Microsoft

Windows Defender Advanced Threat Protection

攻撃シミュレーション

シナリオ 4: 自動調査

(ファイルレス マルウェア攻撃)

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。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。

Windows Defender ATP

Microsoft

はじめに: ファイルレス マルウェア攻撃の自動調査

このシナリオでは、メモリ内で実行されるファイルレス マルウェア攻撃をシミュレーションします。続いて、Windows Defender ATP の自動調査機能を使って、SOC の攻撃対処 (トリアージ、調査、修復) を自動化します。自動調査機能は、攻撃の影響を受けたマシンから既知の攻撃アーティファクトを特定し、除去します。また、攻撃の影響を受ける可能性がある他のマシンに自動的にピボットし、同じ対処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 2: ファイルレス マルウェア攻撃の PowerShell スクリプト』で使用した攻撃を使用します。このシナリオでは、高度なテクニックを駆使して検出を逃れようとする攻撃を取り上げます。この攻撃は、既存のシステムと管理ツールだけを使用し、システム プロセス内にコードをインジェクションすることにより、セキュリティの網の目をかいくぐろうとします。

ここでは、Windows 10 の Exploit Protection 機能を利用して、攻撃者が悪意のあるアクティビティを実行するのを阻止する方法を紹介します。

このシミュレーションのシナリオでは、PowerShell スクリプトの実行から攻撃を開始します。ユーザーが騙されてスクリプトを実行してしまうこともあれば、横移動をねらう攻撃者が、以前に感染させた組織内の別のマシンからリモート操作でスクリプトを実行することもあります。このようなスクリプトの検出は困難です。なぜなら、正規の管理者も、リモート操作でスクリプトを実行してさまざまな管理タスクを実行するからです。

このシミュレーションでは、攻撃者は一見無害なプロセス (ここでは notepad.exe) にシェルコードをインジェクションします。ただし、実際の攻撃者は、svchost.exe のような長期間実行されるシステム プロセスをターゲットにする場合が多いでしょう。インジェクションされたシェルコードは、攻撃者のコマンド アンド コントロール (C&C) サーバーを通じて、次の攻撃に関する指示を受け取ります。

ファイルレス マルウェア攻撃を検出すると、自動調査機能が起動します。自動調査機能は、攻撃にかかわっているエンティティのメモリ コンテキストを分析し、悪意のあるプロセスの証跡を自動的に検出、修復します。

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 October 2018 Update (バージョン 1809) 以降を実行している
- 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

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

この攻撃シナリオを実行するには、次の手順に従います。

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

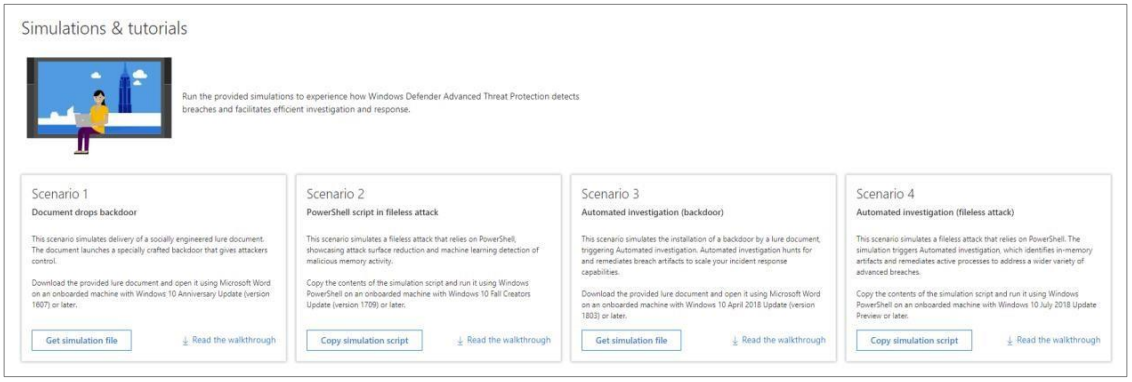

図 1: ポータル内のシミュレーション シナリオ

2. **[Scenario 4: Automated investigation (fileless script)]** の下の **[Copy simulation script]** ボタンをクリックして PowerShell スクリプトをコピーします。

