SageOne
TXOne CPS による保護プラットフォーム

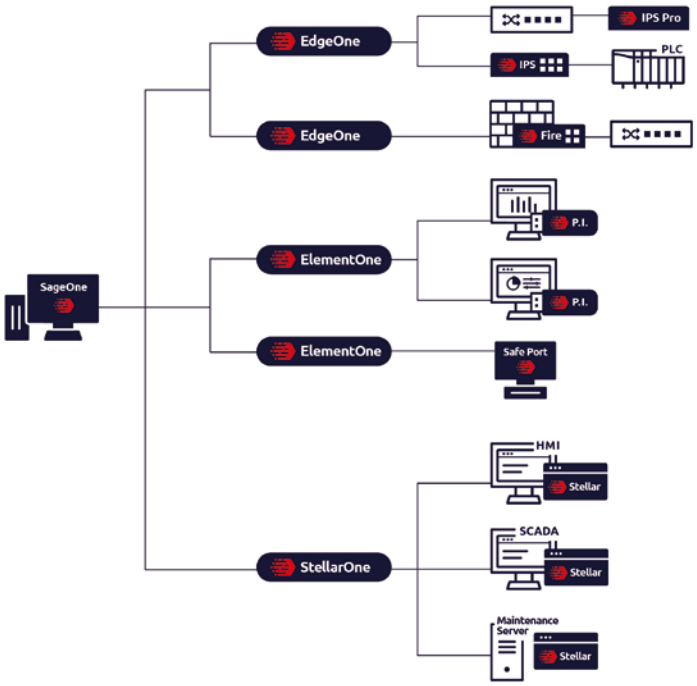
オペレーショナル・レジリエンスの強化：包括的なOT環境可視化、アセット情報連携、管理の簡素化を実現

OT環境において急速に変化するサイバー脅威に備えるため、CPS(サイバーフィジカルシステム)という概念が産業システムに取り入れられ、セキュリティの統制はネットワーク中心のアプローチからアセット中心のアプローチに移行しています。

SageOneは、統合プラットフォームとして、ネットワーク防御、エンドポイント保護、セキュリティ検査の各ソリューションを統合することでオペレーショナル・レジリエンスを強化します。
これは以下の3本の柱によって実現されます。

- CPSによる攻撃対象の管理
- 統合されたアセットライフサイクル保護
- CPSによる検出と対応の連携調和

SageOne1.0は、能動的なサイバーセキュリティ対策を包括的フレームワークの中で提供することにより、TXOne製品のアセットセキュリティ対策と集中管理を実現します。



メリット

能動的なアセットリスク管理
アセットへの攻撃の可能性を特定し、包括的なセキュリティ評価を実施します。そのために、さまざまな観点からアセットを評価し、サイト全体でそれらを比較し、傾向を分析します。優先順位付けを支援するためにさまざまな管理レベルに合わせたビューを作成し、セキュリティ対策を強化して取り組みをより効果的にするための推奨事項を提示します。

集中監視と連携可能情報
集中管理とモニタリング機能でチームを強化し、全製品にまたがるセキュリティ検知の効果的な監視を確実なものにします。チームレベルが異なる場合でも、それぞれが業務に集中できるよう運用を整理し、リソース配置の最適化を行うことで効率アップを実現します。情報が連携可能な状態で得られることにより、マンパワーが限られている場合でも、情報に基づいた意思決定を行い、運用中のセキュリティソリューションの有効性を最大化することができます。

アセットのライフサイクルを通じた保護を統合的に把握
調達から廃棄まで、全ライフサイクルを通じてアセットの保護状態を包括的に把握することができます。アセットライフサイクルのあらゆるステージを網羅するセキュリティ対策を実行することにより、継続的な保護を提供し、サイバーセキュリティのリスクを最小限に抑えます。

データ分析から得られる情報
配下の製品から得られるデータを分析して、セキュリティを強化するために実行可能な情報を提供します。新たな脅威を特定するために得られた情報を利用し、悪意あるパターンの検出や、リスク低減のための先を見越したセキュリティ対策を実行します。

高度な脅威検出と対応の協調
OTに関する深い知識を活用してデータを分析し、疑わしい脅威を特定します。配下の製品を協調動作させることにより、特定された脅威に効果的に対応します。特定された脅威を精査し緩和するために、OTのセキュリティに関するプラットフォームの専門知識を活用して迅速に行動することにより、潜在的なサイバー攻撃を回避し、それらによる影響を最小限に抑えます。

主な機能

- **対処可能な情報**
  高リスクのアセット、接続切れ、旧くなったパターンなど、TXOne ソリューションが検出した重大イベントへ速やかに対応して、緊急に対処すべき推奨情報を受け取ります。

- **アセットセキュリティ対策**
  アセットの保護レベル、健全さ、全体的なリスクレベルなど、すべてのアセットのセキュリティステータスの概要を把握できます。異なるサイトを比較し、アセットの詳細情報、リスク評価および改善の推奨事項を受け取ります。

- **アセット管理**
  アセットのライフサイクルステージおよびセキュリティの状況を容易に閲覧・管理することができ、異なるステージそれぞれに適合したセキュリティソリューションを推奨することができます。アセットのリスクを強調表示し、アセットの絞り込みと検索を行い、情報をエクスポートし、必要に応じてセキュリティソリューションを適用します。

- **センサー管理**
  Edge、Stellar、Element など、接続された TXOne ソリューションの集中管理で、製品間／サイト間の管理を整理します。保護強化のために、ユーザーレベルのセキュリティ操作と各種製品内にある連携可能な情報に対してタスクの概要を提供します。

- **脆弱性管理**
  業務への影響を最低限にしつつ脆弱性の特定を確実にするために、パッシブな脆弱性検出とホストの脆弱性検出を活用します。静的要因と状況的要因の両方を考慮して脆弱性を優先順位付けします。セキュリティ検知を強化するために、仮想パッチと優れたポリシーの適用で代替制御を実行します。

- **CPSによる検出と応答の連携**
  複数のソリューションからセキュリティ情報を収集することにより、潜在リスクを早期検出します。相互解析されたデータで OT 環境内の対応を進めることにより、セキュリティ担当者が IT 環境内で起源を遡って攻撃をトレースできるようになります。

仕様

<table>
<tr><th colspan="5">SageOne－仮想アプライアンス</th></tr>
<tr><th>対応アセット数</th><th>仮想コア数</th><th>必要メモリ容量</th><th>必要ディスク容量（システム）</th><th>必要ディスク容量（データ）</th></tr>
<tr><td>2,500</td><td>4</td><td>12 GB</td><td rowspan="5">20 GB</td><td>100 GB</td></tr>
<tr><td>10,000</td><td>8</td><td>12 GB</td><td>150 GB</td></tr>
<tr><td>20,000</td><td>8</td><td>16 GB</td><td>250 GB</td></tr>
<tr><td>40,000</td><td>12</td><td>32 GB</td><td>400 GB</td></tr>
<tr><td>80,000</td><td>16</td><td>64 GB</td><td>800 GB</td></tr>
<tr><td>対応ハイパーバイザー</td><td colspan="4">VMware ESXi 6.5 / VMware Workstation 17 Pro 以降</td></tr>
<tr><td>対応ブラウザ</td><td colspan="4">Google Chrome 87 / Microsoft Edge 79 / Mozilla Firefox 79 以降</td></tr>
</table>

txOne networks

https://www.txone.com/ja

TXOne Networks Japan合同会社
〒151-0051 東京都渋谷区千駄ヶ谷5-27-5リンクスクエア新宿16階

DS-TXON-011