

ITシステムに侵入したサイバー攻撃を検知するネットワークセンサ

VISUACT™ X

概要

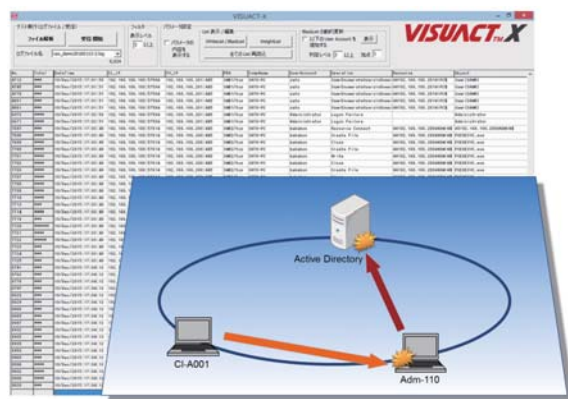
VISUACT-XはITシステムに侵入したサイバー攻撃を検知するネットワークセンサです。ITシステムの内部への侵入を許してしまったサイバー攻撃をリアルタイムで検知します。拡散や基盤構築などの攻撃準備をしている段階でいち早く検知することで、大きな被害が発生する前に対策をとることが可能になります。

機能

- ITシステムを流れる膨大な通信の中からサイバー攻撃だけを抽出し、検知、記録します。
- 管理者レベルのネットワークアクセスを記録できるため、インシデント発生時の調査などに利用できます。
- 外部通知機能により、SIEMなどのセキュリティソリューションと連携できます。

特長

- **サイバー攻撃検知に特化**
膨大なネットワークアクセスの中からサイバー攻撃だけを検知します。
- **新開発「TAAN1(tm)テクノロジー」**
ITシステムを流れるネットワークパケットを多面的に分析し、ITシステムの内部に侵入したサイバー攻撃をリアルタイムに検知します。攻撃者が改竄を施せないネットワーク上の挙動を分析するため、サイバー攻撃を確実に検知できます。
- **サイバー攻撃シーケンスを解析**
攻撃者は攻撃のステップ毎に最適なプロトコルを利用します。VISUACT-Xは、攻撃に複数のプロトコルが使用された場合でも攻撃シーケンスを出力できます。
- **簡単導入**
VISUACT-Xはネットワーク監視型を採用しているため、稼働中のITシステムに悪影響を及ぼすことなく、ミラーポートに接続するだけで使用できます。
- **グローバル対応**
出力形式はUTF-8フォーマットのテキスト形式を採用しており、SIEMをはじめとするグローバルなセキュリティソリューションと連携できます。
- **ソリューション**
弊社のパートナーであるセキュリティ事業者様やシステムインテグレータ様よりトータルソリューションとしてご提供いたします。
- **開発キットの提供**
セキュリティ事業者様向けの開発キットをご用意します(2016年4月予定)。セキュリティ事業者様が独自の検知ノウハウを組み入れた検知エンジンの開発が可能です。



TAAN1™
Technology
TAAN1 テクノロジー

ネットワークパケットの中から特徴的なパラメータを抽出し、サイバー攻撃および管理者アクセスの可能性を判定するフィルタリング技術。

アズビルセキュリティフライデー株式会社 営業部(内田)
〒251-0052 神奈川県藤沢市藤沢89-1 メイキビル3F
TEL: 0466-26-5666 FAX: 0466-26-1130
URL: <http://asf.azbil.com/jp/>
E-Mail: sales@securityfriday.com

※ VISUACTおよびTAAN1は、アズビル株式会社の商標です。