McAfee Enterprise Log Search

膨大なイベントの中から必要な情報を短時間で検出し、脅威ハンティングを迅速に実施

環境で発生するアラートは増え続けています。セキュリティ チームは、このような状況でも迅速な対応を可能にするツールを探しています。このようなチームのアナリストは、詳細なコンテキスト情報を利用し、インシデントに関連するイベント情報をピンポイントで取得する必要があります。McAfee® Enterprise Log Searchは、圧縮されていない未加工のイベント データを高速に検索し、脅威ハンティングを加速化します。バックエンドでElasticsearchを採用することで、クエリーのパフォーマンスを最適化し、未加工ログへの高速アクセスを実現します。高度な検索機能により、簡単なキーワード（自然言語入力）と高度な正規表現パターンで関連するデータを検索できます。

ログ管理の最適化

McAfee Enterprise Log Searchでは、転置インデックスを使用してデータを格納するElasticsearch技術が採用されています。転置インデックスによって構造内のデータがカタログ化されるので、検索語句が効率的に取得されます。Elasticsearchは、高性能な取得とインデックス作成を行うように設計されています。これにより、McAfee Enterprise Log Searchでは、カタログ化された未加工のデータを高速で処理することができます。

McAfee Enterprise Log SearchはSIEM（セキュリティ情報/イベント管理）ソリューションのMcAfee® Enterprise Security Managerを構成するコンポーネントの一つです。SIEMには、McAfee® Enterprise Log Managerというコンポーネントもあります。このコンポーネントは、フォレンジック分析用に受信した未加工ログのハッシュ値（MD5）を生成して圧縮することで、レコードを効率的に格納します。この2つのコンポーネントを併用することで、高速検索（McAfee Enterprise Log Search）とコンプライアンスに必要なログの保存（McAfee Enterprise Log Manager）が可能になるため、使用するツールに悩む必要はなくなります。

McAfee Enterprise Log Searchでは、保存ポリシーをカスタマイズして、非圧縮データの保存期間を年（365日）、四半期（90日）、月（30日）から選択できます。McAfee Enterprise Log Searchと関連付けるデータソースを特定し、最大6個までの保存ポリシーを追加できます。

主な特長

- ログの保存期間と高速検索の両方を最適化するログ管理
- Elasticsearchを利用したバックエンドにより、高速な取得、インデックス化、クエリーを実現
- 自然言語検索
- 解析済みのデータビューから未加工のログに迅速に移動
- McAfee Enterprise Security Managerと完全に統合
- 物理アプライアンスと仮想アプライアンスに対応した柔軟な配備オプション（ミックスアンドマッチ）

McAfeeとつながる

高度な検索機能

McAfee Enterprise Log Searchの検索機能は、人気の検索エンジンと同じように自然言語入力に対応しています。簡単なテキストやキーワードを入力して検索結果を取得できます。ブール論理、ワイルドカード、正規表現（RegEx）など、高度なパターンで検索を実行できます。また、データソースや日付でフィルタリングし、検索結果を絞り込むことができます。日付フィルターでは、過去1時間、今日、昨年など、ログ イベントが生成された時間の範囲を選択できます。選択範囲の定義も可能です。

McAfee Enterprise Security Managerとの統合

McAfee Enterprise Security Managerとの統合により、アナリストは解析済みのデータから未加工のデータにワンクリックで移動できます。McAfee Enterprise Security Managerでイベントが生成されると、解析済みのイベント ファイルがソース ログ ファイルや特定の未加工のログ レコードに直接リンクされます。問題のログを選択すると、未加工ログの検索プロンプトが表示され、レコードやその部分を簡単に確認できます。未加工ログを検索するために、余分な操作を行う必要はありません。この機能を起動するアプリケーションやインターフェースも必要ありません。

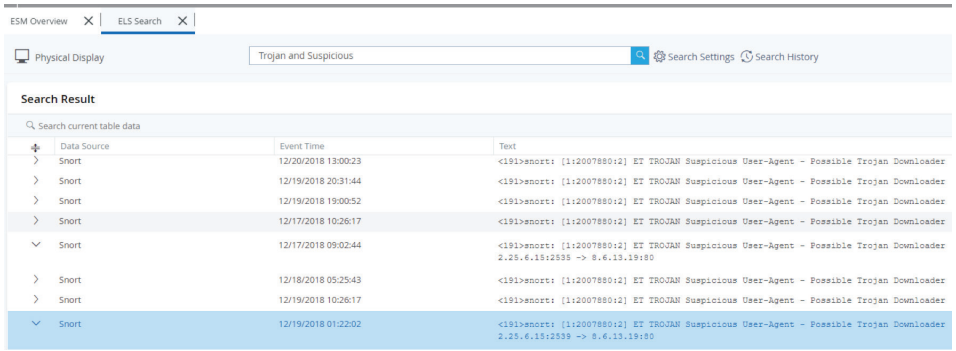

図 1. ブール論理を使用してキーワードを検索すると、トロイの木馬が潜むイベントや不審なイベントを検出できます。

柔軟な配備オプションと料金体系

物理アプライアンスと仮想アプライアンスに対応した柔軟な配備オプションが用意されています。アプライアンスの能力はデータソースあたりの料金、EPSあたりの料金、インデックス付きのデータ量による料金ではなく、イベント数/秒（EPS）で評価され、この能力別に販売されています。仮想（VM）のライセンスも同じ基準で提供され、特定のEPSのサポートで必要なCPUコア数別に販売されています。このため、ハードウェアを交換することなく、必要に応じてコア数を追加できます。

必要なデータを収集し、迅速に検索

McAfee Enterprise Log Searchを配備すると、脅威ハンティングでよく利用される6種類のログを収集し、検索できます。これらのログにより、セキュリティ インシデントのインサイトやコンテキストを確認できます。

ログの種類	利用できるデータ
DNSログ	▪ クエリーで照会されたドメイン名 ▪ DNSクエリーの送信元IPアドレス ▪ DNSクエリーの成否 ▪ 解決されたIPアドレス（クエリーに成功した場合） ▪ 応答のTTL値 ▪ 使用されたDNSサーバー
プロキシ ログ	▪ 接続中のドメイン/IPアドレス ▪ 転送されたバイト数 ▪ 接続のタイムスタンプ ▪ 使用中のURI ▪ リファラー ▪ ユーザー エージェント文字列
SMTPログ	▪ メール送信者のドメイン ▪ メールの件名 ▪ 送信者のIPアドレス
Windowsログ	▪ Windowsセキュリティ ログ イベント ▪ Windowsアプリケーション ログ イベント ▪ Windowsシステム ログ イベント ▪ Windows Code Integrityログ イベント
DHCPログ	▪ 送信元MACアドレス ▪ 許可されたIPアドレス ▪ リース期間 ▪ 要求とリースのタイムスタンプ
VPNログ	▪ 送信元IPアドレス ▪ IDの認証 ▪ VPN接続確立のタイムスタンプ ▪ 接続の種類: 再開または新規 ▪ 失敗した認証（ある場合）と該当するID

詳細情報

詳細については、**www.mcafee.com/enterprise/ja-jp/products/siem-products.html**をご覧ください。

〒150-0043
東京都渋谷区道玄坂 1-12-1
渋谷マークシティ ウエスト 20F
Tel. 03-5428-1100（代表）
www.mcafee.com/jp