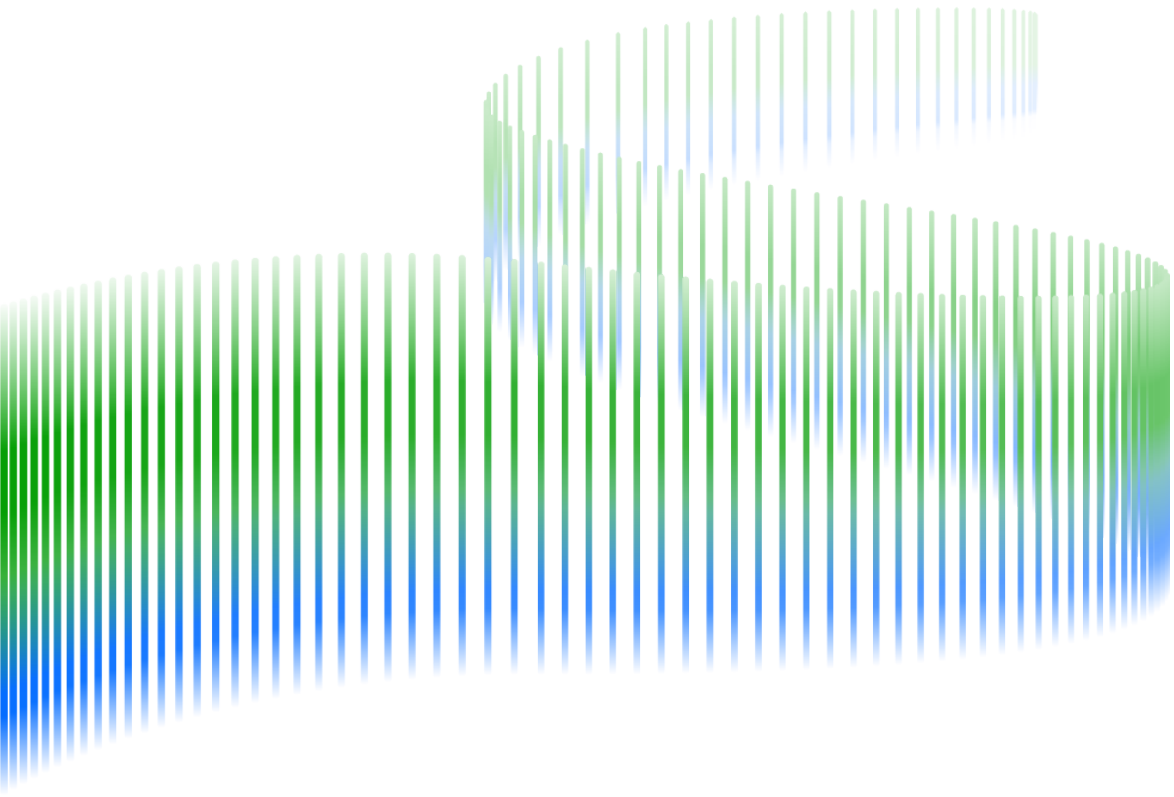
MITRE ATT&CK®を活用した脅威ハンティングと検知



目次

エグゼクティブサマリー

MITRE ATT&CK® は、実環境で観測された攻撃者のタクティクス（戦術）とテクニック（技法）を体系的に整理したオープンなフレームワーク兼ナレッジベースです。

ATT&CKは攻撃者の戦術的目的と手法を共通の分類体系で整理し、セキュリティコミュニティ内の情報共有を円滑化するだけでなく、組織の検知体制を分類して攻撃挙動の盲点を可視化する実践的フレームワークとしても機能します。
本書ではまずMITRE ATT&CKと関連ツールの概要を紹介し、その後、脅威ハンティングと検知に焦点を当てた具体的な活用法を解説します。

MITRE ATT&CKを理解する

本章ではMITRE ATT&CKの構成要素であるタクティクス、テクニック、例、緩和策、検知について概要を説明します。

MITRE ATT&CKの活用

MITRE ATT&CKの多様なユースケースを手短に確認した後、本書ではMITRE ATT&CKを次の目的で活用する方法にフォーカスします。

- 現在監視している悪意ある挙動のギャップを分析する
- 脅威検知とハンティングを強化する
- 検知ルールをテストし、想定どおりにアラートが発生することを保証する
- 5つの代表的テクニックを用いた脅威検知とハンティング

最終章では、MITRE ATT&CKの中から普及度などの基準で選定した5つのテクニックを取り上げ、脅威ハンティングと検知における活用方法を詳しく解説します。攻撃者がこれらをどう利用するか、どのように検知できるかを深掘りし、収集すべきログや有効化すべき監査設定、ログで注目すべきポイントを示します。さらに、ExabeamがNew-Scale SIEMとLogRhythm SIEMにどのように検知ルールを実装しているかも紹介します。

MITRE ATT&CK フレームワークは、攻撃者がシステムを攻撃する際に用いる手法を分類・記述するための、正規化された体系的アプローチです。MITRE ATT&CKはまず上位概念から出発し、攻撃手法を理解するための堅固な概念とその相互関係の枠組みを提供します。さらに、理論だけにとどまらず、さまざまなユースケースに適用できる詳細かつ継続的に更新される技術情報を備えています。MITRE ATT&CKは各手法を示すだけでなく、それぞれの緩和策と検知方法の推奨も提示します。

MITRE ATT&CKを理解する

タクティクス（戦術）

MITRE　ATT&CKフレームワークにおける最上位レイヤーはタクティクス（Tactics）です。攻撃者の戦略目標は、身代金の要求、情報の窃取、あるいは組織のIT環境の破壊など多岐にわたりますが、その達成には一連の短期的・段階的な目的をクリアする必要があります。多くの攻撃は、まず初期アクセス(Initial Access)/（TA0001）の獲得から始まり、次いで実行（Execution)/（TA0002）や永続化(Persistence)/（TA0003）といった基本タクティクスが中間目標としてほぼ必須となります。情報窃取を狙う攻撃者であれば、収集（Collection)/（TA0009）を経て、最終的に持ち出し（Exfiltration（TA0010）に至ります。さらに攻撃者は、横移動（Lateral Movement)/（TA0008）によるシステム／アカウント間の横移動や、防御回避（Defense Evasion)/（TA0005）による監視の回避など、複数のタクティクスを組み合わせることがあります。

ただし重要なのは、タクティクスとは攻撃フェーズごとの短期的な意図を分類・記述したものであり、「どのように実行するか」までは含まない点です。タクティクスは、攻撃者がその時点で「何をしようとしているか」を示すものであり、具体的な手法を示すわけではありません。以下の表は、現在MITRE　ATT&CKを構成するタクティクスを説明したものです。

