

Hardening Designers Conference 2025 Day2 Tech Showcase

生成AIを活用したセキュリティ運用の効率化

2025年7月11日

NEC サイバーセキュリティ技術統括部
リスクハンティング・アナリシスグループ

背景・課題、生成AIを使用する目的

NECが実施するインシデント対応 ファストフォレンジック

早急な原因究明、侵入経路や不正な挙動を把握するため、
必要最低限のデータを抽出及びコピーし、解析すること

デジタル・フォレンジック研究会 「証拠保全ガイドライン 第9版」
<https://digitalforensic.jp/wp-content/uploads/2023/02/shokohoznGL9.pdf>

課題

- チームメンバー間でスキルやノウハウに差が生じやすい
 - ・ 膨大なログの調査には経験・勘所などが必要になる
- 調査対象OSや調査対象製品でログの形式が異なるため網羅的に分析手法を把握する必要がある
- レポート作成に時間がかかる
- 新メンバー向けの育成支援を効率よくすすめたい

生成AIで課題を解決

能力・品質の底上げ、効率化を目指す

インシデント対応の効率化

- ・ 調査の起点のサポート

新人の自走をサポート

AI機能があるセキュリティ製品

- ・ Microsoft security Copilot
- ・ Sentienl × Azure OpenAI × Logic Apps
- ・ Splunk AI Assistant for SPL
- ・ Elastic AI Assistant

Elastic AI Assistant

生成AIを活用して

アラート調査、インシデント対応、クエリ生成、自然言語による
会話など、Elastic Securityでの調査を強化

例えば、主に次のようなユースケースでの利用を想定

アラートの トリアージ

アラートに関する
解釈の支援

脅威の 特定、調査、文書化

脅威の特定や分析、
レポートの生成の支援

ES|QLクエリの 生成

Elasticsearchクエリ言語
(ES|QL)のカスタマイズの支援

Etc...

※ Elastic AI Assistant機能を利用する場合、
Enterprise subscriptionが必要

AI Assistant

<https://www.elastic.co/docs/solutions/security/ai/ai-assistant>

AI use cases

<https://www.elastic.co/docs/solutions/security/ai/use-cases>

デモ～攻撃シナリオと構成図の説明～

攻撃環境：10.3.0.10/24

ホスト名：kali
Kali



仮想スイッチ

偵察

- Recon、nmapで調査

初期アクセス

- ClientのShell取得

認証情報アクセス

- 資格情報を取得
- Adminアクセス

riht.localドメインのやられ環境：10.0.0.0/24

ホスト名：DC
Windows Server 2019

Elastic Agent

ホスト名：bazru
Windows11

Elastic Agent

ホスト名：gozaru
Windows11

Elastic Agent

仮想スイッチ

仮想ルータ用ホスト
VYOS

仮想スイッチ

ELK環境(Ubuntu)：10.2.0.1/24



Fleet Server



Elastic Search Kibana

前提 攻撃者は以下の情報を知っている

- DCとクライアントのIPアドレス
- クライアントのriht.localのbazaruの認証情報を知っている (id、password)

攻撃シナリオ

前提 攻撃者は以下の情報を知っている

- DCとクライアントのIPアドレス
- クライアントのriht.localのbazaruの認証情報（id、password）

偵察 Recon、nmapで調査

- smb（445ポート）が開いている
- C:Users¥Publicが書き込み可能なフォルダである
- Windows Defenderで除外されているフォルダが存在する

初期アクセス

impacket-psexec を使用し、
攻撃してClientのShell取得

認証情報アクセス

- Windows Defenderで除外されているフォルダにMimikatzを格納する
- Mimikatzの「sekurlsa::logonpasswords」で資格情報を取得
- Domain Admins グループに所属確認後、取得したNTLMハッシュを利用して impacket-psexec を実行でAdminアクセス
- Mimikatzで「**event::clear**」を実行してイベントログを削除

Elastic AI Assistantを用いた解析 ～ Attack Discovery ～

機能：Attack Discovery

複数のアラートから重大度の高い攻撃を絞りこんで攻撃の概要を回答してくれる

 Assistant at: 2025/7/6 23:17:31

概要

悪意のあるファイル {{ file.name wJBNGIc.exe twlUPNyK.exe mimikatz.exe }} が win-b180dba9iuJ 上で実行されました。

