Microsoft

Windows Defender Advanced Threat Protection

攻撃シミュレーション

シナリオ 3: 自動調査 (バックドア)

Copyright

Windows Defender ATP

Microsoft

マイクロソフトの攻撃検出の指針

シンプルです。

高度で持続的な攻撃 (APT) の兆候や攻撃手法がテレメトリによって可視化されます。このため、迅速に攻撃の予兆を検知し関連するアラートを発行することができます。

アラートはほぼリアルタイムで発行されます。そのとき、攻撃者の属性、被害に関する情報、地理的な親和性、主な攻撃手法を含むコンテキストも提供します。このようなコンテキスト情報を提供できるのは、以前に実際のマシンで見つかった脅威コンポーネント、感染したサイトや悪意のあるサイトの IP、URL、そこで見つかったスクリプトまたは Web ページの一部、攻撃者のドメインなど、既知の攻撃のサインを集めたリッチでダイナミックなライブラリがあるからです。このライブラリは、新しい脅威インテリジェンスで常に更新されています。脅威インテリジェンスは、マイクロソフト独自の APT ハンティング & リサーチ チームが作成しているものですが、パートナーの協力や共有フィードを通じて内容が強化されています。

常に新しい脅威が生み出され、既存の脅威にも変更が加えられています。マイクロソフトでは、新しい未知の攻撃者の活動を特定するため、膨大な量の疑わしい動作や通常と異なる動作を監視しています。そして、疑わしい動作や通常と異なる動作が見つかると、アラートを発行し、セキュリティ オペレーション センター (SOC) のアナリストに問題の検証と対応を依頼します。SOC のアナリストは、同じマシンやその他の関連するマシンで発生している類似したイベントの情報に基づいて、実際のデータ侵害アクティビティの検証、リスクの判断、データ侵害範囲の特定、攻撃を封じ込めるアクティビティの定義を行います。その後、実際に攻撃を封じ込め、脅威を軽減することで、攻撃に対応します。

自動インシデント対応シナリオの概要

このシナリオでは、新しい Windows Defender ATP 自動調査機能をトリガーする攻撃をシミュレーションします。自動調査機能とは、SOC の対応 (トリアージ、調査、修復) を自動化する機能です。自動調査機能は、攻撃の影響を受けたマシンから具体的な攻撃の要因を特定し、除去します。また、攻撃の影響を受けた可能性がある他のマシンに自動的にピボットし、同じ対応アクションを適用します。

自動調査機能をトリガーするには、『シナリオ 1: ファイル ベースのバックドア型マルウェア』で使用した攻撃シナリオを使用します。攻撃者は、ソーシャル エンジニアリングで攻撃として実装したドキュメントをスピアフィッシング メールに仕込むことによって攻撃を開始します。このドキュメントは、受信者が疑いを持たず、うっかり開いてしまうようなドキュメントを装っています。

しかし、実際には、このドキュメントには、マシン上に実行可能ファイルをひそかにドロップしてロードするマクロ コードが含まれています。このシミュレーションでは、無害な実行可能ファイルをドロップするドキュメントを使用しますが、実際に攻撃された場合、この実行可能ファイルはあたかも持続的なバックドア型マルウェアのようにふるまい、レジストリの Run キーに書き込みを行ったり、タスクスケジューラを活用したマルウェアの実行スケジュールを作成したりします。これらはいずれも自動開始拡張ポイント (ASEP) として知られています。

ASEP が作成された時点でシミュレーションは終了となります。ただし、実際の攻撃では、攻撃者は設置したバックドアを利用して、被害を受けたネットワーク内でさまざまなアクションを実行します。たとえば、他のマシンに横移動したり、特権を得た上で資格情報を収集したり、企業データをひそかに盗み出 s したりします。

このシミュレーションで使用するマシンの条件は、次のとおりです。

- Windows Defender ATP のオンボーディングが完了している
- Windows 10 Spring Creators Update (バージョン 1803 以上) を実行している
- PowerShell が有効になっている
- Windows Defender ウイルス対策が有効になっている
- Microsoft Word がインストールされている

