FORTINET

“FortiSIEMのすすめ”

もう待ったなし、避けられないセキュリティ問題

- □ セキュリティ事故による情報漏洩が増加、そして企業の経営問題に発展
- □ 企業規模には関係がない、今そこにある危機
- □ ネットワーク管理とセキュリティ機器では足りない、高まるSIEMの必要性
- □ もう待てない!導入までのハードルを乗り越え、各企業で対策が求められる

運用管理者の悩みポイント

複合的攻撃への対応

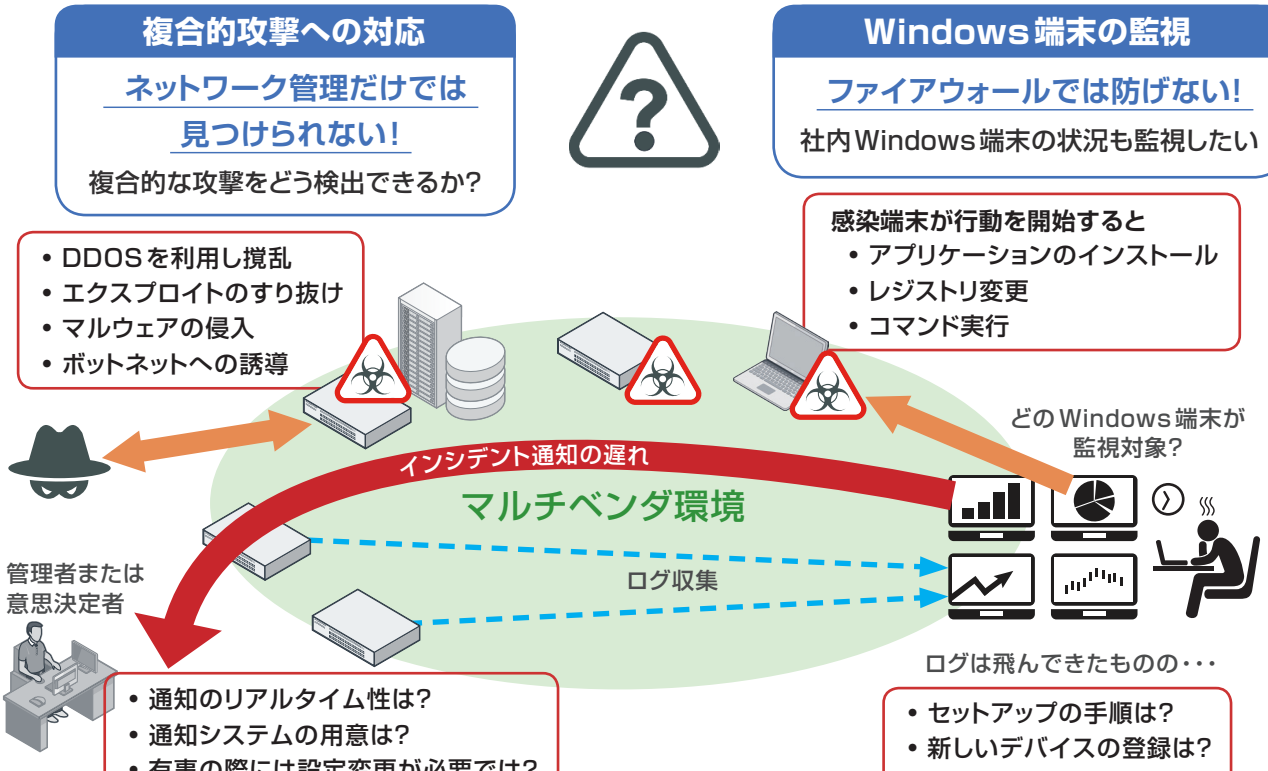
ネットワーク管理だけでは見つけられない!

複合的な攻撃をどう検出できるか?

Windows端末の監視

ファイアウォールでは防げない!

社内Windows端末の状況も監視したい



リアルタイム分析と迅速な通知

企業のリスクを減らすためには迅速な通知と対応が必要

リアルタイムな分析と
通知アクションが求められる

簡易なセットアップ

導入運用までのハードルを低くしたい

分析機能が揃っていても、
運用にこぎ着けなければ意味がない

FortiSIEMで解決、セキュリティリスクを軽減

悩みポイントを解消!
簡易なセットアップで運用を開始
相関分析を可能にし複合的攻撃も撃退

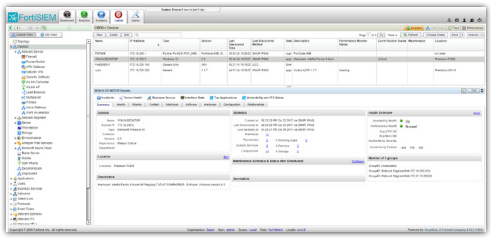
（裏面を参照）

FortiSIEMによる導入運用の実現

- □ ネットワーク管理（NOC）とセキュリティ管理（SOC）を統合
  機器の見落としが無い相関分析を実現
- □ メモリ内リアルタイム分析機能により高速な分析および通知が可能
- □ Windows端末にエージェントソフトを実装すると、より詳細な端末監視が可能
- □ 柔軟な相関ルール作成、多様なインシデント通知方式を設定可能
- □ 簡易なインストールと柔軟なスケーリングを実現

複合的攻撃への対応

様々なネットワーク機器も
統合的に管理し、
リアルタイムに相関分析



Windows端末の監視

専用エージェントソフトの実装により
詳細な端末監視が可能

エージェント追加で拡充する監視機能

- ハイパフォーマンスなSystem,App&Securityログ収集
- DNS,DHCP,DFS.IIS ログ収集
- ローカルパース
- インストールソフトウェア検知
- 各種モニタリング
  レジストリチェンジ、ファイルインテグリティ、
  カスタマーログファイル、WMIコマンド Output、
  PowerShellコマンドOutput

簡易なセットアップ

スーパーバイザ単体の
All-in-One簡易インストールから、
コレクターを利用した大規模展開まで、
柔軟にスケール可能

監視対象の自動検索やレポート機能で
運用をサポート

リアルタイム分析と迅速な通知

インシデント発生時の通知条件や通知方法を
柔軟に設定可能

通知だけでなく、ツール等を自動起動させ
早急な設定変更も可能

FortiSIEM製品一覧 （詳細は製品別データシートご参照）

- ソフトウェアアプライアンス：各種ハイパーバイザに対応
- ハードウェアアプライアンス：FortiSIEM 3500F、2000F、500F（コレクタ専用）

FORTINET

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.co.jp/contact

お問い合わせ

FortiSIEM-JP201711-R1