詳細

攻撃は、win-b180dba9iuJ 上で wJBNGIc.exe が実行されたことから始まりました。このファイルは C:\Windows\wJBNGIc.exe に配置され、services.exe によって実行されました。その直後、別のファイル twlUPNyK.exe が同じホスト上に導入され、実行されました。このファイルは C:\Windows\twlUPNyK.exe に配置され、同じく services.exe によって実行されました。両ファイルとも有効なコード署名を持たず、悪意のある意図が疑われます。

その後、認証情報窃取ツールである mimikatz.exe が同じホスト上で実行されました。このファイルは C:\Users\Public\mimikatz.exe に配置され、powershell.exe を使用して実行されました。コマンド {{ process.command_line "C:\Users\Public\mimikatz.exe" privilege::debug sekurlsa::logonpasswords exit }} は、認証情報の収集を試みていることを示しています。親プロセスである powershell.exe は cmd.exe によって起動されており、信頼されたツールを利用して検出を回避する段階的な攻撃が行われたことが示唆されます。

mimikatz.exe は {{ process.code_signature.subject_name Open Source Developer, Benjamin Delpy }} によって署名されていますが、その使用方法是認証情報窃取の戦術と一致しています。この一連のイベントは、持続性の確立、悪意のあるペイロードの実行、システム上での認証情報の収集を試みたことを示唆しています。

攻撃チェーン

- 実行
- 持続性
- 認証情報アクセス



メリット

- 一連の流れをつかみやすい
- アラートの中身も質問することで一部回答を返してくれる場合がある

デメリット

- アラートとして含まれていないプロセスや通信は回答文にない
- 抽象度が高い内容のため、具体的な挙動や深堀には現時点では不十分である
 - 偵察などの内容は記載されていない

Elastic AI Assistantを用いた解析 ~脅威の特定・調査~

アラートの詳細な内訳

1. 攻撃の概要

- 攻撃の種類: 多段階攻撃 (Multi-Stage Attack)
- 影響を受けたホスト: win-bl80dba9iuj
- 確認された悪意のあるファイル:
 - wJBNGIcZ.exe (services.exe によって実行)
 - twlUPNyK.exe (services.exe によって実行)
 - mimikatz.exe (cmd.exe を介して powershell.exe によって実行)
- 攻撃チェーンの段階:
 - 実行 (Execution)
 - 永続性 (Persistence)
 - 認証情報アクセス (Credential Access)

2. 主な観察点

- 署名のないファイル: wJBNGIcZ.exe と twlUPNyK.exe はどちらも有効なコード署名を持たず、悪意のある可能性が高い。
- 認証情報窃取ツール: mimikatz.exe が以下のコマンドで認証情報を収集するために使用された:

```
"C:\Users\Public\mimikatz.exe" privilege::debug sekurlsa::logonpasswords exit
```

これにより、平文パスワード、NTLMハッシュ、その他の認証データが抽出された可能性がある。

- 実行経路: 信頼されたシステムプロセス (services.exe 、 cmd.exe 、 powershell.exe) を利用して悪意のあるペイロードを実行することで、検出を回避する一般的な手法が使用されている。
- コード署名: mimikatz.exe は「Open Source Developer, Benjamin Delpy」によって署名されているが、その使用方法は悪意のある意図と一致している。

3. 潜在的な影響

- 認証情報の漏洩: Mimikatz の使用により、管理者アカウントを含む機密性の高い認証情報が攻撃者に取得されている可能性がある。
- 永続性と横展開: 複数の悪意のあるファイルが実行されていることから、永続性の確立やネットワーク内での横展開を試みている可能性がある。
- データの流出やさらなる攻撃: 認証情報を取得した攻撃者が、機密性の高いシステムにアクセスしたり、追加のペイロードを展開したりする可能性がある。

インターネットによる調査ではなく、
生成AIから情報を得ることができる

被害の概要

1. 資格情報の抽出:

- sekurlsa::logonpasswords コマンドが実行され、システムのメモリから平文のパスワード、NTLM ハッシュ、Kerberos チケットなどの認証情報が抽出されました。
- 抽出された情報は、攻撃者が横方向移動 (Lateral Movement) や権限昇格 (Privilege Escalation) を行うために使用される可能性があります。

2. 関連するプロセスとファイル:

- ファイル名: mimikatz.exe
- コマンドライン: "C:\Users\Public\mimikatz.exe" privilege::debug sekurlsa::logonpasswords exit
- 親プロセス: powershell.exe (信頼されたコード署名付き)
- 実行権限: システムレベルの権限 (高い特権)

3. その他のマルウェア活動:

- 不審なファイル名
 - 不審なファイルがどのように使われているか回答してくれる
- 不審なコマンド
 - コマンドの意図を回答
- 不審なツール
 - ツールの概要や目的なども回答

Mimikatz とは

- 目的: Mimikatz は、Windows 環境で資格情報 (パスワード、ハッシュ、PIN など) を抽出するために設計されたツールです。
- 使用例:
 - メモリから平文のパスワードを抽出。
 - Kerberos チケット (Golden Ticket や Silver Ticket) の生成。
 - 権限昇格や認証情報の盗難。
- 正当性: Mimikatz は合法的なセキュリティツールとして開発されましたが、攻撃者によって悪用されることが多いです。

Elastic AI Assistantを用いた解析 ～脅威の特定・調査～

提供された情報から、攻撃者が横展開（Lateral Movement）を試みた可能性は高いですが、現時点ではその具体的な証拠は示されていません。ただし、以下の要素から横展開のリスクがあると考えられます：

1. 横展開の可能性を示唆する要素

1.1 認証情報の窃取

- `mimikatz.exe` を使用して認証情報（平文パスワード、NTLMハッシュ、Kerberosチケットなど）を収集しています。
- 攻撃者がこれらの認証情報を利用して、他のホストやシステムにアクセスする可能性があります。

1.2 多段階攻撃の性質

- 複数の悪意のあるファイル（`wjBNSicZ.exe`、`twlUPNyK.exe`、`mimikatz.exe`）が実行されており、攻撃者が永続性を確立し、次のステージ（横展開やデータ窃取など）を準備している可能性があります。

1.3 信頼されたプロセスの利用

- `services.exe` や `powershell.exe` などの信頼されたシステムプロセスを利用しているため、攻撃者が検出を回避しながら横展開を試みる可能性があります。

2. 横展開の確認方法

Elastic Securityを使用して、横展開の痕跡を確認するための具体的な手順を以下に示します：

2.1 ホスト間の通信ログを確認

- Elastic Securityの「ネットワーク」タブを使用して、影響を受けたホスト（`win-bl80da91uj`）から他のホストへの通信を確認します。
- 確認ポイント：
 - 不審なIPアドレスやポートへの通信。
 - SMB（ファイル共有）やRDP（リモートデスクトップ）プロトコルの使用。

2.2 認証ログの分析

- Elastic Securityの「ログ」タブで、認証イベント（ログオン/ログオフ）を確認します。
- 確認ポイント：
 - 影響を受けたホストから他のホストへのログオン試行。
 - 異常な時間帯や場所からのログオン。

2.3 プロセスツリーの分析

- タイムライン機能を使用して、`mimikatz.exe` の実行後に発生したプロセスやイベントを確認します。
- 確認ポイント：
 - 他のホストにアクセスするためのツール（例：`Psexec`、`wmic`、`Powershell`）の使用。
 - 不審なスクリプトやコマンドの実行。

2.4 ファイル共有の利用状況を確認

- SMBや共有フォルダを介して、悪意のあるファイルが他のホストにコピーされていないかを確認します。

複数のアラートから横展開なども調査

- 使用されたツール情報や認証情報から確認
- ただし、具体的な被害をすべて網羅することはできない。
- 影響範囲の漏れなどがある

Elastic AI Assistantを用いた解析 ~脅威の防御策の提案~

Elastic Securityを活用して、今回の多段階攻撃に対する防御策を以下の手順で実施することをお勧めします。

1. 即時対応: 攻撃の封じ込め

1.1 影響を受けたホストの隔離

- Elastic Securityの「ホストの隔離」機能を使用して、`win-bl98dba9iuq` をネットワークから隔離します。
 - 手順:
 - a. Elastic Securityの「ホスト」タブに移動。
 - b. 該当ホストを選択。
 - c. 「ホストを隔離」オプションを選択して実行。