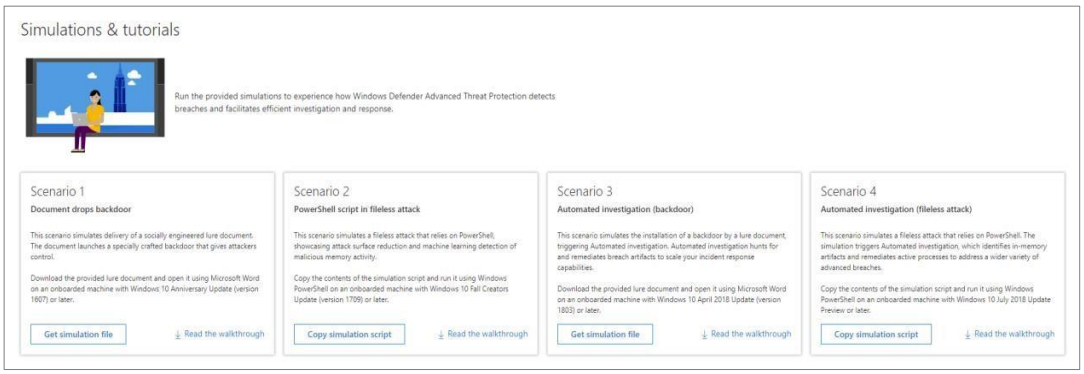
オンボーディングの方法については、製品ガイドをお読みください。テスト マシンのオンボーディングを行うには、ローカルのオンボーディング スクリプトを実行するこ

とをお勧めします。

シミュレーションの実行

攻撃シミュレーションを実行する手順は、次のとおりです。

1. Windows Defender ATP ポータルにログインし、**[Help (?)]**> **[Simulations & tutorials]** を選択します。



2. **[Scenario 3: Automated incident response]** の下の **[Get simulation file]** をクリックして、ルアー ドキュメント **WinATP-Intro-Invoice.docm** をダウンロードします。

3. 攻撃用ドキュメントをテスト マシンにコピーします。

4. ユーザーの一般的な反応をシミュレーションするため、テスト マシン上にコピーされた攻撃用ドキュメントをダブルクリックします。Microsoft Word が起動し、パスワードの入力を求めるプロンプトが表示されます。パスワード **WDATP!diy#** を入力して、パスワードで保護されたドキュメントを開きます。

5. ドキュメントが保護ビューで開いた場合は、**[Enable Editing]** をクリックします。マクロが無効になっているというセキュリティ警告が表示された場合は、**[Enable Content]** をクリックします。多くのユーザーがこうしたセキュリティ セーフガードを回避して、うっかり悪意のある Office ドキュメントを開いてしまいます。

   注: 組織全体で、インターネット経由で入手したドキュメントのマクロをブロックする設定になっている場合、**[Enable Content]** オプションを有効化するには、このドキュメントのブロックを解除する必要があります。ドキュメントのブロックを解除するには、エクスプローラーでファイルの場所へ移動します。エクスプローラーでドキュメントを右クリックし、**[Properties]** を選択します。**[General]** タブ

で、**[Security]** の下の **[Unblock]** オプションをオンにします。

注: サード パーティのセキュリティ製品を利用している場合、シナリオをスムーズに実行できないことがあります。テストには、Windows Defender ウイルス 対策 を有効にした Windows 10 マシンを使用することをお勧めします。

