継続的な脅威露出管理

zcrCTEM

露出を可視化。
次の対応を判断。

EASMで攻撃対象領域を、CAASMでセキュリティツールの適用漏れを、DRPでダークウェブ上の露出を一つのコンソールで把握するCTEMプラットフォームです。AIの提案はアナリストが承認してから実行します。

導入形態

Cloud / SaaS

オンプレミス
ソフトウェア

EASM・CAASM・DRP・脅威インテリジェンス・テイクダウン・AIが提案し、アナリストが判断

01 **検出**

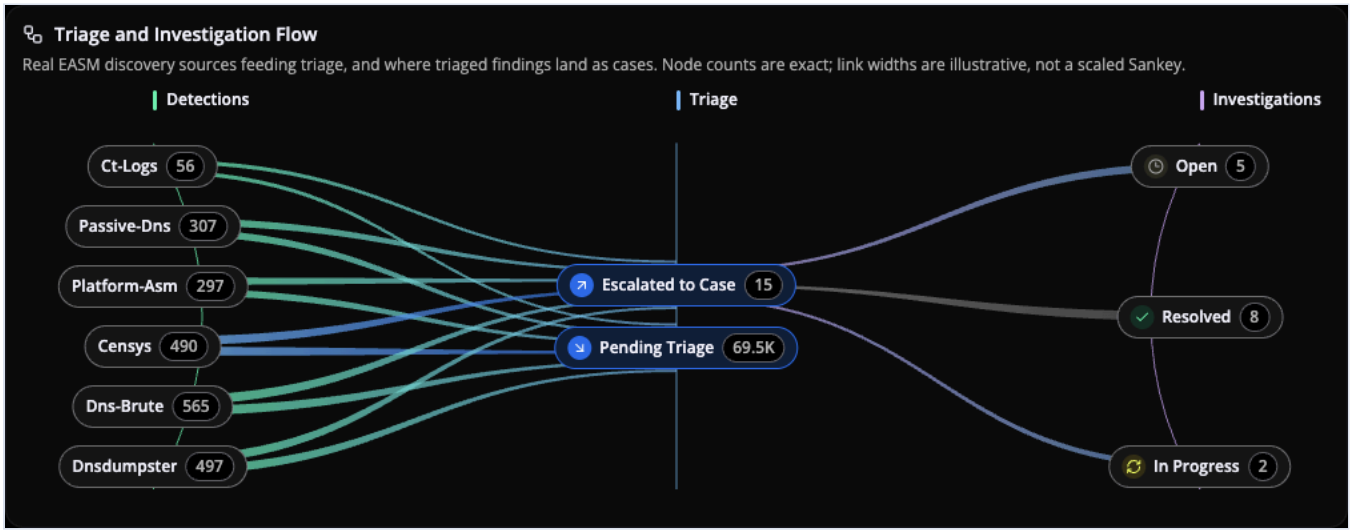
02 **優先順位付け**

03 **調査**

04 **承認して対応**

運用の流れを示す概念図であり、実際の導入構成ではありません。

Agentic SOC ダッシュボード



サンプルテナントの発見ソースから、保留中のトリアージまたはケースへのエスカレーション、調査ステータスまでを追跡できます。線の太さは説明用で、性能指標ではありません。公開デモの実際の画面です。画面上の数値はサンプルデータです。

実際の公開デモ画面です。テナントの数値や線の幅は説明用で、性能測定値ではありません。

対象範囲とモジュールをパートナーと検討

デモを確認 ↗　パートナーに相談 ↗

製品の詳細

運用ワークフロー

02

対象チーム

セキュリティ運用チーム、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MSSP、CISO

運用上の課題

外部スキャン、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。

導入モデル

Cloud / 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）

運用の流れ

発見、優先順位付け、調査の先に、人が承認する対応があります。

01 / 発見
シードドメインとスコープルールを設定すると、EASMが資産を継続的に探索し、CAASMが連携ツールから資産を集約します。データソースからの報告が途絶えると、Sync Healthが警告します。

02 / 優先順位付け
リスクスコア、EPSS、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。

03 / 調査
検出結果やダークウェブのシグナルを開き、エビデンス、信頼度、MITRE ATT&CKとの対応、該当する資産を確認します。

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し、アナリストが1件ずつ承認または却下します。判断は監査証跡に記録されます。

