AhnLab

eBook

MITRE ATT&CK Evaluations Round 7
遮断率 100% 記録!

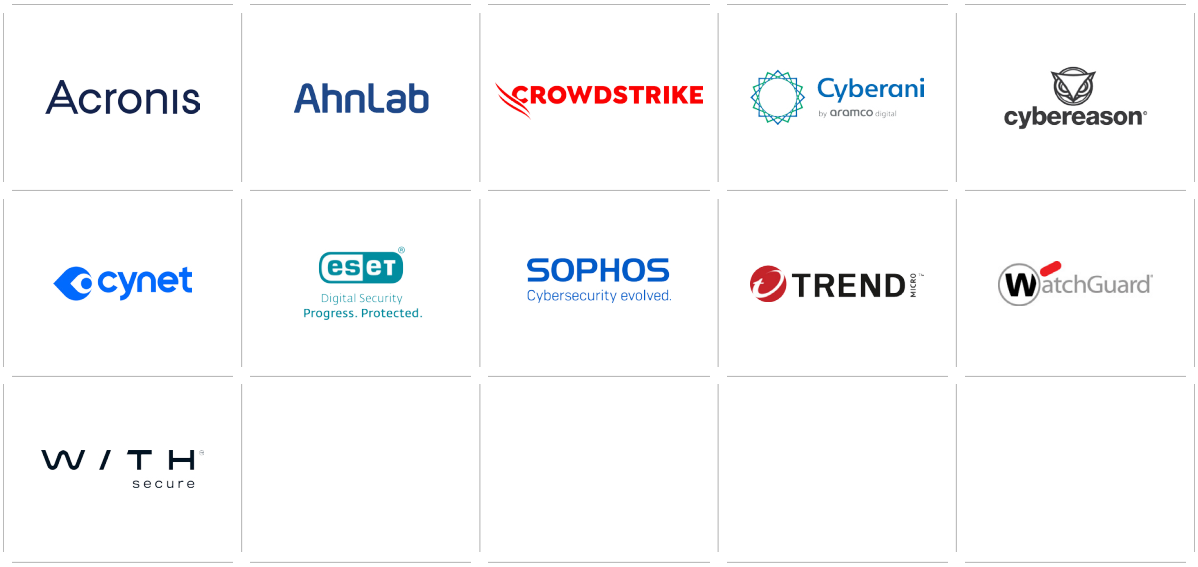
株式会社アンラボがアメリカの非営利研究開発団体である MITRE が実施した「MITRE ATT&CK®評価のエンタープライズ部門ラウンド7 (MITRE ATT&CK® Evaluations Enterprise Round 7、以下 「MITRE ATT&CK®評価」)」に参加し、「保護(Protections)」部門で100%遮断率を記録した。これにより、グローバルレベルの脅威検知および分析力を証明した。

MITRE ATT&CK®評価の紹介

MITRE ATT&CK®評価を主催するマイター（MITRE）は、国家安全のためにアメリカ政府の支援を受けて研究を行う非営利団体であり、政府、民間、学術界などと協力し、公益的な R&D 事業を進めている。サイバーセキュリティ業界では、マイター・アタックフレームワーク（MITRE ATT&CK Framework）を通じて攻撃者の戦術（Tactics）、技術（Techniques）、および手順（Procedures）を研究・定義していることで広く知られている。

「MITRE ATT&CK®評価」は、マイター（MITRE）が実施するグローバルセキュリティ製品評価であり、既知の攻撃グループの行為に対する対応能力と技術力を中心に評価する。主な攻撃グループが使用する最新の攻撃手法を再現し、各攻撃段階におけるセキュリティソリューションの検知有無、検知の証拠およびコンテキストの提供有無などをテストする。各ソリューションの順位付けや競争のための分析ではなく、MITRE ATT&CK®の知識ベースを中心に、各セキュリティ企業が脅威検知にどのようにアプローチしているかを示すことに焦点を当てている。

今年で７回目となる MITRE ATT&CK®評価は、実際の攻撃グループが使用する手法との類似性や脅威シナリオの完成度など、さまざまな面で世界的に最も信頼されるセキュリティ製品テストの1つとして認められている。今回のラウンド７には、11社のグローバルセキュリティ企業が参加し、アンラボは韓国企業として唯一、ラウンド3から5回連続で評価に参加している。



[図1] MITRE ATT&CK®評価ラウンド7参加企業

評価シナリオの構成

MITRE ATT&CK®評価は、大きく分けてサイバー脅威シナリオ（Scenario）を構成する段階（Step）と各段階を構成する詳細段階（Substep）で構成されている。これに基づき、マイター（MITRE）は脅威シナリオを模擬実行し、参加企業のソリューションのセキュリティ能力を評価する。

過去のラウンドと比べて最大の変化は、既存のオンプレミス(Windows/ Linux)環境にクラウド環境を追加したことである。最近、攻撃者がオンプレミスとクラウドを行き来しながら攻撃を実行している点を考慮し、実際の脅威と類似した形で評価を高度化した。

シナリオの観点から見ると、MITRE ATT&CK®評価は大きく▲検知(Detections) ▲保護(Protections)で構成される。

1. 検知(Detections)