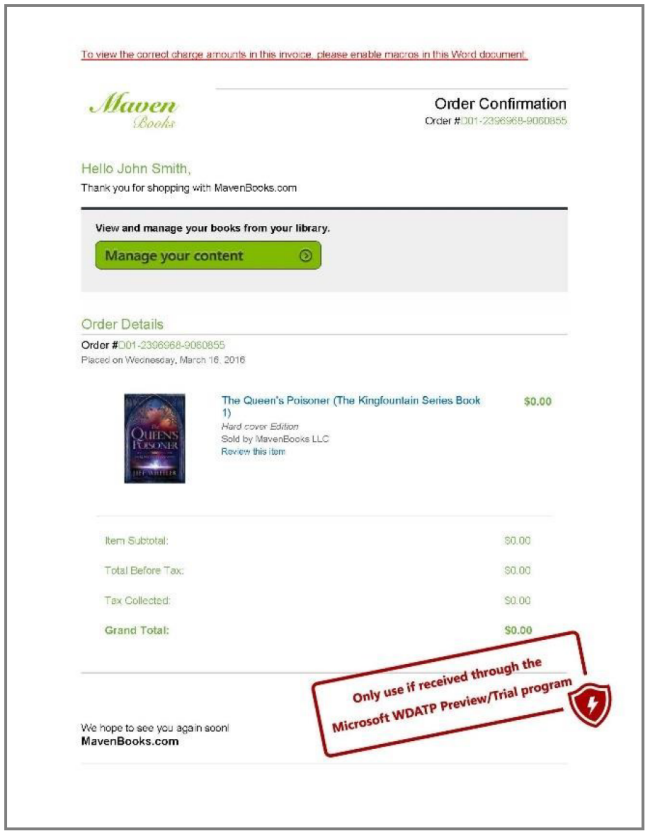
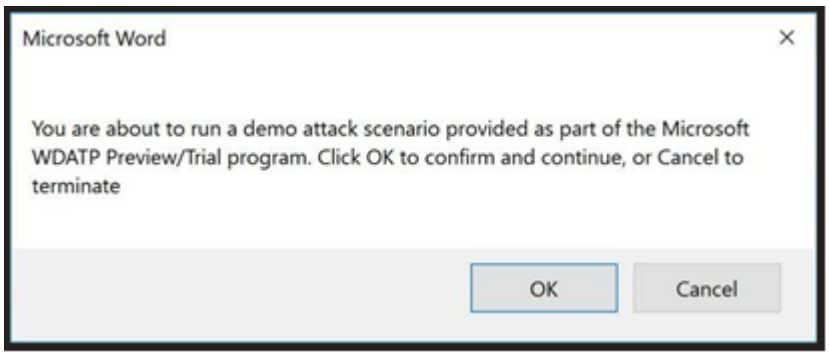


図 1: ルアー ドキュメント

6. メッセージ ボックスが表示されたら、[OK] をクリックして、攻撃シミュレーションを実行します。



7. 数秒後、ドキュメントの悪意のあるマクロによって PowerShell スクリプトが実行

され、[Desktop] フォルダーに **WinATP-Intro-Backdoor.exe** という新しいファイルがドロップされます。これがバックドアになります。

8. 同じスクリプトにより、事前にスケジュールされた時刻にバックドアを実行する予定されたタスクが作成されます。この間接的なプロセス実行のメカニズムは、ドキュメントをトレース バックすることが難しいため、しばしばステルス攻撃に使用されます。

9. バックドアが実行されると、レジストリの Run キーの下に自動起動エントリが作成されます。バックドアは Windows と同時に自動的に起動するため、持続的な脅威となります。[Command Prompt] ウィンドウが開きます。シミュレーションのバックドアの実行中です。

10. [Command Prompt] ウィンドウを閉じて、**WinATP-Intro-Backdoor.exe** プロセスを終了します。

お疲れ様です。攻撃シミュレーションが完了しました。

これで攻撃シミュレーションは終わりです。実際の攻撃者は、多くの場合、情報のスキャンを続け、収集した偵察情報をコマンド アンド コントロール (C&C) サーバーに送信し、この情報を利用して他の魅力的なターゲットに横移動します。

次に、シミュレーションの攻撃を知らせる Windows Defender ATP アラートについて見ていきましょう。

✎ **注**: アラートは、バックドア型マルウェアのシミュレーションの実行後 15 ～ 30 分で発行され始めます。

アラートと自動応答の表示

ここからは、攻撃者の視点から SOC の防御者の視点に切り替えて見ていきます。

1. 任意のマシンから https://securitycenter.windows.com にアクセスし、Windows Defender ATP ポータルを開きます。

