qualys 社が提供するもので、追加の統合手順は必要ありません。このサービスでは、脆弱性スキャンの詳細なレポートが提供され、深刻度の分類も可能です。レポートは、これらの脆弱性を軽減するための規定のガイダンスも提供します。

Azure Security Center コンテナ環境の保護

Azure Security Center は、ベースラインセキュリティ構成に対して、Azure Kubernetes Service（AKS）クラスタとコンテナホスト（Docker Engine を実行している VM）を継続的に監視し、ハードニングに関する推奨事項も提供します。VM で実行されている管理されていないコンテナの場合、その構成を Docker コンテナの CIS ベンチマークと比較します。コンテナのランタイム保護は、Azure Defender for Kubernetes の統合により可能です。

Azure Defender は、Linux AKS ノードの不審な活動や接続、特権的なコンテナの展開、コンテナ内の SSH サーバなどを監視します。AKS クラスタレベルのランタイム保護は、Azure Defender for Kubernetes により、特権役割の作成、脆弱なダッシュボードの展開、機密性の高いマウントの設定などのイベントの監査ログの分析によって有効になります。

セキュリティ情報およびイベント管理（SIEM）

Azure Sentinel

Azure は、Azure Sentinel と呼ばれるクラウドネイティブの SIEM およびセキュリティオーケストレーション自動応答（SOAR）ソリューションを提供します。これにより、複数のソースからのデータを統合し、潜在的な脅威や攻撃について分析できます。Azure Sentinel には、Azure Cloud App Security、Office 365、Azure Active Directory（AD）、Microsoft 365 Defender などの複数のデータソースとリアルタイムで統合するためのコネクタが組み込まれています。

さらに、一般的なイベントフォーマット/ Syslog (シスログ)を使用したり、REST-API 統合を使用したりして、ソースからデータを受信するように Sentinel を構成できます。Azure Sentinel のすぐに使える高度な分析機能は、潜在的に高難度の攻撃を指し示す可能性のある異なるエンティティからのセキュリティインシデントを相互に関連付けるのに役立ちます。Azure Sentinel の高度なハンティングおよびクエリ機能により、カスタマイズされた検知、詳細な洞察、および自動調査を促進します。

Azure Security Center の脅威保護

Azure Security Center は、Windows / Linux マシン、Azure App Service、コンテナ、Kubernetes サービスなどに追加の脅威検出とアラート機能を提供し、不正なデジタル通貨マイニング、システムログの一括削除、不審なファイルのダウンロード、ブルートフォース攻撃の試み等の微妙に高度な攻撃からワ

ークロードを保護します。

Azure でのログとセキュリティの監視

Azure でリソース診断設定を構成することで、Azure Event Hubs、Azure Storage、または Azure Monitor と統合された Log Analytics ワークスペースに送信されるリソースログを設定することができます。リソースの変更、新しい展開、更新など、Azure サブスクリプションレベルのアクティビティはすべて、Azure アクティビティログによってキャプチャされます。

Azure Active Directory ログは、ユーザがアクセスするアプリケーションとリソースの使用パターン、ユーザアカウントに関連するセキュリティリスクに関する洞察を提供します。侵害されたユーザアカウント、危険なサインイン、およびサインインアクティビティに関連する問題にフラグを立てます。

ネットワークセキュリティグループ（NSG）のフローログは、もう 1 つの注目すべき Azure 監視機能であり、VM NIC カードやサブネットに関連付けられた NSG を通過する IP トラフィックフローを監視するのに役立ちます。これにより、環境へのネットワーク接続、侵入の試み、予期しないネットワークトラフィック、およびスループット監視を注意深く監視できます。データをストレージ用の SIEM ツールにインポートしたり、レポート用の視覚化ツールにインポートしたりできます。

まとめ

クラウドサービスプロバイダの代表格である Azure は、セキュリティとコンプライアンスに非常に重点を置いています。マイクロソフトは「破られることを前提とする」戦略をとっており、定期的にレッドチーム/ブルーチームの演習を実施して、脅威を事前に検知し、クラウドプラットフォームのセキュリティ体制を強化しています。セキュリティツールとサービスは、Windows ワークロードとはうまく統合できますが、Linux サーバのオプションは比較的限られています。クラウドでの Linux ワークロードとコンテナの使用が増えるにつれ、 Azure のワークロードの 50%以上が Linux を使用するのは驚くべきことではありません。クラウドワークロードの領域が主に Linux である場合は、Linux 脅威検知に特化した Intezer Protect のような外部 CWPP /ランタイム保護ソリューションを検討することができます。

AWS や GCP などの他のクラウドサービスプロバイダがこれらのセキュリティコントロールをどのようにサポートしているかを理解するには 、本シリーズの他のパートをご参照ください。

■原文

Intezer Blog

Cloud Workload Security: Part 3 - Explaining Azure’s Security Features (December 11 2020)

https://www.intezer.com/blog/cloud-security/cloud-workload-security-part-3-explaining-azures-security-

features/

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 8 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 センターコミュニケーション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

パート 2： AWS のセキュリティ機能

パート 3 ：Azure のセキュリティ機能　<本稿>

パート 4 ：GCP のセキュリティ機能　<準備中>

パート 5：<準備中>

■訳注　用語理解のために参考となる日本語文献を示します

[i] https://japan.zdnet.com/article/35136217/

[ii] https://www.rworks.jp/cloud/azure/azure-column/azure-entry/22465/

[iii] https://www.cloudbric.jp/blog/2020/08/4_kinds_of_ddos_attack/