スタッフモデル	長所	短所
TA0001	初期アクセス	初期アクセス（Initial Access）は、攻撃者がネットワークに最初の足がかりを得るために利用する経路を表します。
TA0002	実行	実行（Execution）は、攻撃者が制御するコードをローカルまたはリモートのシステムで実行させるテクニックを指します。多くの場合、初期アクセス後にコードを実行する手段として、また横移動によってリモートシステムへのアクセスを拡大する際にも用いられます。
TA0003	永続化	永続化（Persistence）は、攻撃者がシステム上に恒常的なプレゼンスを確立・維持するために行うアクセス、操作、設定変更を指します。システム再起動や認証情報の失効などの中断があってもアクセスを維持できるよう、リモートアクセスツールを再起動したり、別のバックドアを設けたりする必要があります。

スタッフモデル	長所	短所
TA0004	権限昇格	権限昇格（Privilege Escalation）は、攻撃者がシステムやネットワークでより高い権限を取得する行為を指します。高度なツールや操作の実行には上位権限が必要となるため、攻撃の多くの段階で不可欠です。攻撃者はしばしば低権限の状態で侵入し、システムの脆弱性を突いてローカル管理者やSYSTEM／root相当の権限を得ようとします。また、あらかじめ管理者相当の権限を持つユーザーアカウントを悪用する場合もあります。特定システムへのアクセス権や、攻撃目的の達成に必要な機能を持つユーザーアカウントを乗っ取ることも、権限昇格に含まれます。
TA0005	防御回避	防御回避(Defense Evasion)は、検知やその他の防御策を回避するために攻撃者が用いるテクニック群です。これらの行為は、他のタクティクスのテクニックを流用・変形して、防御や対策を無力化することがあります。防御回避は攻撃の全フェーズにわたって適用され得る属性集合と見なせます。
TA0006	資格情報アクセス	資格情報アクセス（Credential Access）は、企業環境で使用されるシステム、ドメイン、サービスの資格情報を取得または制御下に置くためのテクニック群を指します。攻撃者は、ネットワーク内部で使用する目的で、ユーザーや管理者アカウント（ローカル管理者やドメイン管理者権限を含む）の正規資格情報を窃取しようと試みる可能性が高いです。攻撃者はそのアカウントになりすまして、システムやネットワーク上で当該アカウントのすべての権限を行使できるため、防御側による検知が困難になります。十分な権限を得た攻撃者は、将来の侵入に備えて新しいアカウントを作成することも可能です。
TA0007	探索	探索（Discovery）は、攻撃者がシステムや内部ネットワークについて情報を収集し、状況を把握するためのテクニック群です。攻撃者が新たなシステムにアクセスすると、自分が支配下に置いた資産や、そのシステムを踏み台にすることで得られる利点を把握する必要があります。多くのオペレーティングシステムには、この侵害後の情報収集フェーズを支援するネイティブツールが数多く備わっています。
TA0008	横移動	横移動（Lateral Movement）は、ネットワーク上のリモートシステムへアクセスして制御を拡大するためのテクニック群です。このテクニックには、リモートシステム上でツールを実行する場合もあれば、実行しない場合もあります。横移動のテクニックを使うことで、攻撃者は追加のリモートアクセスツールを投入せずに別システムから情報を収集できる場合があります。

スタッフモデル	長所	短所
TA0009	収集	収集（Collection）は、エクスフィルトレーション（外部持ち出し）に先立ち、対象ネットワークから機密ファイルなどの情報を特定・取得するためのテクニック群を指します。また、攻撃者が持ち出し対象を探す際に注目する、システム／ネットワーク上の保存場所も含まれます。
TA0010	持ち出し	持ち出し（Exfiltration）は、攻撃者が対象ネットワークからファイルや情報を搬出する、または搬出を支援するテクニックおよび手法を指します。このカテゴリには、攻撃者が持ち出し用データを探し出すシステム／ネットワーク上の保存場所も含まれます。
TA0011	コマンド＆コントロール	コマンド＆コントロール（Command and Control）は、攻撃者が被害ネットワーク内で支配下に置いたシステムと通信する方法を示します。システム構成やネットワークトポロジー、秘匿性の要件によって確立方法は多岐にわたり、MITRE ATT&CKでは代表的な要素のみを抽出して差異を説明しています。実際には、既存の正規プロトコルやサービスを流用して新たなプロトコルを定義できるため、文書化されている以上に多くの具体的テクニックが存在します。
TA0040	影響	影響（Impact）は、システム・サービス・ネットワークの可用性や完全性を直接損なうことを主目的とするテクニック群を指します。業務プロセスに影響を与えるデータ改ざんなどが含まれ、これらは攻撃者の最終目標となる場合もあれば、機密情報漏えいを隠蔽するためのカバーとして用いられる場合もあります。

表1. MITRE ATT&CKのタクティクス

テクニック

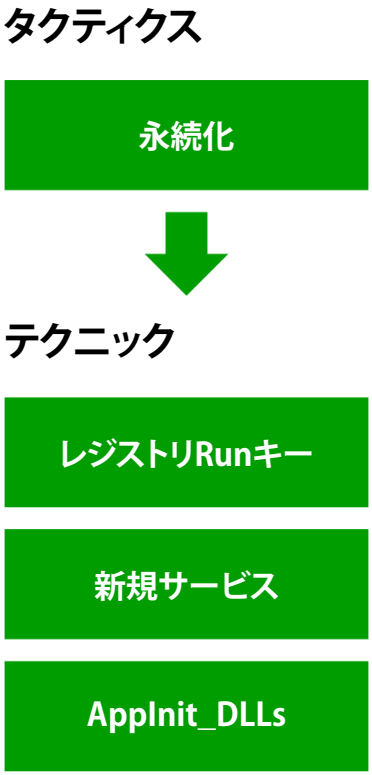
タクティクスが「攻撃者が何をしようとしているか」を示すのに対し、テクニックはそのタクティクスを実現するために攻撃者が編み出した具体的な手段（どのように）を示します。たとえば攻撃者は、システムの再起動やユーザーの再ログオン後もネットワーク上に居座り続けたいと考えます。これはタクティクスTA0003：永続化（Persistence）に当たりますが、永続化を達成する方法は一つではありません。

- Windowsでは、レジストリのRunキーやスタートアップフォルダーに値を仕込み、システム起動やログオンといった予測可能なイベントでコマンドを実行させる方法があります（T1547.001：Registry Run Keys/Startup Folder）。
- あるいは、悪意あるプログラムをシステムサービスとして登録するT1543.003：New Serviceを使うこともできます。
- さらにT1103：AppInit_DLLsを悪用すれば、user32.dllを読み込むあらゆるプロセスに自分のDLLを強制ロードさせることが可能です。