2. Windows Defender ATP の資格情報を使ってログインします。サインアップ時のメールでは、既定のグローバル管理者の資格情報が提供されます。

3. シミュレーションの攻撃から 15 ～ 30 分経つと、ダッシュボードに複数の新しいアラートが表示されます。

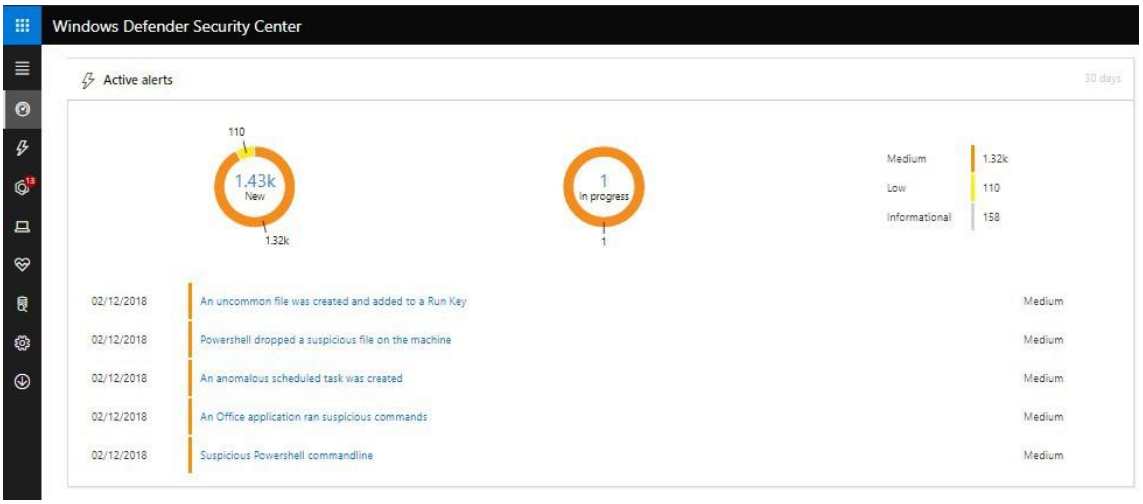


図 2:ダッシュボードにトリガーされたアラートを表示

> **注:** このシミュレーションでは、シミュレーションの攻撃に対処する自動調査と対応機能に注目して説明を進めます。この攻撃で発生する個々のアラートや、これらのアラートの分析に使用する手動の調査機能について詳しく知りたい場合は、『**シナリオ 1: ファイル ベースのバックドア型マルウェア**』を参照してください。

4. **[PowerShell dropped a suspicious file on the machine]** を選択して、対応するアラートの詳細ページを開きます。アラートの詳細ページに表示されているバッジから、自動調査機能が実行されていることがわかります。現在の調査ステータスも表示されています。

