PCI DSS コンプライアンスのための Amazon ECS の設計

2020 年 7 月

注意

お客様は、この文書に記載されている情報を独自に評価する責任を負うものとします。このドキュメントは、(a) 情報提供のみを目的としており、(b) AWS の現行製品とプラクティスを表したものであり、予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤー、またはライセンサーからの契約義務や確約を意味するものではありません。AWS の製品やサービスは、明示または暗示を問わず、いかなる保証、表明、条件を伴うことなく「現状のまま」提供されます。お客様に対する AWS の責任は、AWS 契約により規定されます。本書は、AWS とお客様の間で行われるいかなる契約の一部でもなく、そのような契約の内容を変更するものでもありません。

目次

要約

AWS 内でマイクロサービスやコンテナを使用して機密データのワークロードをサポートしようとする企業が増えています。このホワイトペーパーでは、Amazon Elastic Container Service (Amazon ECS) の設定を通じて、ペイメントカード業界のデータセキュリティ基準 (PCI DSS) バージョン 3.2.1 に対するお客様のコンプライアンスニーズをサポートするためのベストプラクティスを紹介します。このホワイトペーパーは、PCI DSS のすべての統制を網羅しているわけではありません。一部の統制はコンテナに該当せず、お客様間で環境は異なる場合があるためです。

このホワイトペーパーは、PCI DSS コンプライアンスに向けて AWS クラウド環境のアーキテクチャの設計に関心があるシステムアーキテクト、デベロッパー、セキュリティ担当者を対象としています。このドキュメントは、アマゾン ウェブ サービスの全額出資子会社である AWS Security Assurance Services, LLC (AWS SAS) が作成したものです。AWS SAS は、独立した PCI 認定セキュリティ評価機関 (QSAC) であり、AWS のお客様とパートナーに対して、AWS クラウド上で PCI DSS コンプライアンスを達成するための手引きとなる具体的な情報を提供します。AWS SAS は PCI QSAC として、PCI Security Standards Council (SSC) や他の PCI QSAC との間で、PCI セキュリティ基準の機密保持や契約上の枠組みに基づくやり取りを行うことができます。

はじめに

ペイメントカード業界のデータセキュリティ基準 (PCI DSS) は、人、プロセス、テクノロジーに適用される、ペイメントカード処理環境の保護に関する技術および運用上のガイダンスを提供します。カード会員データ (CHD) を保存、処理、または伝送する事業体は、PCI DSS に照らしてカード会員データ環境 (CDE) のコンプライアンスを検証する必要があります。このような事業体の例として、加盟店、ペイメントプロセサー、サービスプロバイダーがあります。

AWS は PCI DSS コンプライアンスを満たしていることが証明された多くのサービスを提供しており、企業はこれらのサービスを活用してコンプライアンスへの取り組みをサポートできます。継続的に成長している 1 つの分野は、コンテナ化されたソリューションの使用です。コンテナを使用すると、基盤となるホストからアプリケーションを抽象化して切り離すことができます。コンテナは、場所を問わない一貫した実行環境を可能にし、コンピューティングのニーズに基づいてすばやく開始および停止できます。

ワークロードをコンテナサービスに移行する利点は、プラットフォームの独立からデプロイの速度やリソースの効率まで、よく知られています。お客様は、コンテナ化された CDE でどのような方法でセキュリティのベストプラクティスを適用できるかに注意する必要があります。

コンテナ関数は、通常、プライマリタスクを実行するように設計されており、これに伴って分散環境が作成されます。コンテナによって実装されるサービスは、ネットワークとの相互依存性が高くなり、スケジューリング、スケーリング、リソース管理が必要になります。コンテナは、仮想マシンとは異なり、オペレーティングシステムのカーネルを共有します。AWS は、コンテナ間の強力なセキュリティ分離を提供します。また、最新のセキュリティ更新プログラムを確実に実行し、コンテナごとにきめ細かいアクセス許可を設定できるようにします。1 つのオペレーティングシステムで複数のコンテナを実行する場合、すべてのコンテナが共通のネットワークインターフェイスを共有できます。

