ソリューション理解から製品比較のポイントまで―EDRまるわかりガイド

アップデートでさらなる機能強化を果たした「ESET Enterprise Inspector」

サイバー攻撃がますます高度化、そして多様化するなかにあって、攻撃を受けたあとの迅速かつ適切なインシデントレスポンスを実現するソリューションとしてEDR(エンドポイント検知／対応)製品への注目度がますます高まっている。『ソリューション理解から製品比較のポイントまで――EDRまるわかりガイド※』という連載でこれまでに紹介したとおり、数あるEDR製品のなかでも高い評価を誇るのが、キヤノンマーケティングジャパン(以下キヤノンMJ)が提供する「ESET Enterprise Inspector(以下EEI)」である。本稿では、その運用性の高さやカスタマイズのしやすさなどを振り返るとともに、さらなる機能強化を果たした最新版の概要とデモ画面による操作性について、担当者の声とともに紹介しよう。

事前対策と事後対策を統合したセキュリティ対策をデザイン

幅広いエンドポイントセキュリティ製品をラインアップしているESETシリーズは、30年にもおよぶ歴史のなかでさまざまな研究を積み重ねており、その成果がEEIにも反映されている。だからこそ、世界中の企業や第三者機関から高い評価を受けているのだろう。では、新型コロナウイルスの感染拡大による社会の変化には、どのように対応しているのだろうか。

キヤノンマーケティングジャパン セキュリティソリューション商品企画部 課長代理の植松 智和氏はこう話す。「コロナ禍を受け、多くの企業では在宅ワークをはじめとしたテレワークを導入するなど、1年ほどの間に大きな変化が起きています。このため以前であれば自社ネットワークの外側から内部へと向けた攻撃を重点的に防御すればよかったのですが、いまや保護すべき対象は自社の境界内部に留まらず、社外にも守るべき資産が存在しています」

キヤノンマーケティングジャパン株式会社
セキュリティソリューション商品企画部
課長代理
植松 智和氏

ESET製品では、アンチマルウェアを中心としたエンドポイントセキュリティ対策の基盤として「ESET Endpoint Protection シリーズ(以下EEP)」という製品があり、攻撃を成立させないことをコンセプトとした防御を行う(事前対策)。一方、EEIでは、エンドポイントのあらゆるイベントを集約・分析することで、EEPだけでは発見しづらい脅威の検知や封じ込めなど、攻撃成立後の対処をコンセプトとしている(事後対策)。つまり、両製品を組み合わせることで、事前・事後どちらの対策もより強固なものとなるのだ。

コロナ禍でテレワークが定着しつつあるなか、従来の「境界防御」では防ぎきれない攻撃が浮き彫りになっている。そのような現状において、エンドポイントを守るためのセキュリティ強化として、両製品の活用はとても有効と言えるだろう。

植松氏も「EEPとEEIを組み合わせることで、幅広い領域を防御可能とする、事前対策と事後対策を統合したセキュリティ対策をデザインできることは、ESET製品の強み

だと自負しています」と語る。

運用性とカスタマイズ性の高さもEEIの魅力

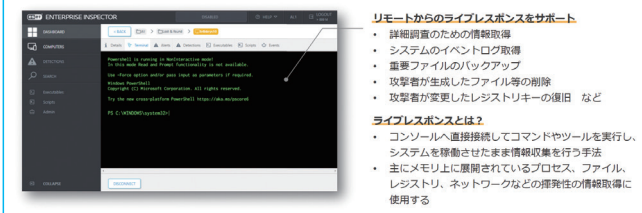
EEIがほかのEDR製品と比べて優れている点は多々あるが、高いレベルの運用性と柔軟かつ容易なカスタマイズ性はその代表的なものと言える。エンドポイントの挙動を継続的に監視して、そこから一定のルールに則って「不審な挙動(＝脅威の可能性)」を検出するのがEDRだが、ある挙動を脅威と判定するか否かの判断基準というのは、企業ごと、さらには部門ごとに異なってくる。そのためEDRの運用にあたっては、脅威を判定するルールを自社環境に最適化したうえで、そのあとも継続的にチューニングしていく必要があるのだ。