このほかにも多数のテクニックが存在し、今後も追加されるでしょうが、いずれも被害システム／ネットワークへの永続的アクセスを確立するという目的は共通です。そのため、すべて同じタクティクス（Persistence）に分類されています。

一部のテクニックは複数のタクティクスを支援しており、MITRE ATT&CKでもその重複が反映されています。たとえばT1543.003：新規サービス（New Service）は、永続化（Persistence）と権限昇格（Privilege Escalation）の二つのタクティクスに掲載されています。

MITRE　ATT&CKではテクニックごとに、対応プラットフォーム（例：Windows、Linux）、悪用に必要な権限レベル、検知に利用できるデータソース（例：ログ）、さらにアプリケーション攻撃パターン集CAPECとの関連情報を整理して提示しています。



タクティクスは攻撃者の「目的（何をするか）」を示し、テクニックはその目的を達成するために攻撃者が考案した「具体的な手段（どのように）」を示します。

例

MITRE ATT&CKでは、テクニックごとに以下のような既知の実例を提示しています。

- グループ（ATT&CK 固有用語）によって1件以上の攻撃で使用された事例
- ソフトウェア（ATT&CK 固有用語）によって実装された事例

MITRE ATT&CK：グループ

https://attack.mitre.org/groups/

MITRE は「グループ」を、セキュリティ業界で共通の名称によって追跡される関連侵入活動の集合と定義しています。

MITRE ATT&CK：ソフトウェア

https://attack.mitre.org/software/

MITREは「ソフトウェア」を、ATT&CKにモデル化された挙動を実行するカスタム／商用コード、OS ユーティリティ、オープンソース・ソフトウェアなどの総称と定義しています。

各実例には参考文献が添えられています。多くの場合、サイバーセキュリティ・コミュニティのさまざまなアナリストチームによるブログ投稿や脅威アラートです。これらの例は、単にテクニックをMITRE ATT&CKに収録する根拠となるだけでなく、攻撃者がどのように行動し、複数のテクニックやタクティクスを大規模なキャンペーンでどのように組み合わせるかを学ぶ手がかりとして、セキュリティ専門家に大きな価値を提供します。

緩和策

MITRE ATT&CKはテクニックごとに、防御側が講じ得る予防策（緩和策）を可能な限り提示しています。もっとも、あるテクニックについては実用的な緩和策が存在しない場合もあり、その点もMITRE ATT&CKでは率直に示されています。たとえば T1055: Process Injection の緩和セクションでは、次のように説明されています。

「この種の攻撃テクニックはOSの設計機能を悪用しているため、予防的コントロールだけで容易に緩和することはできない。特定のWindows APIの呼び出しを遮断すると、正規ソフトウェア（セキュリティ製品など）が正常に動作しなくなるなどの副作用が生じる恐れがある。そのため、防御の重点は攻撃チェーンの前段階で攻撃者ツールの実行を阻止すること、そして後続の悪意ある挙動を特定することに置くべきである。」

検知

攻撃者によるテクニックの行使を阻止することは極めて重要です。同時に、検知対策を備えることも不可欠です。その理由は次のとおりです。

1. 多層防御の考え方では、単一の対策に依存せず層状に防御を重ねる必要がある（“卵を一つのカゴに盛るな”の原則）。
2. 前述のとおり、すべてのテクニックを事前に封じることは不可能だからです。そのためMITRE ATT&CKは、利用可能なログや各種セキュリティ分析データを活用して、攻撃者のテクニック使用を検知する方法について、詳細なガイドラインを提供しています。

MITRE ATT&CKの継続的アップデート

攻撃者と防御側は常に互いの動きに対応し合うため、今日有効な手法が明日も通用するとは限りません。MITREはコミュニティと連携し、変化し続けるサイバー脅威の状況に合わせてATT&CKを継続的に更新しています。たとえば最近は、新しいタクティクス“Impact（影響）”が追加されました。これはNot Petyaに代表される破壊的攻撃の急増を受けて導入されたもので、TA0040: Impactには14種類のテクニックが含まれています。いずれもシステム・サービス・ネットワークの可用性や完全性を直接損なうこと（業務やオペレーションに影響を与えるデータ改ざんなど）を主目的としています。

MITRE ATT&CKの活用

MITRE ATT&CKは非常に汎用性の高いフレームワークで、サイバーセキュリティ・コミュニティにおけるあらゆる役割で活用できます。レッドチームはMITRE ATT&CKを用いることで、実際の攻撃者の手法をより忠実に模倣し、演習の効果を高められます。ブルーチームにとっては、攻撃者を簡潔かつ包括的に理解し、現行のコントロールや防御活動を評価してギャップを特定する枠組みを提供します。またMITRE ATT&CKは、ベンダー製品の脅威カバレッジを標準化された方法で比較する手段ももたらします。本書では、MITRE ATT&CKの「検知ユースケース」、とりわけSIEMテクノロジーでの活用に焦点を当てて解説します。

ギャップ分析

脅威は無数に存在し、ネットワーク全体のあらゆる攻撃テクニックに対して検知対策を常に最新の状態に保てる組織はありません。そこで重要になるのが、継続的な優先順位付けです。では、どこから手を付けるべきでしょうか。どのタクティクスの監視が最も手薄なのか、どれが自組織にとって最大のリスクなのか。今ある情報とツールで検知できるテクニックは何で、まず優先すべきはどれか。実用的な予防策がなく、検知がより重要となるテクニックはどれか。MITRE ATT&CKは、こうした疑問に体系的かつ最新の方法で答えを導く手段を提供します。

強化

組織がより強力な検知を必要とするタクティクスやテクニックを特定したら、MITRE ATT&CKが提供する技術的詳細を活用して、自動監視ルールを構築したり、脅威ハンティングの土台を整備したりできます。

自社環境でのテスト

いかなる技術や対策も、それだけで有効だと決めつけるべきではありません。可能な限り実環境に近い挙動でテストを行い、すべての対策を検証する必要があります。検知対策をMITRE ATT&CKのテクニックにマッピングしたうえで、それらのテクニックを自社環境で実行し、SIEMや関連セキュリティ製品が想定どおりに検知・アラート・対応するかを確認しましょう。

参考リソース

MITREをはじめとするサイバーセキュリティ・コミュニティは、ATT&CKを活用する多様なツールを提供しています。MITRE ATT&CKナレッジベース自体には、以下のサイトからアクセスできます。

