ホワイトペーパー

RED HAT における セキュリティとイノベーションの融合

Gordon Haff

エグゼクティブサマリー

Red Hat は、政府機関や金融サービスを含む、さまざまな業界のお客様と連携してソフトウェアを開発しています。これはイノベーションにつながるだけでなく、製品機能、サービス、プロセスに関するセキュリティ関連に関する決定の、貴重なガイダンスともなります。このアプローチが、Red Hat Enterprise Linux® などの Red Hat® インフラストラクチャソフトウェアや、Red Hat JBoss Enterprise Application Platform などのアプリケーションプラットフォームを、最も規制が厳しいセンシティブな産業におけるビジネス基盤としています。

現在の脅威的な環境では、ハイブリッドクラウド環境を含む、すべての IT でセキュリティを構築して運用可能にすることが、これまでになく重要になります。

このホワイトペーパーでは、現在のセキュリティの状況について考察し、Red Hat との連携によってセキュリティ、リスク管理、コンプライアンスの目標を実現する方法について説明します。また、脆弱性の緩和、構成管理の実装、アクセス制御の確立に共通する基本的な要件への対応についても説明します。これらの要件は、現在のデジタル世界では特に新しいものではありませんが、急激に増加する脅威への対応、オープンな IT アーキテクチャ、そして異種混在とハイブリッド両方のインフラストラクチャのために重要性が増しています。

したがって、ここでは、脆弱性が問題になる前にプロアクティブに修正するために、セキュリティを構築してアップストリームコミュニティで作業するための、Red Hat のアプローチについて説明します。また、システムの技術的な問題をプロアクティブに特定して解決することを可能にするサブスクリプション管理サービスである Red Hat Insights についても考察し、Ansible Tower や Red Hat Satellite などの製品によるセキュリティ運用の自動化やプロセスのコード化の役割についても見ていきます。そして、コードの更新を適用する IT プロセスの迅速化において DevOps が果たす役割についても取り上げます。さらに、Red Hat CloudForms がハイブリッド IT 環境でのポリシーベース管理の一元化をどのように実現するかについても説明します。

ただし、ここで取り上げるセキュリティの問題は、特効薬となる具体的なセキュリティ機能やソリューションに関するものではありません。幅広い視野でセキュリティ（具体的には、リスク管理、コンプライアンス、ガバナンス）を取り上げ、それをビジネスにかなうように運用可能にすることについて重点的に説明します。

「開発テストを活用するオープンソースソフトウェアのプロジェクトが、ソフトウェアの品質を継続的に高め、業界全体の水準を引き上げています」

COVERITY
製品担当シニアディレクター
ZACK SAMOCHA 氏

変化するセキュリティ脅威

中世の城では、その城壁と堀が攻撃者にとって厄介な障壁でした。しかし、その障壁が効果を発揮するのは、攻撃者が弱点を突破するのに失敗するか、新たな戦術を採用できないときに限られていました。従来型の IT セキュリティも、オンプレミスハードウェア、アプリケーション、データに対して強固な境界を構築し、保護することを前提としており、悪意やエラーから発生する内部からの脅威を考慮していません。しかし、従来型の IT セキュリティは、「悪者」を城門から侵入させないために、ファイアウォール、侵入検知システム、アクセス制御に大きく依存しています。

現在、情報セキュリティは変化に適応することが求められています。お客様やパートナーが特定のシステムやデータにアクセスできるようにする、従業員が自身のスマートフォンやラップトップを使用するのを許可する、Software-as-a-Service (SaaS) ベンダーのアプリケーションを使用する、使用量に応じて料金を支払うパブリッククラウドプロバイダーのユーティリティ価格モデルを活用するなど、もはや外部との境界は 1 つではなくなっています。組織の情報資産を最も効果的に利用するには、許可された第三者との情報の共有が必要になる場合がありますが、法令遵守および激しさを増す精巧なサイバー攻撃により、ほとんどの組織では、従来の基準よりも専門的で多面的な IT セキュリティ戦略の必要性が増しています。

このような傾向は、アナリストの調査だけでなく、お客様とのやり取りの中でも見ることができます。たとえば、アンケートを実施すると、通常はパブリッククラウドの導入に関する懸念事項の上位にセキュリティが入りますが、これは特に目新しいことではありません。しかし、アクセスと制御や、懸念の原因となるファイアウォールの設定ミスなど、システムセキュリティの一般的な面ではなく、データ管轄、監査能力、法令遵守、検証可能なエンドツーエンドの暗号化などが上位を占めています。そして、これらは、クラウドプロバイダーが責任を負う領域です。