1.2 認証情報のリセット

- 攻撃者が取得した可能性のある認証情報を無効化します。
 - 対象:
 - 管理者アカウント
 - 該当ホストで使用されていたユーザーアカウント
 - 手順:
 - a. Active DirectoryやIAMツールを使用して、該当アカウントのパスワードをリセット。
 - b. 多要素認証 (MFA) を有効化。

2. 調査: 攻撃の詳細な分析

2.1 アラートの詳細確認

- Elastic Securityのアラートタブで、`wjBNGicZ.exe`、`twlUPNyK.exe`、`mimikatz.exe` に関連するアラートを確認します。
 - 手順:
 - a. 「アラート」タブを開く。
 - b. アラートをフィルタリングして、該当するプロセスやファイルに関連する情報を確認。
 - c. アラートの「プロセスツリー」を使用して、親プロセスや関連するアクティビティを特定。

2.2 タイムラインの作成

- Elastic Securityの「タイムライン」機能を使用して、攻撃の全体像を可視化します。
 - 手順:
 - a. 「タイムライン」タブを開く。
 - b. 該当するホストやプロセスを基にイベントを追加。
 - c. 攻撃の開始点、横断跳、認証情報窃取の流れを特定。

2.3 ネットワークトラフィックの分析

- ネットワークログを確認し、外部サーバーへの通信やデータの流出がないかを調査します。
 - 手順:
 - a. Elastic Securityの「ネットワーク」タブを開く。
 - b. 該当ホストの通信履歴をフィルタリング。
 - c. 不審なIPアドレスやドメインへの通信を特定。

3. 修復: 攻撃の痕跡を除去

3.1 悪意のあるファイルの削除

- `wjBNGicZ.exe`、`twlUPNyK.exe`、`mimikatz.exe` を削除します。
 - 手順:
 - a. Elastic Agentを使用して、該当するファイルを隔離または削除。
 - b. ファイルのハッシュを確認し、他のホストに存在しないかを検索。

3.2 システムの再構築

- 攻撃を受けたホストを再構築し、クリーンな状態に戻します。
 - 手順:
 - a. 重要なデータをバックアップ。
 - b. OSを再インストール。
 - c. 最新のセキュリティパッチを適用。

4. 防御強化: 将来の攻撃を防ぐ

4.1 検出ルールの強化

- Elastic Securityでカスタム検出ルールを作成し、類似の攻撃を早期に検出します。
 - 例:
 - 未署名の実行ファイルの検出。
 - `mimikatz.exe` やそのコマンドの実行を検出。

4.2 エンドポイント保護の強化

- Elastic Agentを全ホストに展開し、リアルタイムでの脅威検出と防御を有効化します。

4.3 ユーザー教育

- フィッシング攻撃や不審なファイルの実行を防ぐため、従業員にセキュリティ教育を実施します。

5. 継続的な監視と改善

- Elastic Securityのダッシュボードを活用して、環境全体のセキュリティ状況を継続的に監視します。
- 定期的に見直しやポリシーを見直し、最新の脅威に対応できるようにします。

防御策の提案

メリット

防御推奨策の候補が一覧として出る

デメリット

本当に防御可能かは
検証や判断スキルが必要

具体的な監視設定や
監視箇所などの記載
は現状ない

Elastic AI Assistantを用いた解析

メリット

- 生成AIから情報を得ることができる
 - 一連の流れ、観察点、不審なファイルや不審な操作についての見解を素早く確認することができる
- ⇒概要の確認やアラートの初期調査には利用可能