製品の詳細

主な機能

03

主な機能

- 発見ソースからトリアージ、ケースへのエスカレーション、調査ステータスまでを追跡するAgentic SOCダッシュボード
- シードドメインを起点としたEASMの資産発見と、サブドメイン・CIDR・ASNによる対象範囲の包含／除外ルール
- 脆弱性、証明書、公開ポートの検出結果を、リスクスコア、CVEのEPSS、マスキング済みのエビデンスとあわせて確認
- 技術的な深刻度とは別に、事業側で設定する「クラウンジュエル」などの優先度ティア
- 資産ごとにEDR、脆弱性スキャン、クラウドポスチャーの適用状況を示すCAASMインベントリと、データソースからの報告が途絶えると警告するSync Health
- ダークウェブの検出結果に信頼度スコアとMITRE ATT&CKのマッピングを付け、EASMインベントリの資産と照合する脅威インテリジェンス
- DRPのテイクダウンポリシー、インシデントのケース管理、サードパーティ向けセキュリティ質問票
- 対応案を作成するエージェントワークフローとAIアシスタント（作成内容は監査証跡に記録され、AIが提案したチケットやテイクダウンはアナリストの承認後に実行）
- 発生可能性と損失規模で整理し、年間予想損失額とエビデンスへのリンクを示すリスクシナリオ
- AI & Complianceモジュール：PDPA・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

検出結果の詳細

検出結果ごとに、リスクスコア、CVEがある場合のEPSS、検出されたポート、マスキング済みのエビデンス、調査経路を確認したうえでチケットを起票できます。公開デモの実際の画面です。画面上の数値はサンプルデータです。

元の画面を開く ↗

製品の詳細

EASM と CAASM

04

EASM

自社のルートドメインを起点に、インターネットへの露出を把握

- シードドメインを起点とした資産発見（一括インポート、サブドメイン・CIDR・ASNによる包含／除外ルール）
- 脆弱性、証明書、公開ポートの検出結果（リスクスコア、CVEのEPSS付き）
- 技術的な深刻度とは別の「クラウンジュエル」などの優先度ティアと、深刻度による自動割り当て
- シードドメインとスコープルールを誰が有効化・編集したかの変更履歴

CAASM

セキュリティツールが実際にカバーしている資産を把握

- 連携したソースのホスト、デバイス、クラウドリソースを統合した一つのインベントリ
- 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（適用済み・未適用・不明）
- 資産ごとのリスクスコアとインターネット上の安全性ステータス
- ソースの切断、不安定化、報告停止を死角として警告するSync Health

スコープ設定と資産発見

次回のEASM同期で使うシードドメイン、包含／除外ルール、発見ソースを設定できます。公開デモの実際の画面です。画面上の数値はサンプルデータです。

元の画面を開く ↗

資産インベントリ

一つのCAASMインベントリで、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、リスクスコア、優先度ティアを確認できます。公開デモの実際の画面です。画面上の数値はサンプルデータです。

元の画面を開く ↗

製品の詳細

DRP・脅威インテリジェンス

05

DRP

なりすましとサードパーティのリスクに、ポリシーに沿ったテイクダウンで対応

- 類似ドメイン、偽のモバイルアプリ、組織の情報を露出させるメッセージングチャネルを検出
- 保護対象資産のポリシーで、テイクダウンの可否、必要な承認数、ロールバックの要否を設定
- 関連する検出結果をまとめたインシデントケース（深刻度、ステータス、SLA、担当者）
- セキュリティ質問票と再利用できるテンプレートを備えたサードパーティベンダー台帳

脅威インテリジェンス

ダークウェブの検出結果が本当に自社に関係するかを判断

- 漏えいした認証情報、スティーラーログ、ランサムウェアのリークサイト投稿、流出したソースコードなどのダークウェブ検出結果
- 確認済みのエビデンスと不足している情報を示す信頼度スコア
- MITRE ATT&CKマッピング、EASMインベントリとの照合、類似シグナルを持つ公開インシデントの参照
- Darkweb、Email Security、Briefsの各ビューと、ダークウェブ検出結果からのトリアージ・チケット作成

脅威評価

ダークウェブの検出結果を、信頼度、未取得のエビデンス、MITRE ATT&CKのテクニック、照合された資産をもとに評価し、トリアージやチケット作成につなげられます。公開デモの実際の画面です。画面上の数値はサンプルデータです。

元の画面を開く ↗

製品の詳細

AI & Compliance

06

01

対応準備

PDPA / CII

02

通知の下書き

漏えい通知

03

レポート支援

AIによる作成支援

対応準備とレポート作成を支援する別料金のモジュール

- PDPA・CIIへの対応準備と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
- 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