3. テストマシンで、管理者権限を使用し Windows PowerShell ウィンドウを開きます。

4. プロンプトが表示されたら、スクリプトを貼り付けて実行します。

   数秒後、notepad.exe が起動し、シミュレーションの攻撃コードがインジェクションされます。この攻撃コードは、シミュレーションの C&C サーバーを示す外部 IP アドレスへの通信を試みます。

攻撃とエクスプロイト対策のシミュレーション

Windows 10 Fall Creators Update (バージョン 1709) の Exploit Protection を使用すると、ポリシーを適用して、マシン上のコードの実行を制限することができます。これにより、多くのエクスプロイト攻撃を軽減することができます。エクスプロイトが検出されると、Windows Defender ATP からアラートが発行され、SOC の担当者にイベントが通知されます。

このセクションでは、所定のプロセスで notepad.exe 内の動的なコード実行を却下するように Exploit Protection を設定してから、シミュレーションの攻撃を再度実行します。

✎ **注**: このセクションでは、Exploit Protection がプロセス インジェクションおよびその他のメモリ内攻撃アクティビティを阻止するようすをデモンストレーションします。このセクションを省略して、自動調査機能の使い方を確認することもできます。

攻撃とエクスプロイト対策のシミュレーションを行うには、次の手順に従います。

1. 管理者権限で Windows PowerShell ウィンドウを開きます。

2. プロンプトが表示されたら、次のコマンドを実行してエクスプロイト対策の設定を行います。

```
$path = “HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\runtimebroker.exe”;
$value =
([byte[]](0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x11,0x11,0x01
,0x01,0x00,0x00));
New-Item -Path $path -Force;
New-ItemProperty -Path $path -Name “MitigationOptions” -Value $value
-PropertyType
Binary -Force
```

   ✎**注**: この設定は、関連する機能について説明する目的で提供されています。どのような影響があるか適切な確認を行わずに、実稼働環境内の他のマシンに適用しないでください。

3. **[Simulations & tutorials]** ページから入手した PowerShell スクリプトを再度実行します。

前回と同様に、notepad.exe が実行され、悪意のあるシェルコードが注入され、その実行が試みられますが、今回はエクスプロイト対策の設定のおかげで、シェルコードの実行が阻止され、notepad.exe は終了します。

4. [オプション] テスト マシン上のエクスプロイト対策の設定を元に戻すには、PowerShell ウィンドウで次のコマンドを実行します。

```
Remove-ItemProperty -Path $path -Name “MitigationOptions” -Force
```

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 Windows Defender ATP ポータルに表示されます。

