内部ネットワークにおけるWindowsファイル共有を監視する

VISUACT-L

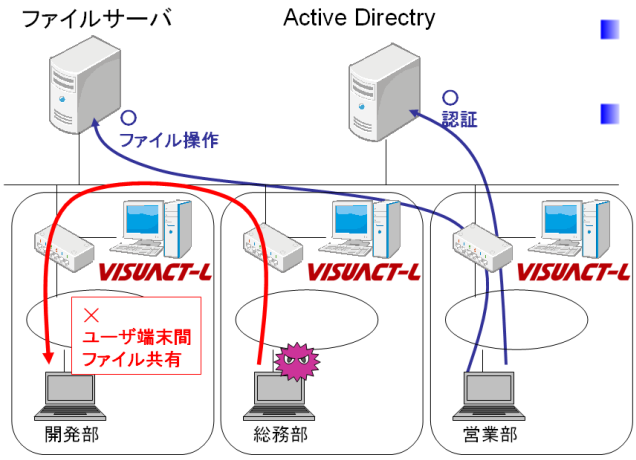
azbil

ネットワークアクセスに偽装は出来ない！

ネットワークアクセスからマルウェアの足跡を早期発見

VISUACT-Lはファイル共有プロトコルSMB/CIFS（SMB2.0)に対応したパケットキャプチャ型のアクセスログ収集ツールです。
ほとんどのマルウェアが、拡散に『ファイル共有の仕組み』を利用するため、VISUACT-Lに足跡（ログ）が残ります。
偽装が困難なファイルアクセスからマルウェアの足跡を発見することが、『早期発見』を可能にします

マルウェア活動監視機能を搭載



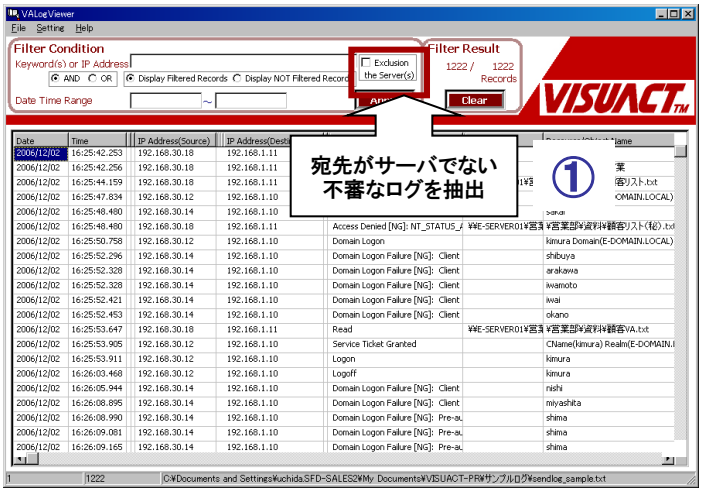
- 各部門のスイッチのミラーポートに接続し、ネットワークアクセスを監視
- 宛先がサーバではない不審なアクセス(*)を検知