アプリケーションのセキュリティに関する考慮事項は、コンテナ化した後でも当てはまります。さらに、お客様は管理レイヤーに対する適切な保護を確保する必要があります。コンテナ内で実行しているアプリケーションが適切にコード化されていない場合、Open Web Application Security Project (OWASP) Top 10 の脆弱性リストに定義されている項目とよく似たアプリケーションレイヤーの脆弱性が露呈します。

AWS のコンテナサービスには、Amazon Elastic Container Service(Amazon ECS) と Amazon Elastic Kubernetes Service (Amazon EKS) があります。各サービスは、AWS Fargate または Amazon Elastic Compute Cloud (Amazon EC2) へのデプロイをサポートしています。Amazon EC2 デプロイの場合、お客様はコンテナを実行する基盤となる EC2 インスタンスを管理します。AWS Fargate はサーバーレスコンピューティングエンジンであり、Amazon EC2 インスタンスのプロビジョニングと管理は不要です。

AWS のサービスにおける PCI DSS コンプライアンスステータス

AWS は、PCI DSS サービスプロバイダーとしての地位を確立しており、お客様のコンプライアンス要件への対応をサポートします。適用範囲のサービスは、お客様から提供されるデータにプライマリアカウント番号 (PAN) や機密認証データ (SAD) が含まれる可能性があること、またはそのようなデータのセキュリティに影響を与える可能性があることを前提としています。PCI DSS 準拠としてリストされている AWS のサービスは、お客様に代わってカード会員データを保存、処理、または送信しているかのように審査されています。これには、PCI DSS の適用範囲内のサービスをサポートする AWS データセンターの物理的なセキュリティ要件が含まれます。

執筆時点で、AWS は 2019 年 7 月の最新の PCI DSS 評価を完了しています。「コンプライアンスプログラムによる対象範囲内の AWS サービス」ウェブサイトには、PCI DSS 年次評価に含まれた AWS のサービスとその他コンプライアンスプログラムの対象となるすべてのサービスを一覧表示しています。AWS のサービスのコンプライアンスは継続的に維持され、通常、新しくリリースされるサービスは準拠済みです (つまり、準拠しているサービスのサブセットである新しいサービスはコンプライアンスを継承します)。お客様は、AWS Artifact を使用して AWS マネジメントコンソールから AWS コンプライアンスのドキュメントにアクセスできます。

PCI DSS に準拠しているサービスとは、それを使用するとお客様の環境がデフォルトで準拠するという意味ではなく、PCI DSS 要件を満たすようにそのサービスを設定できるという意味です。お客様がアクセスしてパラメータを構成できる場合、これらのパラメータがコンプライアンス要件を満たすように構成されていることを確認するのはお客様の責任です。AWS の PCI DSS 評価に含まれていないその他の AWS サービスも、PCI DSS の統制を満たすために利用できます。

AWS 責任共有モデル

セキュリティとコンプライアンスは、AWS とお客様の共有責任です。AWS 責任共有モデルは、ホストオペレーティングシステムや仮想化レイヤーから、サービスを運用する施設の物理的なセキュリティに至るまで、AWS が該当するコンポーネントの運用、管理、制御を引き受けるため、お客様の運用上の負担が軽減します。

次の図に、責任共有モデルの概要を示します。責任範囲は、実装した AWS のサービスによって異なる場合があります。AWS マネージドサービスの場合、AWS はお客様の運用上の責任をより多く引き受けます。

