調査解析システム（IAシリーズ）

ハイライト

- **視覚化：**容易にカスタマイズ可能なダッシュボードで、ネットワークのメタデータとイベントを視覚化し共有
- **高速照会：**パケット・キャプチャする複数のノードに対し、ワイルドカードを使用したアプリケーションレベルの照会と調査を一元的に実施
- **強力な検索：**HTTP、SMTP、POP3、IMAP、SSL、TLS、DNS、FTPなど多様なプロトコルにわたるメタデータをインデックス化し、迅速に検索
- **効率的なワークフロー：**統合されたケース管理機能を使用して、調査中にPCAPファイルをアーカイブし、他のアナリストと共有
- **SIEMとの統合：**RESTful APIを使用して、SIEMのフローやメタデータのインデックスにアクセス
- **IOCの集約と捜索：**単一のワークベンチでFireEyeのネットワーク・セキュリティ製品、Eメール・セキュリティ製品、エンドポイント・セキュリティ製品のアラートを集約し、各セキュリティ侵害の証拠や痕跡（IOC： 侵害インジケーター）の潜在的な相関関係を明らかにして詳細な調査を実施
- **レポートのスケジュールを設定：**一定の時間間隔、またはイベント数のしきい値に基づいてレポートが自動的に作成されるようにスケジュールを設定
- **ワンクリックでファイルを再構築：**疑わしいファイル、Webページ、Eメールを素早く安全に再構築してさらなる解析を実施、およびFireEyeのマルウェア解析（AXシリーズ）アプライアンスに疑わしいペイロードを送信して解析を実施
- **成長に合わせて拡張：**単一の管理コンソールから、大容量化が進むメタデータのストレージに合わせて調査解析システム・アプライアンスをクラスタ化し、分散しているネットワーク・フォレンジック・プラットフォーム・アプライアンスや調査解析システム・アプライアンス全体で検索能力を強化

概要

セキュリティ侵害に関する最近のメディア報道でも明らかなように、セキュリティ・インシデントの影響を最小限に抑えるには、早期発見と迅速な調査が重要です。しかし、この2つを実現するには高度で高速なフォレンジック解析能力が不可欠です。

パケットロスのないキャプチャとその検索を可能にする業界最速のフォレンジック・ソリューションであるFireEyeネットワーク・フォレンジックに、使いやすい解析インタフェースを備える一元的なワークベンチが追加されたことで、FireEye調査解析システムはネットワークに潜むセキュリティ脅威の早期発見と迅速なインシデント対応を実現します。また、高度な解析機能と高速パケット・キャプチャ機能の組み合わせにより、FireEyeが提供する包括的な脅威検知・防御機能がさらに強化されます。

アナリストは、攻撃の前後および攻撃中にやり取りされている特定のネットワーク・パケットやセッションを詳しく把握できます。マルウェアのダウンロードやコールバックを引き起こしているイベントを再現し、視覚的な確認を行えば、素早く効果的なインシデント対応や将来の再発防止につながるとともに、通常ネットワーク内の移動に使用されるプロトコルのデコードにより、攻撃者の活動に対する可視性も高まります。

調査解析システムは、単一ノードまたは分散アーキテクチャの多様な構成をサポートしており、ネットワーク帯域幅の消費やメタデータの集約、照会、解析のパフォーマンスを最適化できます。

FireEye

機能

フォレンジック調査を一元的に実施：調査プロセスを迅速化するためには、単一のワークベンチで詳細な解析が必要なアラートを素早く特定し、絞り込みながら、ネットワーク・フォレンジック調査を一元的に実施するアプローチが求められます。次の基本的な質問に迷わず答えることができれば、お客様の組織や顧客、知的財産のより確実な保護につながります。攻撃者はどのようにネットワークに侵入したか。攻撃者はネットワーク内部でどのように振る舞ったか。攻撃者はどこに移動したか。攻撃者はどのくらいの期間ネットワークに留まったか。攻撃者は具体的に何を窃取したか。

レポート機能：FireEye調査解析システムでは、特定の時刻、またはより高度な設定としてイベントが一定回数に達した時点でレポートが生成されるように設定できます。このレポート機能は、ネットワーク内の異常な活動を可視化し、イベントを監視する際に役立ちます。

イベントの視覚化と情報の共有：イベントを視覚化できれば調査に要する時間を短縮し、ネットワークに潜む脅威も検知できます。この視覚化機能を、最大20 Gbpsの速度でパケット・データをキャプチャするFireEyeネットワーク・フォレンジック・プラットフォームと組み合わせれば、脅威の効果的、効率的な発見が実現します。また調査解析システムでは、ガジェットをドラッグ&ドロップしてダッシュボードをカスタマイズすることで、統合されたケース管理機能を使用してPCAPファイルをアーカイブし、他のアナリストと共有できます。

インテリジェンスの統合：FireEye iSIGHTインテリジェンス・ネットワークからIOCを自動的にダウンロードし、過去のメタデータの解析プロセスを自動化してネットワーク内のIOCの有無を確認します。新しいセキュリティ脅威には、まず過去データの検索を優先して対応します。

ネットワーク全体を一元的に可視化：FireEyeネットワーク・フォレンジックがキャプチャしたパケットのメタデータを集約し、集中ダッシュボードにまとめて表示します。これにより解析時の死角が解消され、攻撃活動のステップ「キル・チェーン」全体が浮き彫りになります。アナリストは、攻撃のコンテキストに基づいて、総合的・効果的な対応計画を策定できます。

膨大なデータを超高速照会：照会への応答に何時間も費やすようでは、素早く脅威に対処できません。調査解析システムでは、膨大なデータセットと多様なプロトコルにわたるアプリケーションレベルの検索を、超高速・柔軟に実施できます。

モデル	オンボードのストレージ容量（合計）	寸法	電源/標準的な動作負荷
IA 1000HN16	16 TB	1Uラックマウント、 4.3×43.7×65.0 cm、20.9 kg	650W高効率（1+1）冗長AC電源、 100～240 VAC、60-50 Hz（自動切替え）、 230～280W（標準的な環境の場合）
IA 2000HN48	48 TB	2Uラックマウント、 8.9×43.7×64.8 cm、23.6 kg	1280W高効率（1+1）冗長AC電源、 100～240 VAC、60-50 Hz（自動切替え）

詳細については、FireEyeのWebサイトをご覧ください。
www.FireEye.jp

FireEyeについて

FireEyeはインテリジェンス主導型のセキュリティ企業です。顧客企業は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデントレスポンスといった、組織がサイバー攻撃対策をするうえでの課題となっていた複雑性や負担を解消します。FireEyeは「Forbes Global 2000」企業の4割以上を含む、世界67か国以上の5,600を超える組織で利用されています。

ファイア・アイ株式会社 | 〒101-0054 東京都千代田区神田錦町3-22 テラススクエア8階 |
03−4577−4401 | Japan@fireeye.com | www.fireeye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 |
877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com