CrowdStrike、MITRE ATT&CK評価テストの20すべてのステップにおいて100%の検知率を達成

21 April 2021 | Michael Sentonas（CrowdStrike）| エグゼクティブの視点

MITRE Engenuityによる**ATT&CK®評価プログラム**の第3ラウンドの結果が公表され、CrowdStrikeの顧客が現実世界で活動する攻撃者グループから保護されていることが改めて実証されました。CrowdStrike Falcon®プラットフォームは、20の各攻撃ステップにおいて実用的なアラートを生成し、重大な攻撃活動をインテリジェントに特定するとともに、アラート疲れを回避しました。

この評価プログラムは、2つの洗練された攻撃者グループである「Carbanak」と「FIN7（CARBON SPIDER）」の攻撃手法をエミュレートするもので、ATT&CKマトリクス全体に及ぶ、20の個別ステップと174のサブステップをカバーする攻撃をLinuxおよびWindows OS上で実行しました。MITREの評価テストは、「俊敏性、包括的な可視性、スピード」という情報セキュリティ業界最大の課題に対して、CrowdStrikeがいかに先駆的なソリューションを提供しているかを披露するまたとない機会でした。MITRE ATT&CKのCrowdStrikeに対する評価結果では、CrowdStrike Falconプラットフォームが、侵害防止、検知、コンテクチュアル・テレメトリを独自に組み合わせて侵入を防ぎ、組織に全領域の保護機能を提供すると同時に、セキュリティチームの負荷を軽減することが示されています。

今回の評価テストにおけるCrowdStrikeの成績は次の通りです。

- CrowdStrike Falconは、20の各ステップとMITRE ATT&CKのすべての戦術に対し実用的なアラートを生成し、攻撃ステージ全体で100%の検知率を達成しました。
- Falconプラットフォームは、MITRE ATT&CKフレームワークの複数のステップにおいて、2つの攻撃者グループを模した侵入を両方とも阻止しました。
- CrowdScoreの検知エンジンは、侵害の兆候やテレメトリデータを分析して微細なシグナルを集約することで、非常に高度かつステルス性の高い敵の攻撃を検知しました。
- Falcon Incident Workbenchは、ATT&CK上の戦術や技術、攻撃者の情報、デバイスやユーザーなどの豊富な背景情報をもとに、検知された攻撃に優先順位を付けて可視化しました。背景情報を考慮したテレメトリデータから得られる実用的なセキュリティインシデント情報が提供され、個別のセキュリティアラートを90%削減したうえ、ほかのベンダーにはない手法を用いることで、対応までの時間を劇的に短縮しました。
- Falconは、複合的な視点から攻撃行動を可視化することで、包括的な検知機能を提供し、攻撃者らが検知をすり抜けできないようにしました。

これらの結果は、Falconプラットフォームが攻撃活動に対する独創的かつ最先端の検知・防止機能を提供することにより、セキュリティオペレーションセンター（SOC）による手作業と総所有コストの大幅な削減を実現できることを証明しています。

MITREE ngenuityの評価方法は、**勝者を選抜するためのものではありません**。むしろ、「敵の攻撃情報を得て、ノイズが排除された完璧な状況下において、特定のATT&CKで定義される攻撃手法に製品ユーザーがどのように対処できたか」に注目するものです。そのようなMITREの方法論にもかかわらず、ベンダー各社は、サイロ化されたテストデータを根拠とし、最高の検知率や最大の可視性などのさまざまな基準を用いて「勝利」を主張することがあります。現実の世界では、知識とは非常に不完全なものであり、ノイズ、誤警報、誤検知によってSOCやITの限られたリソースがむやみに消費されています。このような厳しい環境下における「成

功」とは、単に現実世界の侵害を阻止できるかどうかという基準ではかるものです。私たちはこの点を念頭に置いてこの評価に臨みました。そして、CrowdStrike Falconプラットフォームが再び「成功」したことを誇りに思います。

スマートな優先順位付けでアラート疲れを回避

あなたなら、どちらの製品を利用したいですか？侵害を阻止するために必要なあらゆるデータがすぐにワークフローで提示される製品でしょうか。それとも、攻撃者の痕跡を得るために、インターフェイス、未加工のイベント情報、誤警報をしらみつぶしに探さなければならない製品でしょうか。毎日何百件もの攻撃を受ける組織においては、SIEMのような過去のソリューションで生成される大量のアラートでは持続的なセキュリティを推進できません。何よりも、侵害を阻止しなければならないのです。