- MITRE ATT&CK公式サイト
- ATT&CK Navigatorウェブアプリ

  このアプリを使うと、より動的かつ強力な方法でMITRE ATT&CKのコンテンツを閲覧できます。静的なattack.mitre.orgのWebサイトとは異なり、MITRE ATT&CK NavigatorのGitHubリポジトリでは次のように説明されています。「Navigatorの主機能はlayersを定義できる点です。layersとはATT&CKナレッジベースのカスタムビューであり、例として特定プラットフォームのテクニックだけを表示したり、ある特定の攻撃者が用いると知られるテクニックを強調表示したりできます。layers はNavigatorの画面上で対話的に作成することも、プログラムで生成してNavigator上で可視化することも可能です。」

- プログラムから自動化に利用できるATT&CKの機械可読フォーマット
  - TAXII Server：TAXII™（Trusted Automated Exchange of Intelligence Information）は、サイバー脅威情報をシンプルかつスケーラブルに共有するアプリケーション層プロトコルです。
  - STIX：STIX™（Structured Threat Information Expression）は、サイバー脅威インテリジェンス（CTI）の交換に用いられる言語およびシリアライズ形式で、MITRE ATT&CKもSTIX 2.0形式で公開されています。

5つの代表的テクニックによる脅威検知とハンティング

Outcomes Navigator はNew-Scale Security Operations Platformに搭載された機能で、ライセンス内容を基にMITRE ATT&CKフレームワークと照合したカバレッジの強度をセキュリティチームへインタラクティブに提示します。ユーザーは現在スコアリングされているカバレッジ（カスタム／既成ダッシュボード、カスタム／ネイティブのレポートルールを含む）を製品が提供する想定カバレッジと比較でき、現状と目標セキュリティ水準のギャップを把握できます。

Outcomes Navigatorではユースケースを侵害された内部者・悪意ある内部者・外部脅威の三つに大別しています。

本ガイドでは、次の観点で各テクニックを詳しく取り上げます。

- 各テクニックを掘り下げ、攻撃者の利用方法と検知方法を解説
- 収集すべきログと、ログ内で注視すべき指標を提示
- Atomic Red Teamに用意されている関連テストを紹介し、検知ルールの検証に活用。さらに、Exabeamがこれらのテクニックに対する検知ルールをLogRhythm SIEMに実装している事例を示します（いくつかのルールはMicrosoft Sysmonに依存）

MITRE ATT&CKクライアント

コミュニティではTAXIIやSTIXを利用して、MITRE ATT&CKを照会できるツールが公開されています。

- PoSh_ATTCK
- ATTACK-Python-Client
- DIY (Python with Python-Stix2 library)

前節まででMITRE ATT&CKの構造と関連ツール・リソースを説明しました。本節では、MITRE ATT&CKを脅威ハンティングと脅威検知に実際に活用する具体的な方法に焦点を当てます。

本ガイドで重点的に扱うテクニックは、次の5つです。
T1036.003：マスカレーディング（システムユーティリティのリネーム）
T1090.001：インターナルプロキシ
T1048：代替プロトコル経由の情報持ち出し
T1189：ドライブバイ攻撃
T1569.002：サービス実行

次の理由から、MITRE ATT&CKテクニックを5つに絞りました。

・攻撃での使用頻度が高い
・検知ルールで扱いやすい
・必要なログ／データソースを、すでに多くの組織が収集している

マスカレーディング：システムユーティリティのリネーム（T1036.003）

攻撃者は、防御回避（TA0005）タクティクスの一環としてマスカレーディングを利用します。MITRE ATT&CKは防御回避を次のように定義しています。
「防御回避とは、検知を逃れたり他の防御策を回避したりするために攻撃者が用いるテクニック群である。これらには、別カテゴリのテクニックをそのまま、あるいは変形して流用し、特定の防御／緩和策を無効化するものも含まれる。防御回避は、攻撃オペレーションのすべてのフェーズに適用され得る攻撃者側の属性集合と見なせる。」

「Living-off-the-Land（環境寄生型）攻撃」が広まるなかでも、攻撃者は依然として独自の悪意ある実行ファイルを用いており、それらを隠蔽することの重要性をよく理解しています。隠蔽の対象は、ファイルシステム上の保存場所だけでなく、ログやプロセス一覧にどのように現れるかも含まれます。MITRE ATT&CKでは、マスカレーディングを次のように定義しています。
「実行ファイル（正規・悪意いずれも）の名称や配置を操作・悪用し、防御や監視を回避する行為である。これには複数のバリエーションが確認されている。」

MITRE ATT&CKには複数のマスカレーディング手法が記載されていますが、代表的なのが「Windows LSASSプロセス偽装」です。具体的には、cmd.exeをC:\Windows\System32\tempにコピーしてlsass.exeにリネームし、任意のコマンドやプログラムを実行します。ログやプロセス一覧ではC:\Windows\System32\temp\lsass.exe が表示され、正規のC:\Windows\System32\lsass.exeと酷似しているため、Local Security Authority Subsystem Service（LSASS）として信頼されやすくなります。

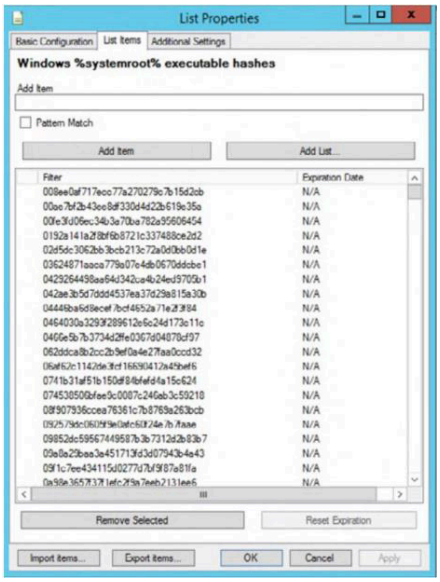


図1. Exabeam へのハッシュリスト取り込み

Exabeamでは、この偽装を検知するために次の手順をとります。まずPowerShellを使い、システムルート配下の実行ファイルすべてのハッシュ一覧を作成します。

```
get-childitem c:\windows\system32 -recurse|
where {$_. extension -eq '.exe'}|Get-
FileHash -Algorithm md5|select hash|Out-File
'.\hashes.txt'
```

そのファイル（hashes.txt）をExabeamにリストとして取り込みます。続いてAI Engine ルールが Microsoft Sysmon の Event ID 1（Process Creation）を監視し、

・実行ファイルのハッシュがそのリストに含まれている
・にもかかわらずファイルのパスがシステムルート外にある

という条件を満たすプロセスを検出します。なお、Windowsの実行ファイルにパッチが適用されればハッシュ値が変わるため、このハッシュリストは随時更新する必要があります。

