ご参考資料（ブログ）

報道関係者各位

2018 年 7 月 20 日

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

AI 技術を実採用したチェック・ポイントの新技術「CADET」

有害ファイルの誤検出を 10 分の 1 に削減すると共に、検出率を大幅に改善

米カルフォルニア州 サン カルロス - 2018 年 6 月 13 日
サイバー・セキュリティの世界で特に難しい課題は、あるファイルが無害か有害かを正確に判断することです。例えば、実行可能ファイルの場合を考えてみましょう。その性質上、実行可能ファイルは、特定のプログラム内だけで機能する Word や Excel などのファイルとは異なり、マシン全体にアクセス可能な形で動作できなければなりません。そのため、各実行可能ファイルが無害か有害かをセキュリティ・ソリューションで正確に判断することは、場合によっては非常に困難となります。実行可能ファイルの動作を単純に分析するだけでは不十分で、その動作の意図まで把握する必要があるからです。しかし、文書を読み込もうとする実行可能ファイルの意図を正しく判断する現実的な方法は、残念ながら存在しないのが実情です。

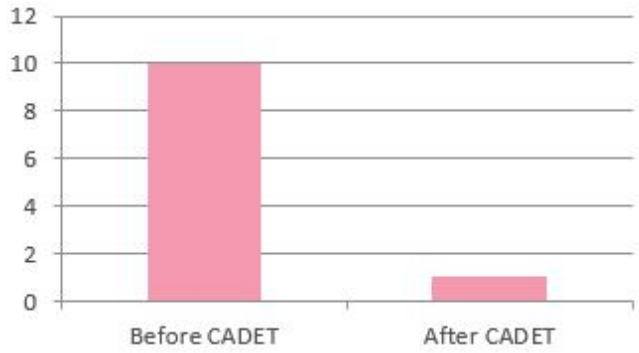
ほとんどのセキュリティ・ソリューションには、この正確性の欠如という欠点が存在します（もちろん、欠点はこれだけではありませんが）。この現状では、多くの IT 担当者がソリューションの防止（ブロック）モードを使いたがらないのも当然といえるでしょう。防止モードを有効にすると、大量に発生する誤検出が原因で、日常業務の遂行に大きな支障が生じる可能性があるからです。

そこで出番となるのが、チェック・ポイントの CADET（Context-Aware Detection and Elimination of Threats）です。AI に基づく最新技術である CADET は、圧倒的な効果を発揮することがすでに実証されています。CADET は、ある特定のリンクやファイルだけを分析するのではありません。有用な情報が多数含まれるチェック・ポイントの「ビッグ・リッチ・データ」をさらに詳しく可視化するための処理を行うアプローチで、コンテキスト情報に基づく的確な意思決定を可能にしています。CADET の AI エンジンは、検査済みの要素とチェック・ポイントが収集したコンテキスト情報の両方から大量のデータ・ポイントを抽出し、実行可能ファイルなどの各種ファイルの信頼性について、正確な 1 つの結論を導き出します。

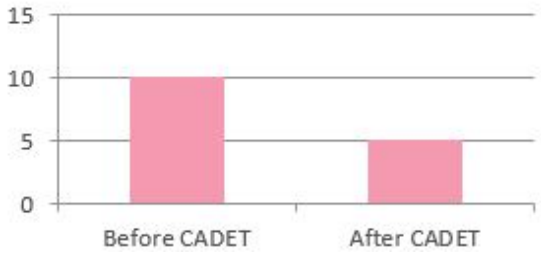
具体的には、セッションのコンテキスト全体を評価し、ファイルに関するすべての証拠を検証して、最終的な結論を引き出します。ここでいうコンテキスト情報には、実行可能ファイルの出所（電子メールか Web からのダウンロードか）、ファイルの提供元、ドメインの登録時期/登録者/登録国、登録者に関係する別のドメイン、これらのドメインが過去数日以内に不正なファイルに関係しているかどうか、などが含まれます。CADET では、数千件に及ぶこれらの変数を分析することで、実行可能ファイルの信頼性を極めて正確に評価し、ゲートウェイの通過を許可すべきかどうかを判断できるようにしています。

CADET はすでに、チェック・ポイントの SandBlast Zero-Day Protection 製品全体に採用されており、誤検出を 10 分の 1 に削減すると共に、検出率を大幅に改善するという効果をもたらしています。より多くのデータから継続的に学習するというフィードバック・ループが組み込まれた CADET の革新的な AI 技術は、業界最高水準の脅威対策技術を提供するというチェック・ポイントの取り組みにおいて、新たな役割を担っています。

■誤検出の低減



■検出漏れの低減



この新しい AI エンジンは、チェック・ポイントの全製品に採用されています。セキュリティ担当者の方は、誤検出の発生を憂慮せずに防御モードを設定し、第 5 世代のサイバー攻撃*から組織を保護できます。

*第 5 世代のサイバー攻撃：
第 5 世代のサイバー攻撃とは、モバイル環境、クラウド環境、およびオンプレミスのネットワークを対象に、大規模かつ高速に展開される攻撃を指します。この高度な攻撃は、組織全体をカバーするセキュリティ・アーキテクチャが考慮されていない場合、多大な影響に発展することが考えられます。

本リリースは、米国時間 6 月 13 日に配信されたものの抄訳です。
米ブログ本文はこちらをご確認ください。
https://blog.checkpoint.com/2018/06/13/introducing-cadet-ai-technology-in-action/
日本のブログ本文はこちらをご確認ください。
https://www.checkpoint.co.jp/threat-cloud/2018/07/introducing-cadet-ai-technology-in-action.html

■チェック･ポイントについて

チェック・ポイント・ソフトウェア・テクノロジーズ（ www.checkpoint.com ）は、世界各国の政府機関や企業などあらゆる組織に対応するサイバー・セキュリティ・ソリューションを提供しています。業界随一の検出率を誇る先進のソリューションにより、お客様のネットワークを、マルウェアやランサムウェアなどの多岐にわたるサイバー攻撃から保護します。企業のクラウドやネットワークのほかモバイル・デバイスに保存されている情報を保護するマルチレベルのセキュリティ・アーキテクチャに加え、直感的で操作性に優れた総合的かつ一元的なセキュリティ管理システムを展開しています。世界の 10 万以上の組織・企業がチェック・ポイントのセキュリティ製品を利用しています。チェック・ポイント・ソフトウェア・テクノロジーズの全額出資日本法人、チェック・ポイント・ソフトウェア・テクノロジーズ株式会社（ http://www.checkpoint.co.jp/ ）は、1997 年 10 月 1 日設立、東京都新宿区に拠点を置いています。

《本件に関するお問い合わせ先》

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社　広報代行　共同ピーアール株式会社

担当　マーケティング　横山

Tel: 03-5367-2500 / Fax: 03-5367-2501
Email: marketing_jp@checkpoint.com

担当　上瀧・花岡

Tel: 03-3571-5238 / Fax: 03-3571-5380
Email: checkpoint-pr@kyodo-pr.co.jp