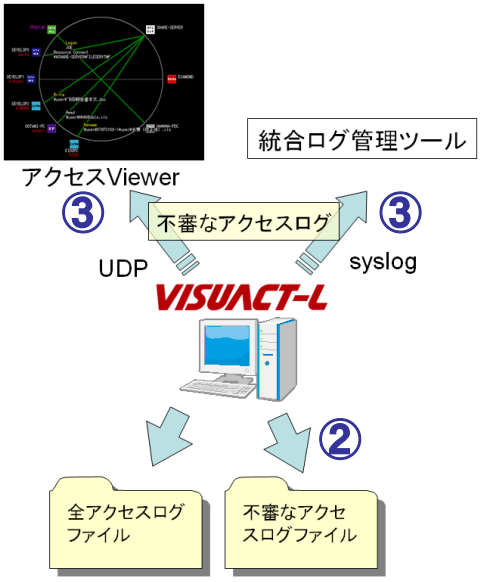
＊：マルウェアによる拡散活動の足跡

① 全ファイルアクセスから不審なアクセスだけを抽出するフィルタ機能

② 一般ユーザによる正常なファイルアクセスログとは別に、不審なアクセスログを別ファイルに保存

③ 不審なアクセスが行われるとUDPまたはsyslogを出力

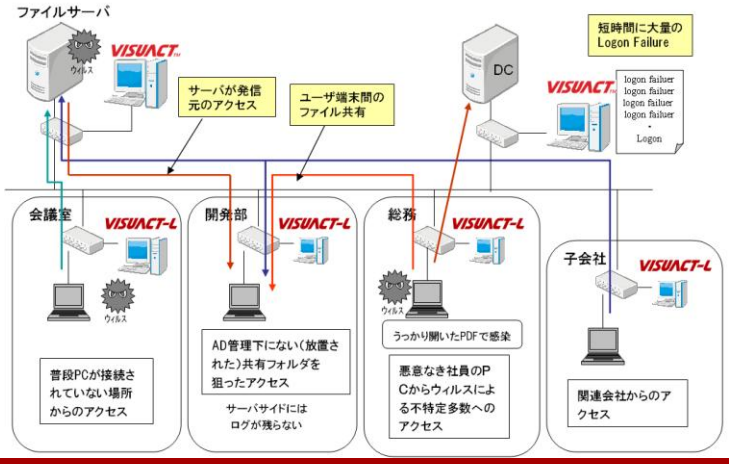




VISUACTシリーズで全社のファイルアクセス監視

【内部漏洩対策】
→ユーザによるファイルサーバへのファイルアクセス

【標的型サイバー攻撃対策】
→マルウェアによる不審なアクセス



アズビル セキュリティフライデー株式会社　URL：http://asf.azbil.com/jp/　sales@securityfriday.com　TEL:0466-26-5666

ファイルサーバ アクセスログ

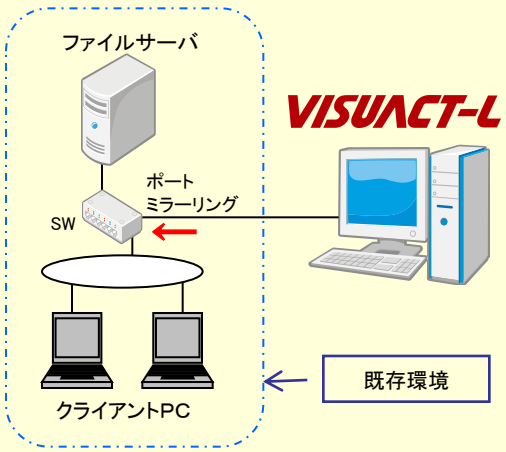
VISUACT-L

azbil

簡単・安全に導入できる、ファイルサーバのアクセスログ収集ツール

VISUACT-Lは、ファイル共有プロトコルSMB/CIFS（SMB2.0)に対応したパケットキャプチャ型のアクセスログ収集ツールです。
企業にとって重要な情報が保存されているファイルサーバへのアクセスをネットワーク上で監視し、詳細なログを出力します。
日本を代表するトップ企業へ多数の導入実績を持つVISUACTテクノロジーを低価格でご提供します。

ミラーポートに接続するだけ。運用中のシステムでも安全に着脱出来ます。



ネットワークスイッチのミラーポートに、VISUACT-Lがインストールされたpcを接続するだけ

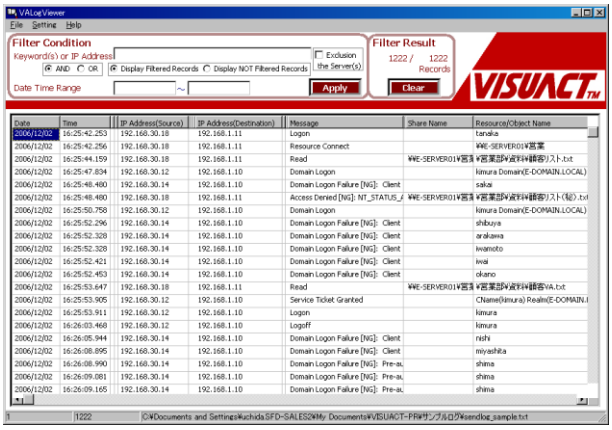
＜特長＞

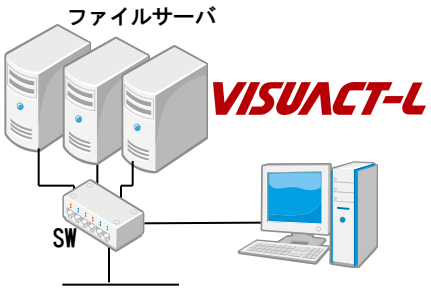
●既存環境にノータッチで導入できます
- ファイルサーバの運用を一時停止する必要はありません
- ファイルサーバの設定変更（監査設定）や、エージェントやスクリプト等ソフトウェアをインストールする必要がありません

●ファイルサーバやネットワークに負荷をかけません
- ファイルサーバのCPU負荷ゼロ
- ファイルサーバのストレージ使用量ゼロ
- ネットワーク負荷ゼロ

●ファイルサーバの種類を選びません
- SMB/CIFS（SMB2.0)に対応したあらゆるサーバに対応。
- サーバを買い替えても流用できます。(Windows⇔NAS⇔samba)

●信頼のVISUACTテクノロジー
- 日本を代表するトップ企業での導入実績多数





＊複数台のファイルサーバに対応
＊1Gbpsネットワークに対応

VISUACTシリーズで内部ネットワーク監視

【内部漏洩対策】
→ユーザによるファイルサーバへのアクセス
　監視

【標的型サイバー攻撃対策】
→内部ネットワークに侵入したマルウェアによる攻撃（SMBを使用した拡散）を監視