Microsoft

Windows Defender Advanced Threat Protection

攻撃シミュレーション

シナリオ 5: カスタム検出

Copyright

This document is provided “as-is.” Information and views expressed in this document, including URL and other internet website references, may change without notice

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2018 Microsoft. All rights reserved.

Please refer to Microsoft Trademarks for a list of trademarked products.

All other trademarks are property of their respective owners.

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。マイクロソフトでは、このライブラリを新しい脅威インテリジェンスで常に更新しています。脅威インテリジェンスは、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マする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。

このシナリオの概要

このシナリオでは、カスタム検出ルールに基づいてアラートをトリガーする攻撃をシミュレーションします。カスタム検出ルールを作成することで、特定の攻撃や攻撃パターンの監視アクティビティの設定をカスタマイズできます。クエリを使うと、対象のインジケーターやイベントをより細かく監視することができます。このクエリをカスタム検出ルールとして保存することで、記録されたすべてのイベントを定期的にチェックして一致するものを探し、対応するアラートを生成することができます。

カスタム検出ルール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』で使用した攻撃用ルアー ドキュメントを使用します。攻撃者は、ソーシャル エンジニアリング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したりします。

このシミュレーションでは、次のようなテスト マシンを使用します。

- Windows Defender ATP のオンボーディングが完了している
- Windows 10 Anniversary Update (バージョン 1607) 以降を実行している
- PowerShell 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。

Windows Defender ATP

Microsoft

カスタム検出について

Windows Defender ATP の高度なハンティング機能を使って、データ侵害と思われる動作を定期的に幅広く捜索することができます。たとえば、疑わしいアクティビティ、新たな脅威と関連するアクティビティなどを検出できます。

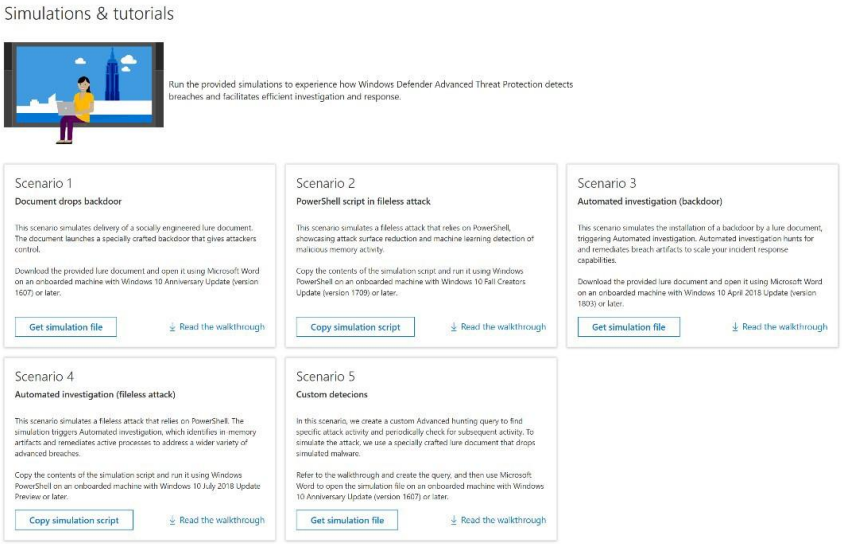
カスタム検出は 24 時間ごとに実行されます。ユーザーが指定した特定の条件セットを検出すると、アラートをトリガーし、Windows Defender セキュリティ センターに通知するように設定することができます。これらのアラートは、システム内で他のアラートと同様に扱われます。

この機能は、特定の脅威にプロアクティブに対処し、新たな脅威について速やかに通知を受けたい場合に便利です。

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 5: Advanced hunting query]** 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. ルアー 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ルアー 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。適切なルアー コンテンツを使うと、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 AV を有効にした Windows 10 の既定の設定のマシンを使用することをお勧めします。