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。

> 脅威インテリジェンスは別途見積もりです。本書で料金を示す4モジュールや、その4モジュールのバンドル割引に自動的に含まれるものではありません。

対象範囲とモジュールをパートナーと検討

資産の対象範囲、モジュール、連携、運用責任をパートナーとご確認ください。

パートナーに相談 ↗

製品の詳細

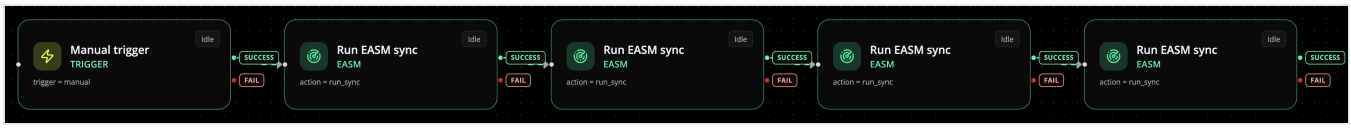
エージェントワークフロー

07

エージェントワークフローのキャンバス

トリガーとアクションをつなぎ、成功時と失敗時の分岐を持つエージェントを作成し、有効化または手動で実行できます。公開デモの実際の画面です。画面上の数値はサンプルデータです。

元の画面を開く ↗



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。 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



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。 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