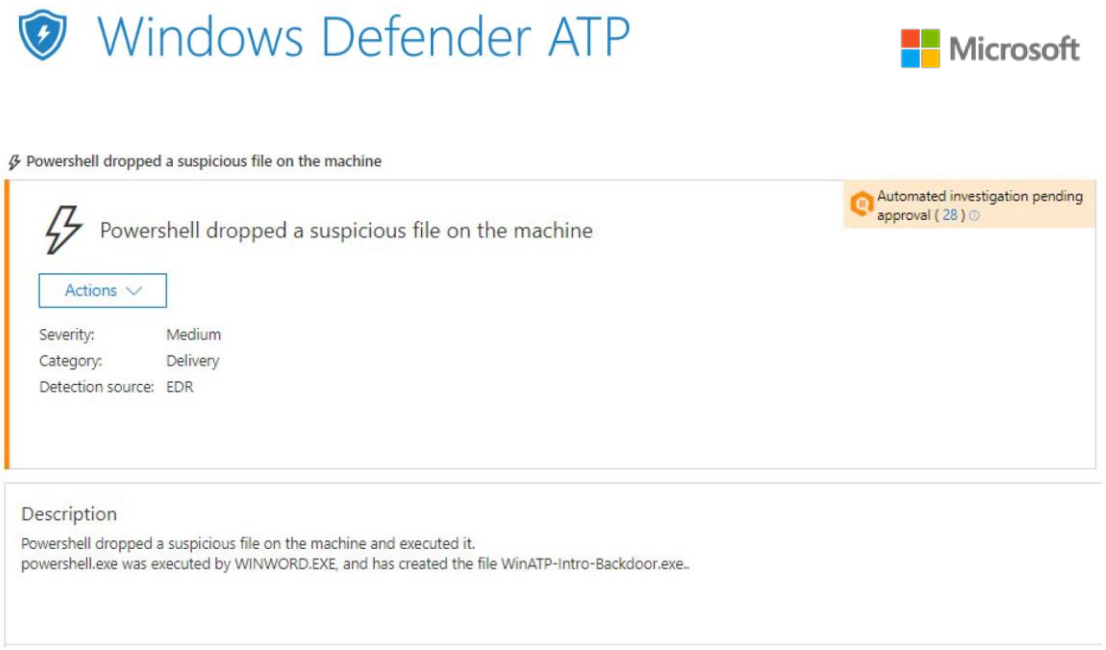


図 3: アラート ページ: 自動調査機能の実行中

調査内容の確認、保留中の修復アクションの承認

Windows Defender ATP は、各調査の詳細情報を提供します。既定では、ユーザーの承認を待ってから修復アクションを実行します。

1. 自動調査バッジの調査 ID をクリックして、詳しい調査情報を表示します。

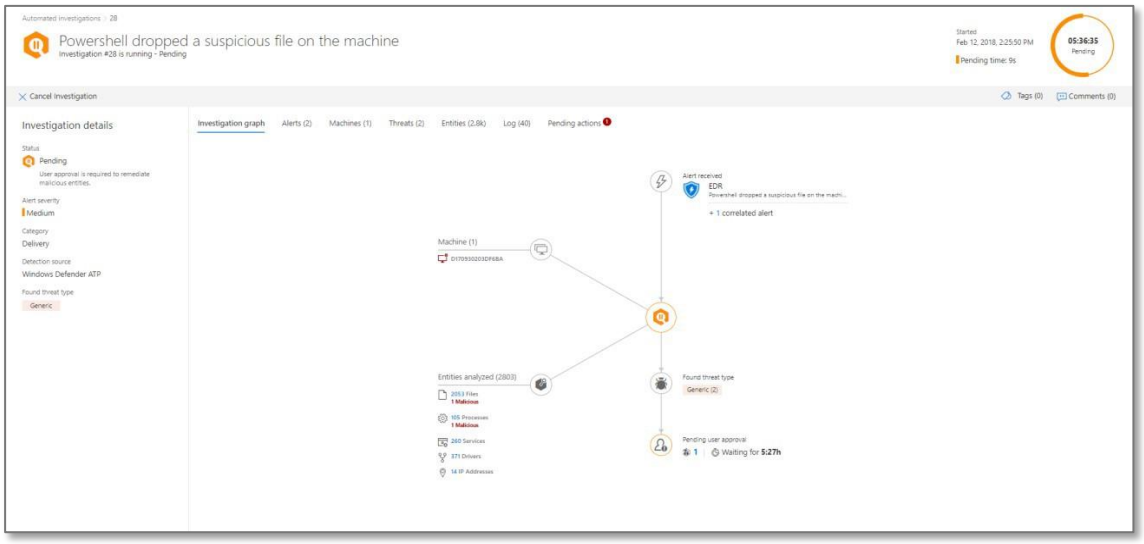


図 4: 調査の詳細ページ

調査の詳細ページには、次の情報が表示されます。

- 自動調査機能をトリガーしたアラート
- 関連マシン: 他のマシンでインジケーターが検出された場合は、それらのマシンも表示される
- 検出された分析対象のエンティティまたはアーティファクト: ファイル、プロセス、サービス、ドライバー、ネットワーク アドレスこれらのエンティティとアラートの関係が分析され、良性か悪性かが評価される
- 検出された脅威 - 調査中に見つかった脅威

  注: タイミングによっては、自動調査機能がまだ実行中の場合もあります。証拠の収集と分析、結果の準備は、数分で完了します。最終結果を表示するには、調査ページを更新します。