また、ワークロードを実行する組織も、ソフトウェアの出所の確定、政府によって適用される規制と認定の把握、ポリシーベースの適切な統制およびアクセスの提供、サプライヤーとの関係の管理、セキュリティとインシデント対応に関する繰り返し可能な、正式なプロセスの一般的な確立などにおいて、独自の役割を担う必要があります。

セキュリティに関する考察

このホワイトペーパーでは、情報セキュリティに関連するさまざまなテクノロジーと機能について触れますが、効果的な防御、検出、抑止を実現する上で重要なのは、特定の製品やコンポーネントを使用することではなく、ビジネスプロセスの自動化、優れたプラクティスの制度化、問題が発生した場合 (発生していない場合) の効果的な修正を可能にする、強固な基盤を確立することです。セキュリティ専門家の Bruce Schneier 氏は次のように述べています。「セキュリティは完全である必要はありませんが、リスクを管理できるようにする必要があります」。[1]

セキュリティ実践の共通概念モデルである CIA Triad では、(重要データ) 保護の次の側面を重視しています。

1. 機密性 - データの使用が許可された人のみにデータアクセスを制限する
2. 整合性 - 許可されていない者によってデータが変更または削除されないようにする
3. 可用性 - 必要時にデータを利用できるようにする

1 https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

「クラウドプロバイダーがお客様のセキュリティにすべて責任を負うという単純な考え方は、企業が従業員にクラウドサービスを適切に利用させるのを思いとどまらせてしまう」

GARTNER
『CLOUDS ARE SECURE: ARE YOU USING THEM SECURELY?』(クラウドは安全:クラウドを安全に利用していますか?)
2015 年 9 月
G00281279

米国標準技術研究所 [2] などのセキュリティの専門家や組織では、リスク評価、適時性、物理的所有、適法性、実用性など、セキュリティについてのその他の側面も含めた複雑なモデルを開発してきました。このホワイトペーパーでは、セキュリティのベストプラクティスについてすべてを取り上げることはできませんが、ハイブリッドアーキテクチャ、クラウドネイティブインフラストラクチャ、DevOps アプローチを使用したアプリケーション開発、商用のオープンソースのセキュリティ脆弱性対応に関連する重要な、または新しいテクノロジーとプラクティスについて重点的に説明します。

戦略的な CISO (情報セキュリティ最高責任者) が普通に配置されるようになり、障害対応の計画が実際の消防活動に類似したものになりつつあるのは、セキュリティ攻撃の重大性と複雑性の尺度となります。これには、複数の理由があります。

1 つは、セキュリティは、単にテクノロジーの問題ではなく、ビジネスのコンテキストの中でアプローチする必要があることです。これは、たとえば、その損失が許容できるかどうかの観点からビジネスのリスク選好を定義するということです。クレジットカードの発行者は、不正使用による損失が発生することを想定しています。不正使用を完全に防止しようとすると、クレジットカードの利用が面倒なものになり、誰もクレジットカードを使用しなくなるため、クレジットカードの発行者は、損失が許容可能なレベルに抑えられるように十分に管理しながら、ユーザーの利便性への全体的な影響を最小限に抑えています。

セキュリティがより深刻に捉えられるようになっているもう 1 つの理由は、火災や自動車事故と同様、セキュリティは一刻を争うものだからであり、役割、責任、プロセスを事前に確立しておく必要があります。これには技術的な専門知識が重要になりますが、インシデントの影響を受ける可能性のある人、そして報道機関などの幅広い支持者と情報を共有するための明確なコミュニケーションの計画を立てておくことも重要です。

セキュリティを始める

セキュリティは、安定性と安全性を目指すことから始まりますが、多くの場合、恐怖や懸念、そしてライフサイクルのあらゆる場所で資産を侵害されないようにする必要性によって注目されます。現在の IT アーキテクチャと外部の脅威環境を複雑化しているものが何であれ、現在の環境に適用可能な、実績のあるテクノロジーとプラクティスから始めることは依然として有効です。

