継続的脅威エクスポージャー管理（CTEM）

# zcrCTEM

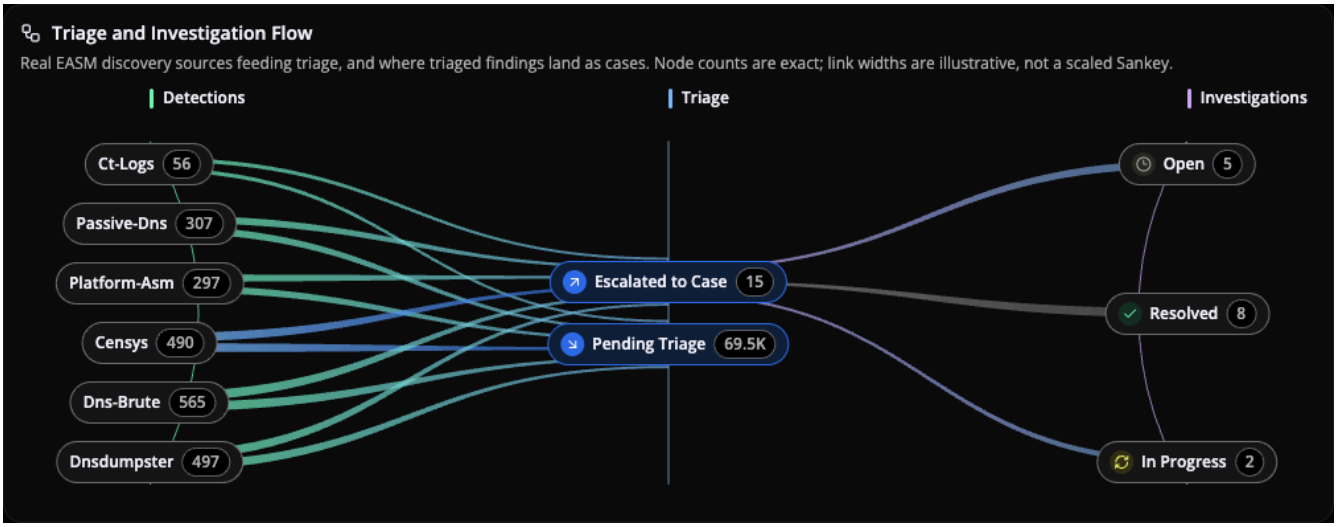
## シグナルから
## 承認済みの対応へ

外部への露出、セキュリティツールの適用漏れ、ダークウェブの検出情報を一つのコンソールに集約。人工知能（AI）が対応案を作成し、アナリストが実行の可否を判断します。

| | |
|---|---|
| **EASM** | 外部から見える攻撃対象領域を発見<br>External Attack Surface Management |
| **CAASM** | セキュリティツールの適用漏れを把握<br>Cyber Asset Attack Surface Management |
| **DRP** | ダークウェブ上の露出を追跡<br>Digital Risk Protection |

**導入モデル**・Cloud / Software as a Service（SaaS）またはオンプレミスソフトウェア。ソリューション設計で確定します。

### 発見から調査までを追跡




セキュリティ運用センター（SOC）のダッシュボード：発見ソース → トリアージ待ちまたはケースへの引き上げ → 調査ステータス。線の太さは説明用で、性能指標ではありません。 元の画面を開く ↗

公開デモの実画面・テナントと数値はサンプル・英語のUIを保持

**対象チーム**・セキュリティ運用・脆弱性管理チーム、リスク管理・サードパーティリスク担当、複数テナントを運用するマネージドセキュリティサービス事業者（MSSP）、最高情報セキュリティ責任者（CISO）

# 一つの運用の流れと、人による承認

外部スキャン、エンドポイント検出・対応（EDR）や脆弱性管理のコンソール、ダークウェブのフィード、ベンダーから回収したセキュリティ質問票は、どれも全体像の一部しか示しません。コネクタの同期が止まっていても誰も気付かず、チームはすでに古くなった情報をもとに優先順位を決め続けることになります。

運用を説明する概念的な順序であり、システム連携の構成図ではありません。

## 01 発見

シードドメインを設定し、サブドメイン、ネットワーク範囲（CIDR）、自律システム番号（ASN）で対象を包含・除外。EASMが継続的に探索し、CAASMが連携ツールから資産を集約します。資産ごとのEDR、脆弱性スキャン、クラウドポスチャーの適用状況を表示。Sync Healthはデータソースの停止を警告します。