サイバー脅威の検知および分析能力を評価する「検知（Detection）」部門では、各詳細段階で収集された証拠のコンテキストと情報を総合し、以下の[表]ように評価する。検知評価は「None」から「General」、「Tactic」、「Technique」の順で、検知された脅威情報の精度と詳細度が高くなることを意味する。

カテゴリ	説明
N/A	評価に反映されない場合
None	詳細な証拠がない、または要件に適合しない場合
General	不正、疑わしい、または異常な行動が発生したかを説明できる証拠
Tactic	特定の行動の背景や潜在的な意図など、戦術的な（Tactic）コンテキストを提供する証拠
Technique	特定の行動の戦術（Tactic）を超えて、方法や詳細な内容など、技術（Technique）に関するコンテキストを提供する証拠

[表 1] MITRE ATT&CK®評価部門評価レベル – 不正なイベント

さらに、不正なイベントだけでなく正常なイベントに対する誤検知（False Positives）の有無も確認する。シナリオには不正なイベントと正常なイベントが混ざっており、ソリューションが不正と正常を正確に区分できるかどうかも確認する。

カテゴリ	説明
N/A	評価に反映されない場合
Reported	正常な行動が発生したが不正と検知し、通知を送信した場合
Not Reported	異常な行動を正しく検知し、通知を送信した場合

[表 2] MITRE ATT&CK®評価「検知」部門評価レベル – 誤検知(False Positives)

2. 保護(Protections)

「保護(Protections)」部門では、ソリューションがサイバー攻撃がシステムに影響を与える前に遮断できるかを評価する。システムが被害を受ける前に防御できたかどうかを、合格／不合格（Pass/Fail）形式でテストを実行する。

カテゴリ	説明
N/A	評価に反映されない場合
Protected	悪性行動発現前に遮断
Not Blocked	悪性行動発現を許可

[表 3] MITRE ATT&CK®評価「保護」部門評価レベル – 誤検知(False Positives)

攻撃グループの説明

MITRE ATT&CK® ラウンド7は、前ラウンド6と同様に様々な攻撃グループの手法を組み合わせてシナリオを構成した。模擬実行した攻撃グループは大きく分けて▲金銭を狙うサイバー攻撃グループ(Financially-Motivated Cybercriminal Collective) ▲中国背後のサイバースパイグループ(People's Republic of China (PRC) Cyber Espionage Group)で構成される。

各攻撃グループに関する説明は以下の通りである。

1. Scattered Spider: 金銭を狙うサイバー攻撃グループ

マイター（MITRE）は、ソーシャルエンジニアリング手法、リモートアクセスツールのインストール、多要素認証(MFA)の回避に熟練した攻撃グループ「Scattered Spider」の手法を模擬実行した。攻撃者は、被害者のクラウド資源を持続的に狙い続け、拠点を確保してネットワークおよびディレクトリの偵察を実行した後、機密システムとデータストレージにアクセスする。攻撃の展開速度が非常に速く、大量のデータに素早くアクセスして流出させる。

2. Mustang Panda: 中国背後のサイバースパイグループ

また、マイター（MITRE）はハッキング能力とツールを継続的に進化させている中国背後のサイバースパイグループ「Mustang Panda」も模擬実行した。攻撃者はソーシャルエンジニアリング手法と合法的なツールおよびサービスの悪用により、パーソナライズドマルウェアを配布する。既知の行動とツールの中の多数は、中国のサイバー攻撃エコシステム全般で広く使用されている。例えば、LOTL(Living off the Land) 手法、パーソナライズドマルウェア、クラウドベースインフラ攻略などがある。

遮断率100%! 業界をリードするアンラボの評価結果

アンラボは、自社の △次世代エンドポイント検知および対応ソリューション「AhnLab EDR」 △エンドポイントセキュリティプラットフォーム「AhnLab EPP」 △SaaS 型セキュリティ脅威分析プラットフォーム「AhnLab XDR」で今回の評価に参加した。保護(Protections)評価で100%を記録したことを始め、オンプレミス-クラウドをアウフレッシングする脅威可視性および検知正確性の面でも注目すべき成果を収めた。

ユーザーの立場から見ると、アンラボの今回の評価結果は以下の観点から注目に値する。

1. 100% 脅威遮断！業界最高水準のセキュリティ能力を証明

アンラボは、保護(Protections)部門において不正な行動を100%遮断し、評価環境のシステムを安全に保護した。MITRE ATT&CK®評価、グローバル認証、実際の顧客環境など、様々な面から検証を受けてきた業界最高水準のセキュリティ能力を再び証明した。

特に、今回の保護評価では不正なイベントだけでなく、「正常なイベントのみ」で構成されたテストもあった。アンラボは、この項目に対しては正常と判別し、遮断を実行しないことで遮断の正確度まで証明した。つまり、遮断すべき不正なイベントのみ遮断し、正常なイベントは許可することで、実際のユーザー環境で強力なセキュリティと実用性を同時に提供するものである。

