

マネージドサービス

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。

対象	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
運用上の課題	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。
zcr サービス基盤	zcrSIEM + zcrSOAR
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。
ケース管理	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。
サービス提供	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。

主な機能

- 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

zcrSOC: シグナルから解決までのマネージド運用

セキュリティテレメトリーを、責任あるトリアージ、エスカレーション、対応、改善へ変換する運用ループです。

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。

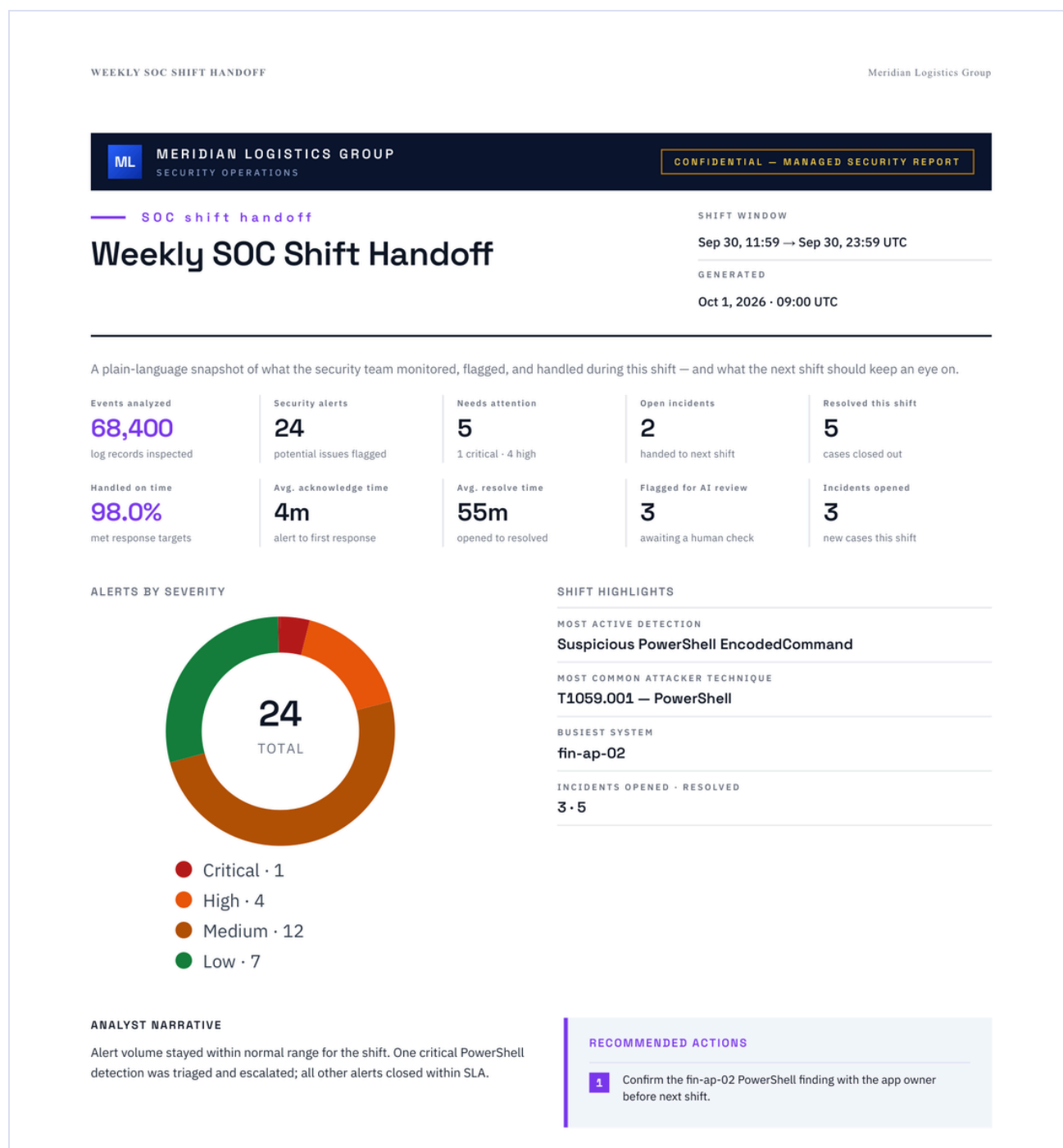
04 改善

FWTicket と月次レポートで運用ループを完結させます。

zcrSOC の運用ティアを選択

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



シフト引き継ぎレポート：SOCのシフト引き継ぎレポートのサンプルです — アラートの重大度別内訳、対応指標、次のシフトへの引き継ぎメモを含みます。（説明用のサンプルであり、実際の顧客データではありません）

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。

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。

明確な責任を伴う対応

zcrSOC はアラート処理、エスカレーション、インシデントレポートをマネージド運用モデルにまとめます。

zcr.ai のチャネルパートナーに相談

組織に合うカバレッジと SLA について zcr.ai のチャネルパートナーにご相談ください。

チャネルパートナーに問い合わせる ↗

zcr.ai/contact/?lng=ja