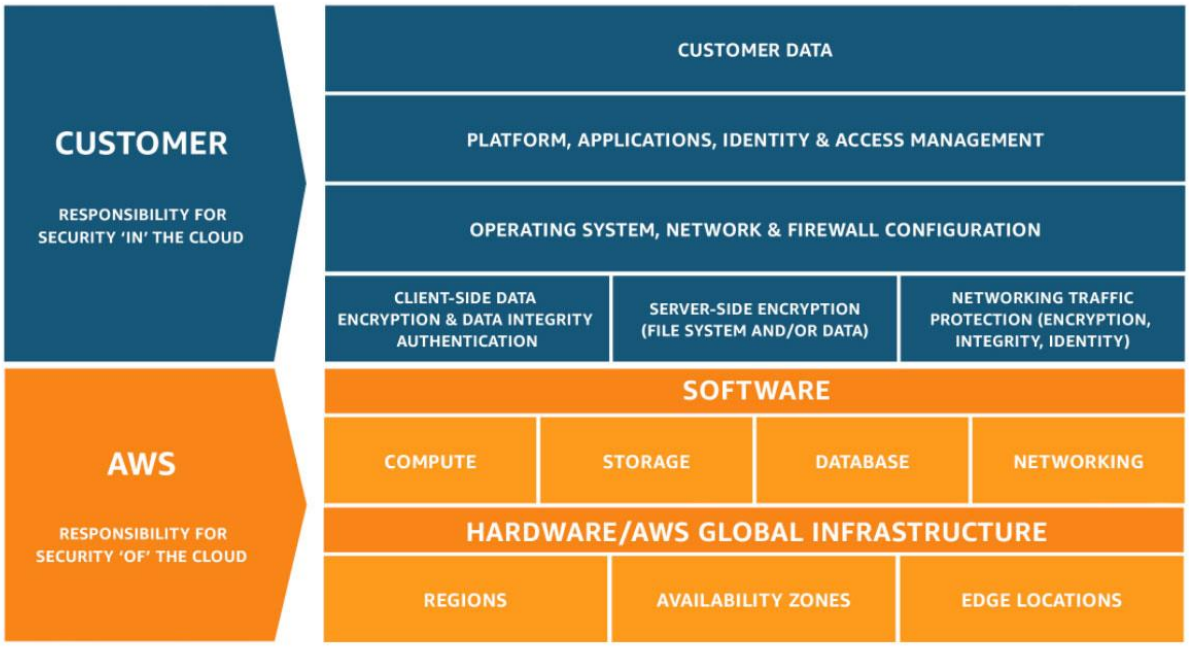

図 1 責任共有モデル

AWS は、AWS クラウド内で提供するすべてのサービスを実行するインフラストラクチャである**クラウドの**セキュリティとコンプライアンスに責任があります。クラウドセキュリティは AWS の最優先事項です。AWS のお客様は、セキュリティ要件が最も厳しい組織の要件を満たすように構築されたデータセンターやネットワークアーキテクチャの恩恵を享受します。このインフラストラクチャは、AWS クラウドサービスを実行するハードウェア、ソフトウェア、ネットワーク、および施設で構成されています。

お客様は、**クラウド内の**セキュリティとコンプライアンスに責任があります。これは、お客様が設

定して AWS でプロビジョニングしたシステムやサービスで構成されます。 PCI DSS コンプライアンスの場合、CDE に含まれているか、接続している AWS リソースを含むすべてのシステムコンポーネントがお客様の責任となります。Amazon S3 や Amazon DynamoDB などの抽象化されたサービスの場合、アクセス制御、ログ設定、暗号化設定など、お客様が設定できる統制は責任に含まれます。

Amazon のサービスに応じて、選択した実装ごとに責任レベルは異なります。Amazon ECS がよい例です。このサービスを使用すると、お客様は AWS Fargate でコンテナのサーバーレスデプロイを選択したり、お客様がアクセスできる Amazon EC2 インフラストラクチャでコンテナを実行したりできます。AWS Fargate では、お客様は基盤となるホストから抽象化されて切り離されるため、ホストシステムの更新やパッチ適用に責任を負いません。一方、Amazon EC2 デプロイでの Amazon ECS では、お客様はアクセスの制御やセキュリティパッチの適用など、より大きな責任を担う必要があります。