#2. オンプレミスとクラウドを網羅する包括的な脅威可視性

前述の通り、今回のラウンド7はオンプレミス(Windows/Linux)とクラウドを組み合わせたシナリオで構成された。アンラボのソリューションは、OS を越える高度な攻撃手法に関する詳細な証跡と分析情報を提示した。これにより、ユーザーが証跡情報を通じて脅威行動に関する「コンテキスト(Context)」を包括的に理解できるようにした。

今年から新たに導入されたクラウドシナリオでは、自社 XDR ソリューション「AhnLab XDR」を評価環境のクラウドリソースと連携させ、検知システムを構築した。柔軟な連携基盤「オープン XDR」である AhnLab XDR は、攻撃者がクラウドを行き来しながら実行する不正な行動を効果的に検知し、コンテキスト情報を提供した。これにより、既存のオンプレミスだけでなく、クラウドでも卓越した検知能力を証明した。

#3. 誤検知（False Positives）90% & 検知遅延「ゼロ」

検知精度と品質を評価するために構成した正常イベントに対しては、約90%の精度を記録した。この結果は「正常な振る舞いに対しては脅威通知を送信しなかった」ということであると理解すればよい。これによって、当社のソリューションが正確な検知力を基盤に実際の顧客がセキュリティーの運用中に困難を訴える過検知の問題を解決できることを示した。

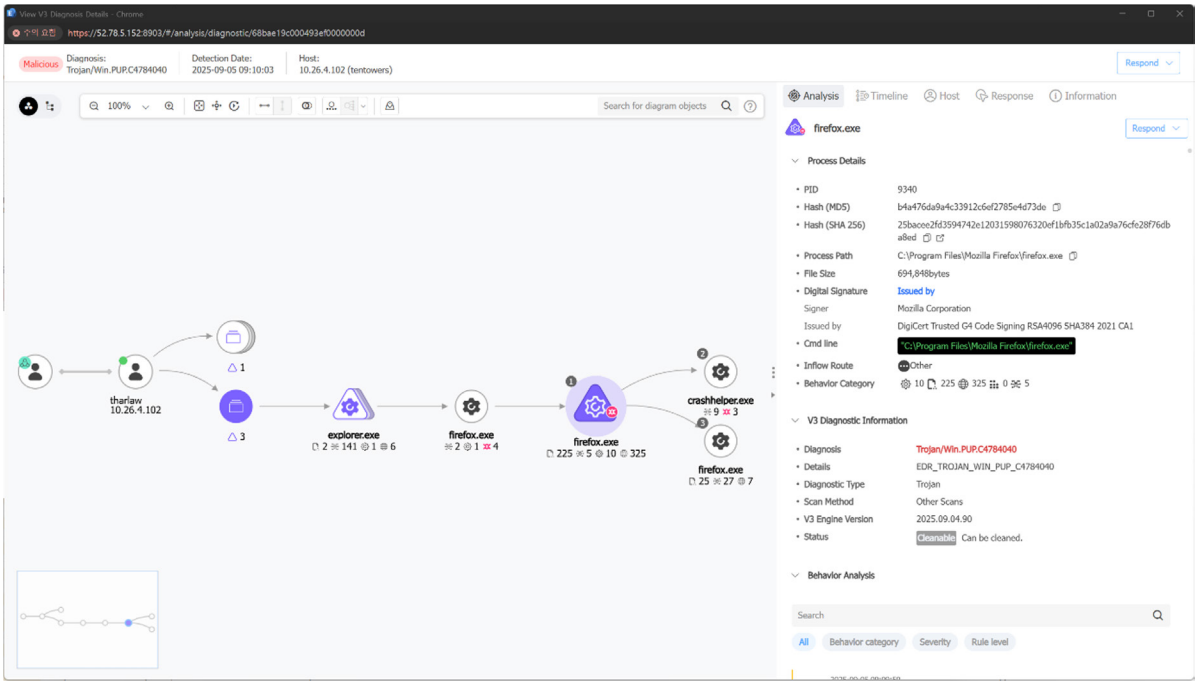
さらに、MITRE ATT&CK®評価は検知通知に遅延(Delay)があったかどうかもともに確認する。実際のユーザーが検知結果を即座に脅威対応に活用する必要があるためである。アンラボのソリューションはすべての検知結果をリアルタイムで提供し、「遅延なしの検知(Zero Delay)」を達成した。

