

AI搭載SIEM

zcrSIEM

AIを活用したセキュリティ情報・イベント管理

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。

対象チーム	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。
セキュリティデータソース	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）

主な機能

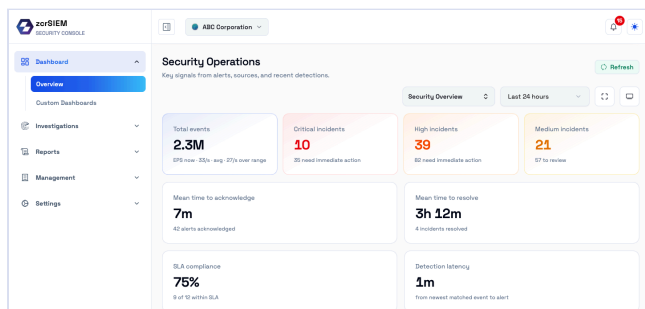
- AIによる脅威検知支援とイベント相関分析
- 脅威を自然言語で説明し、AIが生成した検索クエリを実行前にレビュー
- MITRE ATT&CKのコンテキストと検知カバレッジを用いた調査
- SigmaおよびElasticルールの同期と、戦術・ログソース別のカバレッジ確認
- リアルタイムのダッシュボード、通知、対応状況の可視化
- アラートからインシデント運用、MDRレポート、経営層への報告までを接続
- データとポリシーを分離したマルチテナント運用。クラウドでもオンプレミスでも同じ仕組みで、全パッケージでテナント・ユーザー数無制限

データソースと連携

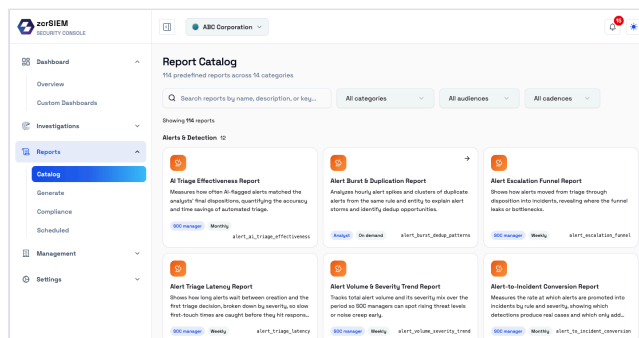
ソース種別	ネットワーク機器・ファイアウォール・IDS/IPS・Windows・Linux・IDシステム・エンドポイントセキュリティ・メールセキュリティ・クラウドプラットフォーム・コンテナ・Kubernetes・EDR・NDR・ネットワークセンサー
クラウドプラットフォーム	AWS・Azure・Google Cloud・Huawei Cloud・GDCC Cloud・GDCC OpenData（API、Webhook、Syslog、ネイティブコネクタで接続）
エンドポイント・メール・ネットワーク	Windows・Linux・macOSのエンドポイントシグナル・Microsoft Defender 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。

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。



セキュリティ運用ダッシュボード — デモ環境の例であり、実測値ではありません



レポートカタログ — デモ環境の例であり、実測値ではありません

コンソール画面

The screenshot shows the 'Threat Hunting' section of the zcrSIEM console. The left sidebar contains navigation links: Dashboard, Overview, Custom Dashboards, Investigations (selected), Incidents, Alerts, Log Search, Threat Hunting, Detection Rules, Asset Inventory, Threat Intel, Reports, and Management. The main content area is titled 'Threat Hunting' and includes a description: 'Search normalized telemetry, investigate patterns, and save repeatable hunts.' Below this are two tabs: 'Query Workspace' (selected) and 'Hunt Library'. The 'Query Workspace' tab features a text input field with the query 'powershell downloading a file from the internet'. Below the input field are several tags: 'powershell downloading a file from the internet', 'rdp logins by an administrator account', 'dns lookups to a suspicious top-level domain', and 'processes spawned by microsoft word'. A 'Translate' button is located to the right of the input field. Below the input field is a 'Run' button. The bottom of the main content area shows a search bar with the example query 'e.g. process_name:powershell* AND event_action:blocked' and a 'Last 24 hours' filter.

AIによる脅威ハンティング — デモ環境の例であり、実測値ではありません

The screenshot shows the 'Detection Coverage' section of the zcrSIEM console. The left sidebar is the same as the previous screenshot. The main content area is titled 'Detection Coverage' and includes a description: 'Measure source and MITRE ATT&CK coverage to expose detection blind spots.' Below this are three tabs: 'Rule Catalog' (selected), 'Coverage', and 'Engine Health'. The 'Rule Catalog' tab displays a table of log sources and their coverage status. The table has columns for the log source name, its status (Ingested), and the number of rules it covers. The data is as follows:

Log Source	Status	Rules
FortiGate network	Ingested	16
Palo Alto network	Ingested	11
Cisco ASA network	Ingested	8
Sangfor NGAF network	Ingested	6
Sangfor Proxy proxy	Ingested	7
CrowdStrike Falcon endpoint	Ingested	12

Below the table is a section titled 'MITRE ATT&CK coverage by tactic' which shows a horizontal bar chart. The chart displays the coverage of various MITRE ATT&CK techniques across different tactics. The tactics and their corresponding coverage are: Reconnaissance (100%), Initial Access (100%), Execution (100%), Persistence (100%), Privilege Escalation (100%), Defense Evasion (100%), Credential Access (100%), and Discovery (100%).

MITRE ATT&CKカバレッジ — デモ環境の例であり、実測値ではありません

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。

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。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。

zcrのチャネルパートナーに相談し、技術デモとソリューション適合性をご確認ください。

パートナーが技術デモを実施し、お客様と一緒にサイジングを行ったうえで、ソリューション設計と見積書をご用意します。

パートナーと評価する ↗

zcr.ai/contact/?lng=ja