統合ログ管理ソリューション

McAfee SIEM

サイバー攻撃の迅速・効率的な検知/調査をログ分析で実現

高度化したサイバー攻撃を、ファイアウォール等の境界線防御で完全に防ぐことは困難です。そのような環境で被害を最小限に食い止めるには、内部に侵入したサイバー攻撃をいかに早期に発見することがカギとなります。
サイバー攻撃の早期発見には、ネットワーク機器、OS、アプリケーション等のログを有効に活用することが重要です。

McAfee SIEM の効果

ログを集中管理

- OS、DB、アプリケーション、セキュリティ機器、ネットワーク機器（フローデータを含む）など、様々なデバイスのログを受信できるので、ネットワーク全体のログ管理が可能
- デフォルトで300以上の製品に対応しているので、ログの収集を短時間で開始可能
- 収集したログは一つのコンソールで閲覧できるので、ログの確認、調査が簡単

ログを見やすい形に

- システムごとの異なったフォーマットのログの整形、および情報の抽出と表示が容易に行えるので、ログ分析に集中することが可能
- 時系列でログを表示することにより、異なる機器のログの関連性について把握が容易
- 統計情報を表示することにより、通信状況の把握が容易

インシデントの調査がしやすい

- 通信状況の「いつもの状態」を容易に判断でき、すぐに「いつもと違う」状態に気づくことが可能
- 各システムのログ確認が必要なく、迅速なログ調査が可能
- すべてのログをまとめて確認でき、ログの相関関係の把握が容易
- システム単体のログでは判明しにくいインシデントに気づける

運用がしやすい

- ケース管理機能により、インシデント発生時の対応状況を管理することが容易
- アラート機能により、インシデント発生時には迅速な対応が可能
- デフォルトでレポートフォーマットが用意されており、報告用のレポート作成が容易

主な機能

ログの正規化

- 豊富なログ取り込み対象システム（デフォルト300以上に対応）
- ログをカテゴリに分類し、ログ分析を効率化
- 正規化ルールの作成、カスタマイズが可能

ログ分析

- 時系列、統計、相関分析など多様なログ分析
- 相関分析ルールをデフォルトで搭載し、ルールの作成とカスタマイズが可能
- フィルタによるログの抽出
- ログ分析結果の多様な表示フォーマットを用意

高速処理

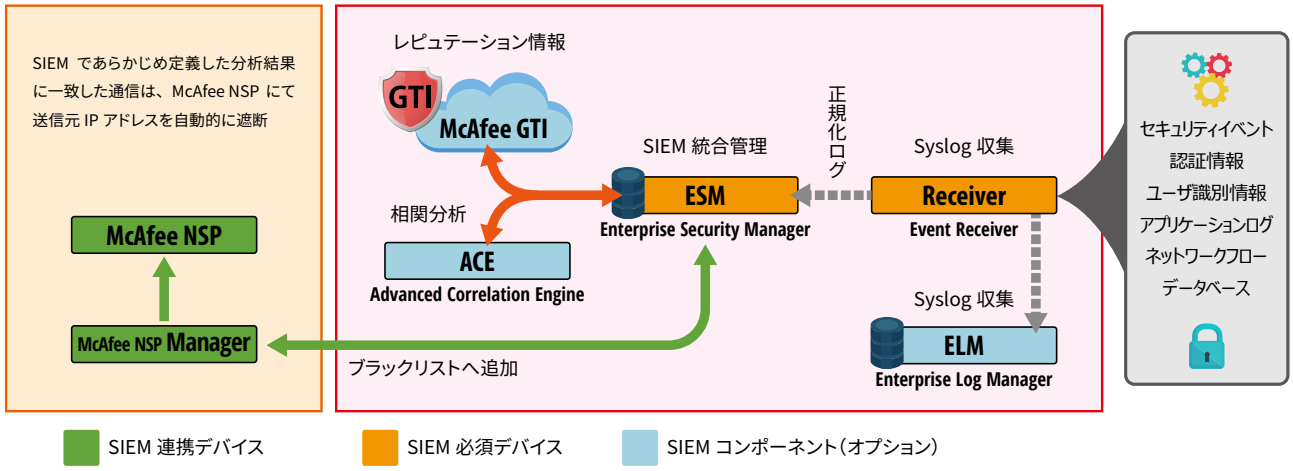
- SIEMに特化した専用アプライアンスと専用データベース
- ログ検索、分析などのログの処理時間を高速化

インシデント対応支援

- ケース管理機能によるインシデント対応状況の記録
- インシデント発生時のアラート通知（メール、Syslogなど）
- レポート作成のフォーマットをデフォルトで用意
- Network Security Platformとの連携で不審な通信の遮断設定を自動化
- 管理GUIへの細かなアクセス制御機能

管理画面サンプル

構成例



McAfee SIEM 運用支援サービス（ディアイティは McAfee SIEM の Service Delivery Provider 認定を取得しています。）

- McAfee SIEM の機能 / 設定 / 操作をより深く知りたい
  McAfee SIEM オンサイトトレーニングサービス
- デフォルト設定にない様々なシステムからログを収集したい
  カスタムパーサ作成サービス
- 社内環境にあったオリジナルの相関分析を作成したい
  相関分析ルール作成サービス
- セキュリティ担当者の疑問や問題点についてアドバイスが欲しい
  セキュリティ担当者支援サービス
- 社内報告用のオリジナル レポート フォーマットを作成したい
  レポートカスタマイズサービス
- インシデント発見後、原因を突き止めたい
  フォレンジックサービス
- 社内に CSIRT を構築したい
  CSIRT 構築支援サービス

ディアイティ サイバーフォレンジックセンター

intel Security Service Delivery Provider

お問い合わせは
株式会社ディアイティ ネットワークセキュリティ事業部　E-mail: info@dit.co.jp　URL: http://www.dit.co.jp/
本社:　〒135-0016 東京都江東区東陽三丁目 23番 21号 プレミア東陽町ビル　Tel: 03-5634-7652
大阪営業所:　〒532-0011 大阪府大阪市淀川区西中島五丁目14番10号 新大阪トヨタビル　Tel: 06-6889-7474