実際の評価脅威検知内容

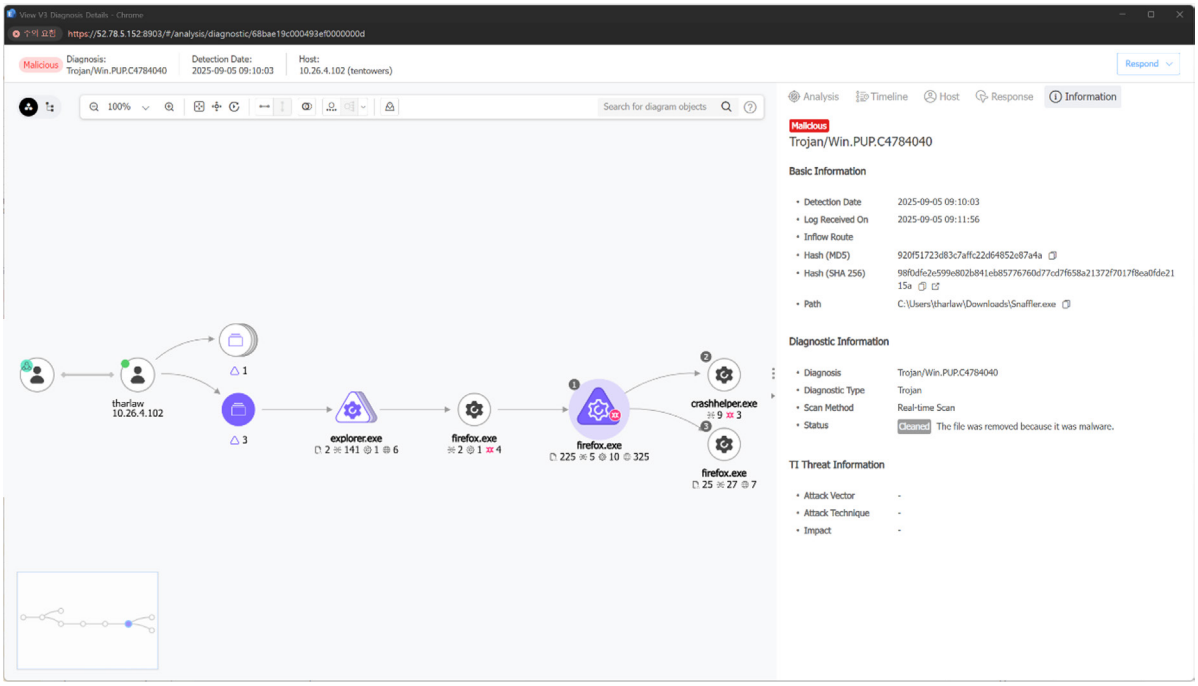
今回のラウンド7で、アンラボのソリューションは Windows、Linux、およびクラウドにわたり卓越した検知 & 遮断力を披露した。その過程が具体的にどう行われたのか、実際の例を通して見ていこう。

1. 保護(Protections): Test 1

被害者環境に侵入した攻撃者は tharlaw というユーザーアカウントでファイルサーバーから Snaffler.exe という実行ファイルをダウンロードした。攻撃者は Snaffler.exe のダウンロードとともに、ローカルドライブおよびネットワーク共有状態を検索する行動を現した。