お客様がサービスパラメータを制御できる場合、お客様は PCI DSS 要件を満たすようにパラメータを確実に設定する責任を負います。

PCI DSS の適用範囲の決定と検証

環境内のカード会員データ (CHD) の完全なフローを理解することが重要です。CHD フローは、PCI DSS の適否を決定し、カード会員データ環境 (CDE) の境界とコンポーネントを定義します。また、これに伴って PCI DSS 評価の適用範囲を定義します。PCI DSS の適用範囲を正確に決定することは、セキュリティ体制を定義し、最終的に評価を成功させるための鍵となります。お客様は、適用範囲の決定に関する手順を用意して、この手順に従って適用範囲の完全性を確保し、適用範囲からの変更や逸脱を検出する必要があります。

コンテナ化されたアプリケーションは、そのエフェメラルな性質のため、設定の監査に伴う複雑さが増します。その結果、お客様は、コンテナのライフサイクルのすべての段階でコンプライアンス要件に確実に対処するために、すべてのコンテナ設定パラメータに常に注意する必要があります。

Amazon EC2 上の Amazon ECS のデプロイの保護

以下のセクションでは、PCI DSS コンプライアンス向けにコンテナベースの環境を設計する際に考慮すべき重要なトピックに関するガイダンスを提供します。これらは、以下のカテゴリに分類されます。

- ネットワークセグメンテーション
- ホストおよびコンテナイメージの強化
- 保管中および伝送中のデータの暗号化
- ユーザーアクセスの制限
- イベントのログ記録
- 脆弱性のスキャンと侵入テスト

セクションごとに、要件の概要と、従うべきベストプラクティスの推奨事項を示します。お客様ごとに環境は異なるため、ガイダンスは包括的なものではありません。以下の推奨事項は、コンテナベースの環境を保護するための多層防御アプローチを提供します。

ネットワークセグメンテーション

PCI DSS の要件 1 の統制では、カード会員データを保護するためにファイアウォールをインストールして維持することを定め、システムを不正アクセスから保護することを義務付けています。この要件は、インバウンドおよびアウトバウンドのアクセスを、承認されたポートとサービスのみに制限する必要があることを意味します。ネットワークセグメンテーションの使用は PCI DSS の要件ではありませんが、お客様の環境の適用範囲を狭めるために、その使用を強くお勧めします。
コンテナネットワークは、ソフトウェアブリッジを活用することで、ホスト上のすべてのコンテナが、コンテナ管理アプリケーションが提供する仮想ネットワークを介して通信できるようにします。各コンテナはプライベート IP アドレスを受け取りますが、インスタンス外のエンドポイントとの通

信では、実行元のホストのプライマリ Elastic Network Interface を共有します。
セキュリティグループは Elastic Network Interface に適用できますが、コンテナ間の共有相互通信により、コンテナ化された機密性の高いワークロードが適用範囲外のサービスに露出する可能性があります。このような露出は、適用範囲を拡大し、コンプライアンスに影響を与える可能性があります。
AWS 内では、セキュリティグループが仮想ファイアウォールとして機能し、ステートフルな検査を行います。セキュリティグループを使用することで、IP アドレス、ポート、プロトコルに基づいて通信を制限できます。デフォルトでは、セキュリティグループはすべてのアウトバウンド通信を許可することに注意してください。そのため、PCI DSS コンプライアンスを満たすようにアウトバウンド接続ルールを設定する必要があります。
コンテナ化されたワークロードは、ネットワークセグメンテーションを容易にするために、データの機密性レベルに基づいてグループ化するのが最適です。コンテナ間の通信は、マイクロセグメンテーションを使用して制限する必要があります。ユーザー定義のブリッジは、ホスト内のコンテナ間通信を制限するために使用できますが、ホストからのすべての通信は、共有ネットワークインターフェイスを通過します。
タスク通信のきめ細かな制御は、awsvpc ネットワークモードでタスクネットワーキングを使用して実行することもできます。このモードでは、Amazon ECS タスクが Elastic Network Interface に割り当てられます。セキュリティグループをインターフェイスに適用すると、特定のタスクに対してネットワークトラフィックの制限を設定できます。awsvpc ネットワークモードを使用する場合、インスタンスで実行するタスクの数は、Amazon EC2 インスタンスネットワークインターフェイスの数に制限されます。
結論として、コンテナ化されたアプリケーションの通信を分離する場合は、以下のオプションを検討します。