**出力：対象資産の一覧とツールの適用漏れ**

## 02 優先順位付け

リスクスコア、EPSS（Exploit Prediction Scoring System）、自社で設定した事業上の優先度ティアで検出結果を並べ、最重要資産から対応します。

**出力：確認すべき順に並んだ検出結果**

## 03 調査

検出結果やダークウェブのシグナルから、エビデンス、信頼度スコア、EASMインベントリ内の資産との照合を確認。攻撃者の戦術・技術の知識ベースであるMITRE ATT&CKとの対応も確認できます。脅威インテリジェンスは別売りです。

**出力：影響を受ける資産に結び付いたエビデンス**

## 04 承認して実行

エージェントとAIアシスタントがチケットやテイクダウン依頼を起案。アナリストが1件ずつ承認・却下してから進めます。AIの全回答、下書き、判断は監査証跡に記録されます。

**人の判断：承認または却下 → 追跡可能な対応記録**

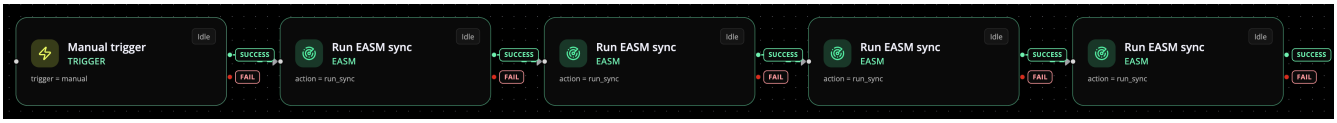
FIRSTのEPSSは、公表された脆弱性が今後30日間に悪用される確率を推定します。悪用された事実を示すものではありません。

FIRST · EPSS ↗

CIDR = Classless Inter-Domain Routing（ネットワーク範囲の表記）；ASN = Autonomous System Number（自律システム番号）。

# 実行前に対応案を確認

## 01 / エージェントワークフロー




全体表示：手動トリガー → 四つのEASM同期アクション。成功・失敗の出力と両端を保持し、ノードはIdleです。チケットやテイクダウンの実行実績を示す画面ではありません。 デモ画面を開く ↗