オープンソースがその良い例です。オープン開発モデルであれば、業界全体が合意する標準に基づいて、各組織の最も優秀な開発者が継続的にテクノロジーをテストすることで改善を進めることができます。政府機関や金融サービスを含む、さまざまな業界のお客様とのコラボレーションを通じてソフトウェアを開発することで、セキュリティ関連のディスカッションと製品機能の実装に役立つ貴重なフィードバックが提供されます。IT セキュリティの問題は 1 人では解決できません。コミュニティと連携して問題を解決することこそが、テクノロジーの未来です。

Linux は、オープンソースモデルを使用して構築されたセキュリティ関連の幅広いテクノロジーの利点を活用してきました。それには次のようなものがあります。

- 動的に管理されるファイアウォール
- SELinux による強制アクセス制御
- 幅広いユーザー空間とカーネル強化機能
- ID 管理とアクセス制御
- SHA-512 ベースのパスワードハッシュ
- ファイルシステムの暗号化

2 NIST Special Publication 800-27 Revision A

さらに、オープンソース開発プロセスでは、脆弱性が発見された場合に、開発者とベンダーのコミュニティ全体が協調してコード、セキュリティアドバイザリー、ドキュメントを更新します。

Red Hat Enterprise Linux は、最も規制が厳しいセンシティブな業界における IT 基盤であり、オープンソースのセキュリティに関する進歩が予測可能で利用しやすい形で取り込まれています。オペレーティングシステムの役割が進化、拡大し、Linux コンテナなどの新たな機能が導入されるのに伴い、これと同じプロセスとプラクティスがハイブリッドクラウドインフラストラクチャ全体に適用されます。さらに、コンポーネントは、マイクロサービスの形式や、アプリケーションプログラミングインターフェース (API) を使用してやり取りを行う、疎結合されたその他のアーキテクチャの形式で再利用されます。このため、これらのコンポーネントのソースの信頼性と、アプリケーションの開発時にその依存関係を維持することがより重要になります。

セキュリティの運用

従来、セキュリティは、多くの場合において、一元管理された機能としてアプローチされてきました。これまで組織は、環境全体でユーザー、マシン、サービスアイデンティティの信頼できる唯一の情報源を構築し、アクセスできる情報と実行できるアクションについて規定してきました。

現在は、多くの場合、状況はより複雑になっていますが、ユーザー ID を管理するアクセス制御ポリシーを構築して、必要に応じて権限を委任し、他の ID ストアと信頼できる関係を確立することは依然として重要です。しかし、Linux または他のオペレーティング環境上で実行されるアプリケーションコンポーネントは、複数の認証システムとアクセス制御リストに従っている場合があります。

重要な点は、このような複雑なハイブリッドおよび異種混在環境を把握して管理することです。たとえば、ポリシーのリアルタイムの監視と適用により、パフォーマンスと信頼性の問題が深刻なる前に対応できるだけでなく、コンプライアンス問題の検出と緩和も可能になります。このような方法で自動化することで、必要なシステム管理の作業量を削減できます。また、プロセスを文書化し、エラーが発生しやすい手作業を削減する方法にもなります。人的エラーは、セキュリティ違反や停止の主要な原因として常に挙げられています。

運用の監視と修正は、システムのライフサイクルを通して継続する必要があり、これはプロビジョニングから始まります。継続的なシステム管理の他の側面と同様、完全なレポート、監査、変更履歴を保持することも重要です。

セキュリティポリシーと計画の必要性は、アプリケーションの利用が終了しても終わることはありません。保持要件と個人を特定できる情報 (PII) のサニタイズに準拠するために適切な措置を講じることができるように、アプリケーションに関連付けられているデータに関する所有権とポリシーを十分に把握する必要があります。

従来型の長命のアプリケーションインスタンスでは、安全なインフラストラクチャを維持することは、設定の傾向を分析して自動的に修正し、ホストを最適な状態にすることも意味します。これは多くの場合、重要な要件になりますが、クラウドネイティブ環境において、寿命の短い、多くの「不変の」インスタンスが果たす役割は増しているため、最初からセキュリティを組み込むことが同様に重要になります。たとえば、コンテナ化されたソフトウェアスタックのレイヤーで有効化されたサービスに関して、規定に基づくポリシーを確立して適用できます。

セキュリティに対してリスク管理アプローチを採用することは、効果的なテクノロジーを導入するだけでなく、ソフトウェアのサプライチェーンを検討し、問題を迅速に解決するためのプロセスも必要になります。