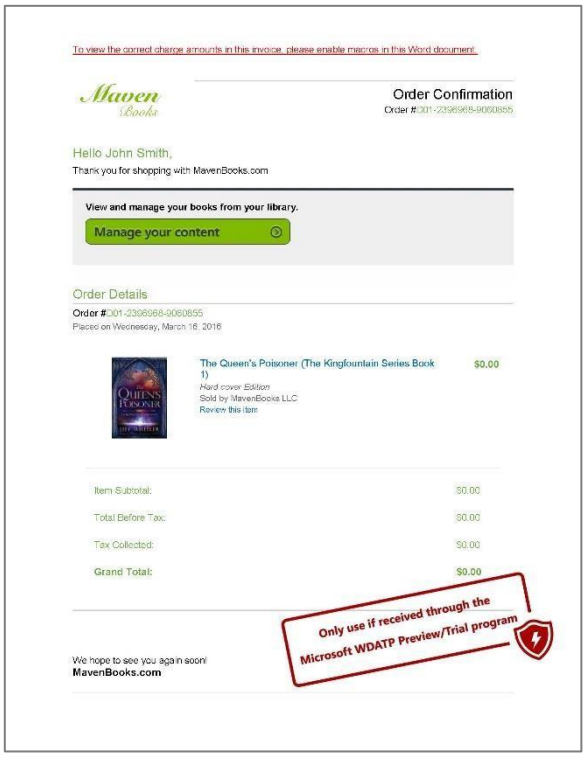
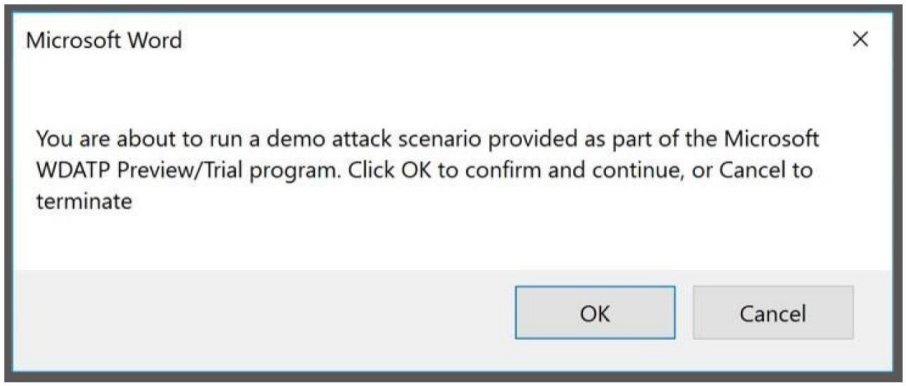


図 1: ルアー ドキュメント

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、タスクスケジューラを活用したマルウェア（バックドア）の実行スケジュールが作成されます。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。

攻撃シミュレーション シナリオ 5: カスタム検出

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。これはシミュレーションのバックドアが実行中であることを意味します。

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。

続いて、予定されたクエリを作成し、手動で指定されたアラート条件に基づいてアラートがトリガーされるようすを確認しましょう。

Windows Defender ATP

Microsoft

カスタム検出の作成

ここからは、攻撃者の視点から SOC の担当者の視点に切り替えて見ていきます。まず、シミュレーションの攻撃の動作に一致するようなクエリを作成します。次に、このクエリが定期的に実行され、自動的にアラートを生成するように設定します。

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. **[Advanced hunting]** ページに進みます。

4. 攻撃を捕捉するため、ダウンロードされた Microsoft Office ファイルが PowerShell コマンドを実行するイベントを検出するクエリを作成します。次のサンプル クエリを使用できます。

