マネージドセキュリティサービス・承認済みパートナーが提供

zcrSOC

SOC-as-a-Service

アラートの受領、トリアージ、対応調整、月次インシデントレポートを提供する、タイとASEAN向けの包括的なマネージドセキュリティ運用サービスです。

マネージド対応調整が必要な組織・セキュリティ運用・IT チーム・MSP・MSSP・長時間稼働する顧客

インシデントが確認された際、チームには明確なエスカレーション、責任ある対応調整、発生内容の記録が必要です。

01 監視
zcrSIEM がセキュリティテレメトリーをアラートへ変換します。

02 調査
SOC が重大度、影響範囲、担当を検証します。

03 調整 zcrSOC Response のみ
Response が SLA に基づきエスカレーションと IR 支援を調整します。

04 改善
FWTicket と月次レポートで運用ループを完結させます。

MDR と SOC：運用範囲で選ぶ

どちらもアラート運用とレポートを提供します。業務が重複しないよう、承認済みパートナーと範囲を決めます。

	サービス範囲	必要な基盤	提供する記録
zcrMDR	アラートのトリアージとレポート。Complete は顧客承認後のパートナーによるリモート対応を追加。	zcrSIEM	月次レポート・FWTicket でのケース管理
zcrSOC	監視とトリアージ。Response は対応調整、エスカレーション、インシデント対応支援を追加。	Essential：zcrSIEM・Response：zcrSIEM + zcrSOAR	月次レポート・週次シフト引き継ぎ・FWTicket

zcrSOC の運用ティアを選択

zcr サービス基盤	Essential：zcrSIEM が必要・Response：zcrSIEM + zcrSOAR が必要
前提条件	zcrSOC EssentialはzcrSIEM上で、zcrSOC ResponseはzcrSIEM + zcrSOAR上で提供します。イベントの保持期間はお客様のzcrSIEMプランに従います（zcrSIEMのSaaSプランは90日間、オンプレミスプランはお客様自身のストレージに応じて無制限です）。サービスに含まれるプラットフォームのライセンスは、パートナーの見積書に記載されます。

含まれるプラットフォームライセンスは、パートナーの見積書に明記します。

Essential はアナリスト監視とトリアージ、Response は対応調整、エスカレーション、IR 支援を追加します。

	zcrSOC Essential SOC · ESSENTIAL	zcrSOC Response SOC · RESPONSE
内容	監視とトリアージ	対応調整ワークフロー
含まれるもの	• 継続監視、アラートトリアージ、月次レポート • 1 / 3 / 5 / 10 GB/日はzcrSIEM SaaS（90日間保持）、20 GB/日はzcrSIEMオンプレミス（保持は無制限、お客様自身のストレージに応じます）で算定 • 週次シフト引き継ぎレポート	• Essential 監視に対応調整を追加 • エスカレーション、IR 支援、経営層向けレポート • Essentialと同じ 1 / 3 / 5 / 10 / 20 GB/日の規模で算定 • 週次シフト引き継ぎレポート
基盤	検知基盤として zcrSIEM が必要	zcrSIEM + zcrSOAR が必要

> Response は SOW に沿って対応を調整します。承認者、実行権限、クローズの役割はパートナーと合意します。

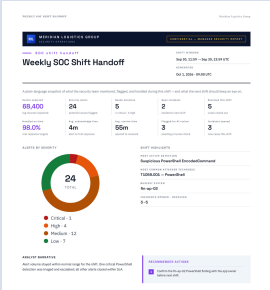
サービス対応時間

ワークロード課金の SOC 運用を 8×5、16×5、24×7 の対応時間に合わせられます。

8×5 対応	営業時間内のセキュリティ運用カバレッジ。
16×5 対応	平日のセキュリティ運用カバレッジを拡張します。
24×7 対応	合意したサービス範囲に合わせた常時マネージド運用。