このチューニングやカスタマイズを効率的に行えるよう、さまざまな機能を有しているのがEEIである。たとえばEEIからあがってくる個々のアラートの内容をみていくと、なぜ脅威として検知したのか、その理由が詳しく記述されている。この情報をもとに、セキュリティ担当者は個々のアラートについて、きっかけとなった動作に応じた挙動をワンクリックで設定していくことができる。加えてEEIは、企業ごと、部門ごと、さらにはチームごとなど、それぞれの事情に応じたチューニングも容易に行える。キヤノンMJでは、こうした導入先の事情に合わせたEEIの最適化をはじめ、実運用が軌道に乗るまでの支援も行っており、最終的には自社だけでルールを設定していけるよう手厚いサポートを提供している。

新バージョンで加わる数々の新機能

2021年2月26日より提供を開始したEEI V1.5ではさまざまな新機能が加わっているが、そのひとつとなるのが「ターミナル(Remote PowerShell)機能」の実装である。これにより、Webコンソールから端末に対してRemote PowerShell経由でアクセスし、PowerShellコマンドを実行することが可能となった。侵害端末の調査や修復、重要情報の保全などが、担当者が利用現場に直接出向くことなく、さらにはユーザーの業務利用を止めることなく、リモートで実施できるようになったのである。キヤノンITソリューションズで技術検証にあたる西村亮氏は「EDRとしての機能に加え、Windowsの強力なPowerShellを用いることにより、よりきめ細やかに対応できるようになりました。これにより、侵害などが発生した場合の速やかな対処や、さまざまな調査がEEIの管理コンソール上だけで実現できるようになっています」と語る。

キヤノンITソリューションズ株式会社
サイバーセキュリティ技術開発本部
技術部技術検証課
西村 亮氏



もうひとつの大きな機能追加はMITRE社が開発しているセキュリティに関するナレッジベース「MITRE ATT&CK Framework」のリファレンスを、コンソール上に表示される検出アラートのリンクからワンクリックで参照可能となったことだ。リファレンスは攻撃に使われたテクニックの詳細について解説されているため、状況の把握とそのあとの対応について、迅速かつ的確な判断を促せるようになる。

そして最後に紹介するのが、Googleが運営するウイルス判定サイト「VirusTotal」もしくはサードパーティーのソースに対し、ハッシュ値を用いたカスタムリンクを設定可能となったことだ。「EEIでももちろん、ハッシュ値によるブロックや、プロセスの強制停止をワンクリックで実施可能です。サードパーティーのソースを利用することで、ファイルをブロックする根拠をより明確にすることができます」と西村氏

は語り、外部ナレッジの活用に期待を込めた。

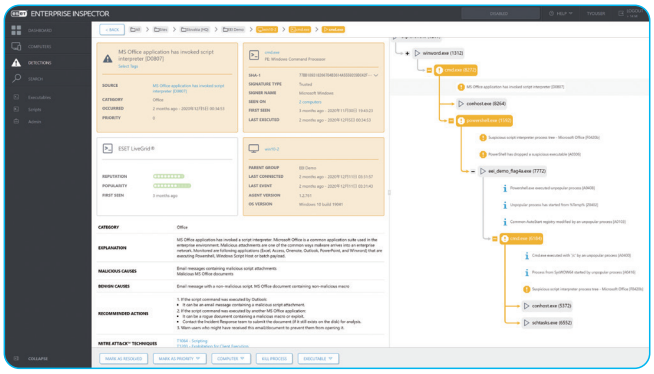
ほかにも新バージョンでは外部連携も強化されており、REST APIによる外部連携によってアクションの自動化が可能となるとともに、RSET APIを介してEEIそのものの運用自動化もサポートする。「こうしてルールベースで自動化することによって、貴重な人間による手間をおさえつつ、速やかな対処が可能になっています」と西村氏は語る。

デモ画面にみる、正規ツールであっても グレーな挙動に警告

ここでEEIのコンソール上にアラートが表示された際の対処法を知るべく、実際の画面をみてみよう。

西村氏はEEI V1.5のデモ画面を操作しながら「EEIのコンソールが、直感的なUIとなっているため、ある程度のセキュリティ知識があれば、アラートに対する的確な操作が容易にできます。V1.4を利用しているユーザーがこの画面を一見すると、ユーザーからみたときの画面上にそれほどの変化はないかもしれませんが、その内部で取れるイベントが増えていて、検知性能の向上につながっています」と説明した。