Windows Defender ATP

Microsoft

ポータル内の攻撃の調査

ここからは、防御者の役割に切り替えて、Windows Defender ATP ポータルから SOC の視点で攻撃を分析していきましょう。

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。

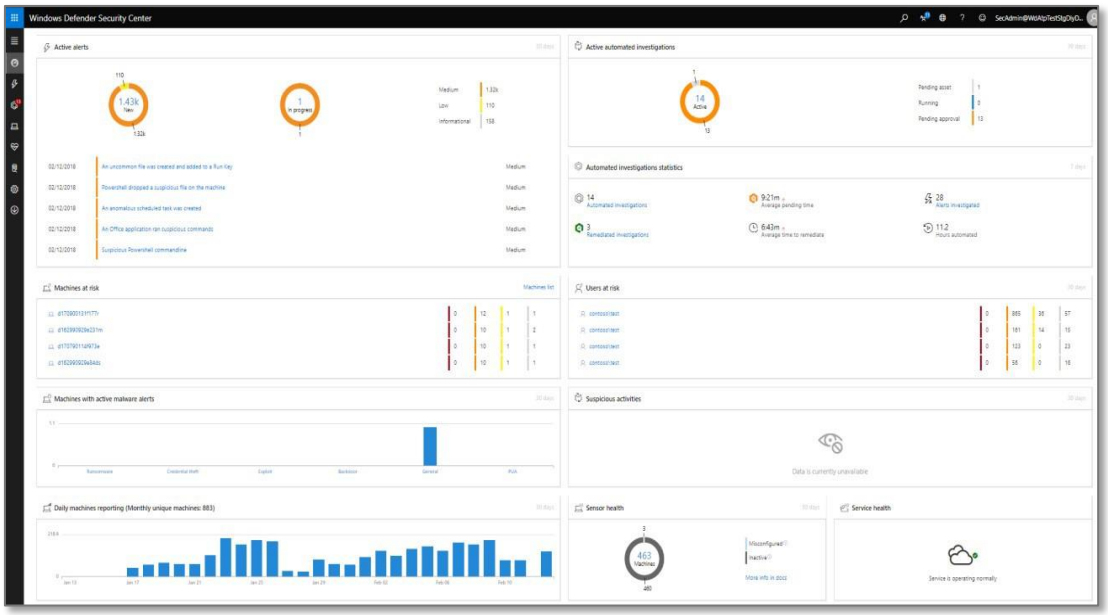

図 2: ダッシュボード上のアラート

4. **[Suspicious process injection observed]** 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。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

自動調査内容の確認、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対応する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。

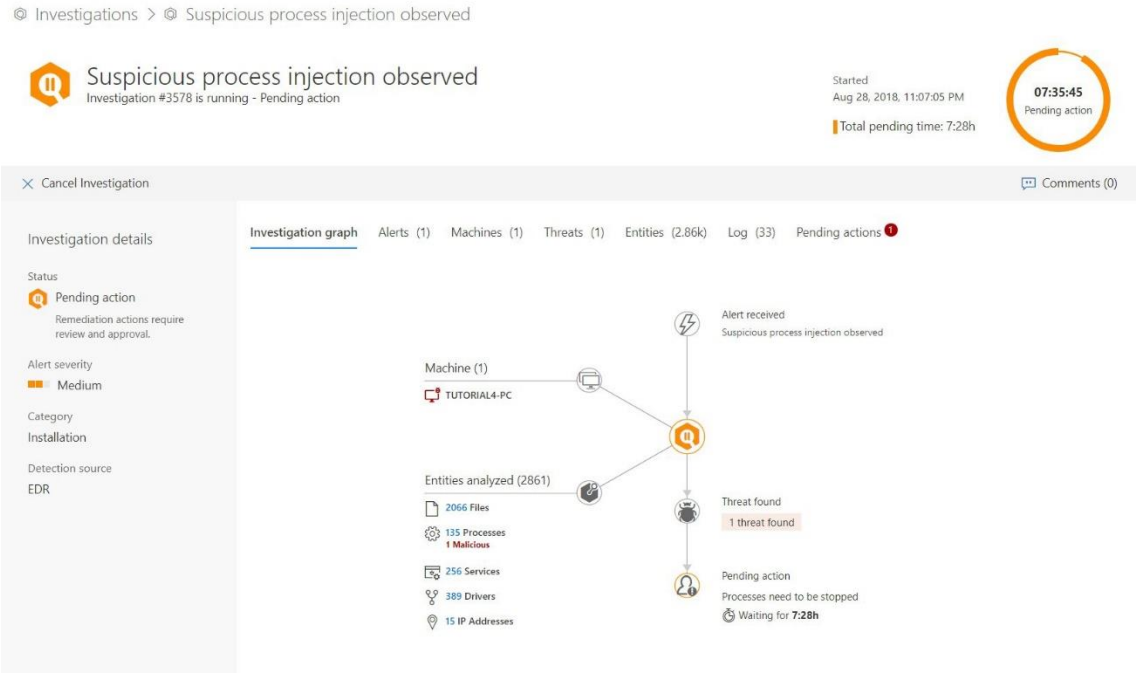

図 4: 調査の詳細ページ

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既知の脅威

  📝 **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。証跡の収集と分析、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、ユーザー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。

