

マネージドサービス

zcrMDR

マネージド検知・対応

タイとASEAN のセキュリティチーム向けに、zcr プラットフォームのシグナルを対応可能なアラート、専門家によるレビュー、明確なレポートへ変える MDR サービスです。

対象	マネージド検知を始める組織・IT・セキュリティチーム・MSP・MSSP・明確な月次レポートを必要とする顧客
運用上の課題	多くのチームはデータを持っていても、アラートの継続的な確認、優先順位付け、関係者へのイベント説明に十分な時間がありません。
zcr サービス基盤	zcrSIEM
前提条件	zcrMDRはzcrSIEM上で提供します。イベント証跡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

- zcr による検知とアラート
- 月次レポートの自動化
- FWTicket 顧客ポータル
- 8×5、16×5、24×7 の SLA 対応

zcrMDR: 検知から記録されたアクションへ

zcrSIEMに集約したセキュリティシグナルをトリアージ、対応、顧客向けの記録へ変換する運用ループです。

01 検知

zcrSIEMに集約したセキュリティシグナルを対応可能なアラートへ変換します。

02 トリアージ

MDR が重大度、影響範囲、次のアクションを検証します。

03 対応

zcrMDR Complete のみ

Complete がアクティブ対応と IR（インシデントレスポンス）支援を調整します。

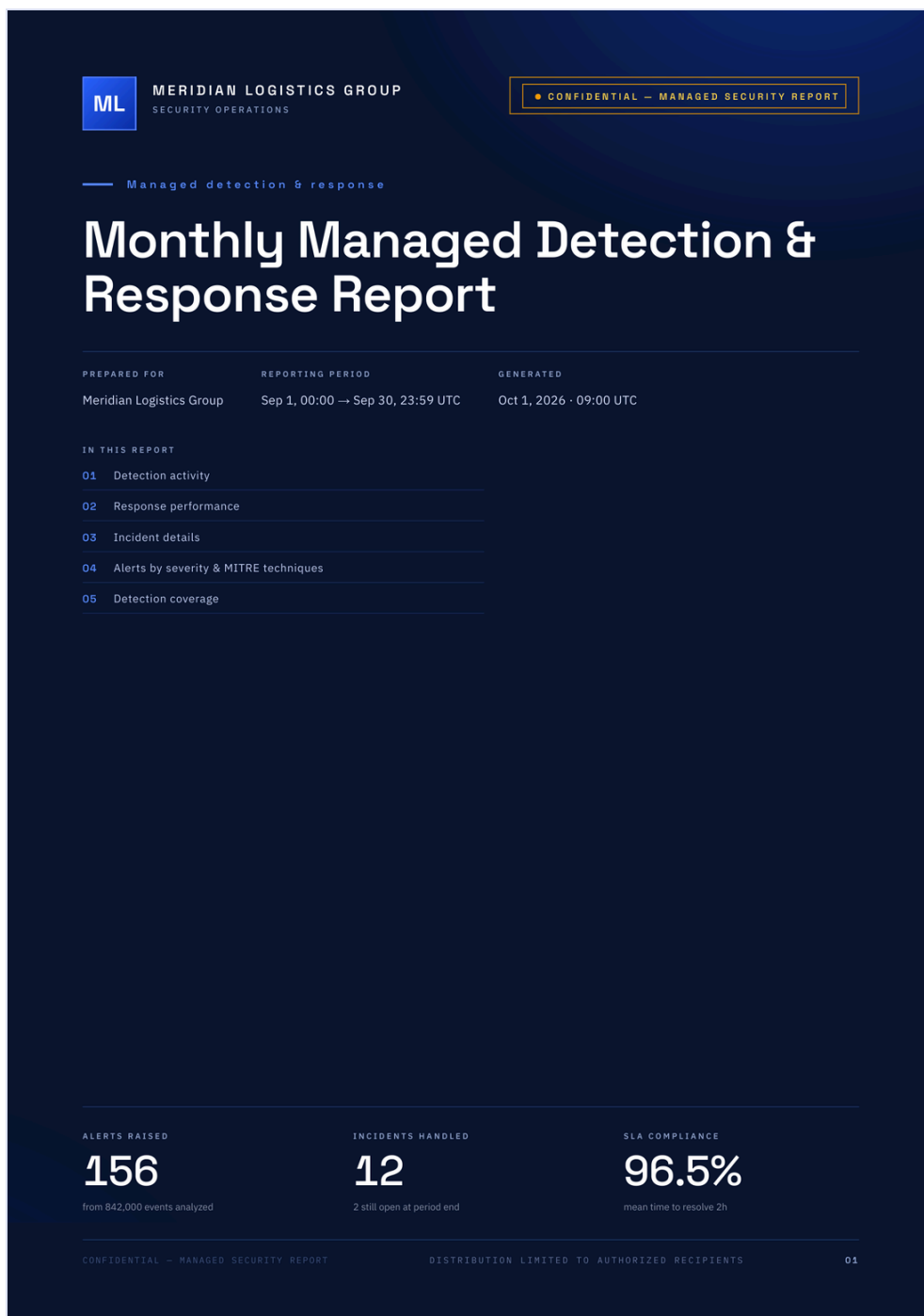
04 レポート

FWTicket と月次レポートで運用ループを完結させます。

zcrMDR エディションを選択

アラート・レポート運用と、アクティブ対応・インシデント対応支援を2つのサービスレベルに分けます。

	zcrMDR Essential MDR ・ ESSENTIAL	zcrMDR Complete MDR ・ COMPLETE +IR
内容	検知とレポート	Essential にアクティブ対応を追加
含まれるもの	- アラートトリアージと月次レポート自動化 - FWTicket 顧客ポータル - SOC Radar および CVE チェックのポータル範囲は含みません	- Essential のアラート・レポートサービスをすべて含む - アクティブ対応とインシデント対応支援 - 選択した SLA に合わせた対応コミットメント
基盤	zcrSIEM: zcr のシグナルを zcrSIEM に集約し、MDR アナリストがトリアージと対応を行います。イベント証拠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）。	



月次サービスレポート：MDRレポートのサンプルです — SLA実績、インシデント件数、対応時間を報告する構成を示します。（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）

zcrMDR FAQ

zcrMDR Essential には何が含まれますか？

zcr による検知とアラート、月次レポートの自動化、FWTicket 顧客ポータル、zcrSIEMでのイベント保持（お客様のzcrSIEMプランに従い、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）が含まれます。

対応時間はどのように選べますか？

適用される SLA と作業範囲記述書により、8×5、16×5、24×7 の対応時間を選択できます。

zcrMDR Complete のアクティブ対応の範囲は？

対応アクションはすべてリモートで行われ、お客様の承認後にのみチャネルパートナーが実施します。zcrMDR Complete にオンサイト対応は含まれません。

サービス対応時間

同じ zcrMDR サービスを 8×5、16×5、24×7 の対応時間で契約できます。

8×5 対応	営業時間内のマネージド検知、アラート、月次レポート。
16×5 対応	より長い稼働時間の組織向けに、平日の対応時間を拡張します。
24×7 対応	合意したサービス範囲に応じた常時対応。

明確な運用記録を備えた検知

zcrMDR はイベントの文脈保持、アラートレビュー、継続的なレポートによるサービス活動の共有を支援します。

zcr.ai のチャネルパートナーに相談

運用時間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