[図 2] Protections: Test 1 –ファイルダウンロード証跡

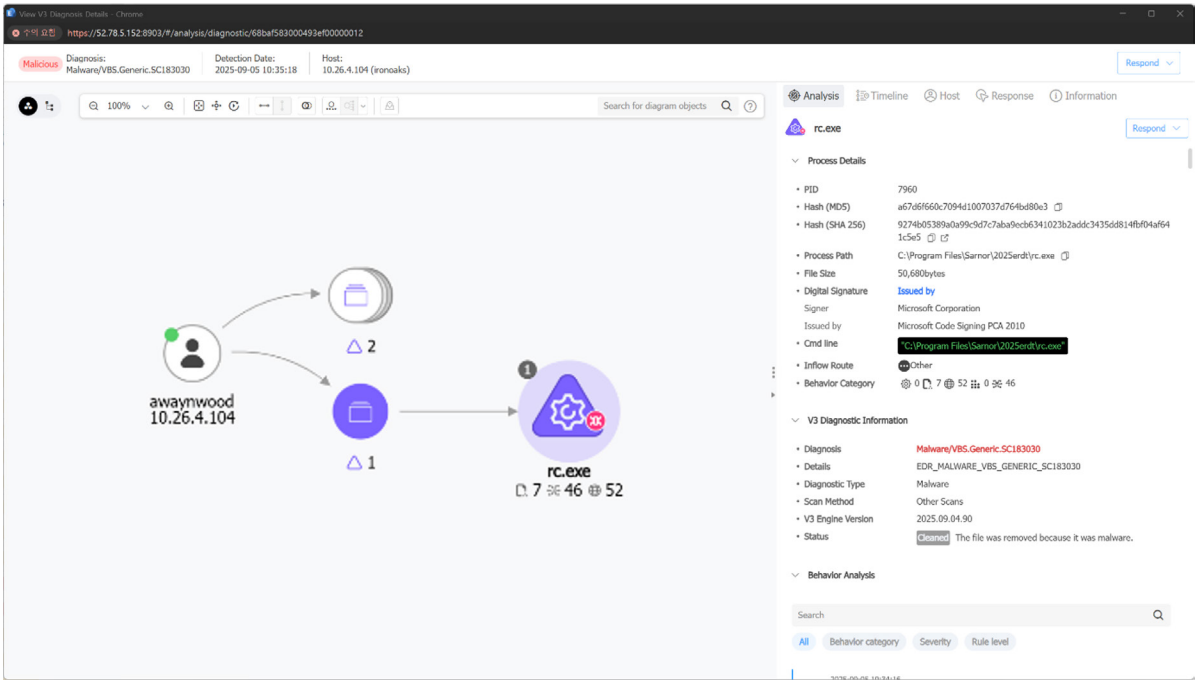


[図 3] Protections: Test 1 – ファイル遮断証跡

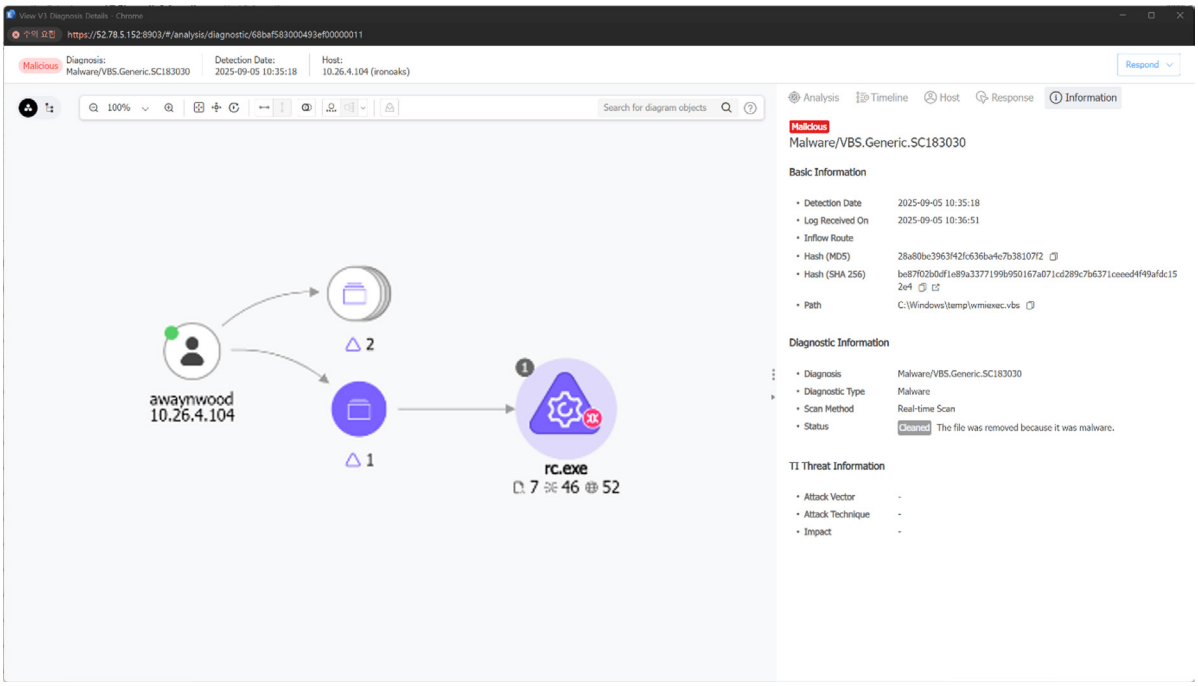
AhnLab EDR は、外部からダウンロードされた実行ファイル Snaffler.exe が不正なシグニチャを含んでいることを検知した。これについて、当社のアンチウイルスソリューション AhnLab V3 と連携し、実行ファイルを Trojan/Win.PUP.C4784040 と診断して遮断し、不正な行動の発現を事前に防いだ。単純に不正なファイルを遮断しただけでなく、EDR とアンチウイルスの連携を通じて具体的にどのようなコンテキストで遮断が行われたのかをユーザーが理解できるようにしたという点で大きな意味がある。

2. 保護(Protections): Test 5

感染した環境に侵入した攻撃者は、awaynwood というユーザーアカウントで遠隔コマンド実行ツールを通じ wmiexec.vbs を C:¥Windows¥Temp パスにダウンロードした。その後、このスクリプトを活用し、ファイルサーバー heartshome(10.26.3.106)にネットワーク共有を作成した。



