セキュリティ分析ソフトウェア・パートナー主導で評価

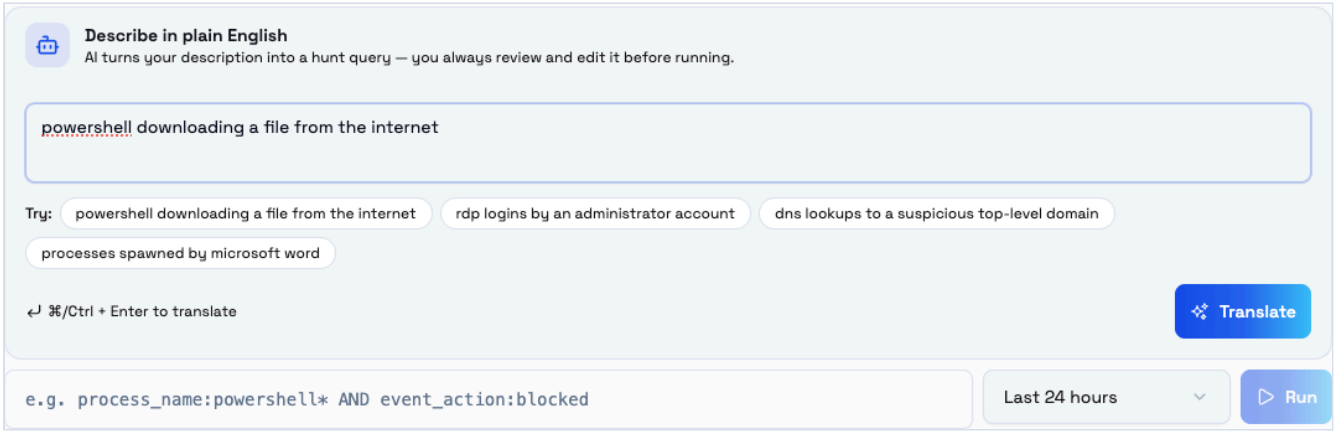
zcrSIEM

セキュリティのシグナルを、確認できる調査記録へ。

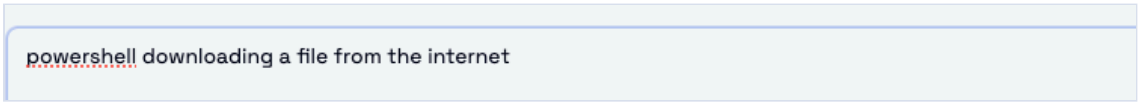
セキュリティイベントの検知、調査、関連付けを一つのアナリストワークフローに集約します。

> zcrSIEMは入力元から直接データを収集でき、zcrLogは必須ではありません。監視・インシデント対応サービスはソフトウェアと別契約です。自動対応Playbookは別製品のzcrSOARで提供します。

問いを入力し、クエリを確認してから実行する。



Threat Hunting：例示画面の質問欄とクエリ操作部です。変換・実行前の状態を示します。説明用のデモデータであり、顧客の調査や検知結果ではありません。画面は英語です。 元の画面を開く ↗



入力済みの質問例を拡大しています。実際の入力欄は切り抜き範囲の外へ続きますが、質問文は全文を保持しています。 元の画面を開く ↗

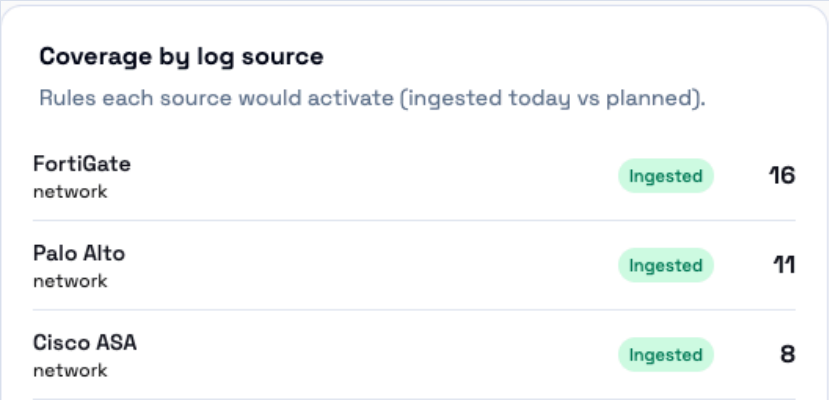
01
問いを入力
調査したい内容を記述します。

02
クエリを確認
生成されたクエリを確認・編集します。

03
実行を選択
アナリストが確認済みクエリの実行を指示します。

例示画面は英語入力を求めています。必要な入力言語はパートナーとの技術デモで確認してください。

どの入力元が検知ルールを有効にするかを確認する。



Detection Coverage：ログ入力元の例を3行とルール数を示します。入力元一覧の一部であり、全体ではありません。デモデータは検知効果や網羅性の保証ではありません。画面は英語です。 元の画面を開く ↗

主な機能

- AIによる脅威検知支援とイベント相関分析
- 脅威を自然言語で説明し、AIが生成した検索クエリを実行前にレビュー
- MITRE ATT&CKのコンテキストと検知カバレッジを用いた調査
- SigmaおよびElasticルールの同期と、戦術・ログソース別のカバレッジ確認

シグナル検知から、担当者が明確な対応まで

01 / 検知
イベントを相関分析し、不審な活動を把握します。

02 / 調査
レビュー可能なハンティングクエリで関連イベントを追跡します。

03 / 対応
インシデント、担当者、対応の進捗を管理します。

04 / 報告
運用上の証跡をMDR・経営レポートへまとめます。

自社の運用モデルに合うソフトウェア構成を選ぶ。

SOC、MDR、MSSP、CISO、エンタープライズセキュリティチーム

運用上の課題	大量のセキュリティデータ、分断されたツール、アラート量の増加により、何が起きたか、次に何をすべきかの判断が難しくなります。
セキュリティ入力元	ファイアウォール · Active Directory · エンドポイント · ネットワーク · Microsoft 365 · クラウドサービス
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）
取り込み	zcrSIEMは各ソースからログを直接取り込みます。全パッケージに独自の日次取り込み容量があり、zcrLogの導入は必須ではありません。

- リアルタイムのダッシュボード、通知、対応状況の可視化
- アラートからインシデント運用、MDRレポート、経営層への報告までを接続
- データとポリシーを分離したマルチテナント運用。クラウドでもオンプレミスでも同じ仕組みで、全パッケージでテナント・ユーザー数無制限

zcrSIEMはソフトウェアです。コンソール上のインシデント、ダッシュボード、MDR・経営向けレポートは、アナリストによる監視やインシデント対応サービスを含むものではありません。これらは別のサービスです。

容量、保持期間、オンボーディング、導入、連携、サポート、SLAは、該当するソリューション設計と見積書で確定します。

承認済みチャネルパートナーが一次サポートを提供し、zcrはそのパートナーに製品サポートを提供します。対応条件は該当する契約で定めます。

入力元、導入方式、プラン、評価範囲はzcrSIEM Product Overviewで確認できます。

承認済みパートナーと技術評価を計画する。

入力元一覧、1日あたりの想定取込量、保存期間、希望する導入方式をご用意ください。パートナーが範囲を確認し、ソリューション設計と見積もりを提示します。

パートナーに評価を相談する ↗　製品資料 ↗