自動化によって強力で安定した IT セキュリティポスチャを実現

「当社のお客様は、重要なモダナイゼーションとデジタル・トランスフォーメーションの真っ只中にあり、限られた時間の中でそのプロジェクトを進めています。自動化は、新たなレベルの効率性、アジリティ、回復力を実現する鍵となります」

Kurt Sand 氏
CyberArk
DevSecOps
ゼネラルマネージャー

概要：
DevOps、SecOps、ITOps を妨げることなく、自動化によっていかに IT セキュリティ全体が強化され、運用効率が向上するのか、ご覧ください。

先進的な IT 環境全体でセキュリティを確保

組織は開発とイノベーションを加速するために、オープンソース・アプリケーション、自動化された IT インフラストラクチャ、DevOps 手法を導入しています。これらの環境において、アプリケーション、スクリプト、自動化ツールなどの人間以外のすべての ID は、何らかの形式の特権認証情報を介してツール、アプリケーション、データにアクセスします。

IT 環境をセキュリティ上の問題から保護し、潜在的なサイバー攻撃に対抗するには、既存の日常的な運用プロセスと開発パイプラインにセキュリティを組み込む必要があります。

そこで、DevOps、SecOps、または ITOps を妨げることなく IT セキュリティ全体を強化し、運用効率を向上するために、重要なシステムやデータへの特権アクセスを管理する自動化に目が向けられています。

包括的な IT 自動化を、最も特権的なアカウントやキーを管理するための完全なライフサイクル・ソリューションに組み込むことで、IT 自体やこれらのサービスを使用する ID など、エンドツーエンドのプロセスを自信を持って自動化できます。

自動化によって一貫したセキュリティ重視の認証情報を管理

CyberArk と Red Hat® Ansible® Automation Platform の統合により、シークレットと特権アクセス管理の自動化を通じてセキュリティが強化され、企業全体で、クラウド内で、そして DevOps パイプライン全体を通じて、データ、インフラストラクチャ、資産が保護されます。

Red Hat Ansible Automation Platform と、IT 環境全体での特権アクセス管理に使用されるプラットフォームである CyberArk Privileged Access Manager (PAM) を組み合わせることで、特権認証情報のローテーションと管理が効率化され、高リスクのアクティビティの防止と修復が自動化されます。

自動化のアジリティとセキュリティのベストプラクティスのバランス

CyberArk PAM の設定を自動化することで、Red Hat Certified Content Collection はセキュリティポスチャを大幅に強化し、運用プロセスを最適化し、規制要件へのコンプライアンスを確保します。

CyberArk PAM の SaaS (Software-as-a-Service) バージョンとオンプレミスバージョンはいずれも、Red Hat Ansible Automation Platform のアプリケーション・プログラミング・インタフェース (API) と統合し、エンドポイントの自動化のシークレットプロバイダーとして機能します。

この統合により、CyberArk PAM での新しいユーザーまたはグループの修復とオンボーディングを自動化し、宣言型の IaC (Infrastructure-as-Code) アプローチに必要に応じて変更を加えることができます。

Red Hat Automation Platform は、CyberArk Conjur および CyberArk Vault と連携して、保護されたデータにアクセスするためのパスワードやクラウドサービスへの接続に使用されるキーなど、機密情報を伴う自動化を実行するために必要なシークレットへのアクセスを保護します。Red Hat Ansible Automation Platform を使用してシークレットにアクセスするための一時的な認証情報を作成し、自動化のセキュリティリスクをさらに軽減することもできます。

この統合により、自動化プロセスのセキュリティを強化し、特権情報へのアクセス制御を確保し、CyberArk PAM の原則に沿った強力なセキュリティポスチャを維持することができます。

さらに、CyberArk の認定済み Ansible Content Collections により、CyberArk PAM を簡単に管理できます。このコレクションには、ユーザーとグループの修復、権限の調整、CyberArks PAM 内のその他の一般的な管理アクティビティに関連するタスクの自動化を促進するモジュールとロールが含まれています。

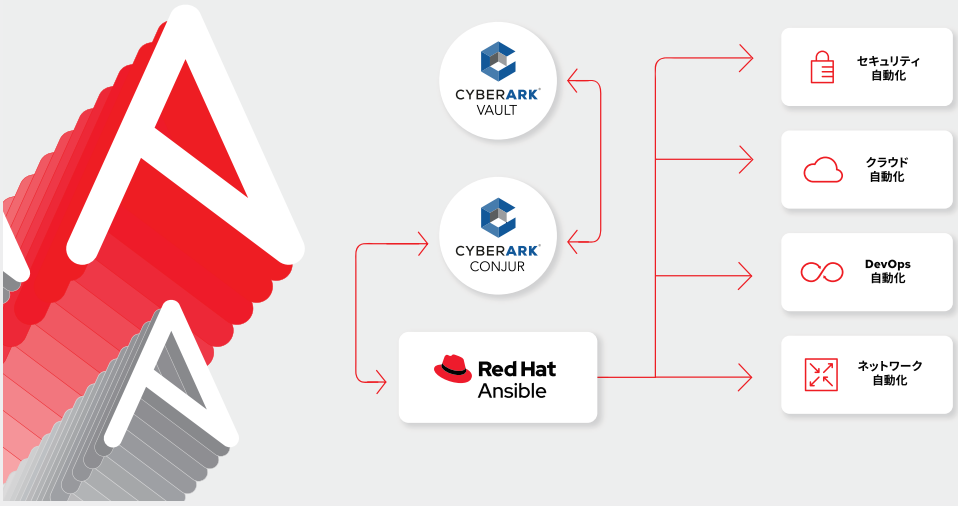

図 1. Red Hat Ansible Automation Platform と CyberArk による自動化セキュリティのフロー

自動化によって一貫したセキュリティポスチャを実現

CyberArk と Red Hat Ansible Automation Platform により、自動化を通じてエンタープライズ環境を保護し、ネットワーク、DevOps、クラウド、セキュリティ設定にわたって一貫したセキュリティポスチャを維持できます。これらのソリューションを組み合わせることで、次のことが可能になります。

- 複雑でセキュリティの影響を受けやすいタスク、認証情報の管理、ローテーション、および一般的な CyberArk 管理タスクを自動化することで、運用を単純化する。
- IT 環境全体のセキュリティを強化し、リスクを軽減し、コンプライアンスを向上する。
- 開発部門に対するセキュリティの負担を最小限に抑え、開発速度に影響を与えることなくセキュリティポスチャを強化する。

IT 環境全体でセキュリティを強化

Red Hat Ansible Automation Platform と CyberArk Privileged Access Manager によって、DevOps、SecOps、または ITOp を妨げることなくいかに組織を安全に自動化できるのか、詳細をご覧ください。

- シークレット管理の一元化および自動化のためのアプローチの開発に関する動画を見る
- Trusted Automation シリーズのデモを見る
- Red Hat と CyberArk のパートナーシップの詳細

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。

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

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

jp.redhat.com
#693383_0124