報道関係各位

2019 年 10 月 21 日

オープンソース全文検索の Elastic

Elastic Endpoint Security を発表

~SIEM、エンドポイントセキュリティの革命的融合へ~

2018 年 10 月、NYSE（ニューヨーク証券取引所）に上場し、 Elasticsearch／Logstash／Kibana などオープンソースプロジェクトを開発・支援する Elastic（本社：オランダ／アムステルダム、代表取締役：Shay Banon）は、MITRE ATT&CK™マトリックスに基づくエンドポイントの脅威防御、脅威検知分野の草分けであり、業界の牽引役として高い評価を誇る Endgame 社との合併により誕生した、Elastic Endpoint Security を発表いたします。

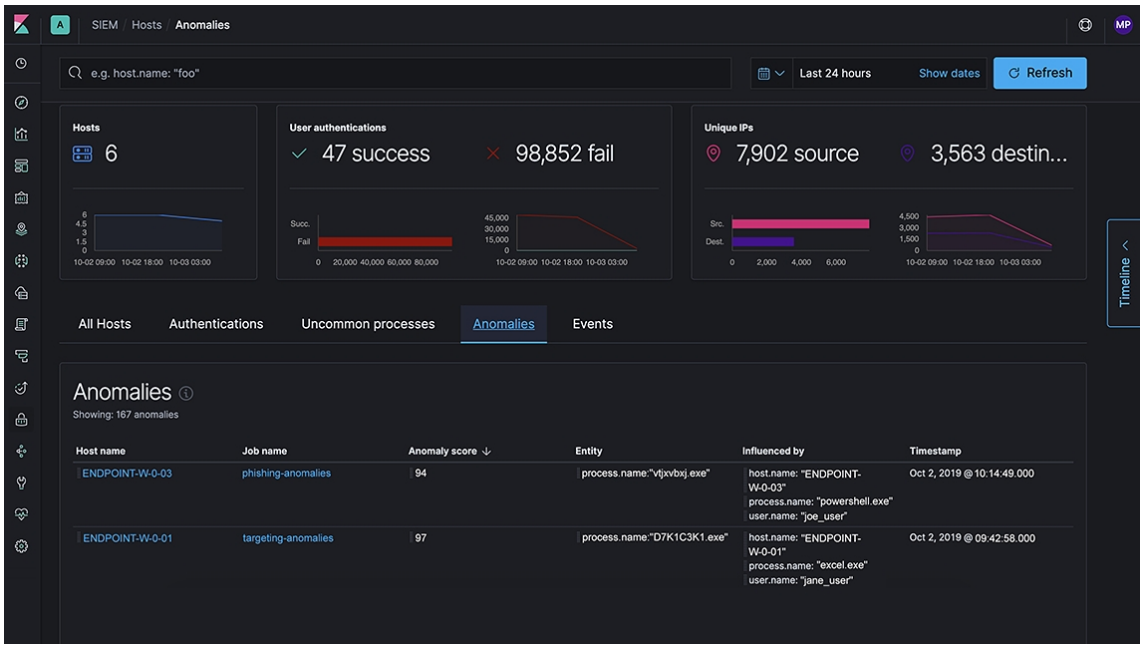
Elastic は SIEM とエンドポイントセキュリティを統合し、単一のソリューションとして提供してゆく予定です。このソリューションで、組織はクラウド、オンプレミス、ハイブリッドのいずれの環境を使用するかにかかわらず、自動的に、フレキシブルに、かつリアルタイムに脅威に応答することが可能になります。Elastic Endpoint Security の導入と併せて本日、Elastic はエンドポイント毎の料金を廃止いたします。

451 Research でプリンシパルアナリストを務めるフェルナンド・モンテネグロ氏は次の見解を述べています。「エンドポイントセキュリティには 2 つの主要なトレンドが存在しています。1 つはバックエンドでの強力な分析の重要性。もう 1 つは MITRE ATT&CK フレームワークが共通言語として普及していることです。両者はケースの重点を脅威ハンティングに置く上で、またインシデントレスポンスのユースケースに役立ちます。Elastic による Endgame の合併は、この 2 つのトレンドに確かに沿うものです。SIEM とエンドポイントセキュリティの統合により、組織はこうしたユースケースで効率性を追求することが可能になります」