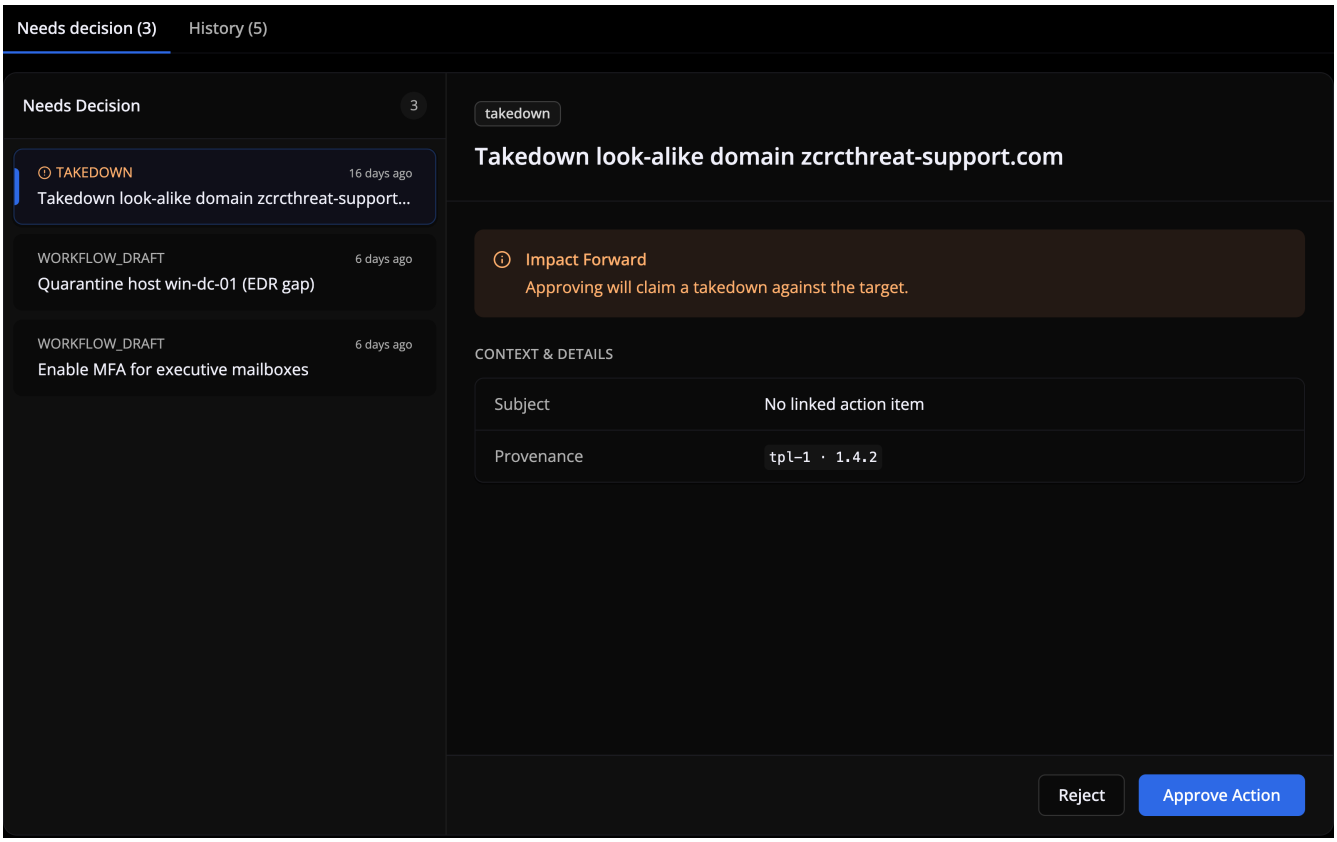
公開デモの実画面・テナントと数値はサンプル・英語のUIを保持




同じフローの開始部分を拡大。トリガーとアクション、成功・失敗の分岐を設定し、有効化または手動実行できます。この読み取り専用サンプルでは、失敗出力は未接続です。 デモ画面を開く ↗

公開デモの実画面・テナントと数値はサンプル・英語のUIを保持

## 02 / 判断待ちの提案と生成元




zcrcthreat-support.comのテイクダウン提案は判断待ち。生成元はtpl-1 / 1.4.2、SubjectはNo linked action itemです。Impact Forwardは、承認すると対象へのテイクダウンを申告すると警告。Reject / Approve Actionは操作せず、本書作成のための承認・実行は行っていません。 デモ画面を開く ↗

公開デモの実画面・テナントと数値はサンプル・英語のUIを保持

> ワークフローと監査証跡は別々のサンプル画面で、同一ケースの一連の実行を検証したものではありません。

# パートナーと導入範囲を決める

## モジュールと契約範囲

| | |
|---|---|
| EASM · CAASM · DRP | 対象資産とモジュールを承認済みパートナーと選定。デモで見える機能が購入済みの権利を示すものではありません。 |
| Threat Intelligence | 別売りで、zcrが承認したパートナーがお見積りします。有料の四つのモジュールにもバンドル割引にも含まれません。 |
| AI & Compliance | 別料金：タイの個人情報保護法（PDPA）・重要情報インフラ（CII）への対応準備、漏えい通知の下書き、AIによるコンプライアンスレポート作成支援。 |

**コンプライアンスの範囲**・適用する枠組み、エビデンス要件、ワークフローは、zcrが承認したパートナーとご確認ください。本書は認証や法令遵守を証明するものではありません。

**公開デモで確認できる範囲**・公開デモはサンプルデータで動作し、EASM、CAASM、DRP、脅威インテリジェンス、エージェントワークフロー、監査証跡を確認できます。コンプライアンスモジュールはデモに含まれないため、zcrが承認したパートナーにご相談ください。

テイクダウンの成功を保証するものではありません — 対象のホスティング事業者やレジストラの協力状況によります。

### zcrが承認したパートナーを通じて評価を依頼

シードドメイン、対象資産と事業上の優先度、使用中のツールとコネクタ、希望するSaaS／オンプレミス形態、承認責任者、必要なエビデンスを整理してください。

承認済みパートナーが、これらをもとにモジュール、オンボーディング、導入、連携、サポート、サービスレベル合意（SLA）、料金をソリューション設計と見積書で確定します。

ログイン不要のzcrCTEMデモを試す

パートナーと評価する ↗　現行プラン ↗　デモを開く ↗

一次サポートはチャネルパートナーが担当し、zcrがパートナーを支援します。