[図 4] Protections: Test 5 – ファイルダウンロード証跡

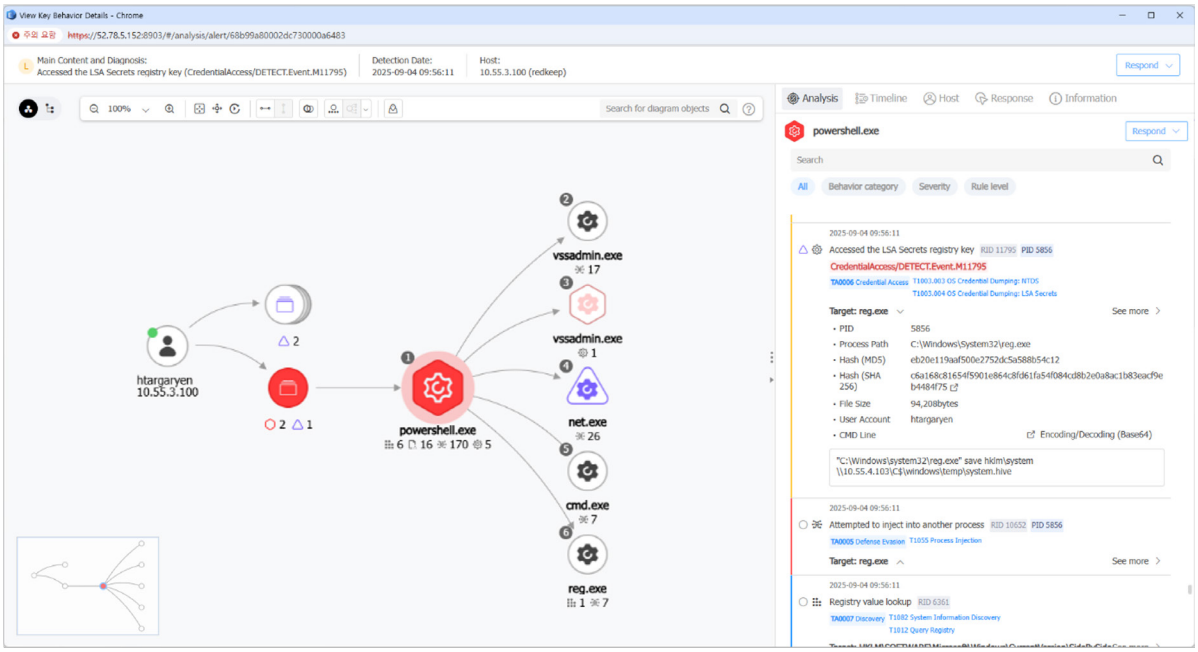


[図 5] Protections: Test 5 – ファイル遮断証跡

上記 Test 1 と類似して、AhnLab EDR は外部から C:¥Windows¥Temp パスにダウンロードされた実行ファイル wmiexec.vbs が不正なシグニチャを含んでいることを検知した。これについて、AhnLab V3 を活用し Malware/VBS.Generic.SC183030 と診断してファイルを遮断した。

3. 検知(Detections): Substep 7.5 – オンプレミス

攻撃者は htargaryen というユーザーアカウントでドメインコントローラー redkeep(10.55.3.100)で NTDS を活用した資格情報ダンプにより NTDS ファイルを抽出し、オフラインクラッキングを実行した。これのための詳細段階として redkeep(10.55.3.100)で reg.exe を実行し、システムハイブを遠隔地である harrenhal(10.55.4.103)の Windows¥Temp¥system.hive パスに保存しようとした。



[図 6] Detections: Substep 7.5 –ステムハイブ流出の検知

AhnLab EDR は、攻撃者がドメイン資格情報の窃取のために署名されていない reg.exe を活用し、システムハイブを遠隔地に保存しようとするフローをダイアグラムで提示した。レジストリハイブパス(HKLM¥SYSTEM)と遠隔 UNC 保存位置(¥10.55.4.103¥C$¥Windows¥Temp¥system.hive)を正確に検知し、これに対応する TID(TA0006 Credential Access & T1003.002 OS Credential Dumping: Security Account Manager)を提供した。これにより、攻撃者の資格情報窃取のためのシステムハイブ流出を詳細に理解できるようにした。