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。

製品の詳細

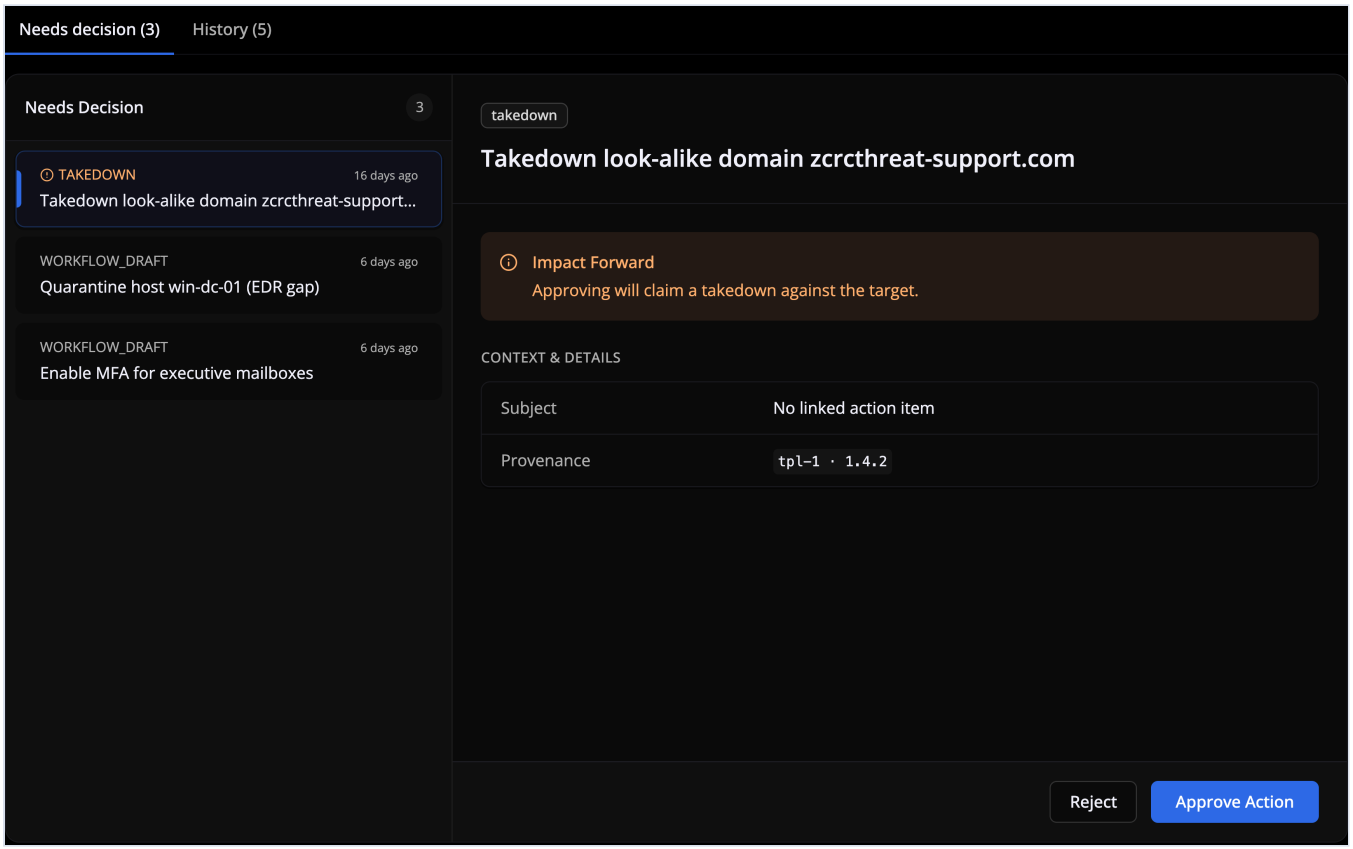
証跡と承認

08

監査証跡

AIが作成したチケットやテイクダウンの提案を承認・却下でき、各提案を生成元のテンプレートとバージョンまでたどれます。公開デモの実際の画面です。画面上の数値はサンプルデータです。

元の画面を開く ↗



テイクダウン提案の表示内容、テンプレートtpl-1、バージョン1.4.2、Approve / Rejectの両ボタンを保持。提案は判断待ちで、本書作成のための承認・実行は行っていません。 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

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。

製品の詳細

プランと課金単位

09

パッケージ

EASM — ฿10,600/月から	外部攻撃対象領域の発見。CTEM1〜5の5段階で最大2,000資産（月額฿10,600〜85,500）、超過分は1資産あたり月額฿21。ドメイン、サブドメイン、公開IP、SSL/TLS証明書など、数えられる資産の数で課金します。12か月契約の月額払い、税込。
CAASM — ฿10,600/月から	クラウドおよび社内資産のインベントリ（AWS/Azure/GCP/M365/OT）。5段階で最大20,000資産（月額฿10,600〜85,500、各段階ともEASMと同額）、超過分は1資産あたり月額฿2.35。12か月契約の月額払い、税込。
DRP + Dark Web — ฿21,300/月から	デジタルリスク保護とダークウェブ監視、テイクダウンサービス付き。5段階で監視キーワード最大100件（月額฿21,300〜160,400）、超過分は1キーワードあたり月額฿856。ティアに応じて年間3〜60件のテイクダウン申請を含みます。12か月契約の月額払い、税込。
AI & Compliance — ฿10,600/月から	PDPA/CII対応、漏えい通知、AIによるコンプライアンスレポート作成。5段階で従業員数最大10,000人（月額฿10,600〜96,200）、超過分は従業員1人あたり月額฿5.35。12か月契約の月額払い、税込。

モジュールごとに独自の単位で課金します。12か月契約の月額払い、税込。全ティアと4モジュール一括割引は zcr.ai/pricing/ をご覧ください。

参考価格の通貨はタイバーツ（THB）、税込です。12か月契約の月額請求です。発注前に提案内容と対象範囲をパートナーにご確認ください。

> 脅威インテリジェンスは別途見積もりです。本書で料金を示す4モジュールや、その4モジュールのバンドル割引に自動的に含まれるものではありません。

提供範囲

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。

製品の詳細

パートナーと進める評価

10

よくある質問

zcrCTEMはどの領域に対応していますか？

外部攻撃対象領域（EASM）、社内・クラウド資産のカバレッジ（CAASM）、デジタルリスク保護（DRP）、脅威インテリジェンスを一つのコンソールで扱います。タイのPDPAやCII向けのコンプライアンスレポートは、別料金のAI & Complianceモジュールで提供します。

AIが自動で対応を実行しますか？

同期など、あらかじめ設定した定型ステップはエージェントが実行できます。一方、AIが作成したチケットやテイクダウンの案は、アナリストが承認または却下するまで提案のままです。AIの回答と下書きはすべて、生成元のテンプレートとバージョンとともに監査証跡に記録されます。

公開デモでコンプライアンス機能を確認できますか？

公開デモには含まれていません。公開デモの対象は、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など露出管理の画面です。PDPA/CII対応、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はAI & Complianceモジュールの機能です。ご確認の際はzcrが承認したパートナーにご相談ください。

確認事項

資産範囲、モジュール、オンボーディング、導入、連携、サポート、SLA、料金はソリューション設計と見積書で確定します。

zcrが承認したパートナーを通じて評価を依頼

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 ↗

zcr.ai/contact/?lng=ja · zcr.ai/pricing/?lng=ja · demo.zcrctem.zcr.ai/dashboards