VMware の脆弱性評価

サービスの一般的な概要[1]

VMware セキュリティ評価は、Park Place Technologies（PPT）が提供するアドバイザリのみのセキュリティおよびコンプライアンス評価サービスです。サービスでは、読取り専用のコンフィギュレーションデータを収集し、自動的にセキュリティ評価レポートを生成して配信するために、PPT が管理する全自動の VMware スキャニングツールおよびセキュリティ分析エンジンを使用します。すべての分析、検証、および推奨活動は、PPT のセキュリティ専門家が実施します。

このサービスは、vCenter サーバー、ESXi ホスト、クラスタ、仮想ネットワーキング、仮想マシン、ストレージコンポーネントを含む、お客様の VMware 仮想化環境の包括的な評価を提供します。

評価は、CIS ベンチマーク、DISA STIGs、VMware ハードニングガイドライン、NIST サイバーセキュリティフレームワークおよび SOC 2 トラストサービス基準などの主要なフレームワークに合致した、コンフィギュレーションミス、セキュリティの欠陥、コンプライアンスの逸脱を特定します。

サービスおよび成果物

PPT は、VMware-特有の脆弱性特定、コンフィギュレーション分析、およびコンプライアンス評価（「本サービス」）を提供します。すべてのサービスはリモートで提供します。

評価活動

PPT は、以下を実施するため、PPT が管理する、読取り専用の自動 VMware スキャニングスクリプトおよび分析エンジンを活用します。

- 資格情報を一切保存せず、コンフィギュレーションの変更も一切行わずに、VMware コンフィギュレーションメタデータを収集。
- 200+の Vmware に適合するセキュリティ制御に対するコンフィギュレーションの評価。

[1] スキャニングツール（「ソフトウエア」）は、Kalosys の専有の製品であり、PPT によりライセンスされます。全ての特許権、著作権、営業秘密、およびその他の知的財産権は、Kalosys およびそのライセンサーに独占的に帰属します。お客様は、権利全体の保有ではなく、ソフトウエアを使用する限定的な権利のみを取得します。お客様は、(a) コピー、改変もしくは派生物の作成、(b) リバースエンジニアリング、逆コンパイルもしくは分解 (c) 専有権の通知もしくはラベルの除去、(d) サブライセンス、賃貸、リースもしくは譲渡、(e) 第三者に対するサービスの提供目的での使用、または(f) 保護措置の回避はできません。エンドユーザーは、このソフトウエアがセキュリティ評価のために設計されたもので、テストをする権限を与えられたシステム上でのみ使用することに同意します。

- コンフィギュレーションミス、インセキュアセッティング、およびコンフィギュレーションドリフトの検出。
- 複数のコンプライアンスフレームワークに同時にマッピング。
- vCenter、ESXi ホスト、クラスタ、VM、ネットワーキング、証明書、認証、およびログに関する問題の特定。
- 結果の検証および識別可能な誤検知の除去。

成果物

オンボーディング

- 導入および初期評価。
- エグゼクティブブリーフィングでの、ベースラインセキュリティスコア、全体的な所見、コンプライアンスステータス、および推奨する次のステップの要約。

定期的な自動レポート

お客様が選択した頻度（月毎、四半期毎、または週毎）で自動配信。

- CIS、DISA STIG、VMware ハードニングガイド、NIST CSF、SOC 2 にマッピングされたコンプライアンスの結果。
- 重大度別に分類したセキュリティ検出事項。
- CVE および CVSS 重大度スコアを含む脆弱性の分類。
- 是正措置付きの修正ガイド。
- リスクおよび運用への影響に沿った優先順位を付したアクションプラン。
- さまざまなサポート形式でのレポート配信。

アドバイザリスコープ

PPT は分析および推奨のみを提供します。お客様は、全ての修正、コンフィギュレーションの変更および運用アクションの実施に全面的に責任を負います。

サポート対象の VMware スコープ

- VMware vSphere 6.7 以降
- vCenter Server のサービス、認証、許可、ロギング
- ESXi ホストのハードニング（サービス、ファイアウォール、証明書、NTP、パスワード／ロックダウンポリシー）
- クラスタサービス（HA、DRS、EVC、vSAN）
- vSwitch/vDS コンフィギュレーションおよびポートグループセキュリティ
- VM コンフィギュレーション設定、VMware Tools、分離ポリシー

- データストアおよび vSAN コンフィギュレーション

プロセスおよび SLA

初期評価と導入

- お客様の指定システム上へのスキャニングスクリプトの展開。
- ツールの前提条件の検証。
- vCenter の接続および許可の確認。
- ベースライン VMware 評価の実行。
- 自動レポート配信の設定。

エグゼクティブおよびテクニカルブリーフィング

- ベースラインの所見の概要。
- コンプライアンスステータスの要約。
- 優先順位を付した修正の推奨（アドバイザリのみ）。

継続的な評価

- お客様が定義した頻度で実行する自動スキャン。
- 新たな脆弱性およびリグレッションの検出。
- コンフィギュレーションドリフトのモニタリング。

進捗報告

- VMware のセキュリティ態勢の傾向。
- 繰り返し発生する問題の検出。
- 修復の進捗状況の可視化。

サービスの制限

このサービスには以下が含まれません:

- リアルタイムモニタリング、SIEM/SOC、またはインシデント対応。
- 侵害の調査またはフォレンジック分析。
- VMware のパッチ適用、アップグレード、またはライフサイクル運用。
- 修正またはコンフィギュレーション変更の実施。
- パフォーマンスのトラブルシューティング（コンピュート、ストレージ、またはネットワーク）。
- アーキテクチャ設計、エンジニアリング、または容量の計画。
- カスタム自動化、スクリプティング、または統合。
- コンプライアンス認証の準備（ISO、PCI、SOC 2）。

- ITSM サポート（チケット、ワークフロー、CAB）。
- ライセンスの調達または権利管理。
- オンサイトエンジニアリングまたはハードウエアサービス。

お客様の責任

お客様は以下を行わなければなりません。

- 取組みをサポートする VMware およびセキュリティ担当者の選任。
- 評価目標のための読取り専用の資格情報および権限の提供。
- スキャンウィンドウの間、すべての VMware システムへのアクセスの確保。
- すべての修正および運用活動を保有。
- 評価データの分類、取扱い、および保持の管理。
- 評価中の一時的なリソースの負荷の認識。
- すべての VMware コンフィギュレーションのガバナンスおよび変更管理の維持。

スキャニングツールのセキュリティ、データ保護、および収集範囲

PPT はスキャニングツールの安全かつ制御された運用を確保します。主な要素は以下を含みます。

- 読取り専用かつ非侵入的なデータ収集。
- エージェントのインストールなし。コンフィギュレーションの変更なし。
- 資格情報のアクティブセッション中のみの使用、保存なし。
- VMware コンフィギュレーションメタデータのみ（vCenter、ESXi、クラスタ、ストレージ、ネットワーキング、認証、証明書、ロギング、NTP、マスクされたライセンスの詳細）を収集。
- VM ゲスト OS の内容、アプリケーションデータ、ユーザーデータ、パスワード、または完全なライセンスキーの収集なし。
- HTTPS（443）ですべての通信を暗号化。
- 評価成果物の転送中および保管時の暗号化。
- アクセスは PPT およびお客様の許可された担当者に限定。