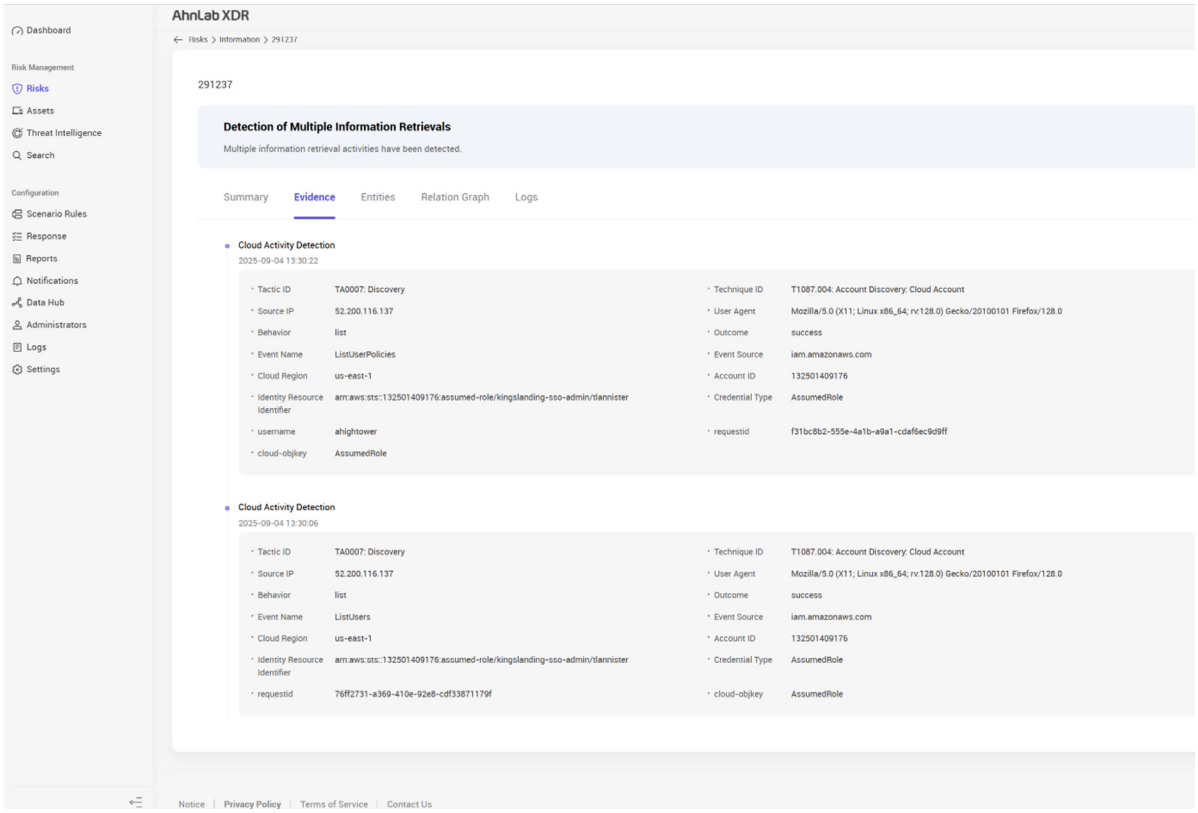
4. 検知(Detections): Substep 7.2 – クラウド

最後に、クラウド領域で攻撃者は tlannister というユーザーアカウントで ahightower という AWS アカウントを作成した。ここで、正常なユーザーを偽装するために被害者環境の既存ネーミング規則を参照し、その規則に従って ahightower アカウントを作成した。

AhnLab XDR は、攻撃者が既存のネーミング規則参照するためにユーザーリストを取得したあと、アカウントを作成したことを確認した。ネーミング規則は「ゲーム・オブ・スローンズ」に登場する家門名に一つのアルファベットを追加した形であった。

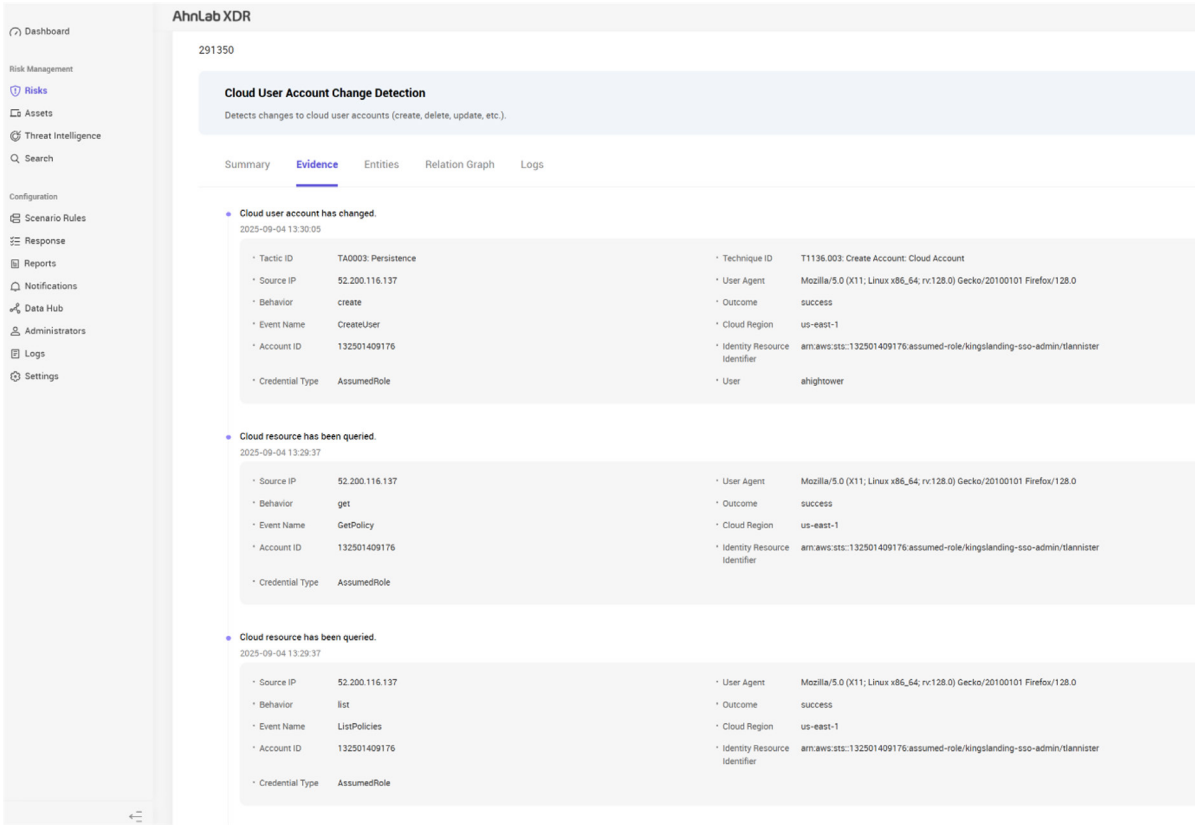
- a + targaryen
- t + lannister
- j + mormont
- a + hightower