脅威をすばやく探し、数分のうちに特定して状況を把握し、攻撃者がネットワークに侵入して目的を達成する前に攻撃を封じ込めなければいけない。それが、実際の業務です。つまり、SOCアナリストには、攻撃テクニックを特定したり、ある振る舞いが悪質であることを突き止めるためにデータをあちこち探し回るような時間がありません。FalconのCrowdScore™検知エンジンが非常に画期的である理由はここにあります。

CrowdScoreの目的はシンプルです。人工知能を使って、未警告のデータの中からシグナルを見つけ出し、環境内に潜んでいる攻撃者をユーザーの手を借りずにFalconプラットフォームに検知させることです。これは、単一のプロセスや個々の悪意な行動を検知したり、単純な時間ベースの相関を調べるというものではありません。

数ペタバイトにもおよぶ振る舞いに関するテレメトリデータや、顧客が開発したアラート、悪質な行動の可能性を示すさまざまなレベルの痕跡を積極的に活用して、データが実際の攻撃の存在を示している確率を正確に特定します。当社が独自開発したCrowdStrike Threat Graph®は、このような課題の解決に最適です。これを利用して、CrowdScoreが見逃される可能性のある未知の攻撃をリアルタイムで検知し、SOCに引き継ぐことができます。

CrowdScoreの採用により、ATT&CKテストにおいても、現実の世界でも、アラートを90%減少させました。

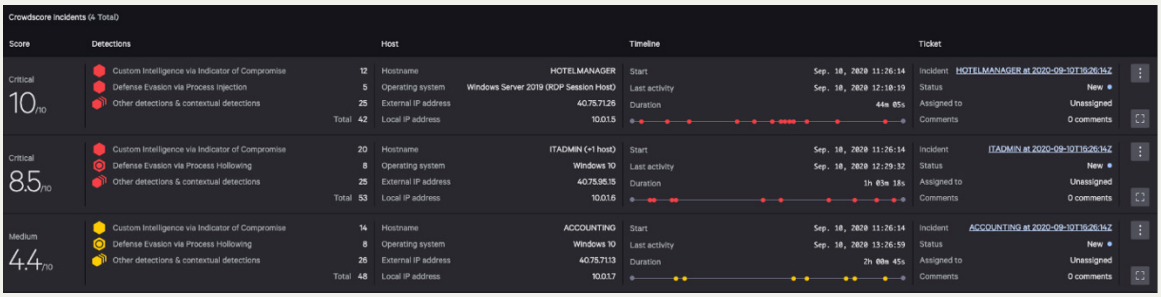

図1：評価テスト中に発生したインシデント。アナリストによるレビュー用に優先順位付けされている（クリックして拡大）

CrowdStrikeは常に限界に挑戦しており、テスターの採点方法とは必ずしも一致しない革新的な方法で攻撃者を検知しています。CrowdScoreは、防御側の状況を一変させる革新的な検知技術の好例です。Falconが侵害予防を目的に設定されていれば、攻撃はすぐに阻止できていたでしょう。テスト方針に従って、検知のみを目的とした設定が行われたCrowdScoreは、攻撃者がMicrosoft Wordを使用した「ユーザーによる実行」を伴うスピアフィッシング攻撃を実行して、システムへの侵入に成功したことをすぐに特定し、リアルタイムでインシデントのサマリーを表示開始しました。