- サービスの機密性に基づいて、コンテナを別々のホストに分離します。
- マイクロセグメンテーションを実装して、コンテナ間の通信を制限します。
- awsvpc ネットワークモードを使用して、セキュリティグループを特定のコンテナタスクに適用します。

次のセクションでは、コンテナベースのワークロードを強化するための推奨事項を示します。

ホストとイメージの堅牢化

PCI DSS の要件 2 は、ベンダーが提供するシステムパスワードやその他のセキュリティパラメータに関して、ベンダーが提供するデフォルト値の変更の必要性を強調しています。Amazon ECS などの Amazon コンテナサービスは、コンテナに最適化された Amazon マシンイメージ (AMI) で実行されます。これらのオペレーティングシステムは、コンテナのデプロイに不要な余分なライブラリを含んでいないため、攻撃ベクトルを最小限に抑えるのに役立ちます。

お客様は、オペレーティングシステム、ネットワーク、アプリケーションの各レイヤーで、すべての設定と機能のコンプライアンスを引き続き維持する責任があります。オペレーティングシステムには AWS Systems Manager を使用して定期的にパッチを適用する必要があります。一方、重要でないサービスやライブラリは無効化または削除する必要があります。EC2 インスタンスタイプの Center for Internet Security(CIS) のベンチマークなど、業界で認知されたシステム堅牢化ガイドラインに準拠した設定基準を確立する必要があります。AWS クラウドセキュリティの学習ページには、AWS の安全な設定基準に関する追加のサポートがあります。

コンテナビルドは、必要なリソースのみに制限し、マイクロサービスのモデルを採用してコンテナが 1 つの主要な機能を提供するようにします。ソフトウェアアーキテクトは、イメージが既知の脆弱性を含む可能性のある古いソフトウェアライブラリやアプリケーションに依存しないようにする必要があります。ベストプラクティスは、コンテナレジストリ内のコンテナイメージを定期的に再構築して、最新のアプリケーションバージョンが使用されていることを確実することです。脆弱なライブラリを使用すると、見逃されがちな攻撃手段をもたらす可能性があります。

コンテナを管理する場合、コンテナはイミュータブルであること、およびインプレースでパッチを適用しないことが必要です。お客様は、パッチが適用されたライブラリやアプリケーションを使用していることが評価・確認された、信頼できるベースコンテナイメージを作成する必要があります。Amazon Elastic Container Registry (Amazon ECR) などの信頼できるレジストリを使用して、コンテナイメージを保護します。Amazon ECR は、Common Vulnerabilities and Exposures (CVEs) データベースに基づくイメージスキャンを提供し、一般的なソフトウェアの脆弱性を特定できます。

お客様は、Amazon EC2 インスタンスで適切なアンチウイルスおよびファイル整合性モニタリングソフトウェアを確実に実行する責任があります。多くのコンテナベンダーは、これらの要件に対処するために、コンテナの使用に最適化したソリューションを提供しています。

データ保護

PCI DSS の要件 3 および 4 の統制は、保管中および伝送中の機密データを保護する必要性に重点を置いています。AWS は、PCI DSS に準拠しているサービスや機能を数多く提供しており、これらのコンプライアンスの取り組みを支援します。

カード会員データなどの機密データを含むワークロードでは、すべての保存データをセキュリティで保護する必要があります。データは、基盤となるコンテナホストではなく、安全なファイルストアまたはデータベースに保存する必要があります。システムアーキテクトは、ホストファイルシステムや一時ストレージなど、コンテナのボリュームマウントとコンテナ間でのデータの共有に注意する必要があります。