Endgame の技術は、NSS Labs 社、SE Labs 社、MITRE 社を含む多数の、独立したテスト実施企業による検証において、最も強力な防止と検知機能を兼ね備えることが証明されています。直近では AV Comparatives 社の Independent Anti-Virus Test（個別抗ウイルス試験）におけるパフォーマンスで、クラウド接続を必要としない Endgame の技術が、現実世界の脅威に対して 99.7%のマルウェアを防止するという驚異的な保護能力が明らかになりました。

さらに Elastic Endpoint Security は既存のロギング・セキュリティ・APM・インフライベント収集と並び、エンドポイントセキュリティデータに関する強力なソースや生のエンドポイントイベントデータ、Elastic Stack へのアラートを提供するソリューションとなります。脅威の平均的な滞留時間が 100 日間超であるのに対し、データのシッピング、スケーリングから格納までを効率的に実行する Elasticsearch なら、相互にかけ離れたあらゆるセキュリティ関連データを横断して、実践的かつ簡単に、すばやく検索することが可能です。また、エンドポイントセキュリティは Elastic Stack とスムーズに連携し、脅威を防止しながら、可能な限り早い段階での攻撃検知と応答を実現します。

Elastic 創業者で CEO のシャイ・バノンは次のコメントを発表しています。「ユーザーは、デプロイするツール以上の恩恵を手にするべきです。Elastic はその方針に基づき、1 つのスタックで検索、格納、分析、データの安全確保までを行うシンプルな設計で、バリューをすみやかに提供するサービスを開発しています。この度、最高品質の脅威ハンティングソリューションを、最高品質のエンドポイント防御と共に提供することが可能になりました。これは、検索を複数のユースケースに適用するという Elastic のビジョンを実現する大きな一歩です」