たとえば、ソフトウェアコンポーネントのソースが信頼できるものかを検証することが重要になりますが、効率的で俊敏性に優れたアプリケーション提供のモデルであるコンテナは、まさにその良い例です。コンテナは、ソフトウェアをまとめる、配布、導入するためのシンプルで効率的な方法ですが、すべてのソフトウェアのソースが信頼できるかどうか、また、セキュリティとサポート性の最高水準を満たしているかどうかを IT 部門が確認できない場合は、このような簡素さは頭痛の種になることがあります。

前述のように、インシデント対応は、コードのパッチ適用だけでなく、統合テストによる迅速なソフトウェア導入プラットフォームとプロセスも、速やかに問題を修正（および本番環境に適用される間違ったコードを削減）する際に重要になります。自動化された反復的な DevOps ソフトウェア提供プロセスの一部である、継続的な統合/継続的な提供（CI/CD）のパイプラインは、モジュールコードの要素を体系的にテストして、適時にリリースできることを意味しています。さらに、セキュリティプロセスをソフトウェア導入ワークフローに明示的に融合することで、セキュリティは、本番環境への経路をブロックするゲートキーパーとしてだけではなく、ソフトウェア開発の持続的な要素になります。

ハイブリッドクラウドにおけるガバナンスとコンプライアンス

パブリッククラウドにおけるセキュリティの欠如に関して反射的に懸念を抱くことは神経質と思われることかもしれませんが、ハイブリッドクラウドでは、リスクとコンプライアンスを考慮しており、従来型のオンプレミスデータセンターにおいて抱く懸念とは異なる課題があります。重要な点は、パブリッククラウドを使用する場合に責任を維持する領域を理解することです。たとえば、Infrastructure-as-a-Service（IaaS）の場合は、オペレーティングシステムとアプリケーションのソーシングと維持に、オンプレミスで実行する場合と同様に注意を払う必要があります。

さまざまなフレームワークにより、IT エグゼクティブとアーキテクトは、パブリッククラウドプロバイダーの使用に伴うリスクを評価して緩和することができます。Cloud Security Alliance（CSA）の Cloud Controls Matrix（CCM）は、その良い例です。[3]

CSA CCM では、以下を含む、16 の分野にわたるフレームワークを統制します。

- ビジネス継続性管理と経営の回復力
- 暗号化と鍵管理
- ID とアクセス管理
- モバイルセキュリティ
- 脅威および脆弱性の管理

CCM v3.0.1 では、133 種類の制御を定義しており、各制御と、業界で認められたその他のセキュリティ基準、規制、および制御フレームワーク（例: ISO 27001/27002、ISACA COBIT、PCI、NIST、Jericho Forum、NERC CIP）の関係を明記しています。

3 https://cloudsecurityalliance.org/group/cloud-controls-matrix/

CCM を参照フレームワークとして使用した場合、Red Hat の製品とパートナーシップは、次の領域に最も適しています。

- 変更管理と構成管理
- データセキュリティと情報ライフサイクル管理
- 暗号化と鍵管理
- ID とアクセス管理
- インフラストラクチャと仮想化セキュリティ
- 相互運用性と可搬性

Red Hat では、これらすべての領域でパートナーと連携し、悪用が検出された場合に効果的かつ迅速に対応することで、脅威やインシデント管理など、他の領域もサポートします。

ハイブリッドアーキテクチャによるサービス提供の設計でも、従来型の IT 手法の知識を活用できます。たとえば、IT インフラストラクチャライブラリ (ITIL) サービス戦略は、5 つある ITIL ライフサイクルモジュールの 1 つです。ITIL は、組織の戦略に合致したサービスプロバイダー戦略の設計、開発、実装の指針として利用できるため、ITIL プラクティスを使用して、ハイブリッド IT に適した完全なサービスを設計できます。

技術的観点からのガバナンスとコンプライアンスの重要な要素は、Red Hat CloudForms などのポリシーベースのハイブリッドクラウド管理プラットフォーム (CMP) です。効果的な CMP により、仮想プラットフォームとクラウドプラットフォームで、ロールを委譲した自動プロビジョニング、クォータの適用、チャージバックを使用してサービスにアクセスできます。CMP では、ポリシーベースの複雑なタスクおよびリソースのオーケストレーションと自動化をサポートしており、サービスの可用性とパフォーマンスを確立します。これにより、IT 部門はアプリケーションとインフラストラクチャの処理能力を管理できます。