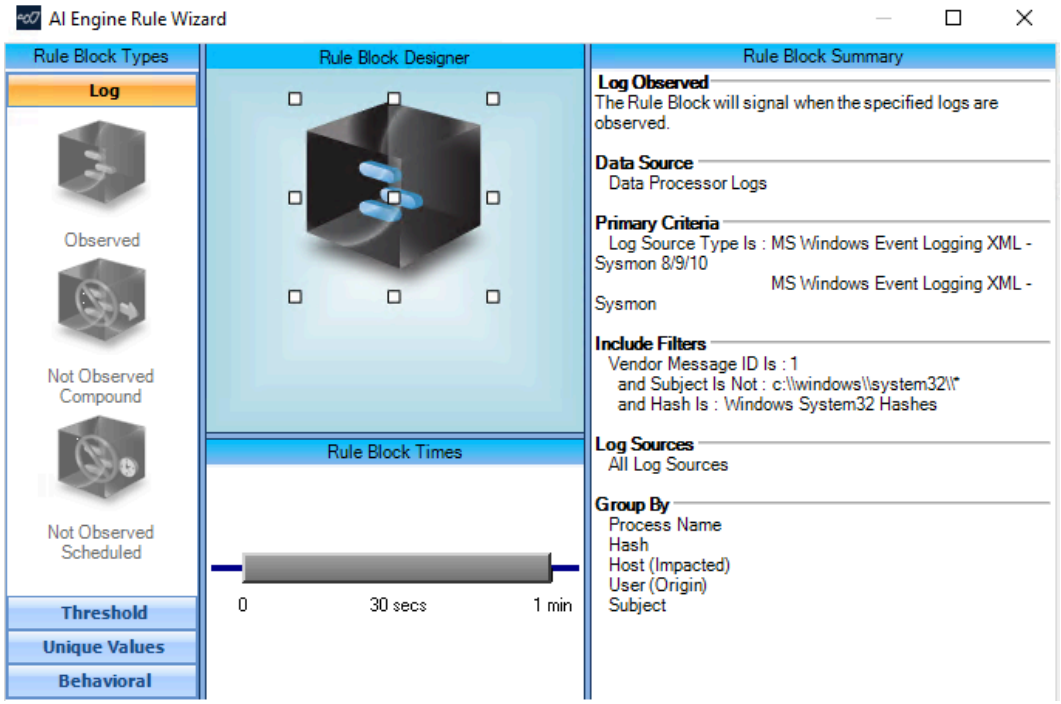


図2. AI EngineはMicrosoft SysmonのEvent ID 1（Process Creation）を監視します。

インターナルプロキシ（T1090.001）

次に紹介するテクニックは、コマンド＆コントロール（Command and Control／TA0011）タクティクス を遂行しやすくするために攻撃者が用います。TA0011は、攻撃者が標的ネットワーク内で支配下に置いたシステムとどのように通信するかを示すものです。ネットワーク構成やトポロジー、秘匿性の要件によってコマンド＆コントロールを確立する方法は多岐にわたり、MITRE ATT&CKではその差異を説明するために代表的な要素のみを抽出しています。しかし実際には、正規プロトコルやネットワークサービスを流用して新たなプロトコルを定義できるため、文書化されている以上に多くの具体的テクニックが存在します。

Internal Proxy とは「システム間のトラフィックを転送したり、ネットワーク通信の仲介役として機能する仕組み」です。トラフィックをプロキシやポートリダイレクトで迂回させるツールとしてHTRAN、ZXProxy、ZXPortMapなどが知られています。

MITRE ATT&CKは内部プロキシを検知する方法として、「通常ネットワーク通信を行わない、あるいはこれまで観測されたことのないプロセスが通信している場合は疑わしい」と推奨しています。また、通常はユーザー操作を必要とするプロセスから、ユーザー操作と無関係に発生したネットワークアクティビティも不審であるとしています。

ネットワークデータを解析し、通常とは異なるデータフロー（例：クライアントがサーバーから受信する量を大きく上回るデータを送信している場合や、本来通信しない／ほとんど通信しないクライアント同士が大量に通信している場合など）を特定します。また、普段ネットワーク通信を行わない、あるいはこれまで観測されたことのないプロセスが通信している場合は疑わしいと判断します。さらに、使用ポートで 期待されるプロトコル挙動 に合致しない通信を検出できるよう、パケット内容を詳細に解析します。

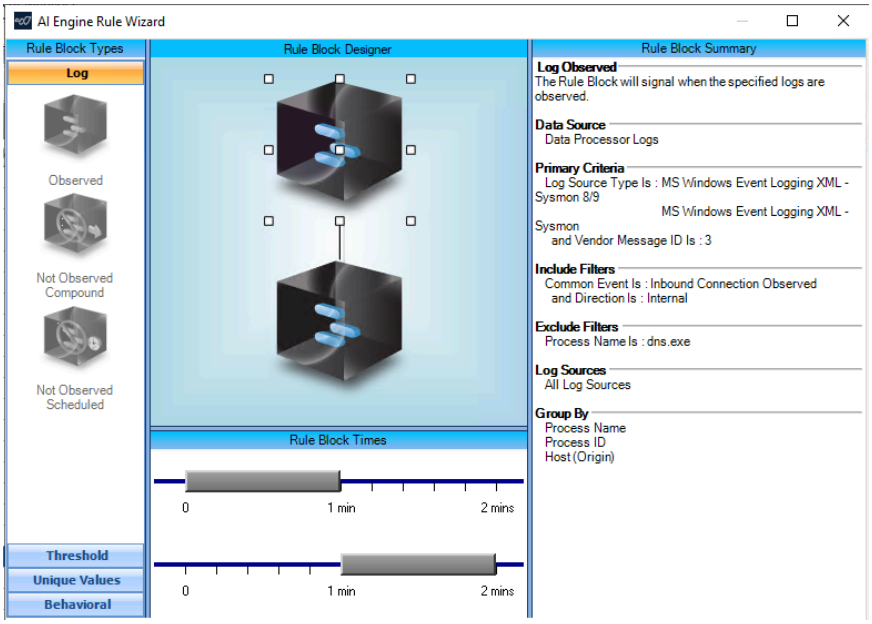


図3. AI Engineルールは HTRANなどの接続プロキシ・ツールを検知

Exabeamは、Microsoft SysmonのEvent ID 3（Network Connection）に記録される接続情報を利用し、HTRANなどの接続プロキシツールを検知するルールを開発しました。このルールは、同一プロセスが内部で接続を受信した直後に外向き接続を開始するパターンを検出します。なお、SIEMが通信の内向き／外向き（方向性）を正確に判断できるよう、エンティティ構造を適切に設定しておくことが前提となります。