次に、Officeアプリからスクリプトインタープリターが呼ばれたことを検出した際のアラート画面をみていく。まずは情報確認のためプロセスツリーをみてみると、エクスプローラーからWordを実行し、コマンドプロンプトからPowerShellを実行している。次にPowerShellでは2つのアラートが上がっているので内容を確認すると、実行ファイルが2つあって、最終的にスケジューラーのタスクが実行されていることがわかる。



「EEIでは、アラートの危険度によって表示するときの色をわけており、悪質で危険な挙動の場合は赤色のアラートで表示されます。しかし、このデモ画面ではいずれも赤色ではなく黄色のアラートとなっているのがおわかりいただけるかと思います。黄色は完全に危険というわけではないグレーな領域を指しており、Officeアプリのような正規のツールであっても、グレーな挙動を検出できるのがEDR製品の強みと言えます。特に最近のサイバー攻撃では、正規ツールを使うことでマルウェア検知を逃れるという手法が増えていますので、非常に有効と言えるでしょう」と西村氏は語る。

このように、EEIの管理画面ではわかりやすい操作性はもちろん、脅威に関する情報について、一貫して同じ画面で確認することができる。さらに、同じくESET製品であるEEPとも連携しているので、EEPで検出したマルウェアなどの情報も確認することができ、ここでも管理者の手間を省くことができるようになっている。

＊＊＊

ここまでコロナ禍における事前・事後対策の重要性と、その対策において効果を発揮するEEIについて、運用性やカスタマイズ性、そしてまもなく提供開始される新バージョンの機能追加について紹介してきた。

植松氏は最後に「バージョンナンバーでは一般的に言うところのマイナーバージョンアップかもしれませんが、最新版ではメジャーバージョンアップと言っていいほどのかなりの機能強化を行っています。EDRという製品自体が比較的新しく、脅威も日々更新されていますので、不審な挙動に対す

る検出機構などもそうした変化に対応してアップデートすることが欠かせないからです。今後もバージョンアップの際には、最新のセキュリティトレンドに対応した数多くの新機能が搭載されていくことでしょう」と今後も変化する状況に対応していく姿勢を語ってくれた。

新たな生活様式へと変化するなかで、さまざまな脅威が新たな手法で攻撃を続けている。これからもEEIはそうした攻撃に対応し、さらなるバージョンアップをしていくことだろう。コロナ禍においてセキュリティ強化を図ろうと検討している方は、ぜひキヤノンMJに相談してみてはいかがだろうか。

※マイナビニュース「ソリューション理解から製品比較のポイントまで ―EDRまるわかりガイド」では、標的型攻撃に代表される高度なサイバー攻撃への対策に有用とされるEDRの解説と、導入検討に役立つ製品の比較ポイントの紹介を中心に、エンドポイントセキュリティの新定番たるEDRを紹介してきた。本稿はその第4回目として、アップデートでさらなる機能強化を果たした「ESET Enterprise Inspector」について紹介する。

https://news.mynavi.jp/series/edr_eei/

EDR (Endpoint Detection and Response)

ESET ENTERPRISE INSPECTOR
イーセット エンタープライズ インスペクター

製品の詳細情報はこちら

▶https://eset-info.canon-its.jp/business/eei/

ESET Enterprise Inspectorは、エンドポイントレベルでのマルウェア対策を30年にわたり手がけてきたESET社の経験を基に開発されたEDR製品です。組織内の端末から収集したさまざまなアクティビティをもとに、端末上の疑わしい動きを検出・分析・調査し、組織内に潜む脅威をいち早く割り出し、封じ込めることができます。

EDR運用監視サービス

製品の詳細情報はこちら

▶https://eset-info.canon-its.jp/business/eei/mdr.html

ESET Enterprise Inspectorを用いたEDR運用監視サービスです。24時間365日体制で専門のセキュリティエンジニアがESET Enterprise Inspectorのアラートを監視・分析。危険度に応じて速やかにお客さまへ通知します。侵害端末のネットワーク隔離や不正プロセスの強制停止など、インシデントレスポンスの初動対応も行い、セキュリティ侵害を抑制します。

製品に関する情報はこちらでご確認いただけます。

セキュリティソリューション ホームページ
canon.jp/it-sec

●お求めは信用のある当社で

2021年3月現在

開発元：ESET, spol. s r.o.

キヤノンマーケティングジャパン株式会社
〒108-8011 東京都港区港南2-16-6 CANON S TOWER

MESET2103CMJ-PDF