ドメイン	製品と機能の例
アプリケーションとインターフェースセキュリティ	Red Hat では、業界標準に準拠した API を提供しています。 たとえば、Red Hat JBoss Middleware 製品では、標準の Java™ SE と Java EE API、SAML 2.0 (Web シングルサインオン)、 WS-Security (Web サービスのセキュリティ保護) をサポートしています。
監査保証とコンプライアンス	Red Hat CloudForms の監査機能と各種製品のロギング機能では、監査プロセスをサポートしています。Red Hat では、ロギングおよび分析製品を提供する企業とも提携しています。
変更管理と構成管理	Red Hat Satellite と Ansible Tower では、構成管理とプロビジョニングツールを提供しています。
データセキュリティと情報ライフサイクル管理	アクティブアーカイブなどの Red Hat Gluster Storage 機能は、情報ライフサイクル管理をサポートします。 Red Hat JBoss Data Grid では、Java SE 認証と暗号化機能を使用して、インメモリデータストアに格納されている機密データを保護します。

ドメイン	製品と機能の例
暗号化と鍵管理	Red Hat Enterprise Linux の暗号化機能には、SHA-512 ベースのパスワードハッシュ、ファイルシステムの暗号化、NSA Suite B 暗号拡張と認定が含まれています。OpenJDK も付属しており、Java Community Process で標準化されている Red Hat JBoss Middleware の暗号アルゴリズムインターフェースを備えています。
ガバナンスとリスク管理	Red Hat CloudForms のポリシーに基づく自動化は、組織がガバナンス計画の実施に利用することができる機能の一例です。
ID とアクセス管理	一元化された ID 管理は、Red Hat Enterprise Linux の一部であり、SELinux で提供されている強制アクセス制御です。 アプリケーションレベルの認証、承認、監査機能は Red Hat JBoss Middleware で利用できます。
インフラストラクチャと仮想化	Red Hat Enterprise Linux、Red Hat Enterprise Virtualization、Red Hat OpenStack® Platform、および Red Hat Atomic Host はすべて、堅牢でセキュアなインフラストラクチャです。
相互運用性と可搬性	オープンスタンダードに準拠した Red Hat の製品では、オープン API が提供されます。 コンテナでは、環境間のワークロード可搬性の新たなアプローチが提供されます。
モバイルセキュリティ	Red Hat Mobile Application Platform では、セキュリティとポリシー管理を一元的に制御できます。
セキュリティインシデント管理、E ディスク、クラウドフォレンジクス	セキュリティの脆弱性が発生すると、これらの脆弱性を解決してシステムを保護するための方法をお客様に提供します。
サプライチェーン管理、透明性、説明責任	Red Hat では、リリースされているすべてのパッケージ (コンテナを含む) をデジタル署名し、安全なチャネルを経由して配信することで、サプライチェーンを保護することもできます。
脅威および脆弱性管理	Red Hat Insights は、Red Hat Enterprise Linux と Red Hat Cloud Infrastructure 環境の技術的問題をプロアクティブに識別して解決できるホスト型サービスです。 Red Hat では、Open Vulnerability and Assessment Language (OVAL) パッチ定義の開発とサポートも実施しており、機械的に読み取り可能なバージョンのセキュリティアドバイザリーも提供しています。 OpenSCAP では、標準と仕様に基づいたルールを使用して、システムのセキュリティ構成設定をチェックし、システムを検査して危険な兆候がないかどうかを確認できます。

精選された Red Hat 機能が CSA セキュリティドメインに割り当てられています (組織内部の物理的セキュリティとビジネスプラクティスを重視したデータセンターセキュリティや人的リソースセキュリティなどのドメインを除く)。

「Red Hat CloudForms はまさに万能ナイフです。これさえあれば、インフラストラクチャに関する知見やインテリジェンスの取得など、IT 環境でさまざまなことを実践できます。数値を分析することで、私たちが導入したリソースが何で、導入にどのぐらい時間がかかったかを知ることができました。私たちはそれを Red Hat ソリューションによって実現しました。リソース提供を待つ時間を約 10 年分節約し、2014 年以来、約 500 万ドルのソフトウェア費用を節約することができました。さらに、Red Hat Insights を利用すれば、重大な問題をそれが発生する前に解決できます」

