セキュリティとコンプライアンスを向上させるための 8 つの技術的なヒント

リスクの緩和、セキュリティ構成とポリシーの適用、Red Hat® Enterprise Linux® のセキュリティ機能とコンプライアンス機能への準拠継続に役立ちます。

1 標準ベースのコンプライアンス設定を管理する

システム全体の暗号化ポリシーにより、インフラストラクチャの標準ベースのコンプライアンス設定を一貫した方法で実装し、維持することができます。

単純化された 1 つのコマンドで、組み込みの暗号化ポリシーを選択し、それをシステム上のアプリケーション全体に一貫して適用できます。さらに、特殊な規制コンプライアンス要件がある場合は、目的に合わせてカスタムポリシーを作成できます。

コンプライアンス管理の詳細

2 システムロールでセキュリティ構成を自動化する

Red Hat Ansible® Automation Platform を備えた Red Hat Enterprise Linux システムロールにより、管理者は自動化を使用して、セキュリティ設定を短時間で大規模にインストールし、管理できます。

システムロールは、さまざまなフットプリントでの複数の Red Hat Enterprise Linux リリースで機能するように作成されており、管理者は Red Hat ソリューションのベストプラクティスを使用できます。単一のコマンドまたはワークフローによって新しいセキュリティ設定を構成し、それらをすべてのシステムで維持できます。

セキュリティ自動化についての詳細

3 認証と認可を一元化する

Red Hat Enterprise Linux は、一元化された ID 管理 (IdM) 機能を備えており、データセンター全体にまたがる単一の拡張可能なインタフェースを使用して、ユーザー認証とロールベースのアクセス制御 (RBAC) の実装を行うことができます。Red Hat Enterprise Linux のアイデンティティ管理は、標準のアプリケーション・プログラミング・インタフェース (API) を通じて Microsoft Active Directory、軽量ディレクトリ・アクセス・プロトコル (LDAP)、およびその他のサードパーティの ID およびアクセス管理ソリューションと統合できます。

また、証明書ベースの認証および認可技術を使用したサービスの認証と認可を一元的に管理することも可能です。

ID 管理の詳細

4 ポリシーをカスタマイズする

Security-Enhanced Linux (SELinux) は、Linux カーネルに強制アクセス制御 (MAC) を実装したものです。Red Hat Enterprise Linux コンテナは、デフォルトで SELinux で動作します。これにはオペレーティングシステム (OS) での追加のセキュリティレイヤーが含まれ、コンテナが壊れてシステム上の基盤となるホスト OS や他のコンテナを上書きするのを防ぎます。Udica を使用すると、システム管理者とコンテナ開発者は実行中のコンテナを分析し、コンテナ固有の SELinux ルールを使用してポリシーを自動生成することができます。これにより、スーパーユーザー権限でコンテナを実行する必要がなくなるため、ポリシー作成が単純化され、リスクが軽減されます。

ポリシーのロックダウンを実際に操作してみる

5 最小限のダウンタイムでシステムにパッチを適用する

Red Hat は、延長アップデートサポート (EUS) リリースで、非常に重要または重要と評価された CVE (Common Vulnerabilities and Exposures) に対応するカーネルライブパッチを追加費用なしで提供します。カーネルライブパッチ (KLP) を使用すると、システムを再起動せずに実行中のカーネルにパッチを適用して脆弱性に即座に対処し、セキュリティを損なうことなくダウンタイムを最小限に抑えることができます。

KLP を実際に操作してみる

6 セキュリティとコンプライアンスを大規模に管理する

Red Hat Enterprise Linux サブスクリプションに含まれており、追加費用なしで利用できる Red Hat Insights は SaaS (Software-as-a-Service) オファリングであり、ユーザーのデプロイメントに関する実用的なセキュリティデータを提供します。運用上のリスクと脆弱性のリスクを検出して対処し、システムを迅速にスキャンして欠落しているパッチを特定し、優先順位をつけて重要なパッチから順に適用できます。すべての Red Hat Enterprise Linux システムのセキュリティ構成ポリシーの作成、変更、実装、保守は、単一の Web インタフェースから行えます。さらに、Red Hat Smart Management サブスクリプションによって、Red Hat Insights から修復計画を実行、拡張、および自動化することができます。

コンプライアンスの詳細

7 コンプライアンス目標に対応するためにシステムアクティビティを記録する

Red Hat Enterprise Linux には、セキュリティ管理者がシステム上で任意のユーザーグループのキーストロークとアクティビティをキャプチャーできる監査およびログ機能を備えたセッションレコーディングが含まれています。このデータは、他のすべてのアクティビティと同じシステムジャーナルまたはログファイルに記録され、再生ツールに搭載されている再生機能と一時停止機能を使用して分析し、関連付けることができます。

セッションレコーディングを実際に操作してみる

8 許可されていないアプリケーションの実行を停止する

アプリケーションの許可リストを作成すると、潜在的な攻撃ベクトルを減らし、システムで不正なアプリケーションが実行されるのを防ぐことができます。ファイルアクセスポリシーデーモン (fapolicyd) は、組み込みのアプリケーション許可リストを提供します。これにより、ユーザーがシステム上で実行できるのは承認されている実行ファイルのみになります。システム管理者は、デフォルトのポリシーを使用して fapolicyd を構成するか、独自のポリシーを作成して、変更されたアプリケーションや許可されていないアプリケーションが実行されるのを防ぐことができます。

アプリケーションの許可リストの詳細

Red Hat について

Red Hat は、受賞歴のあるサポート、トレーニング、コンサルティングサービスをお客様に提供し、複数の環境にわたる標準化、クラウドネイティブ・アプリケーションの開発、複雑な環境の統合、自動化、セキュリティ保護、運用管理を支援します。

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

アジア太平洋
+65 6490 4200
apac@redhat.com

オーストラリア
1 800 733 428

インド
+91 22 3987 8888

インドネシア
001 803 440 224

日本
03 4590 7472

韓国
080 708 0880

マレーシア
1 800 812 678

ニュージーランド
0800 450 503

シンガポール
800 448 1430

中国
800 810 2100

香港
800 901 222

台湾
0800 666 052

jp.redhat.com
O-F31208