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

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。

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

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。

アラートの確認を支援

zcrSIEM に集約したシグナルのアラートをトリアージし、次の対応の検討を支えます。

ケースの状況を追跡

サービスに含まれる zcr の顧客ポータル FWTicket でケースを追跡できます。

サービスを振り返る記録

自動作成の月次レポートを使い、パートナーとサービス活動を振り返れます。

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

zcrMDR エディションを選択

zcr サービス基盤	zcrMDR は zcrSIEM 上で提供します。顧客側の EDR は必須ではありません。
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。

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。

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 • SOCRadar 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 > Complete のみ：顧客承認後に承認済みパートナーがリモートで実施します。オンサイト対応は含みません。
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。

概念図：シグナルからサービス記録へ

01
zcrSIEM のセキュリティシグナル

02
アラートのトリアージ

03
FWTicket でのケース管理 + 自動月次レポート

確認済みサービス範囲を示す概念図です。レポートの抜粋やシステム構成図ではありません。提供内容の詳細は SOW に従います。

説明用サンプルです。実際の顧客データではありません。



形式を示すレポート表紙のサンプルです。実際の顧客データやサービス成果の証明ではありません。 元の画面を開く ↗

- 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

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。

zcrMDR: 検知から記録されたアクションへ

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・Complete のみ
承認済みパートナーが、顧客承認後に合意範囲内でリモート対応とインシデント対応支援を行います。

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。

> Complete のみ：顧客承認後に承認済みパートナーがリモートで実施します。オンサイト対応は含みません。

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。

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 ↗