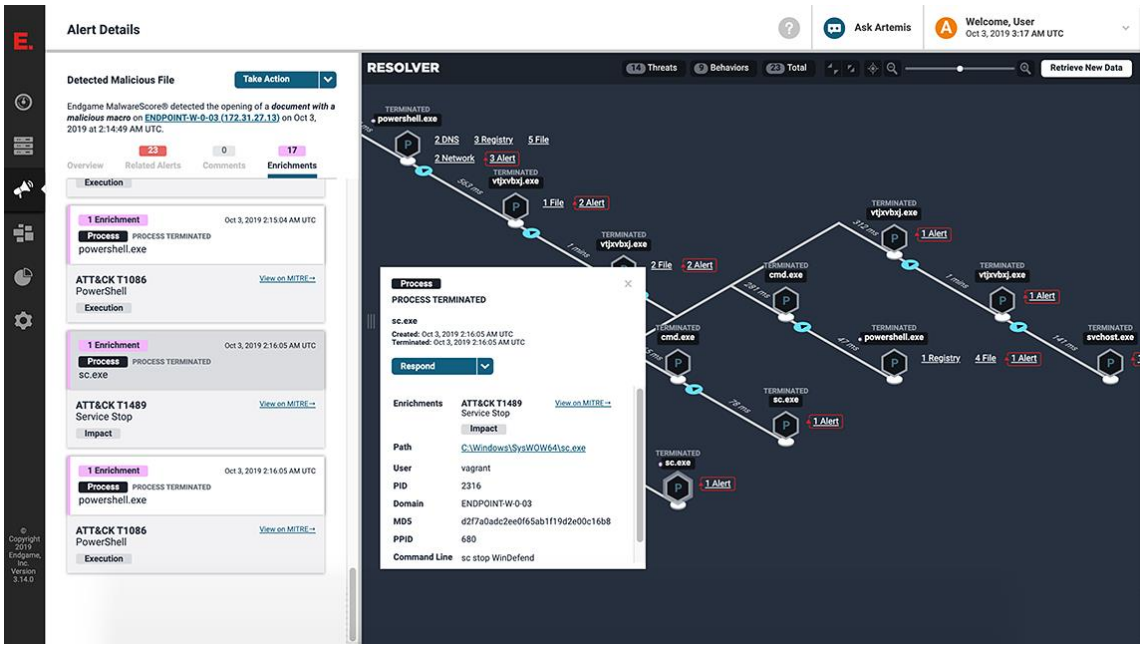
SIEM とエンドポイントセキュリティが目指す場所

組織内で複数のツールが独立に動作していても、安全装置の役割は果たしません。個々のツールが収集するデータを実用的な情報に変換するには、一元的な管理コンソールが必要です。多くのセキュリティチームは、サイロ化されたデータや遅すぎるクエリ時間、関連性やコンテクストの不足による不十分な分析といった問題に直面しています。リアルタイムな作業を実施する必要性はすでに認識されています。たとえばあらゆる種類のデータを制約のない形で投入、および格納する必要があります。関連性を算出し、既存の、あるいは新たなセキュリティワークフローで自動的に運用することも必要です。

Elastic が組織におけるセキュリティの取り組みを進化させるプロジェクトに着手したのは 2 年近く前でした。すでに Elastic Stack は脅威ハンティングや不正検知、セキュリティ監視といったセキュリティソリューションとして利用されていましたが、Elastic はセキュリティ向けにより簡単にプロダクトをデプロイできるようにしたいと考えました。はじめに、コミュニティとの共同作業によって Elastic Common Schema（ECS）が開発されました。ECS はネットワークやホストデータなど、かけ離れたソースから来るデータを簡単に正規化します。次にリリースされたのが **Elastic SIEM**、世界初の無料かつオープンな SIEM です。もちろん、これで終わりではありません。

今回の Elastic Endpoint Security 導入により、Elastic SIEM 用にデータ収集エージェントをデプロイすると同時に、エンドポイントを保護することができるようになりました。タイムリーな応答のできない複数ソリューションの併用など、非効率なスキームを排除し、損害や損失を回避できます。

前 Endgame CEO で現在は Elastic Security のジェネラルマネージャーを務めるネイト・フィックは次のように述べています。「できる限り早期に攻撃を止めることが目標です。そのために、エンドポイントでは最高水準の防止策と高精度の検知機能が求められます。Endgame のすぐれたエンドポイント防御テクノロジーと Elastic SIEM を組み合わせることで、セキュリティ運用・脅威ハンティングチームが攻撃を阻止し、組織を保護するためのインタラクティブな作業スペースが誕生します」



エンドポイント料金の廃止

Elastic は、世界初の無料かつオープンな SIEM へ最高水準のエンドポイントプロテクションテクノロジーを導入すると同時に、エンドポイント毎の料金を廃止します。

シャイ・バノンは次のように説明しています。「保護を必要とするデバイスの数をユーザーが数えなければならないというのはナンセンスです。脅威インテリジェンスデータを保持するのに、何日分の費用をかけるか選択するというのもおかしなことです。Elastic は組織に最高水準の防御を提供し、組織がその防御をどこでも活用できるように、そしてエンドポイント毎の費用で組織が負担を被ることのないようにしたいと考えています」

Elastic のソリューション（Elastic ログ、APM、SIEM、App Search、Site Search、Enterprise Search、そして今回加わった Endpoint Security など）をご利用いただく場合、ソリューションの種類を問わず、費用はリソースキャパシティに関しての請求となります。これにより、ユーザーに一貫性のある、明瞭な料金体系が提供されます。この料金体系は、組織がデータの価値を最大に引き出す取り組みを支えます。Elastic Endpoint Security を利用するユーザーは、必要なエンドポイントの数だけ完全な保護を受けることができ、またエンドポイントを危険にさらすことなく、完全なデータ収集とシッピングを実施することができます。

各種資料

- Elastic Endpoint Security ソリューションページ
- Elastic Endpoint ドキュメント

Elastic について

全文検索エンジンを提供する企業、Elastic は Elastic Stack（Elasticsearch、Kibana、Beats、Logstash の製品群）の開発元です。検索、ログ、セキュリティ、分析などのユースケースで大規模データをリアルタイムに処理するサービスを、オンプレミスと SaaS で提供しています。

報道関係者からのお問合せ先

Elastic 広報事務局　（カーツメディアワークス内）
担当：村上、伊藤、ジェレミー
TEL：03-6427-1627　E-mail：contact@kartz.co.jp