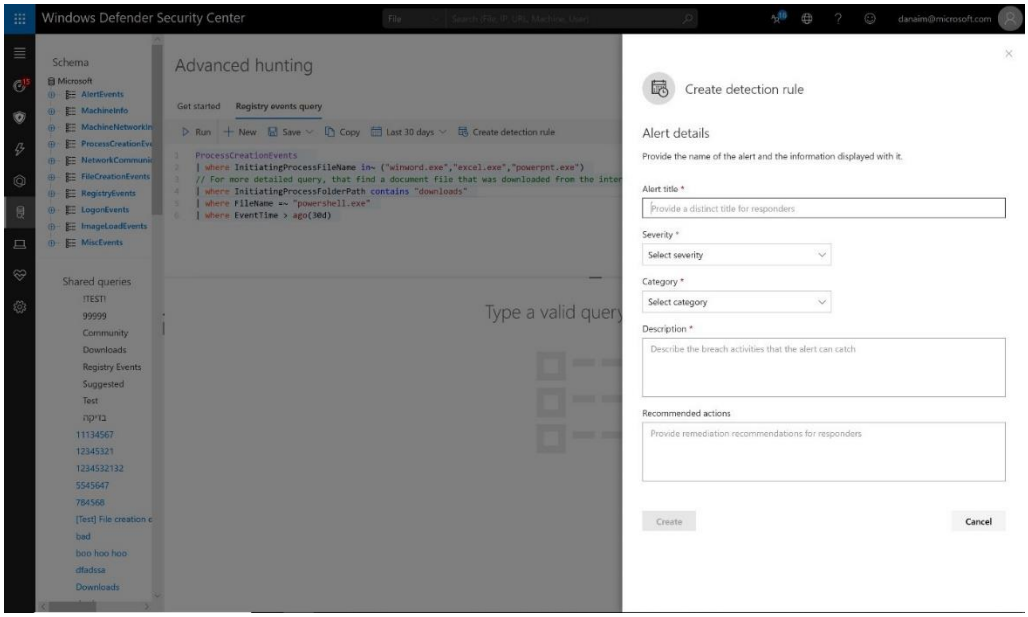
```
ProcessCreationEvents
| where InitiatingProcessFileName in~ (“winword.exe”,”excel.exe”,”powerpnt.exe”)
// For more specific query, that find a document file that was downloaded from the internet, comment out the following line. Also modify if the document resides in a folder other than “downloads”
| where FileName =~ “powershell.exe”
| where Eventtime > ago(30d)
```

5.より詳しく包括的なクエリが必要な場合は、次のクエリを使用してください。

```
let wordProcessesOpeningDownloadedDocuments =
ProcessCreationEvents
| where FileName =~ “windord.exe” and ProcessCommandLine contains @”\”
// Parse the document name from the winword commandline. Document name comes after the /n argument.
| parse ProcessCommandLine with * “ /n \”” DocumentPath “\”” 
| project ComputerName, OpenDocTime=EventTime, DocumentPath, ReportId, MachineId;
let wordProcessesRunningPowershell =
```

```
ProcessCreationEvents
| where InitiatingProcessFileName =~ “winword.exe” and FileName =~
“powershell.exe”
| project ReportId, MachineId, ComputerName, EventTime,
Powershellcommandline=ProcessCommandLine,
WordProcessCreationTime=InitiatingProcessCreationTime;
wordProcessesRunningPowershell
| join kind=inner (wordProcessesOpeningDownloadedDocuments) on ComputerName
// Look for documents opened up to 5 minutes before the suspicious Powershell was
run, but only if opened after this winword process was run already.
| where OpenDocTime between (max_of(EventTime-5m, WordProcessCreationTime)..
EventTime)
| summarize makeset (DocumentPath) by ReportId, MachineId, ComputerName,
PowershellCommandline, bin(EventTime, 1tick)
```