2. 自動調査機能の実行が完了すると、アナリストの承認を求める修復アクションのメッセージが表示されます。

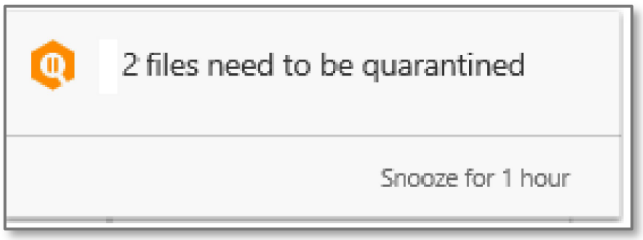


図 5: 保留中の修復アクションの通知

3. 通知をクリックすると、保留中のアクションが表示されます。または、調査の詳細ページで **[Pending actions]** をクリックします。

   自動調査の実行中、Windows Defender ATP により、修復の必要なすべてのアーティファクトが検出されます。対象は、バックドア、ASEP (レジストリ エントリと予定されたタスク)、ルアー ドキュメントなどです。修復アクションはユーザーの承認を待ってから適用されますが、このステップを省略して自動的に修復アクションを適用するように Windows Defender ATP を設定することもできます。

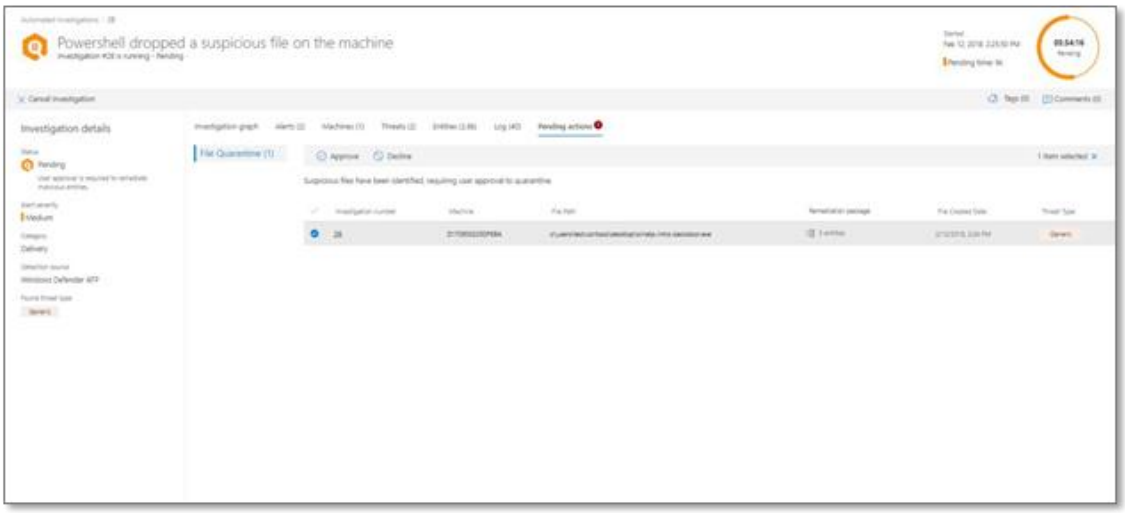


図 6: 保留中のアクション

4. **[Approve]** をクリックして、攻撃にリンクされたすべてのアーティファクトの修復アクションを承認します。ユーザーの承認が得られると、自動調査機能により、関連プロセスが停止し、疑わしいファイル (バックドア、ルアー ドキュメント) が検疫され、ASEP が削除されます。

完了すると、調査ステータスが **[Fully remediated]** に変わります。

攻撃シミュレーション シナリオ 3: 自動調査 (バックドア)