詳しく見ると、AhnLab XDR はまず tlannister(攻撃者)が ListUserPolicies および ListUsers イベントを通じて既存のユーザーリストおよびポリシーを取得する振る舞いを検知した。



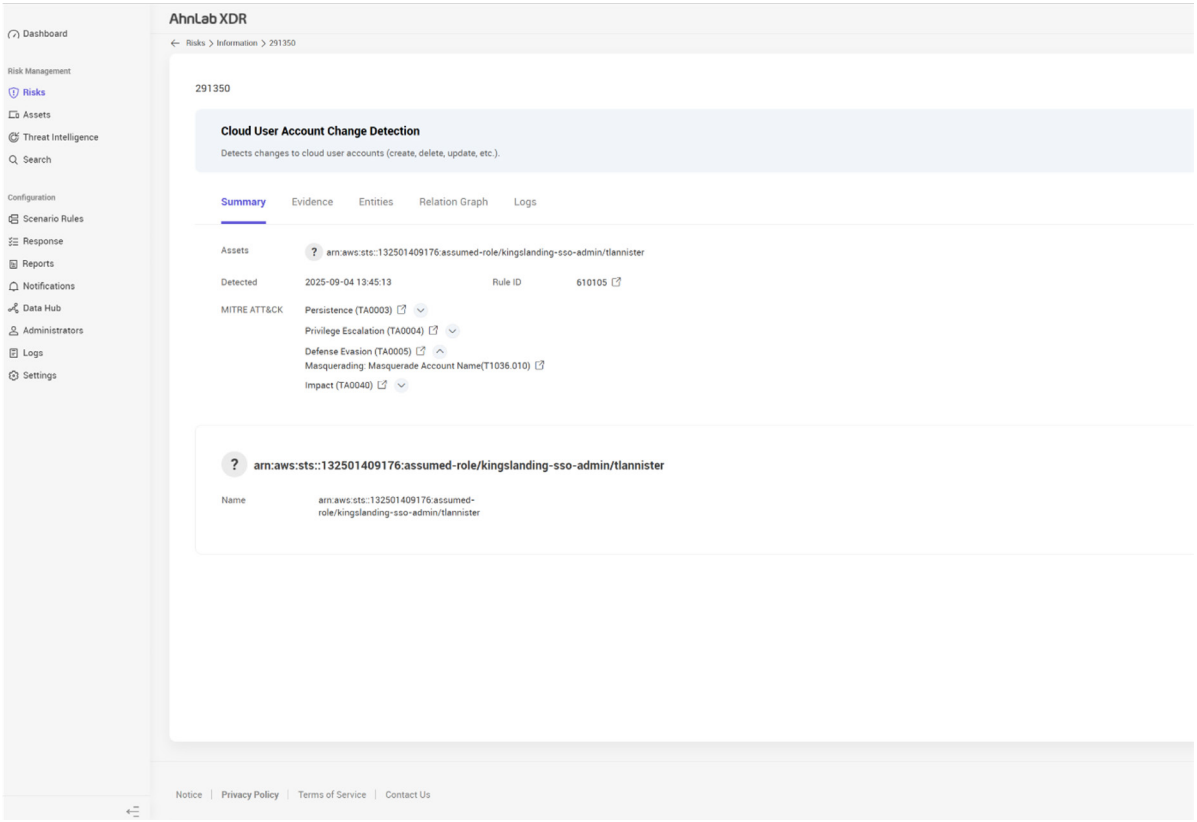
[図 7] Detections: Substep 7.2 – ユーザーリストおよびポリシーのインポート

そして, tlannister(攻撃者)が CreateUser イベントを通じて ahightower を作成する過程を検知した。



[図 8] Detections: Substep 7.2 – ahightower の作成

AhnLab XDR は、該当行動に対し、Defense Evasion (TA0005) と Masquerading: Masquerade Account Name(T1036.010) という適切な TID と説明を提供した。



[図 9] Detections: Substep 7.2 – 適切な TID 提供

まとめると、攻撃者が検知回避を目的にアカウント名を偽装し、正常なアカウントのように見せる行動を行ったことを明確に理解できるようにした。

結論：検証された技術力で顧客を安全に

MITRE ATT&CK®評価は、全世界で公信力を認められている評価であり、実際の脅威と類似した精巧な手法で構成されている。アンラボは、この評価でオンプレミスとクラウドにわたり強力な遮断、包括的な脅威可視性および正確な検知力を証明した。さらに、この評価に5年連続で参加し、客観的な検証を持続すると同時に、絶え間ないソリューションの高度化を通じて顧客の信頼を高めているという点で大きな意味がある。

MITRE ATT&CK®評価ラウンド7の結果は、マイターのウェブサイトで確認できる。本評価に参加したアンラボの製品に関する詳細情報は、アンラボのウェブサイトで確認できる。

▶AhnLab EDR さらに詳しく見る

▶AhnLab XDR さらに詳しく見る

▶AhnLab EPP さらに詳しく見る

AhnLab

〒108-0014 東京都港区芝 4丁目 13-2田町フロントビル 3階
ホームページ: www.ahnlab.com/jp
Tel：+81 3-6453-8315 | Fax：+81 3-6453-8316