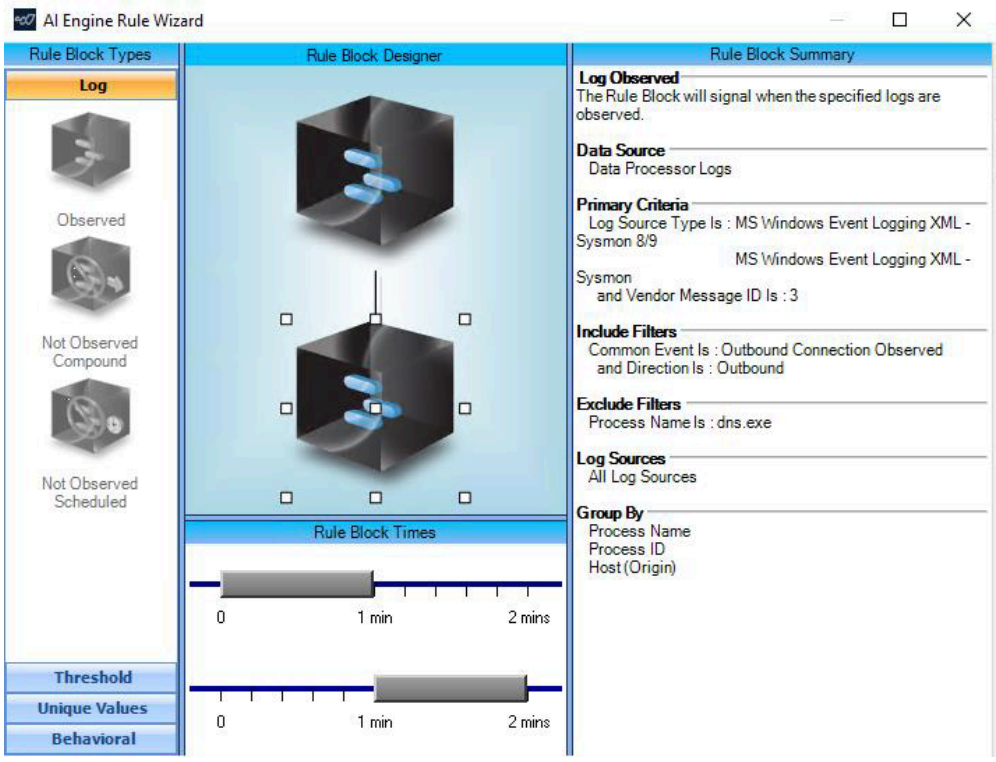


図4. Connection Proxyテクニックを検出するルールのBlock 2

代替プロトコル経由の情報持ち出し（T1048）

攻撃者が目的の情報を入手したら、気付かれずに被害ネットワーク外へ搬出する必要があります。これは Exfiltration t アクティクス（TA0010）の一部であり、代表的なテクニックがExfiltration Over Alternative Protocolです。

「本来のC2（コマンド＆コントロール）チャネルとは異なるプロトコルを使ってデータを流出させる。データはC2サーバーとは別のネットワーク地点に送られることが多い。代替プロトコルにはFTP、SMTP、HTTP/HTTPS、DNSなどが含まれ、チャネルとしてはクラウドストレージなどのインターネットWeb サービスも利用され得る。」

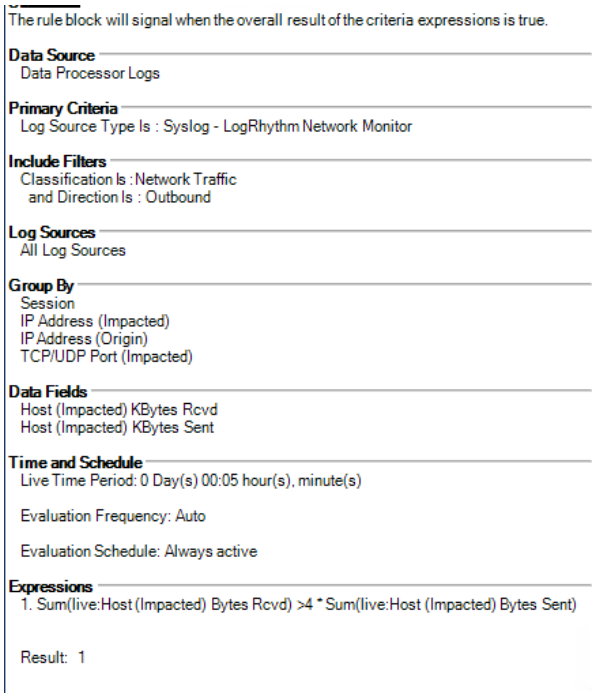


図5.AI Engine ルール「代替プロトコル経由の情報持ち出し（T1048）」を検知

検知にあたってMITRE ATT&CKは、「通常とは異なるデータフロー（例：クライアントがサーバーから受信する量よりはるかに多く送信している）をネットワークデータから解析すること」を推奨しています。

Red CanaryのAtomic Red Teamには、Exfiltration Over Alternative Protocol-SSHなど複数の検証テストが用意されており、大容量のtarballを指定ドメインへ送出する挙動を再現できます。Exabeamはトレンドルールを用いてこのテクニックを検知します。

まずNetMonのデータを観測し、多くのネットワークアプリケーション（HTTP、FTP、SMTP など）は通常、受信量>送信量となるベースラインを学習します。次に、送信量が受信量を上回った場合にルールを発火させ、アラートを生成します。

1	Application	Host (Impacted) KBytes Rcvd	Host (Impacted) KBytes Sent	Outbound percent of Inbound
188	stickyads	3.651367188	9.385742188	39%
189	stun	122.6367188	112.5019531	109%
190	symantec	2.853515625	6.615234375	43%
191	t_mobile_app	4.754882813	306.4355469	2%
192	taboola	30.06835938	13.54296875	222%
193	tcp	539.9072266	3697.595703	15%
194	teads	6.299804688	21.07910156	30%
195	teamviewer	1.93359375	2.16796875	89%
196	telegram	2.594726563	2.05859375	126%
197	tidaltv	13.5	6.525390625	207%
198	truste	18.41210938	81.93261719	22%

図6.ネットワークアプリケーション別：送信量と受信量の比較分析

ドライブバイ攻撃（T1189）

攻撃者が永続化を確立し、横移動を行い、情報を窃取する前には、まず Initial Access（TA0001）を獲得する必要があります。Initial Accessは、攻撃者がネットワークに最初の足場を築くために利用する侵入経路（ベクトル）を示すタクティクスであり、その手段は多岐にわたります。その一例がDrive-By Compromise（ドライブバイ攻撃）です。これは「ユーザーが通常のブラウジングで Webサイトを閲覧した際、攻撃者がブラウザーを悪用してシステムへアクセスを得る手法」を指します。