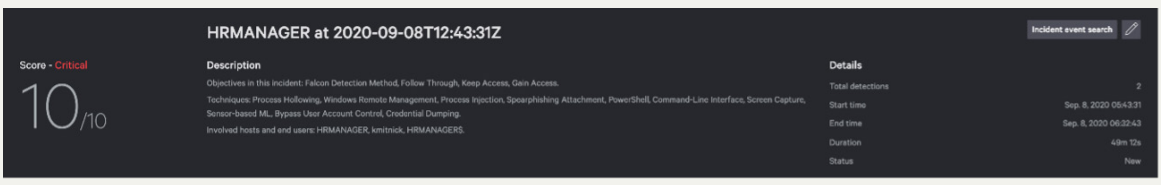

図2a：CrowdScoreの検出機能が進行中の攻撃の開始を表示

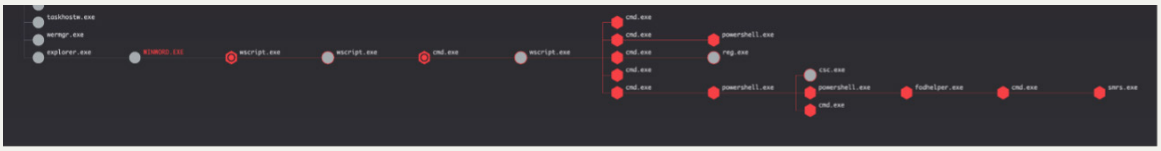

図2b：CrowdScoreの検出機能が進行中の攻撃の開始を表示

CrowdScoreを活用すれば、防御側は、脅威の構成要素の把握に必要な情報を得ようと、優先順位付けのされていないデータを何時間もかけて探し回る必要がなくなります。CrowdScore Incident Workbenchは、SOCアナリストが攻撃の迅速な特定、把握、封じ込めを行ううえで必要となる情報を収集し、提示します。これらはCrowdScoreによって自動的に行われるため、防御側の作業は不要です。

包括的な検出を可能にする仕様

包括的な攻撃検知は、非常に堅牢なデータソースと、複合的な視点での可視性なくては始まりません。エンドポイントソリューションにおいて、データは均等に生成されるわけではありません。また、攻撃者らは防御側組織と、それらが用いるセキュリティツールを常に回避しようとしています。CrowdStrikeはそれを理解しているため、複数の高度なデータソースを活用し、センサー上とクラウド内の両方で強化を行っています。そのため、攻撃者らが単にファイル名やコマンドラインを変更したり、AMSI機能の迂回を図ったり、あるいは正当なプロセスの動作を変更したり、フックされた機能を復元するだけでは検知を回避することが難しくなっています。

ATT&CKの評価テストのほとんどのステップで、2つ以上のデータソースを活用して検知機能を強化したFalconプラットフォームが、リーダーとしての能力を証明しました。

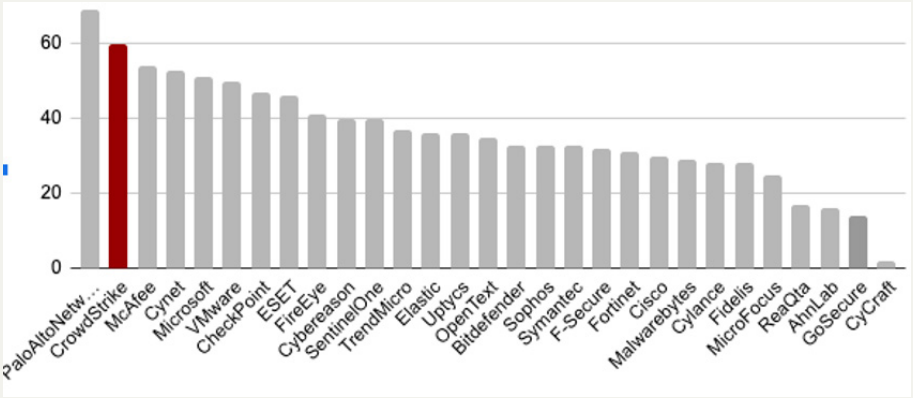

図3：2つ以上の異なるデータソースが使用された検知ステップの数

包括性を証明するには、複数のプラットフォームに対応することが求められます。CrowdStrike Falconは、皆さんが使用するあらゆるプラットフォームに対応しています。今年、MITREは、テスト環境のオプションコンポーネントとしてLinuxを採用し、参加企業はクロスプラットフォーム機能をアピールする機会を得ました。MITREの評価結果では、Falconが、「LinuxマシンとWindowsマシンから他のネットワークマシンやサービスへのリモートSSH接続（T1021.004）」あるいは「SMBプロトコルの不正使用（T1021.002）」を利用した水平展開を検知・防御し、悪意のある者がターゲットを評価することを効果的に阻止したことが示されています。MITREがテストする「ターゲット評価」は、特にWindowsホストやLinuxホスト上での攻撃者エミュレーションにおける攻撃チェーンの重要なステップです。