コンテナのビルドファイル内のデータベース接続文字列などの機密データや環境変数は、セキュリティで保護する必要があります。AWS Secrets Manager と AWS Systems Manager Parameter Store は、コンテナのビルドファイル内の機密データを保護するために使用できる 2 つのサービスです。AWS Systems Manager Parameter Store は、データの安全な階層ストレージを提供し、サーバーの管理を不要にします。きめ細かなアクセス制御と監査制御を確立することで、コンプライアンス要件を満たすための適切な制限を確実に設定できます。AWS Systems Manager Parameter Store 内に保存したデータは、AWS Key Management Service (AWS KMS) を使用して暗号化できます。

AWS Systems Manager Parameter Store と同様に、AWS Secrets Manager 内の保護されたデータでも AWS KMS を活用します。AWS Secrets Manager には、ランダムなパスワード生成や自動パスワードローテーションなどの追加機能もあります。AWS KMS は PCI DSS に準拠しているサービスであり、多くの AWS プラットフォームサービスに統合されています。ユーザーは、暗号化キーマテリアルを作成および管理し、誰が暗号化キーにアクセスして使用できるかを制御できます。

伝送中のデータに関しては、オープンなパブリックネットワーク経由で伝送する機密情報は暗号化する必要があります。お客様は、強力な暗号化およびセキュリティの統制を設定する責任があります。AWS では、Transport Layer Security (TLS) の使用をサポートするために Amazon API Gateway や Application Load Balancer などの複数のサービスを提供しています。ポリシーをサービスに適用して、TLS 1.1 以上のみをサポートするように強制できます。

また、Amazon API Gateway と Application Load Balancer は、統合された AWS WAF (ウェブアプリケーションファイアウォール) の使用をサポートしており、アプリケーションレイヤーでの

通信を保護します。AWS WAF は、OWASP Top 10 で特定されているような、一般的なウェブの悪用からアプリケーションと API を保護します。

ユーザーアクセス

PCI DSS の要件 7 および 8 の統制は、権限を与えられた担当者のみにアクセスを制限し、適切なアクセス制御を確実に設定することに重点を置いています。リソースへのアクセス権は、職務の実行に必要な最小特権モデルに基づく必要があります。コンテナおよび基盤となるホストへのユーザーアクセスは、PCI DSS に準拠した厳格な認証要件に従って認証する必要があります。

コンテナイメージは、特権のあるユーザー以外のアカウントで実行する必要があります。例えば、デフォルトでは、定義されたユーザー認証情報を含まないコンテナのビルドファイルは root として実行します。これは、侵害されたコンテナサービスが root 権限を攻撃者に与える可能性があることを意味し、攻撃者は昇格したアクセス権を使用して、基盤となるホストをさらに悪用する可能性があります。

ホストアクセスを使用できない AWS Fargate とは異なり、Amazon EC2 上の Amazon ECS のデプロイには、基盤となるシステムを管理するための Secure Shell (SSH) アクセスを有効にするオプションがあります。SSH の使用を無効にして、代わりに AWS Systems Manager の Run Command を使用することを検討してください。Run Command は、管理対象の SSH キーを持たず、非インタラクティブです。また、呼び出したすべての操作は AWS CloudTrail 内で監査できます。

安全なコンテナイメージを作成して確立するために、コンテナイメージへのすべてのアクセスを制限します。コンテナのデプロイでは、アクセスと書き込みの許可を制限するプライベートコンテナレジストリを使用する必要があります。例えば、Amazon ECR を Identity and Access Management (IAM) と統合してアクセスを制御します。Amazon ECR は、コンテナイメージの安全な保存と伝送を提供する、スケーラブルなコンテナリポジトリです。また、ワークフローの簡素化と Amazon ECR と AWS サービスの統合により、コンテナホストへの認証アクセスを過度に提供する必要性も減ります。