MITRE ATT&CKの検知ガイダンスでは、次のように述べられています。
「正規サイト経由のドライブバイ型エクスプロイトのみで侵害を検知するのは難しい。ブラウザープロセスの異常動作、不審なファイルの書き込み、実行隠蔽を狙ったProcess Injectionの痕跡、Discovery活動の痕跡、追加ツール転送を示唆する異常なネットワーク通信など、エンドポイントの挙動を併せて監視すべきである。」

Exabeamは、このテクニックに対して次のようなルールを実装しています。

- IDSやAVログでマルウェアを検知するとトリガー。
- 同一タイムライン上でブラウザープロセスが、%temp%フォルダーにファイルを書き込んでいるイベントを相関。
- 上記の手順によって、ドライブバイ侵入後の後続活動をコンテキスト付きで可視化します。

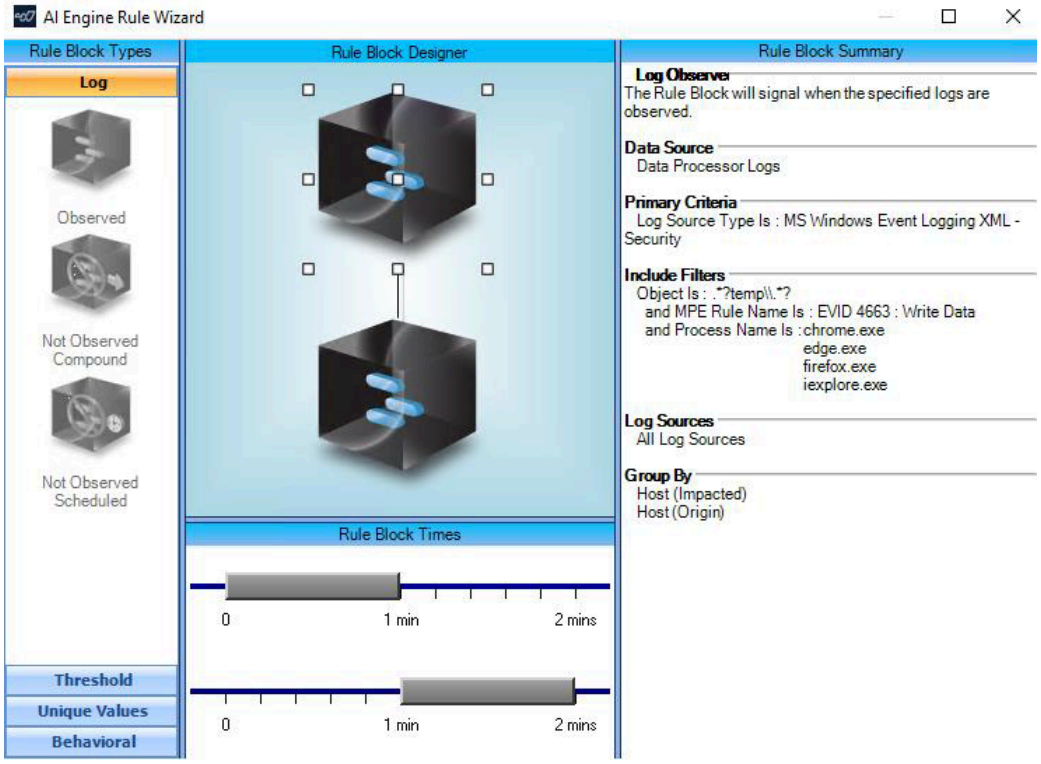


図 7：AI Engine ルール（Rule Block 1）— Drive-By Compromise テクニックの検

サービス実行（T1569.002）

ほとんどの攻撃では初期段階で Execution（TA0002）を実行する必要があります。このタクティクスは、攻撃者が制御するコードをローカルまたはリモートのシステムで実行させるテクニック群を指します。通常、初期アクセスで侵入した後にコードを実行する手段として、また横移動によってネットワーク上のリモートシステムへのアクセスを拡大する際にも用いられます。

「サービス実行（Service Execution）」は、攻撃者がWindowsのService Control Managerを利用して自身のコードを実行する一般的なテクニックです。攻撃者はService Control ManagerなどWindowsサービスと連携する方法を通じて、バイナリ、コマンド、スクリプトを実行することがある。これは新しいサービスの作成（New Service）や既存サービスの変更（Modify Existing Service）によって実現でき、サービスを利用した永続化や権限昇格の一環として用いられる。

検知の観点では、MITRE ATT&CKは次のように示しています。
サービス関連のレジストリ値の変更や、サービスを変更できるツールのコマンドライン実行が既知のソフトウェアやパッチサイクルと一致しない場合は不審と見なすべきです。バイナリやスクリプトの一時実行のみに使われたサービスは永続化を目的としていないため、サービス再起動後に元の状態へ戻されるのが通常です（たとえば管理者ツール PsExecを使用した場合など）。