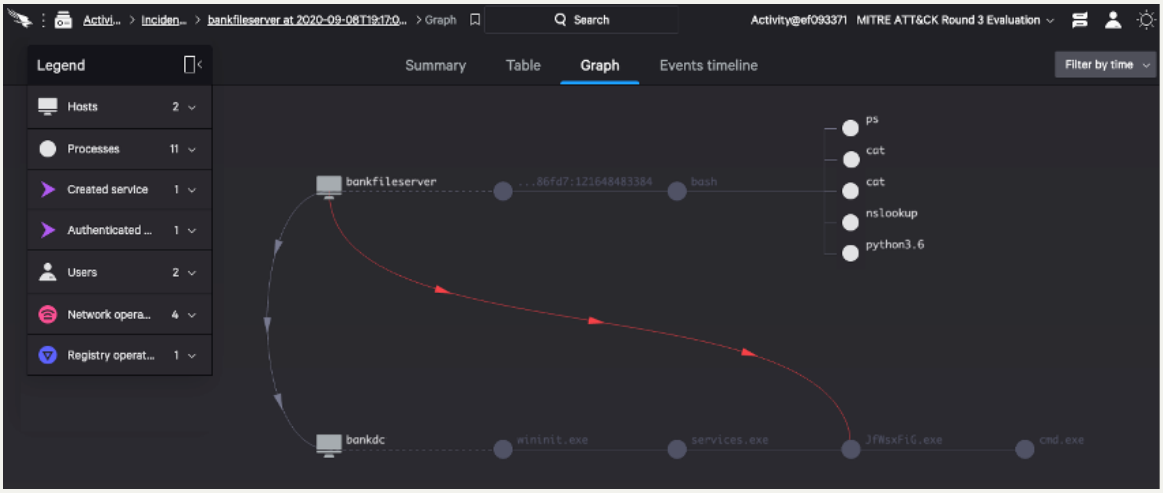

図4：CrowdScoreでは、水平展開を行うクロスプラットフォームインシデントを自動的に検出・表示する（クリックして拡大）

攻撃チェーンのこのステップで、人が介入することなく、攻撃を100%ブロックすることのできる革新的な機能は、すべてのインフラ環境で強力なセキュリティ態勢を確保するうえで大きな助けとなります。

Falcon Intelligenceの自動化されたインテリジェンス機能でチームを強化

攻撃者の戦術、技術、ツールの高度化に伴い、高度なマルウェアに対する可視性を高め、より詳細に分析することが重要になっています。潜伏するマルウェアを撃退し、セキュリティインフラ全体の有効性を強化すると、セキュリティチームはより高い可視性を得て、適切な判断をより迅速に下せるようになるとともに、脅威の技術を詳細に調査し、高度な敵を効果的に検知する方法を見いだすことができるようになります。

評価テスト中、CrowdStrike Falcon Intelligence™とその強力な自動サンドボックス分析機能は、攻撃全体を通して、攻撃者の活動に関する包括的な可視性とインテリジェンスを提供しました。Falcon Intelligenceは、15のテストステップをカバーする知見を提供し、PowerShellスクリプトによる特権昇格や水平展開など、攻撃者らが日常的に使用している多くのテクニックを特定しました。

Falcon Intelligenceの分析からは、可視性と検知機能のみならず、攻撃者の手口に関する深いインテリジェンスと指標を得ることができます。これにより、防衛側は防衛力の向上に必要となる重要な情報を得て、攻撃を検知するだけでなく、将来の執拗な攻撃をも阻止できるようになります。