次のシフトへ文脈を引き継ぐ

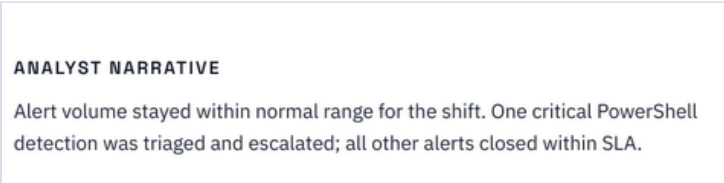
説明用サンプルです。実際の顧客データではありません。



説明用サンプルであり、実際の顧客データではありません。英語原文の分析メモと推奨対応を拡大し、日本語の説明を添えています。
元の画面を開く ↗

- アラートの受領とトリアージ
- 対応調整とエスカレーション（zcrSOC Response のみ）
- 月次インシデントレポートの自動化
- 8×5、16×5、24×7 の SLA 対応

ケースの追跡には、zcrが運営しサービスに含まれるFWTicket顧客ポータルを使用します。



元のサンプル本文（英語）

Alert volume stayed within normal range for the shift. One critical PowerShell detection was triaged and escalated; all other alerts closed within SLA.

分析メモにトリアージとエスカレーションの内容を記録。 説明用サンプルです。実際の顧客データではありません。 元の画面を開く ↗



元のサンプル本文（英語）

Confirm the fin-ap-02 PowerShell finding with the app owner before next shift.

次シフトの確認事項：検知内容をアプリ担当者に確認。 説明用サンプルです。実際の顧客データではありません。 元の画面を開く ↗

> Response は SOW に沿って対応を調整します。承認者、実行権限、クローズの役割はパートナーと合意します。

zcrSOC FAQ

zcrSOC の Essential と Response の違いは何ですか？

Essential は zcrSIEM 上でアラートの受領、トリアージ、月次レポートを提供します。Response はさらに zcrSIEM + zcrSOAR 上で対応調整、エスカレーション、IR 支援を追加します。いずれも、イベントの保持期間はお客様の zcrSIEM プランに従います（zcrSIEM の SaaS プランは 90 日間、オンプレミスプランはお客様自身のストレージに応じて無制限です）。

zcrSOC は 24×7 運用を支援できますか？

はい。適用される SLA と作業範囲記述書により、8×5、16×5、24×7 のサービス対応を選択できます。

zcrSOC はパートナー経由で提供されますか？

はい。zcrSOC は、zcr.ai が承認したチャネルパートナーのみが提供します。対応時間とサービスレベルは、そのパートナーのサービス契約で定めます。

役割と引き継ぎの概念図

01

基盤・zcrSIEM

セキュリティシグナルを集約し、検知とアラートにつなげます。

02

承認済みパートナー・トリアージとケース管理

アラートをトリアージし、サービスに含まれる FWTicket でケースを追跡します。

03

顧客 + パートナー・範囲の合意

承認者、アクセス権、実行・エスカレーション・クローズの役割を SOW で定めます。

役割を示す概念図であり、実行手順ではありません。開始前に SOW で役割と権限を合意します。

対応時間、サービスレベル（SLA）、範囲、実行権限は、パートナーとの契約と SOW に従います。

承認済みチャネルパートナーが一次サポートを担当し、zcr がそのパートナーに製品サポートを提供します。

zcr.aiが承認したチャネルパートナーが提供します。対応時間とサービスレベルは、そのパートナーのサービス契約で定めます。

サービス範囲の検討に向けて

データソース一覧と、利用中または予定している zcrSIEM プラン。・希望するサービスエディションと対応時間。・インシデント連絡先、承認者、検討が必要なアクセス範囲。

見積書：サービスエディション、基盤プラン、明示された付属ライセンス。

SOW：範囲、対応時間、SLA、役割、承認、実行権限、エスカレーション、クローズ。

zcr.ai の承認済みチャネルパートナーに範囲を相談 ↗