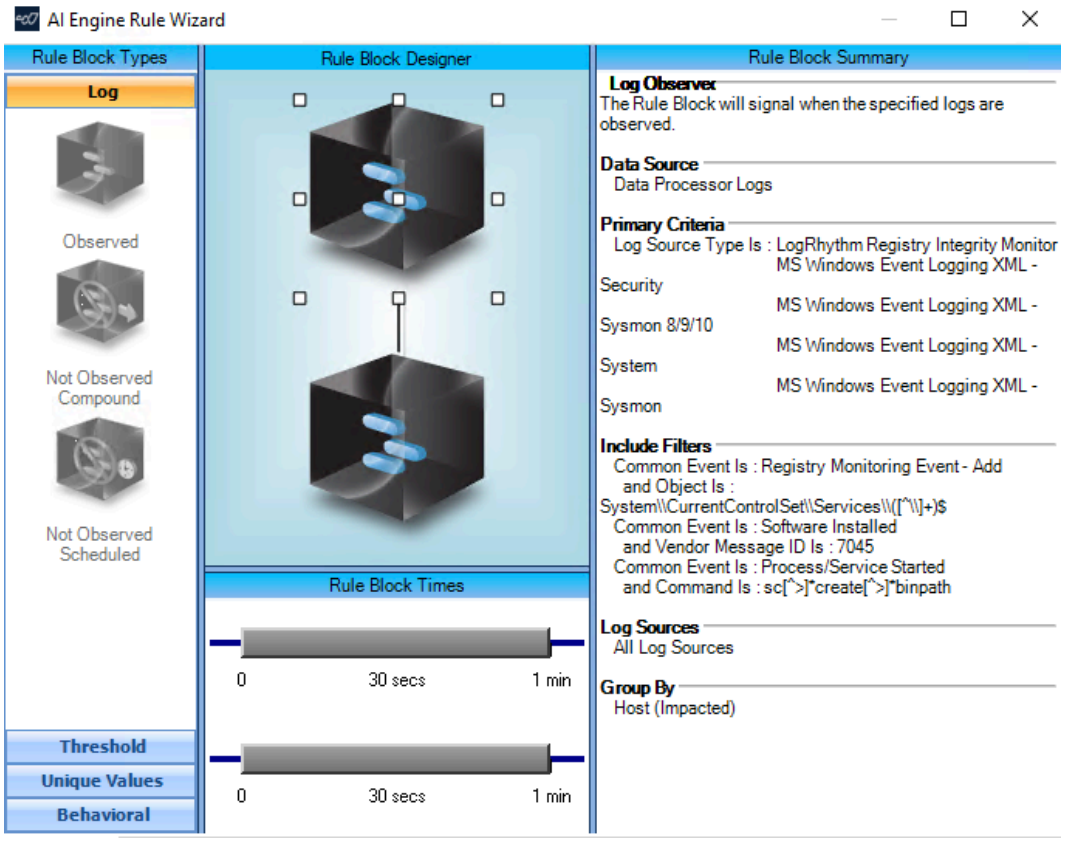


図 8：AI Engineルール（ブロック1）— Service Executionテクニックの検知

Atomic Red Teamには、本テクニックを検証するテスト「Execute a Command as a Service」が用意されています。

サービスが定義されているレジストリキー（SYSTEM\CurrentControlSet\Services）に対するレジストリ監査を有効にし、イベントID 4657（レジストリ値の変更）を監視すると、このテクニックを検知できます。とくに変更対象の値名がImagePathである場合は要注意です。ID 4657は、新規サービスの作成や既存サービスの変更という根本的な操作を、手法にかかわらず捉えます。

既知サービスのホワイトリストと照合すれば、サービスの作成や起動を記録する他のイベントも有効です。たとえばSセキュリティログのイベントID 46977は「新しいサービスが作成された」ことを示します。またプロセス開始イベント4688のコマンドラインがsc startやsc createに類似していれば、scコマンドでサービスが操作された可能性があります。ただし攻撃者は、既存サービスのImagePathを直接書き換えたりWin32 APIのStartServiceを呼び出したりしてscを回避できるため、ID 4697や4688だけでは網羅的ではありません。

Exabeamはサービス実行（Service Execution）を検知するルールセットを実装しており、複数ログソースに対応する複合フィルターを活用しています。このルールでは、①レジストリ変更、②サービスを操作するコマンドライン実行、③ソフトウェアをサービスとして登録したことを示すイベントID 7045などを組み合わせ、サービスインストールを検知します。

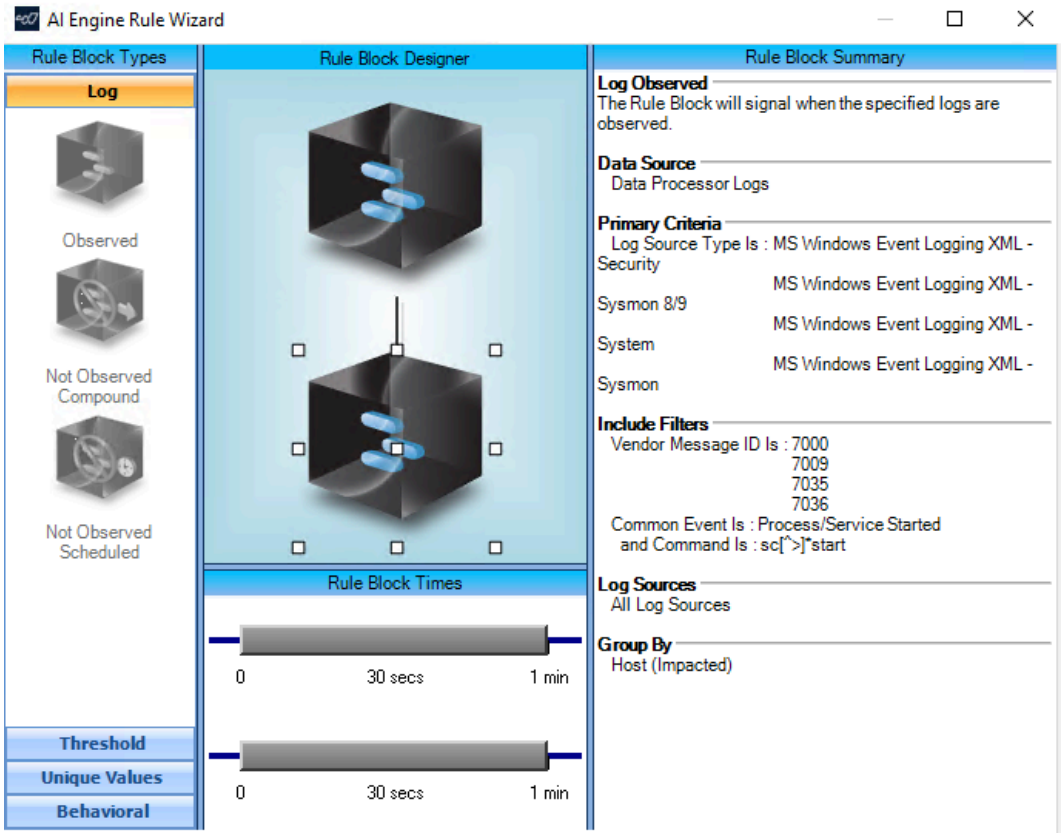


図 9：Service Executionテクニックを検知するAI Engine ルール―ルールブロック2

結論

MITRE ATT&CKは、攻撃者のテクニックを分類し、その意図を理解するうえで非常に強力なフレームワークです。活用方法は多岐にわたり、サイバーセキュリティ強化に大きく貢献します。

本書では、MITRE ATT&CKを用いて脅威検知を「分析（Assess）・強化（Enhance）・テスト（Test）」する手法に焦点を当てました。Exabeamは、クラウドネイティブ版とオンプレミス版の両SIEMにMITRE ATT&CKを組み込み、包括的・最新・検証可能な脅威検知を実現し続けています。

Exabeamについて

ExabeamはAIドリブンのセキュリティオペレーションを提供するグローバルリーダーです。高整合性のデータ取り込み、強力な分析エンジン、ワークフロー自動化により、オンプレミス／クラウドネイティブ双方で業界最高水準の脅威検知・調査・対応（TDIR）プラットフォームを実現しています。SIEMとUEBA分野での実績、AIを核とした技術基盤を通じて、世界中のセキュリティチームがサイバー脅威と戦い、リスクを軽減し、運用を最適化できるよう支援します。

exabeam

Learn more at www.exabeam.com →