アクセスの追跡とモニタリング

イベントのログ記録

PCI DSS の要件 10 の中心となる統制は、イベントのログ記録メカニズムを活用して、異常と思われるアクティビティの追跡、モニタリング、アラートを行う必要性に重点を置いています。
AWS イベントログサービスを活用して、ネットワーク、ホスト、コンテナでのイベントログのモニタリングを設定します。VPC フローログを有効にして、プロトコル、ポート、送信元アドレス、送信先アドレス情報など、パケット情報の詳細を示すネットワークトラフィックをキャプチャします。コンテナホストをモニタリングして、Amazon CloudWatch エージェントや Amazon Kinesis エージェントを確実に有効化および設定することで、ヘルス、効率、可用性を確保します。
コンテナ化されたアプリケーション内でイベントログ機能を有効にして、アプリケーションとコンテナのイベントログデータをキャプチャします。CloudWatch を 1 つのペインとして使用して、すべてのキャプチャしたイベントログアクティビティをモニタリングおよびアラートします。キャプチャしたイベントデータは、暗号化した Amazon Simple Storage Service (Amazon S3) バケット内に安全に保存し、保持要件を満たします。Amazon Athena と Amazon CloudWatch Logs Insights を使用すると、VPC フローログ、AWS CloudTrail、および Amazon CloudWatch から、Amazon S3 に保存した監査証跡ログにクエリを実行して分析できます。

ネットワーク侵入検出

PCI DSS の要件 11 の統制では、ネットワークへの侵入を検出または防止するために、侵入検出または侵入防止手法の使用を指定しています。基準では、CDE の境界および重要なポイントを通過するすべてのトラフィックをモニタリングすることを義務付けています。ほとんどのオンプレミス環境の場合、これらの要件に対処するには、通常、侵入検出システム (IDS)/侵入防止システム (IPS) アプライアンスを使用します。AWS 内でも同様のアプローチを使用できます。
コンテナ化された環境を考慮した場合、ネットワークトラフィックの検査は、コンテナホスト外のネットワークレイヤー、およびコンテナ管理ソフトウェアの仮想コンテナネットワーク内で実施できます。
AWS のコンテナホスト外のネットワークデータを検査するために検討できるオプションがいくつか

あります。Amazon GuardDuty は、AWS CloudTrail、DNS クエリ、Amazon VPC フローログなど、AWS データソース全体の異常検出、機械学習、イベントの脅威インテリジェンスを通じて脅威検出を提供します。

従来の IDS/IPS ソリューションを検討する場合は、Amazon VPC トラフィックミラーリング の設定を通じて、1 つ以上の Amazon EC2 インスタンスで実行している仮想アプイアンスに、すべてのネットワーク通信のコピーをルーティングできます。

もう 1 つの一般的なソリューションとしては、IP ルーティングを使用するトランジットネットワークアーキテクチャを作成して、すべてのネットワークトラフィックが 1 つのネットワークを通過するようにします。このアーキテクチャでは、AWS Marketplace から入手した仮想 IDS/IPS デバイスを使用して、ネットワーク間を通過するすべてのトラフィックを検査できます。VPC ゲートウェイを使用して、すべてのトラフィックをオンプレミスの IDS/IPS インフラストラクチャにルーティングすることもできます。最後に、ホストベースの IDS または IPS ソリューションを使用して、Amazon EC2 インスタンスへのトラフィックの配信時にトラフィックを検査することもできます。仮想コンテナネットワーク上のコンテナ間通信を検査することも、実行可能な選択肢の 1 つです。AWS Marketplace 内には IDS コンテナソリューションを提供するベンダーがあり、その多くはサイドカーコンテナを使用して異常なトラフィックパターンを監視してアラートを通知します。また、機械学習を利用してコンテナ間の異常な通信パターンを検出するエージェントベースのソリューションも利用できます。

どのセキュリティ対策を使用するかは、環境のアーキテクチャによって大きく異なります。ネットワークレイヤーでのトラフィック検出には、コンテナの配置とトラフィックパターンを事前に検討する必要があります。