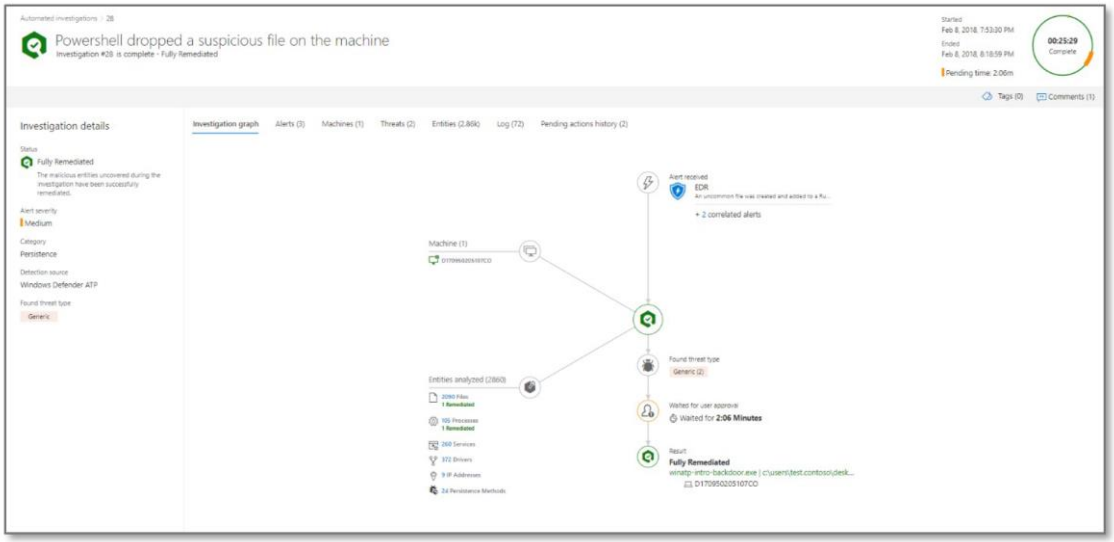


図 7: 調査の詳細ページ (修復の完了後)

アラートの解決

手動または自動でアラートの調査と修復が完了したら、アラートを解決します。これは、アラートをアクティブなアラート キューから削除するということです。

アラートを解決するには、次の手順を実行します。

1. **[Alerts] > [New]** または **[Alerts] > [In progress]** を選択してアラートを探します。
2. アラートの**詳細メニュー [...]** から **[Manage alert]** を選択します。アラート管理ウィンドウが開きます。
3. アラートのステータスを [Resolved] に変更して、その内容を分類します。
   - [True alert] - 悪意のあるアクティビティが正確に検出された
   - [False alert] - 問題のないアクティビティが悪意のあるアクティビティとして誤検出された

どちらの場合も、適切な分類を選択して、検出の性質に関する追加情報を入力します。

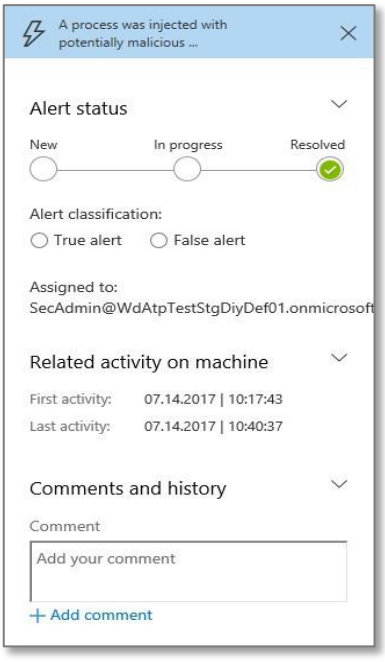


図 8: アラート管理ウィンドウ: 解決済みのアラート

まとめ

ここでは、一般的な攻撃をシミュレーションし、Windows Defender ATP が攻撃を検出し、自動調査機能をトリガーするしくみを紹介しました。さらに、自動調査機能を使ってオンボーディング済みのマシンから攻撃アーティファクトを自動的に検出し、疑わしいアーティファクトを修復することにより、SOC の担当者の能力を拡張する方法について解説しました。自動調査機能は、事前に修復アクションの承認を求めることにより、マシンに不要な変更が行われないように保護しますが、修復アクションを自動的に適用するように設定することも可能です。

シミュレーションを楽しんでいただけましたら幸いです。自動調査機能だけでなく、他の機能もぜひ利用してみてください。詳細については、製品ガイド (docs.microsoft.com) をご覧ください。

また、Windows Defender ATP ポータルのフィードバック アイコンから、このシミュレーションや製品に関するご意見、ご感想をお寄せください。お寄せいただいたご意見やアイデアは、今後のシミュレーションやチュートリアルのために利用させていただきます。ご協力よろしくお願いいたします。