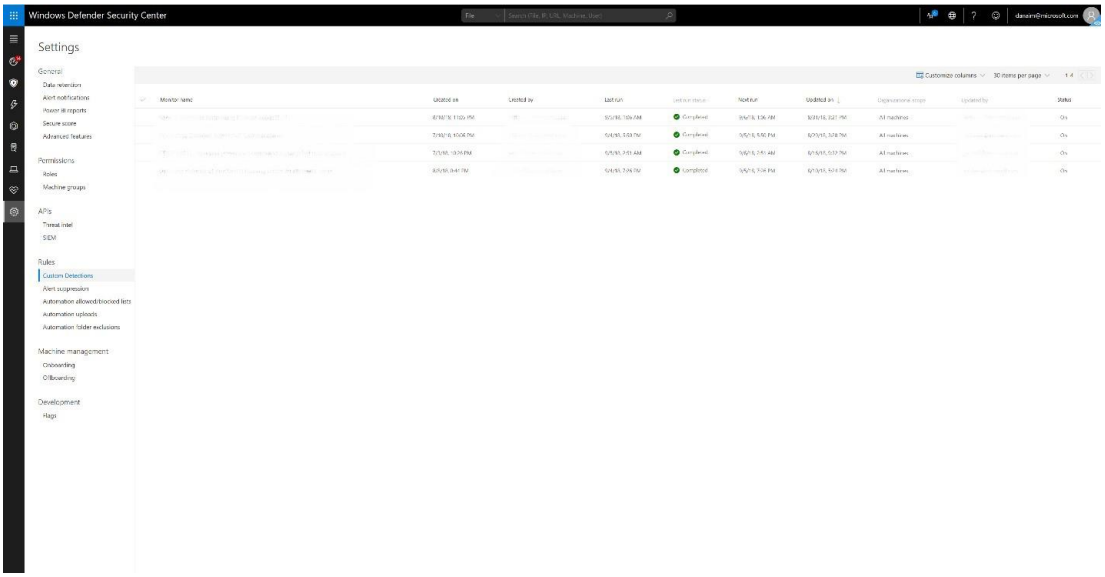
6. クエリを保存し、**[Create detection rule]** を選択します。



7. 次のようなカスタム検出ルールを作成します。
   - [Alert title]: Custom Detection | Downloaded Office file executes PowerShell
   - [Severity]: Medium
   - [Category]: Suspicious behavior
   - [Description]: A downloaded Microsoft Office file executed PowerShell commands. This alert is based on a scheduled Advanced hunting query.
   - [Recommended actions]: Check the Microsoft Office file and determine if the PowerShell activity is expected.

カスタム検出ルールが作成されると、直ぐに 1 回実行されます (アラートの発行までに数分間かかる場合があります)。その後、このルールは 24 時間に 1 回の間隔で自動的に実行されます。

既存のすべてのカスタム検出ルールにアクセスするには、[Setting] > [Custom Detections] を選択します。



カスタム検出でトリガーされたアラートの確認

Windows Defender　セキュリティ　センターで攻撃を調査しましょう。予定されたクエリによってトリガーされたアラートを使用します。シミュレーションの攻撃の結果、ダッシュボードには、テスト　マシンで発生した新しいアラートがいくつか表示されています。

