VIRSEC®
CASE STUDY

業界初！

大手水道事業者 、Virsecの協力を得てSCADAシステムをセキュリティ保護

上下水道施設の運用の整合性を確保する必要があった

多くの重要インフラ施設が運用の中断の原因となるサイバー攻撃を受け、産業セクターに対して環境保護庁(EPA: Environmental Protection Agency)から警告が出たことに伴い、ある郡 の水資源部は、きれいで安全な水を顧客に提供するために使用されるAVEVA社のWonderware **SCADAソフトウェアに攻撃者が不正アクセスするのを防止するツールを探していました。**

顧客プロフィール

・米国上位5社の水道事業者
・100万人以上に供給
・複数の水処理設備 及びポンプ場
・1日当たり約1億ガロンの水を処理

米国最大の水道事業者の1社として、この顧客はリモート テレメトリユニット(RTU: remote telemetry unit)及びプログラマブルロジックコントローラ(PLC: programmable logic controller)の運用を監督するためにAVEVA社のWonderware制御&監視ソリューションを使用し、水管理プロセス全体を通じて生成される情報を管理しています。

この顧客は、攻撃が既知であるか未知であるかにかかわらず、システムの脆弱な側面に対する攻撃に対処するために、自動化されたセキュリティが配備されているという保証を得たいと思っていました。この顧客の目標は、攻撃が発生した場合に、最も初期の段階で攻撃に対する対応性を確保することでした。

●Virsecセキュリティプラットフォームがデジタルトランスフォーメーションをセキュリティ保護

水インフラ整備で全国的に認識されているこの水資源部は、重要インフラに対するサイバー攻撃のリスクが高まることによる給水の運用及び制御の中断を防止するために、**Virsecセキュリティプラットフォーム™(VSP: Virsec Security Platform)を使用してフルスタックアプリケーションセキュリティ戦略を本格展開しました。**

この顧客はAVEVA社の制御&監視ソリューションを実装していたので、その**全体的なICSセキュリティを改善しようとしていました。**
この顧客のチームは、脅威カバレッジを拡大するとともに、散在した配水施設、集水施設及び水処理施設における施設運用及びサービスに対するサイバー攻撃によって引き起こされるサービス中断のリスクに対処するように調整されたソリューションを希望していました。

慎重な評価の後、この顧客は、アプリケーション制御及びメモリの制御フローの整合性(CFI: control flow integrity)のためにVSPを選定しました。
VSPは、異なる環境で動作するSCADAアプリケーション及び基礎となるワークロードコンポーネントの全ての側面をセキュリティ保護します。

VSPは、この顧客が、許容できるプロセス挙動の本質的知識、プロセスフローに対する可視性、並びにファイルシステム及びメモリの継続的な監視に基づいて、被害が生じる前に壊滅的な攻撃を阻止することを可能にします。

「壊滅的な攻撃に対する懸念が高まる中で、Virsecにより、水道区の運用の重要な側面のためのロバストなセキュリティを確保することができました」
設備セキュリティ運用担当責任者

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

CASE STUDY: Water Resources Utility

VIRSEC

ケーススタディ: 水資源施設

● 主な課題

Virsecと連携する前まで、郡の水道事業者には複数のセキュリティ課題がありました。

・サイバーセキュリティの監視及び維持を支援するITリソース及びセキュリティスペシャリストが限られていた
・ 様々なアプリケーション、並びに可視性及び制御が欠如していることが多い領域における統合されたコンポーネント及びサービスにわたる持続的な脆弱性
・重要インフラに対する高度な攻撃には、施設のITチームにおいて一般的ではない深いセキュリティ専門知識が必要であった
・運用を脅かすイベントに対する迅速な対応がコミュニティのヘルスおよび安全に不可欠であった

● VSPがICS環境を内部から保護

・計画外のファイル変更及びマルウェアのインストールについてファイルシステムを監視する
・アプリケーションプロセスがスポーンされるときはいつでも、確実に正規のライブラリのみをロードする
・ 許可されたプロセスを見分け、ライブラリインジェクション、又は実行ファイル若しくはコアアプリコンポーネントのいずれかの一部ではないコードを検出する
・重要なシステムファイルをハイジャック、不正アクセス、又は利用しようとする悪意のある試みを抑える
・ メモリベースの脅威、ファイルレスマルウェア、及び未知の攻撃又はゼロデイ攻撃を防止するために、プロセスメモリのランタイム可視性を提供する

● Virsecを用いたことによる決定的結果

・ヒストリアン、SCADA及びHMIサイバーエクスプロイト並びにランサムウェアを含む、AVEVA社のWonderwareソフトウェアを強化した
・IDPS、EDR及びEPPを回避する既知の脅威及び未知の脅威に対する100%の攻撃カバレッジを提供した
・特にメモリベースの攻撃、ファイルレスエクスプロイト及びファイルシステム変更について、攻撃にさらされることを数ミリ秒に短縮した
・自動化、チューニング又はフォールスポジティブ解析が不要で、セキュリティリソースを解放した
・従来のEPPソリューションやEDRソリューションとは異なり、シグネチャ更新に依存しないので、エアギャップされた施設に理想的に適している

「Virsecは、攻撃者の可能なドウェルタイムをゼロに減らします。
このソリューションの精度とリアルタイム修復のおかげで、今では運用を中断することなしにセキュリティを強化する 自信があります」

Director of Plant
Security Operations

Recognition

Cyber Catalyst　CRN　Gartner　CYBER SECURITY EXCELLENCE AWARDS WINNER 2019　MITRE　Info Security Products Guide 2020 GLOBAL EXCELLENCE GOLD　Ovum

Partners & Customers

CISCO　Tech Mahindra　NCUA　Raytheon Technologies　Godrej　Schneider Electric　YOTTA
NUTANIX　du　AVEVA　BROADCOM　inspirage　etisalat　GDIT

● Virsec Systems, Inc.(米国、サンノゼ)について

Virsecは、巧妙化した攻撃、未知の攻撃及びゼロデイサイバー攻撃を決定的に防止するセキュリティソリューションを提供しています。
Virsecの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ための画期的な決定論的手法を使用します。

Virsecのテクノロジーの詳細については、弊社までご連絡ください。
詳細については、www.virsec.comをご覧ください。

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