VIRSEC
SOLUTION BRIEF

業界初！

銀行及び金融サービス向けの より良いセキュリティ

オープンバンキングシステム、デジタルトランスフォーメーションの複雑性、及び当業界を標的とする攻撃の増大により、サイバーリスクを管理することは、顧客の信頼を維持し、成長を確保するうえで非常に重要になっています。

Virsecは、サイバーリスクを管理するためのより良いアプローチを金融サービスに提供して、顧客の資産及びデータを常に安全に保ちます。

大規模な金融サービス組織であるか、地方銀行であるか、オンライン決済サービスであるか、支店を持たないネオバンクであるかに関わらず、Virsecは、すぐに攻撃に立ち向かう責任がある社内のセキュリティチームを支援して 、適切なセキュリティ制御が確実に実施されるようにします。

Virsecは、攻撃者が最も価値のあるアプリケーションを支配して顧客データ及び口座情報 を盗み、無断で預入れ資金に影響を及ぼすことができる、保護の重大なギャップを埋めるのに役立ちます。

Virsecセキュリティプラットフォームを選ぶ理由

- 進化する攻撃及びゼロデイ攻撃を特定する
- 現実の攻撃と優先度の低い脅威を区別する
- エクスプロイト挙動のパターンをキャプチャし、コンテキスト的な知識を確実にする
- フォールスポジティブの負担を軽減する
- リアルタイムのアナリティクスを共有し、ファイアウォール、IDS/IPS 、及びADC（Application Delivery Controller）をよりスマートにする
- AppSecが新しい脆弱性を学習するのを加速させる
- 圧倒的な量のタスクから運用部門を解放する

特に下記のメンバーやマネージャに貢献します！

●SOCチーム
今まで見たことのないセキュリティイベントをアプリケーションドメイン内から収集し、プロダクションを中断させることなしに迅速な対応策を推進しながら、アプリケーションを検出・保護します。

●セキュリティリーダー
ITセキュリティソリューション(ファイアウォール、ADC 、WAF 、IPS/IDS など)を有効にすることで、セキュリティポリシーが保護を正確に実施して、攻撃がアプリケーションに到達しないようにします。

●CISO
より強力なサイバーリスクプロファイル及び集約セキュリティ技術によって脅威ランドスケープをより正確に把握して、コンプライアンス及び適切なレベルの通信を効果的に維持します。

●AppSec及びDevOps
専門知識を必要とせずに、スピード、詳細及び自動化を伴う真のシフトレフトの実践を促進します。

「Virsecを用いれば、パッチ適用やフォールスポジティブの追跡といった頭痛の種なしに、今まで見たことがなかった攻撃をプロアクティブに阻止することができます。これは、より良いセキュリティであり、管理もより容易です」

– ITセキュリティ担当ディレクター、世界の トップ100銀行

Raytheon　AVEVA　GHD　Schneider Electric

" We're deploying Virsec in mission-critical areas and seeing very good success. " – Julian Zottl, Cyber & Information Ops, Raytheon

●全業界にわたってクリティカルなアプリケーションを保護
Virsec独自のテクノロジー及び他に類を見ない結果により、VSPは世界中に展開されており、金融サービス、ヘルスケア、政府、防衛、電力、石油・ガス、輸送、テクノロジーなどを含む業界におけるミッションクリティカルなアプリケーション及びインフラを保護しています。

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

VIRSEC

ソリューション概要:バンキング&金融サービス

● 金融マルウェアに対するより深い可視性&認識

巧妙なハッカー、窃盗犯、及びテロリストは、非常に回避的な攻撃から防御する最前線に銀行及び金融機関を立たせることが多くなっています。Virsecは、サービス又はユーザビリティに影響を与えないように、作業を必要とせずに 、システムへの不正アクセスに対する早期の可視性をもたらします。

SecOpsは、アプリケーションが実行される時にアプリケーションを注意深く監視することによって、実行中のアプリケーション及びシステムのアクティビティ、データ、及びメモリ使用量に対する深い可視性を得ることができます。

アプリケーションがクラウドにあるか、データセンタにあるか、仮想環境にあるかに関わらず、巧妙なエクスプロイトが即座に見えるようになります。このことは、サーバ側の金融マルウェア、ランサムウェア又は複雑なファイルレスエクスプロイト、及びゼロデイ攻撃を発生時に特定するプロセスを加速します。

Virsecを用いれば、情報セキュリティ責任者及びサポートチームは、アプリケーション及びサービスを危険にさらす弱点についてのより正確な知識及び理解を得ることができます。

● より高いFSI (Financial Condition Index) サイバーレジリエンス(耐性)

Virsecでは、金融機関がサイバーレジリエンスを保証するのを支援するべく努力しています。
Virsecは、変化する脅威の条件に適応すること及び攻撃に耐えること(又は攻撃から迅速に回復すること)が金融業界にとって不可欠であるということを知っています。

VSP を用いれば、銀行及び金融サービスプロバイダは、危険な攻撃に直面したときにオンラインアプリケーション、ウェブポータル、及びホストされるシステムの完全性を確かなものにすることができます 。

サイバー犯罪者がどれほどマルウェアを導入し、情報システムの変更及び中断を試み、データを破損するとしても、Virsecは、他に類を見ない精度で脅威を検出、アプリケーションを意図した通りにしか機能させません。

Virsecを用いれば、攻撃サイクルに関与している可能性があるイベントの急増への対応を強化して 、ビジネス、パートナー、及び顧客に与える影響を軽減することができます。Virsecは、従来方式では不可能であった防御テクノロジー(特許)により、脅威又は侵害からバンキングビジネスを守ります。

● よりシンプルな金融サービスセキュリティ

Virsecは、最もクリティカルなアプリケーションを多層防御するためのより容易でより包括的な手段をセキュリティ運用部門に提供 します。

VSPが展開されると、増加するアプリケーションインベントリにわたって、ウェブ、ホスト、及びメモリレイヤにおける保護を拡張することができます。VSPは、手作業による継続的なサポートなしに、セキュリティ戦略をネットワークベースのセキュリティツール及び評価管理を超えてアプリケーションスタックまで大きく拡大します。

VSPは以下を含めてクリティカルなファイルをプロファイリング及びモニタリングします。

- コア属性
- 認証情報
- 権限&セキュリティ設定
- コンテンツ
- ハッシュ値
- 設定値
- ファイルサイズ
- ディレクトリ構造
- メタデータ
- ライブラリ
- OS及びファイルシステムのタイプ

Run time Application Memory Protection

最新のファイルレス攻撃や Spectre/Meltdown など プロセスメモリを介したアプリケーションハイジャックを防止 !

● Virsec Systems, Inc.(アメリカ、San Jose)について

Virsec社は、今日の最も巧妙化されたサイバー攻撃 から組織を保護する革新的なサイバーセキュリティリーダーです。
特許を有する高度なテクノロジーは、クリティカルアプリケーションに対する複雑で巧妙化した攻撃を**ほぼ100%の精度でリアルタイム**に阻止する脅威検出の為の画期的な決定論的手法を使用します。

Virsecは、よくある脆弱性エクスプロイト、未知の攻撃及びゼロデイサイバー攻撃や Spectre/Meltdown のような最も巧妙化した脅威から保護する**唯一のソリューション**を提供しています。

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp