MITER ATT&CK評価

IBM Security ReaQtaは、最高クラスの機能を示します

ハイライト

セキュリティー・チームをサイバー脅威の手動分析から解放しつつ、事業継続性を促進

必要最小限の脅威アラートを生成することでアラート疲労を軽減し、サイバー・セキュリティーを簡素化する

エンドポイントを完全に可視化し、あらゆる段階での迅速な対応を可能にする

レポートについて

IBMの子会社である ReaQtaは、MITRE ATT&CKの評価を完了しました。このレポート[1]では、ReaQtaが最高品質のアラートを生成しながら、実質的に人間の介入なく高度な攻撃に完全に対応できることが示されています。

MITRE ATT&CK評価とは?

MITRE ATT&CKは、サイバー攻撃時の一連のステージを定義し、脅威を検出する能力でソリューションを評価します。記載されている各ステージは、キルチェーンに沿った「戦術」を表しています。

- 初期アクセス
- 実行
- 永続性
- 権限のエスカレーション
- 防衛回避
- 認証情報へのアクセス
- 検出
- 横方向の移動
- 収集
- 流出
- 指揮とコントロール

REAQTA
an IBM Company

IBM

MITRE評価が組織を支援する方法

この評価は、ソリューションの採点や評価を行うものではなく、企業がそれぞれのセキュリティーの課題に対応するための最適なソリューションを特定することを目的としています。ただし組織は、この評価が孤立した環境で行われ、限界があることに十分注意する必要があります。あるソリューションの特定の機能が、今回の検証インフラストラクチャーに対応していないため、無効化されてしまう場合があります。例えば、ReaQtaNanoOSがその一例です。NanoOSはライブ・ハイパーバイザーを活用して高度かつ悪質な動作を検出しますが、これは今回の環境では利用できませんでした。しかしこのプラットフォームは、中核となるコンポーネントがないにもかかわらず、良好なパフォーマンスを示しました。

MITRE には一式の特定された技法があり、それぞれの技法は評価のために選択された脅威アクターに基づく戦術グループに属しています。MITREは、今回の評価で APT29 を選択しました。

侵害

収集と回避

偵察

アクセスの拡大

流出

クリーンアップ

セキュリティー・チームをサイバー脅威の手動分析から解放することで、事業継続性を促進

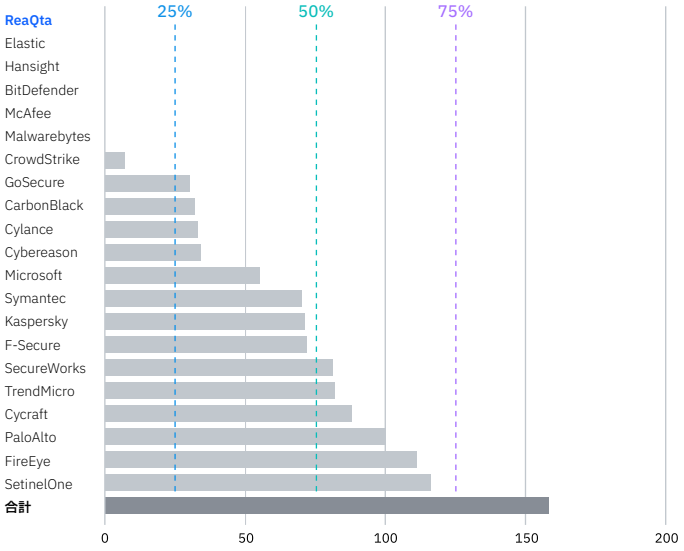
ReaQtaは評価を始める前に、マネージド・セキュリティー・サービス・プロバイダー(MSSP)なしで、すなわち、攻撃中に人間が一切介入しない方針で参加することを決定しました。MITREは技術評価の枠組みの中で、人間を含めることは不誠実と判断しました。加えて、MSSPによる検出が結果に貢献することは、評価に大きなバイアスをかけます。セキュリティー・オペレーション・センター(SOC)チームは、攻撃が起こっていること、そしてどこでどのように起こっているかを正確に把握しています。

MSSPのアプローチでは、ReaQtaのクライアントに技術の公正な評価を提供することはできなかったでしょう。MITREはフィードバックを積極的に受け入れ、ラウンド3からはすべての企業が人間を介さずに評価されるようになります。

MSSPは確かに大きな価値をもたらします。しかしながら、お客様はMSSPかスタンドアロン・デプロイメントかを自由に選択可能にすべきです。

下のグラフに示すように、人間が行う検出の数が、生成された検出に大きな影響を与えていることがわかります。複数の例では、50%以上、最大で73%が手動で作成されています。人間が介入しないという方針で参加を決めたのは、わずか6社でした。

MSSPによる検出(手動で生成)



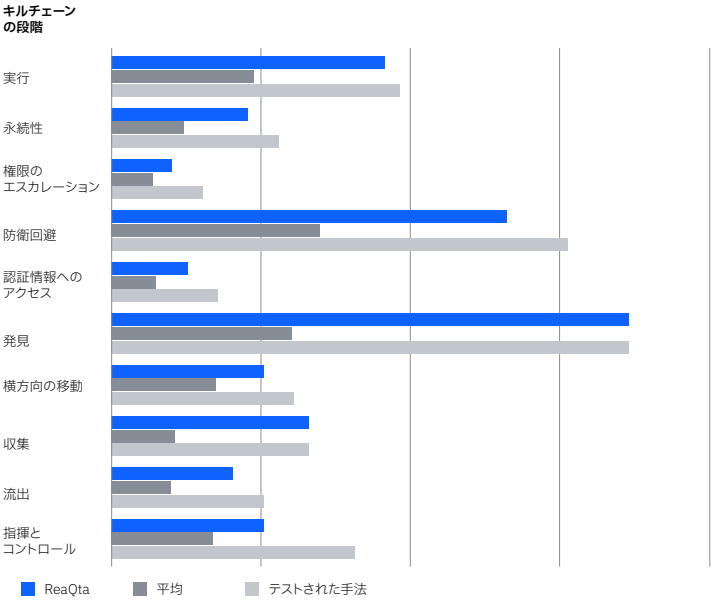
各ベンダーによって生成された手動検出

MITRE評価ラウンド2 - APT29

ベンダーは、ステルス・アプローチで知られる、洗練され、国家レベルの攻撃者である APT29(The Dukes、Cozy Bear、CozyDukeとも呼ばれる)が使用する戦術や技法を検出する能力についてテストが行われました。APT29は、2015年のペンタゴン、2016年の民主党全国委員会、2017年のノルウェーおよびオランダ政府という、注目すべき攻撃の背後にいることで広く知られています。

前ラウンドからの変化は重要で、APT3(ラウンド1)は、目立たないことに対する考慮が少なく、様々なツールを採用した、よく目立つ行動を取る脅威アクターです。一方、APT29はステルス性が高く、非常に目立たないように活動し、LOLBinsとファイルレス型マルウェアに大きく依存しています。

手法検出範囲(自動)



平均と比較したReaQta自動検出範囲

ReaQta評価結果

この攻撃は 2 日間にわたって行われ、攻撃者は最初にアクセスを得た後に、徐々にネットワークの深部へと侵入していきました。検出プロファイルを低く抑えるため、ほとんどの操作はカスタムツールやマルウェアではなく、Microsoft PowerShell を使用して実行されました。評価目標は、テスト対象となったソリューションが攻撃にどのように対応し、キルチェーン全体においてどのような可視性が提供されるかを示すことです。

評価結果の概要から明らかなように、ReaQtaはキルチェーン全体において完全な可視性を提供しました。ReaQtaは、テスト対象となった戦術や手法の90%を検出し、攻撃のあらゆる段階で脅威に対応し、修復する能力を証明しました。

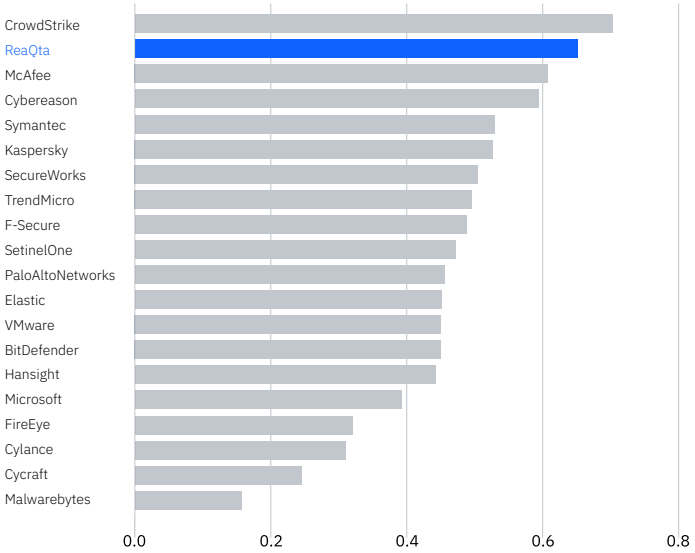
ReaQtaは、MSSPによる手動検出に依存するベンダーと比較しても、世界トップクラスのアクション可能率を示しています。

必要最小限の脅威アラートを生成することでアラート疲労を軽減し、サイバー・セキュリティーを簡素化する

プラットフォームは実行、持続、権限のエスカレーション、防御回避の段階から検出してアラートを生成し、セキュリティー・チームが APT29 とその行動を追跡することを可能にしました。プラットフォームのアラートは、キルチェーンの後半の段階である横方向の移動、収集、流出、指揮とコントロールにおいて一貫しており、ReaQtaがサイバー攻撃の後半の段階でも対応し、被害を抑えることができることを示しています。

アクション可能率により、アラート発生数を減らすことでノイズを低減するプラットフォームの機能が強調されました。戦術と手法毎に1つのアラートが発生し、SOC チームが調査および対応すべきアラートの数が管理しきれないほど発生してしまうプラットフォームもありましたが、このReaQtaプラットフォームでは、すべての戦術と手法を少数の相関したアラートで捕らえることができました。

アラートのアクション可能性

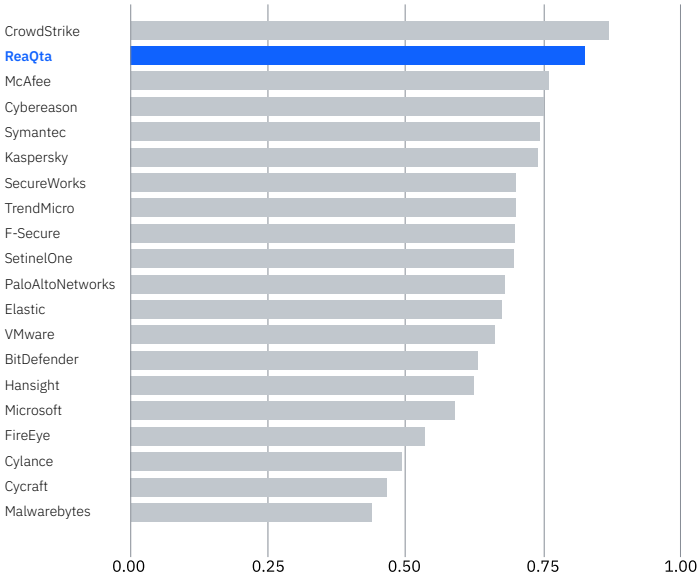


アクション可能性率(データには、MSSPに依存するベンダーに対する手動検出が含まれる)

再度、ReaQtaは人間の介入なしに高品質のアラートを提供しました。しかしながら、1番目と3番目のベンダーは評価中に手動分析に依存していました。

ReaQtaが提供する可視性の量により、データのフィルタリングと関連付けを行い、可能な限り最小数のアラートを生成することが必要となります。アラートの数は最小にしますが、それぞれが最大量の関連情報を含むようにすることも必要です。テレメトリーを収集し、関連付け、要約することが、ReaQtaのAIエンジンの目的です。アラートの品質は、以下の表で示すForresterによる分析でも確認されています。

アラート品質



アラート品質(データには、MSSPに依存するベンダーに対する手動検出が含まれる)

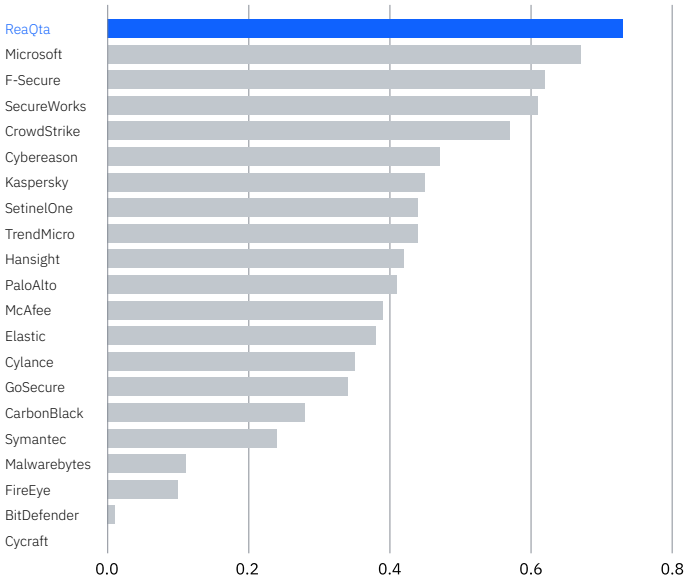
「アクション可能性は、アラート効率とアラート品質の産物です[...]アラートの効率(多すぎない)とアラートの品質(ストーリーを理解するのにどれだけ役立つか)はどちらも関連しており、特定のアラートの「アクション可能性」を理解するために重要です。」

Forrester[2]

高精度かつ包括的なアラートを提供することは、優れたプラットフォームと単なるノイズの原因を区別するための基準です。

以下のグラフは、手動検出を削除した場合のReaQtaの動作を、他のソリューションと比較したものです。それぞれの棒グラフは、生成された各アラートの下で収集されたインシデント関連の情報の量を表しています。ReaQtaのエンジンは最大の情報量を取得しました。これは、実環境でのワークロードを大幅に軽減させることができることを意味します。

生成された各アラートに対する攻撃範囲(信号対雑音比)



各アラートに対して提供される攻撃範囲の割合

ReaQtaは、テストが行われた1つの手法ごとに158件のアラートを生成する代わりに、わずか25件のアラートを生成し、それぞれのアラートの中で攻撃者を追跡するために必要なすべての情報を正しく収集しました。

アラート疲労を軽減するためには、統一されたインシデント解決ワークフローを提供できることが重要です。

ReaQtaは、MITREの評価中にストーリー展開を関連付けました。これにより、アナリストは、元のインシデントとの直接的な相関関係がない何百ものアラートが生成されることに気を取られることなく、アクティブな攻撃者を簡単に理解し、研究することができました。実際の分析では、もっと対応が難しかったであろうと思われます。

ReaQtaのアプローチは、攻撃全体における完全な可視性を維持しながら、アラート疲労を85%減少させました。ReaQtaは、インシデントごとに最小限のアラートを生成するよう特別に設計されており、スムーズで中断のない分析体験を促進します。単一ビューですべてを管理できることにより、アナリストが迅速に対応でき、イベントを完全に理解するために異なる画面に移動する必要がありません。

エンドポイントを完全に可視化し、あらゆる段階での迅速な対応を可能にする

このプラットフォームは、ATT&CKキルチェーンのすべての段階において、アクション間の相関関係を維持することができました。イベントを自動的に関連付けることで、攻撃者が実行したさまざまなアクションをつなぎ合わせるのに必要な時間を短縮し、最終的に実際の攻撃時の対応時間を短縮することができます。

行動ツリー

MITRE 評価中にReaQtaにより関連付けられたストーリー展開

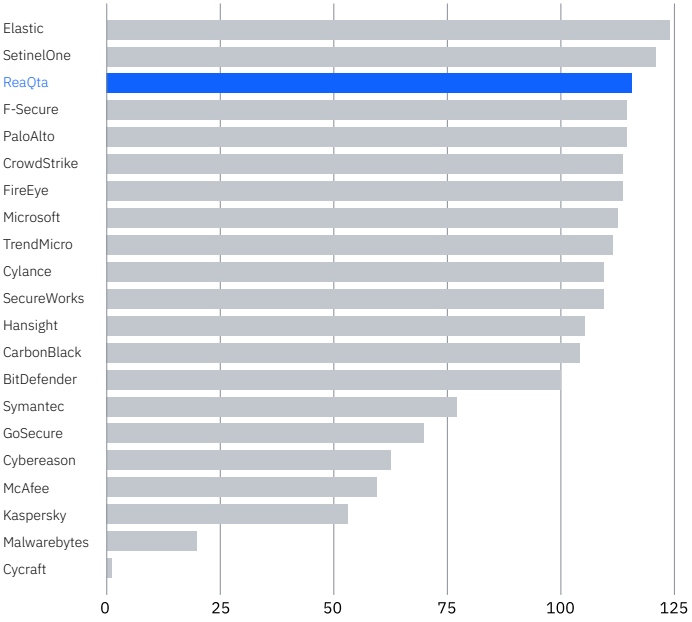
評価に関連する例として、上記のグラフは、1つのアラートで攻撃のすべての捉えた様子を示しています。ReaQtaは、すべての情報を理解しやすいストーリー展開に関連付けたことで、SOCチームにタイムリーな優先順位付けに必要なすべての情報を提供しました。人間の介入は不要で、手作業によるアクティビティーを必要とせずに、攻撃の説明やリスク評価を明確に行うことができました。

APT29の戦術と手法の検出を詳しく見ると、ReaQtaはキルチェーンの初期段階から、検出が困難とされる、より高度な段階まで可視化することができました。ここで注目すべきことは、あらゆる段階において脅威を一律に検出し、それによってあらゆる段階での対応と修復の機会を提供する、プラットフォームの機能です。

ReaQtaは、情報を凝縮してリスクを評価することが可能な素晴らしいAIエンジンと組み合わせて、最高のテレメトリーの1つを示しました。常にアラートを管理する代わりに、脅威ハンティングに時間を費やしたいと考えているSOCやチームにとっては、強力なツールとなるでしょう。

ReaQtaは、最高のテレメトリーの1つを示しました。

テレメトリー



ReaQtaによって提供されるテレメトリーの量

結論

ReaQtaのAI搭載プラットフォームは、セキュリティー・チームに高度な検出能力と迅速な対応能力を与え、人間の介入を最小限に抑え、サイバー・セキュリティーのプロセス全体を簡素化し、あらゆる規模の組織の事業継続性を促進します。

この評価により、ReaQtaの高度な脅威アクターの検出に対するアプローチが検証されました。ReaQtaは今後も、独立したサード・パーティーのテストに継続的に参加します。

ReaQtaは、これらの評価によって組織が十分な情報に基づいた意思決定を行えるよう支援するMITREの活動に感謝し、称賛しています。

詳細については、次の Web サイトをご覧ください。

ibm.com/jp-ja/products/reaqta

日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町19番21号

Produced in the United States of America
2022 年 3 月

1 MITRE ATT&CK評価、The MITRE CorporationおよびMITRE Engenuity、2020年。
2 Further Down the Rabbit Hole With MITRE's ATT&CK Eval Data、Forresterブログ、2020年5月4日。