COX AUTOMOTIVE
クラウドおよびインフラストラクチャ自動化
担当マネージャー
JASON CORNELL 氏

RED HAT でセキュアなクラウドを構築する方法

ここまで、Red Hat 製品を利用したハイブリッドクラウドインフラストラクチャのセキュリティ保護について、重要な機能の分野を見てきました。これには以下のものがあります。

- Red Hat Enterprise Linux 7 の暗号化、強制アクセス制御 (SELinux)、ID 管理
- ポリシーベースの詳細なロギングと可視アラート通知: Red Hat CloudForms により提供され、異種混在ワークロードと複数の種類のクラウドに対して迅速な自動対応を可能にします。
- 自動プロビジョニングと管理: Ansible Tower と Red Hat Satellite により提供され、構成のずれを監視して必要に応じて修正することもできます。
- Red Hat JBoss BRMS と Red Hat JBoss BPM Suite: ドメイン固有のビジネスルールに違反するトランザクションを監視して、対応するワークフローを作成できます。

たとえば、Payment Card Industry (PCI) データセキュリティスタンダード (DSS) は成熟し続けていますが、その要件のより厳しい適用が求められています。新たなアプリケーションと最新のテクノロジーソリューションの導入に伴い、企業は、共有環境のコンプライアンスの影響について考慮する必要があります。Red Hat CloudForms により、クライアントは、プライベートまたはハイブリッドクラウド環境を構築または管理する場合に、仮想化環境を管理できるようになります。Red Hat CloudForms では、高度な仮想化管理、プライベートまたはハイブリッドクラウド管理機能、運用の可視化テクノロジーによるクラウドインフラストラクチャの堅牢なメカニズムが提供されます。[4] これには、ユーザー、グループ、場所、その他の属性別にリソースの分離、ロギング、割り当てが可能な集計ロギング機能も含まれ、Cgroups と SELinux ポリシーに基づくきめ細かい制御が可能です。

Red Hat は製品テクノロジーに対して多額の投資をしていますが、セキュリティへの取り組みは、それよりも広範囲で専門的なものです。お客様によるセキュアな環境とプロセスの運用を支援するということは、最新の専門知識を入手し、アップストリームプロジェクトに直接参加し、再現可能なビルドとテストシステムを実装し、パッケージをセキュアに提供し、脆弱性に対して迅速で効果的に対応することも意味します。

セキュリティの脆弱性が発生すると、Red Hat のカスタマーポータル、テクニカルサポートチーム、製品のセキュリティチームは、脆弱性への対処方法とシステムを護る手段をお客様に提供します。Shellshock と Heartbleed にセキュリティインシデントがあったときに、Red Hat のお客様は、危険に晒されていることを認識し、バグが拡大する数時間以内に問題を適切に修正するのに必要な知識、パッチ、アプリケーションを有していました。

たとえば、Red Hat Insights では、Red Hat Enterprise Linux と Red Hat Cloud Infrastructure 環境の技術的問題をプロアクティブに識別して解決できます。このサービスでは、セキュリティと厳しい導入管理を重要視しており、エンジニアのグローバルネットワーク、技術的ソリューションと解決された問題の Red Hat の広範なナレッジベースを活用しています。ナレッジベースでは、システム情報を分析し、決定論的法則のデータベースに照合してチェックします。これらのルールは、Red Hat のカスタマーエクスペリエンスとエンゲージメントのチームが連携して、ワークロードの最適化と問題回避のためのベストプラクティスを特定して文書化した結果です。Red Hat Insights では、この情報をプロアクティブに提供し、修正手順を容易で使いやすい形式で共有します。Red Hat Insights により、運用を効率化して業務上の問題を回避することができます。

4 PCI-DSS 関連の統制の持続的管理およびポリシーの適用をサポートする基盤を Red Hat Enterprise Linux、Red Hat Satellite、Red Hat CloudForms で実現する方法についての詳細は、http://www.redhat.com/ja/resources/pci-dss-compliance-red-hat を参照してください。

「私たちは、病院と診療所のパブリックネットワーク全体のデータ管理と私保険プランの情報を含む、ミッションクリティカルなアプリケーションの高い安全性と信頼性を保証したいと考えています」