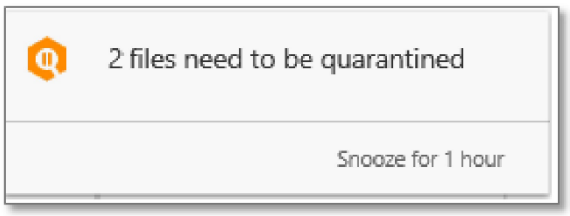

図 5: 保留中の修復アクションの通知

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、notepad.exe プロセスのインジェクションが検出されます。これは、修復が必要なアーティファクトの 1 つです。既定では、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、Windows Defender ATP のマシン グループ設定から、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。

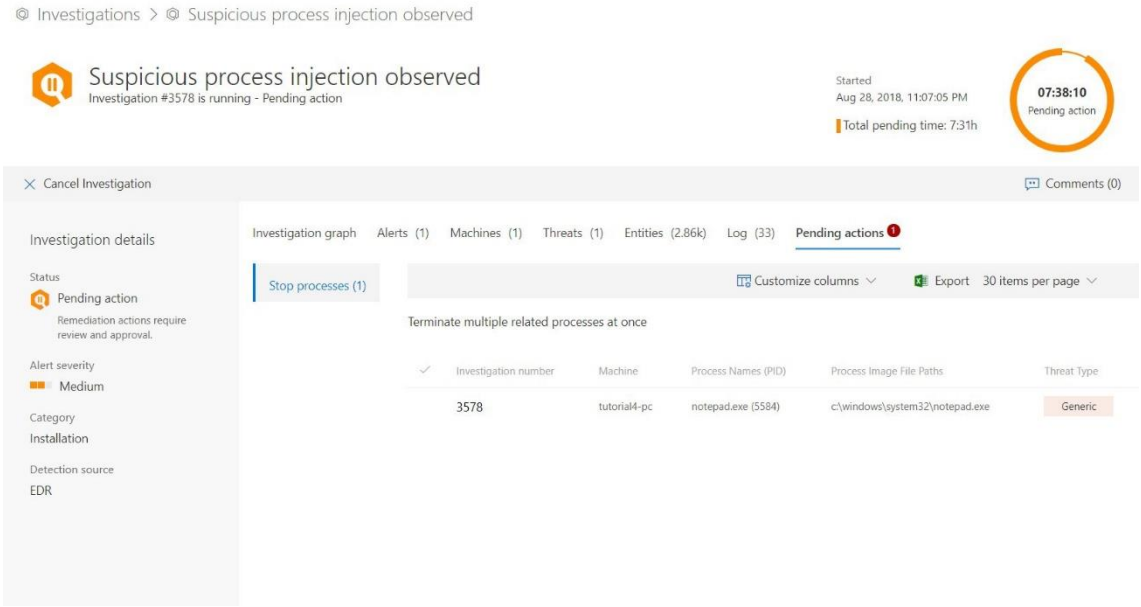

図 6: 保留中のアクション

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、自動調査機能はインジェクションされたプロセスを停止します。

   これに伴い、テスト マシンの実行中のプロセスのリストから、notepad.exe 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。