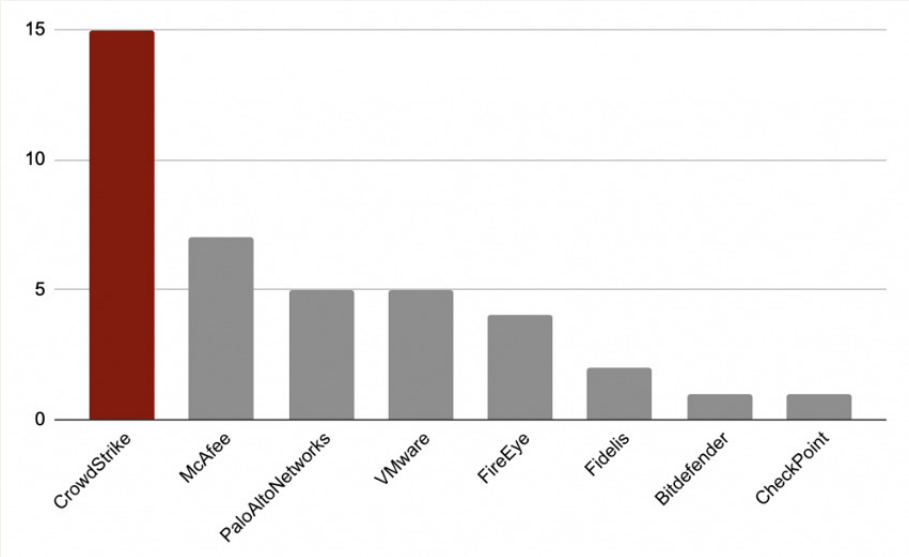

図5：CrowdStrike Falcon Sandbox™が現在の脅威の把握と将来の脅威の阻止を可能にする自動インテリジェンス機能を提供

プラットフォームの威力

このテストは、エンドポイントにおける検知と対応に焦点を当てるものでしたが、狡猾な攻撃者は常に複数の攻撃領域を探し回り、防御の最も手薄な部分を狙って目的を達成しようとするでしょう。クラウドネイティブなCrowdStrike Falconプラットフォームは、当初からエンドポイントとその先までの包括的な可視性を防御者に提供する目的で構築されました。Falconは、次世代型アンチウイルスFalcon Prevent™と、EDR（エンドポイントにおける検知と対応）を提供するFalcon Insight™、アイデンティティ保護（Falcon Identity Protection）およびクラウドワークロード保護（Falcon Cloud Workload Protection）を組み合わせて、永続的な攻撃から組織を守るために必要な機能をセキュリティアナリストに提供します。

それだけではありません。攻撃者を阻止した後、防御側は、同様の攻撃のリスクを低減するために、セキュリティ態勢と攻撃対象領域を見直すことが非常に重要です。そこで、Falconプラットフォームが提供する優れた機能が威力を発揮します。セキュリティトレーニングが必要なユーザーを特定するほか、**Falcon Spotlight™**で脆弱性をあぶり出し、**Falcon Discover™**で攻撃に悪用される可能性のあるソフトウェアを発見します。また、当社の最先端のインテリジェンスデータを用いて、再攻撃の可能性を把握します。

侵害阻止への絶え間ない努力

CrowdStrikeは、数々の**主要な独立テスト機関**でFalconプラットフォームをテストすることで、実世界に近いテストシナリオにおいて当社の能力がどのように評価されるかについての透明性を提供するとともに、我々が最高レベルのプロテクションを提供し続けていることをお客様に理解していただいています。このテスト結果は、CrowdStrike Falconの脅威検知機能が一貫してクラス最高レベルであることを浮き彫りにしています。また、当社は**SE Labsの「Breach Responseテスト」**および**AV-Comparativesの「Endpoint Protection and Responseテスト」**でも戦略的リーダーに選出され、その能力を立証しています。

攻撃者らが進化を止めないのと同様に、CrowdStrikeも開発の手を止めません。CrowdStrikeの高度な検知技術は進化し続けており、新たな手口を特定・阻止すべく新機能を開発しています。当社は、2020年夏にMITRE ATT&CK評価テストに参加して以来、既知および未知の脅威を防御すべく、さまざまな新機能を追加し、検出機能を強化してきました。また、MITRE Center for Threat-Informed Defenseへの参加を通じて、ATT&CKの運用方法を含めたセキュリティプログラムの構築方法に関して、コミュニティの全体的な理解の推進に引き続き貢献しています。

そうしたなか、実証された俊敏性、包括的な可視性およびスピードを備えたFalconは、高度な敵に対する戦いにおける重要な武器であり続けます。私たちは、実世界の侵害から組織を保護するうえで、誰もが認めるリーダーシップを再び立証できたことを誇りに思います。

追加のリソース

- 攻撃者らのTTPに関する最新のトレンドについては2020年版 CrowdStrikeグローバル脅威レポートをご一読ください。
- CrowdStrikeの製品紹介ページでは、パワフルでクラウドネイティブなCrowdStrike Falcon®プラットフォームについて説明しています。
- 攻撃者に関する情報を御社のセキュリティ戦略に活用する方法については、Falcon Intelligence™のページをご覧ください。
- CrowdStrike Falcon Prevent™の無料トライアル版（フル機能提供）を入手して、真の次世代型AVが、今日の非常に高度な脅威にどのように対抗できるかをご覧ください。

原文：CrowdStrike Achieves 100% Detection Coverage in MITRE ATT&CK Evaluations in All 20 Steps of the Evaluation
https://www.crowdstrike.com/blog/crowdstrike-falcon-mitre-attack-evaluation-results-third-iteration/