ブラジル保健省
分析および保全担当統括責任者
JOSE MARQUES 氏

Red Hat では、リリースされているすべてのパッケージをデジタル署名し、安全なチャネルを経由して配信することで、サプライチェーンを保護することもできます。脆弱性とエラータの情報は、Security Content Automation Protocol (SCAP) スキャナーを使用するなど、大規模に活用できるように、機械的に読み取り可能な形式で提供されます。Red Hat Container Registry を利用すれば、コンポーネントのソースが信頼できる、プラットフォームが改竄されていない、コンテナイメージでプラットフォームコンポーネントまたはレイヤーに既知の脆弱性がない、完全なスタックが商用サポートされていることなどを確認することができます。

エンタープライズオープンソースソフトウェアでは、コードの確認とテスト手法も必要になります。たとえば、Red Hat Enterprise Linux 7 リリースプロセスでは、新しいパッケージをレビューしてセキュリティバグとパッケージングの問題の有無を確認するだけでなく、アップストリームのコードベースに事前の修正を加え、未解決の問題がないかどうかを確認することもできます。Red Hat では、すべてのアクションをロギングする再現可能なビルドシステムにより、所定のビルドの発生場所、時間、方法の把握が可能になり、場合によっては数年後でも、必要に応じてビルドを再作成できます。

以上のように、Red Hat はソフトウェアを一貫して提供できます。その理由は、適切に連携するエクスペリエンスとプロセスによるものだけでなく、Red Hat エンジニアが、Red Hat サブスクリプション製品に関連するアップストリームコミュニティの専門知識を活かして大きく貢献していることも挙げられます。これにより、セキュリティに関連する変更など、Red Hat のお客様にとって重要な変更に影響を与えることができます。

Red Hat では、Red Hat のすべての製品に対する脅威と脆弱性を日々分析し、関連するアドバイスと更新を、カスタマーポータルを通して提供する専門の製品セキュリティチームを擁しています。このチームでは、理論的な問題ではなく、実際に重要な問題を膨大な情報の中から見つけ出します。お客様は、このような専門知識を利用して、重要な問題に迅速に対応できます。Red Hat では、Linux などのオープンソースソフトウェアの他のコミュニティや企業と連携し、情報共有と専門家による評価を通じて、セキュリティの問題によるリスクを軽減します。

結論

現在のセキュリティは、変化を最小限に抑えることを中心とした戦略から、変化に対して最適化される戦略へと移行しています。知見に基づいたワークフローでは、存続期間が数分間の資産でも、複数の環境を可視化して情報を集約し、是正措置を講じる必要があります。セキュリティは、接続されていないチェックボックスではなく、ソフトウェア提供のパイプライン全体を通して不可欠な要素である必要があります。

Red Hat は、このような変革のパートナーになることができます。Red Hat の製品は、テクノロジーを提供し、お客様が必要とする認定資格 (コモンクライテリアや FIPS など)[5] を取得しています。Red Hat は、オープンソースソフトウェアのサプライチェーンに深く組み込まれており、革新的なオープンソース製品を安全、確実に、一貫して提供するための専門知識とプロセスを有しています。

5 http://www.redhat.com/ja/technologies/industries/government/standards

RED HAT について

オープンソースソリューションのプロバイダーとして世界をリードする Red Hat は、コミュニティとの協業により高い信頼性と性能を備えるクラウド、Linux、ミドルウェア、ストレージおよび仮想化テクノロジーを提供、さらにサポート、トレーニング、コンサルティングサービスも提供しています。Red Hat は、お客様、パートナーおよびオープンソースコミュニティのグローバルネットワークの中核として、成長のためにリソースを解放し、ITの将来に向けた 革新的なテクノロジーの創出を支援しています。

アジア太平洋
+65 6490 4200

インドネシア
001 803 440224

ニュージーランド
0800 450 503

ベトナム
800 862 6691

オーストラリア
1 800 733 428

日本
03 5798 8510

フィリピン
800 1441 0229

中国
800 810 2100

ブルネイ / カンボジア
800 862 6691

韓国
080 708 0880

シンガポール
800 448 1430

香港
852 3002 1362

インド
+91 22 3987 8888

マレーシア
1 800 812 678

タイ
001 800 441 6039

台湾
0800 666 052

facebook.com/redhatjapan
@redhatjapan
linkedin.com/company/red-hat

jp.redhat.com
INC0374232_0416