デメリット

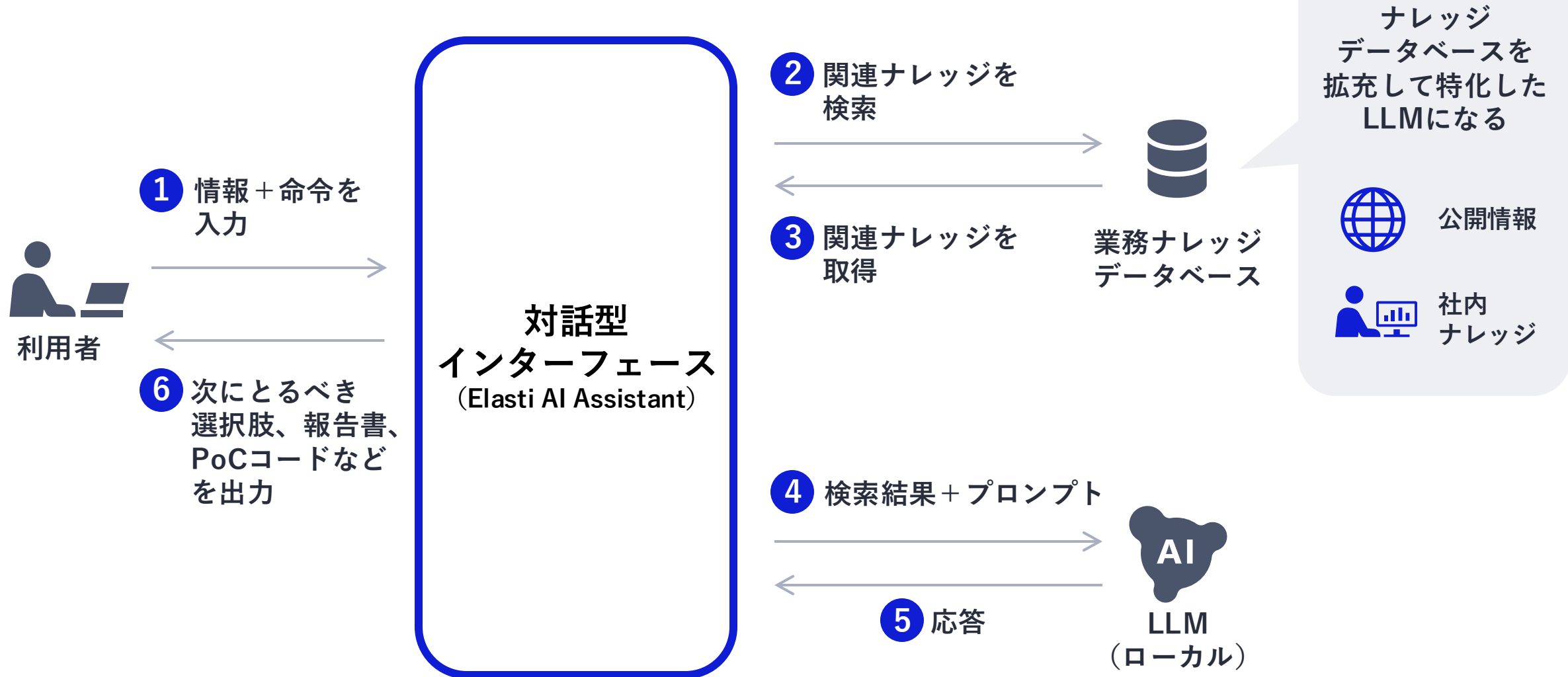
- Elasticがアラートとして含んでいない内容は回答に含まれていない
- 詳細な調査はできない。まだ人力が必要



ナレッジデータベース（RAG）などを活用することで自社のノウハウを生かした生成AIを作成し、調査することができる場合がある

ナレッジデータベース(RAG)を用いた性能向上

ナレッジデータベースを用いた性能向上をおこなう



おわりに

- 今回紹介できたAIの活用は日々のセキュリティ分析やインシデント対応の負担を軽減するツールとして、一部の業務を任すことができる可能性が高い。
まだ足りない部分があるが、大きな期待が持てると感じている。
- AIでできること、我々が目視で見ること、AIに今後してほしいことなど整理して活用できれば効率化を目指すことができる。
- さらに、
セキュリティに特化したLLMやRAG（Retrieval-Augmented Generation）を組み合わせることで、より高精度な回答が得られる可能性もある。

NEC

\Orchestrating a brighter world