脆弱性スキャン

PCI DSS では、組織が定期的にシステムやプロセスをテストして、脆弱性を特定し、特定した結果を適時に修正することを義務付けています。脆弱性スキャンは、四半期に 1 回および環境への大幅な変更の後に実行します。これには、ビルドプロセスへの脆弱性スキャンによってスキャンの実行回数を増やすことが含まれます。同様に、侵入テストを毎年 1 回および環境の大幅な変更の後で実施します。AWS リソースの侵入テストは、許可されたサービスに対して実施できます。詳細については、侵入テストに関する AWS サポートポリシーを参照してください。ネットワークセグメンテ

ーションを使用しているサービスプロバイダーの場合は、セグメンテーション統制の有効性を 6 か月ごと、またはセグメンテーション統制を変更した後にテストする必要があります。

評価アクティビティの適用範囲には、CDE と、CDE のサポートに使用する補助システムが含まれます。侵入テストを実行する際の適用範囲と方法論のガイダンスについては、PCI DSS Information Supplement: Penetration Testing Guidance を参照してください。

お客様の環境によっては、テスト要件がオンプレミス、クラウドリソース、およびコンテナ化された環境に適用される場合があります。Amazon ECS を Amazon EC2 インスタンスにデプロイする場合、お客様は基盤となるホストの脆弱性スキャンを実行する必要があります。PCI DSS に従って、セキュリティの脆弱性を特定するプロセスを確立し、新たに発見されたセキュリティの脆弱性にリスクのランクを割り当てることは、お客様の責任となります。Amazon Inspector はセキュリティ評価ツールであり、脆弱性を特定し、特定した結果に対して重要度のレベルに基づく優先順位を付けます。DevOps プロセス内に Amazon Inspector を統合することで、評価を自動化し、脆弱性を事前に特定できます。

また、お客様はコンテナ固有のスキャンツールを使用してコンテナイメージをスキャンし、脆弱性を検出する必要があります。コンテナのスキャンでは、準拠していないコード、脆弱なライブラリ、漏洩した可能性があるシークレットを特定します。 Amazon ECR のイメージスキャンは、Common Vulnerabilities and Exposures (CVE) データベースに基づいて、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。AWS Marketplace 内のセキュリティベンダーは、システム、コンテナ、アプリケーションをスキャンできるソリューションも提供しています。

内部および外部の侵入テストを実行する場合、評価アクティビティはネットワークレイヤーとアプリケーションレイヤーの両方で行い、基盤となるホストとコンテナ化されたアプリケーションを対象にする必要があります。コンテナホストにパッチを適用して脆弱性に対処し、コンテナイメージを更新して特定したコンテナの脆弱性を軽減します。強化したコンテナイメージを作成し、Amazon ECR などのプライベートコンテナレジストリ内に安全に保存します。

まとめ

AWS は、お客様のコンテナ化されたワークロードをサポートするために複数のサービスを提供しており、お客様はデータ処理のニーズに合わせてサービスを最適に構成することができます。このような柔軟性があるため、組織はコンテナ展開のライフサイクル全体を通じて、すべてのコンプライアンス要件を絶えず意識しておく必要があります。このホワイトペーパーで説明しているセキュリティ対策の方法は、お客様がコンテナ化されたワークロードの PCI DSS コンプライアンス要件に対応するのに役立ちます。

寄稿者

本書の執筆に当たり、次の人物および組織が寄稿しました。

- Tim Sills、AWS セキュリティアシュアランスサービス、シニアアシュアランスコンサルタント

参考資料

詳細については、次を参照してください。

- AWS における PCI DSS (Payment Card Industry Data Security Standard) 3.2.1 コンプライアンスガイド
- PCI DSS スコーピングおよび AWS 上でのセグメンテーション のためのアーキテクチャの設計
- AWS クイックスタート「AWS での PCI DSS コンプライアンスのための標準化されたアーキテクチャ」
- AWS セキュリティドキュメント
- AWS クラウドセキュリティ
- AWS ホワイトペーパー、技術ガイド、参考資料
- セキュリティの柱 AWS Well-Architected フレームワーク

ドキュメントの改訂

日付	説明
2020 年 7 月	初版発行