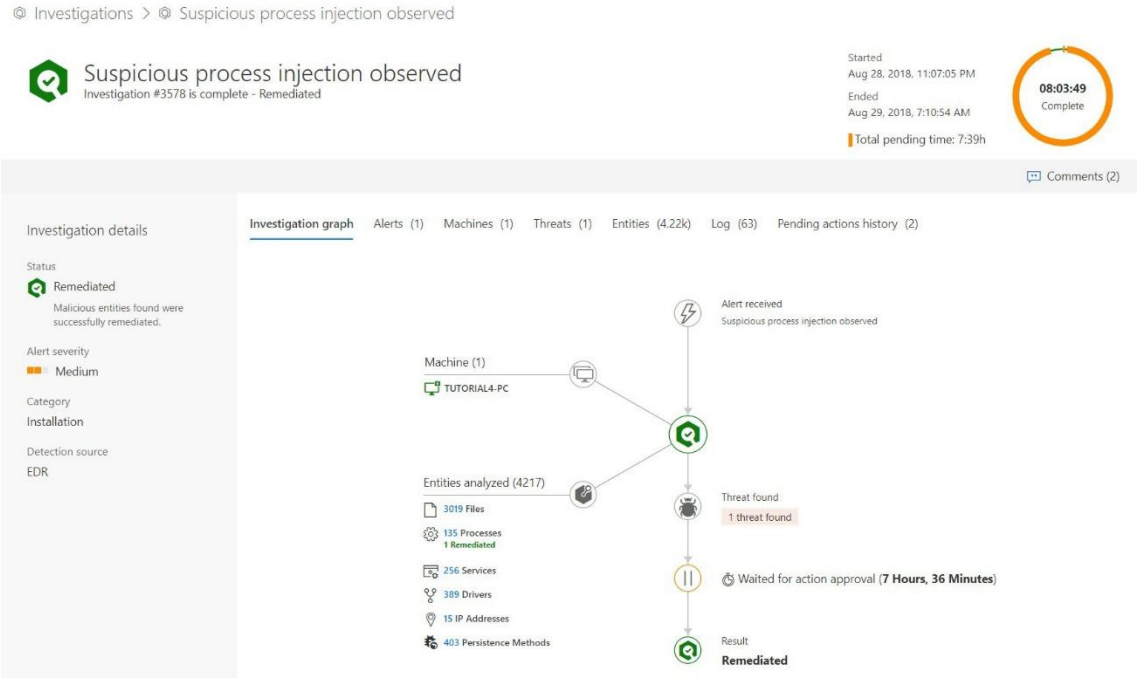

図 7: 調査の詳細ページ (修復の完了後)

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。

シミュレーションの攻撃は、次の Windows Defender ATP アラートを生成します。

- Suspicious process injection observed
- Unexpected behavior observed by a process run with no command line arguments
- EAF violation blocked by exploit protection (エクスプロイト対策に関するセクションを省略した場合は生成されない)

これらのアラートの詳細については、『シナリオ 2: ファイルレス マルウェア攻撃の PowerShell スクリプト』を参照してください。

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。

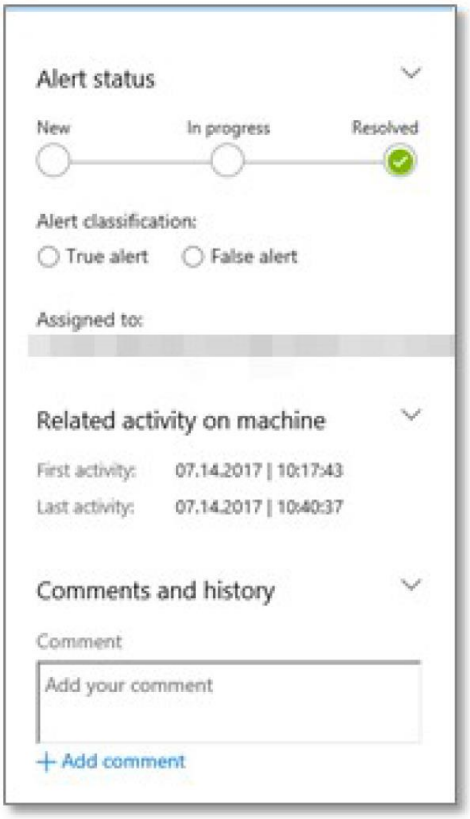

図 8: アラート管理ウィンドウ: 解決済みのアラート

まとめ

ここでは、高度なメモリのみの攻撃 (ファイルレス マルウェア攻撃) をシミュレーションし、Windows Defender ATP がディープ OS センサーを利用して、ステルス性の高い悪意のあるアクティビティをどのように検出し、アラートを発行するのかを確認しました。Exploit Protection 機能を使って、高度な攻撃を阻止し、ポータルにアラート情報を表示する方法についても確認しました。

その後、Windows Defender ATP を使って、メモリのみの攻撃にかかわった要素を自動的に調査、修復しました。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にかかわった要素を自動的に検出し、疑わしいものを修復することにより、SOC の担当者の対処能力を高め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。