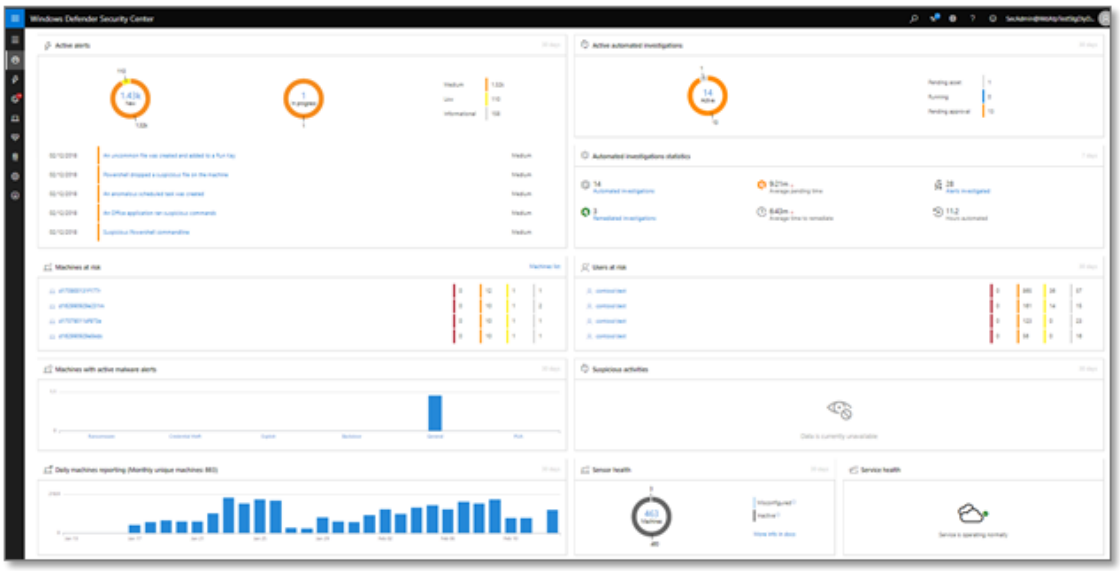


図 2: ダッシュボードに表示されたアラート

[Machines at risk] ウィジェットで、テスト　マシンをクリックしてマシンとすべての関連アラートの詳細を表示します。

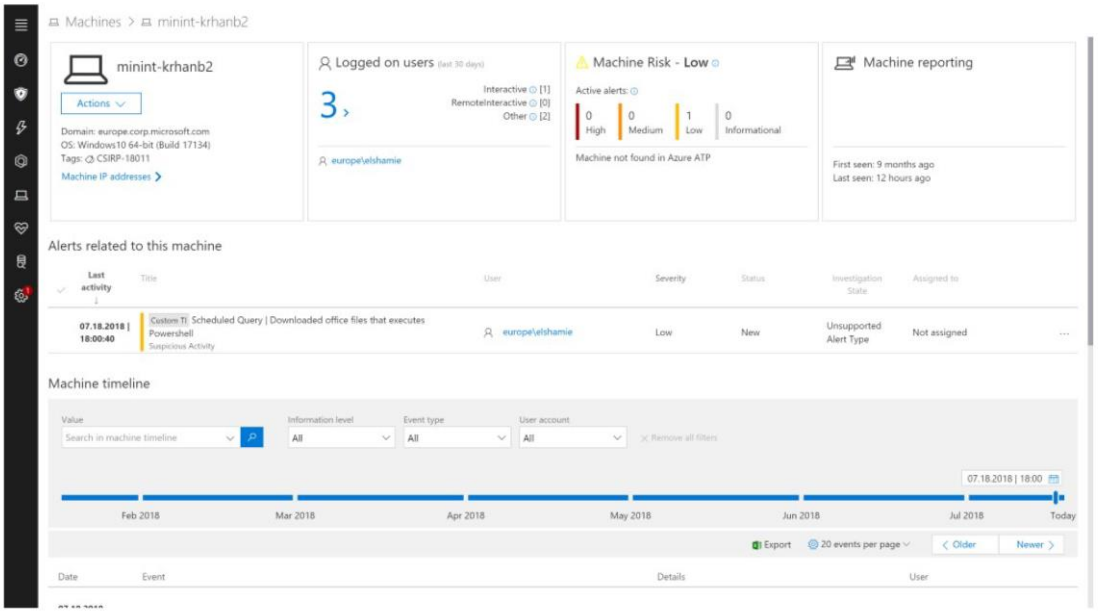


図 3: テスト マシンとアラート

✎ **注:** このシナリオでは、カスタム検出ルールによってトリガーされるアラートに注目しています。この攻撃でトリガーされるその他のアラートや、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。

まとめ

ここでは、一般的な攻撃をシミュレーションし、カスタム検出メカニズムを使って、Windows Defender ATP が攻撃を検出するしくみを紹介しました。また、高度なハンティング機能を活用してクエリをカスタマイズすることによって、新手の攻撃を監視する方法を詳しく説明しました。

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。高度なハンティング機能だけでなく、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。