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

入力元・運用フロー・プランを、自社の要件に合わせて確認する。

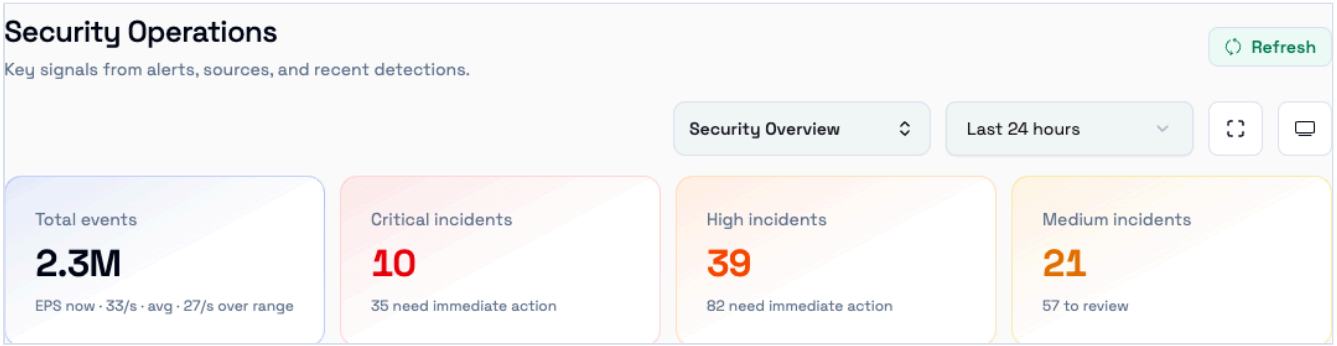
セキュリティイベントの検知、調査、関連付けを一つのアナリストワークフローに集約します。

SOC、MDR、MSSP、CISO、エンタープライズセキュリティチーム

> 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。

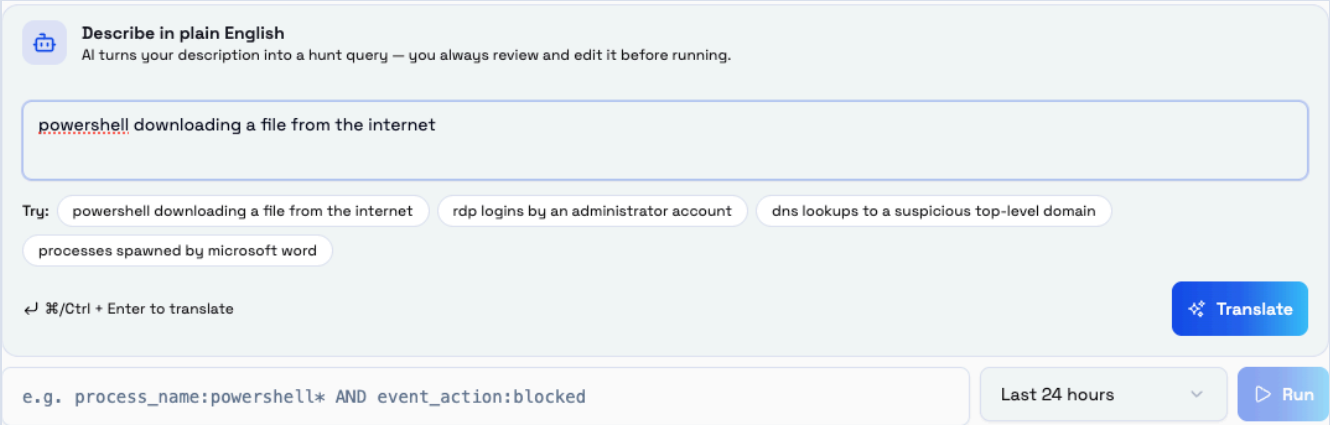
データソースと連携

ソース種別	ネットワーク機器・ファイアウォール・IDS/IPS・Windows・Linux・IDシステム・エンドポイントセキュリティ・メールセキュリティ・クラウドプラットフォーム・コンテナ・Kubernetes・EDR・NDR・ネットワークセンサー
クラウド基盤	AWS・Azure・Google Cloud・Huawei Cloud・GDCC Cloud・GDCC OpenData（API、Webhook、Syslog、ネイティブコネクタで接続）
エンドポイント・メール・ネットワーク	Windows・Linux・macOSのエンドポイントシグナル・Microsoft Defender for Office 365・NDR・ネットワークセンサー・IDS/IPS
脅威インテリジェンス	オープンソースおよび商用の脅威インテリジェンス（API、フィード、STIX/TAXII）
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。

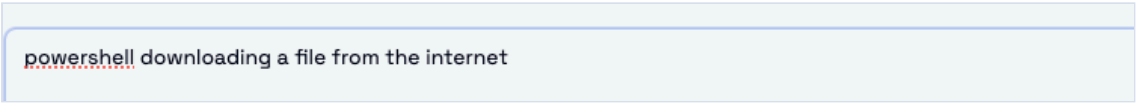


Security Operations：イベントとインシデントの例を重要度別に表示します。デモデータであり、顧客の処理量、容量上限、性能の証拠ではありません。画面は英語です。 元の画面を開く ↗

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。

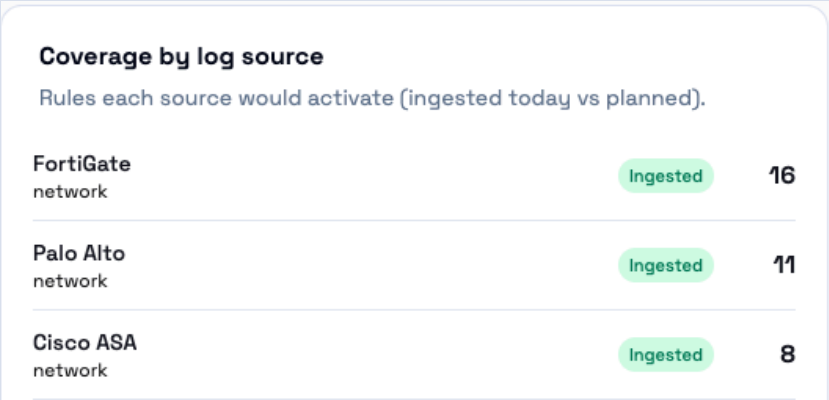
主な機能

- 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

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。

調査の流れを簡潔に把握するにはzcrSIEM Brochureをご覧ください。本書は技術要件とプランの評価用です。

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 ↗

- 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
- 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

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。

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。

パッケージと価格

パッケージ	日次取り込み量	保持期間	月額（税込）
SaaS（クラウド）			
zcrSIEM-1	1 GB	90日	฿6,000
zcrSIEM-3	3 GB	90日	฿18,000
zcrSIEM-5	5 GB	90日	฿30,000
zcrSIEM-10	10 GB	90日	฿45,000
オンプレミス（ソフトウェア）			
SITE-10	10 GB	お客様提供のストレージ次第	฿31,500
SITE-20	20 GB	お客様提供のストレージ次第	฿52,500
SITE-50	50 GB	お客様提供のストレージ次第	฿92,400
SITE-100	100 GB	お客様提供のストレージ次第	฿158,900

全パッケージとも月額課金・12か月契約（税込）で、テナント・ユーザー数は無制限です。オンプレミスはソフトウェアのみの提供で、お客様のハードウェアまたはVM上で稼働します。

> オンプレミスの導入・設定費用は月額サブスクリプションとは別に、実際の作業範囲に応じて承認済みパートナー経由で見積もります。

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。

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 ↗