Response

zcrSOAR

セキュリティオーケストレーション・自動化・対応

zcrSOARはトリアージを共有のプルキューに変え、Playbookをステップごとに自律実行・承認待ち・ブロックのいずれかで運用し、通知SLAと対応SLAを深刻度別に分けて追跡します。承認と対応アクションは役割に基づく1つのキューを通じて処理されます。

対象	大量のアラートをトリアージするSOCチーム・MSSP・MDRプロバイダー・Playbookの標準化を進めるチーム・SLA遵守を証明する必要があるチーム
運用上の課題	共有キューがなければ、アナリストは同じアラートに重複して対応してしまいます。監視なしで完全に自動実行されるPlaybookはリスクをもたらし、すべてのステップで人の判断を待つPlaybookは規模の拡大に追いつかず、SLAも事後にしか把握できないことが多くなります。
連携先	zcrSIEM（双方向ブリッジ）・SentinelOne EDR（隔離・スキャン）・MISP Threat Intelligence（インジケーター同期）・OpenAI互換AIアシスタント
導入形態	SaaS（クラウド）またはオンプレミスのソフトウェアから、ソリューション設計時に選択

主な機能

- トリアージボード：プルキュー方式 — ケースを取ると他のアナリストのキューから外れます
- バージョン管理、承認ステップ、ドライランに対応したPlaybookライブラリ
- プロンプトからAIがPlaybookを下書き生成、YAML/JSON形式のインポートにも対応
- ステップ単位のゲーティング（自律・承認待ち・ブロック）
- Approvals & Tasks：ロール別の1つのキュー。期限は種類ごとに異なり、リビジョンには期限なし
- 通知SLAと対応SLAを深刻度別に分けて追跡し、違反一覧を提供
- Attack Flows：MITRE ATT&CKにマッピングされたケースごとのタイムライン
- IPアドレス・ドメイン・ハッシュ・URL・メールに対応したIOCライブラリ。MISP同期対応
- ドライランを含む実行履歴を証跡として保持

シグナルから説明責任のある対応へ

1つのキュー、適切な監視レベルを持つPlaybook

zcrSOARは連携元（zcrSIEMとの双方向ブリッジを含む）からインシデントを受け取り、プルキュー方式のトリアージボードに登録します。アナリストがケースを取ると、そのケースは他のアナリストのキューから外れます。Playbookはステップ単位でゲーティング（自律・承認待ち・ブロック）され、ケース承認、Playbookのステップ承認、対応アクションはすべて1つのApprovals & Tasksキューを通じて処理し、通知SLAと対応SLAは深刻度別に分けて追跡します。

判断の前に申請内容を確認する



最初の申請のケース名とCONTAINED → CLOSEDの状態遷移を表示しています。承認待ちの例であり、承認済みの結果ではありません。 製品の詳細を見る ↗

同じ最初の承認待ち申請：REQUIRED: OPERATOR、待機時間、デモのSLA表示、Reject／Approve操作を確認できます。この画面例は契約上のサポートSLAを保証しません。 製品の詳細を見る ↗

01・申請

状態遷移とケースに記載された背景を確認します。

02・ロール

操作前に必要な権限を確認します。

03・判断

権限に従って承認または却下します。静止画は実行完了を示しません。

> 説明用のデモデータです。顧客実績、処理容量、性能の証拠ではありません。元の英語UIを保持しています。

複数のツールにまたがる対応を一つの流れで

SentinelOneでのエンドポイントの隔離・解除やスキャンの実行、MISPでの属性検索・イベント公開・インジケーター同期を、ケースやプレイブックのステップから直接実行できます。

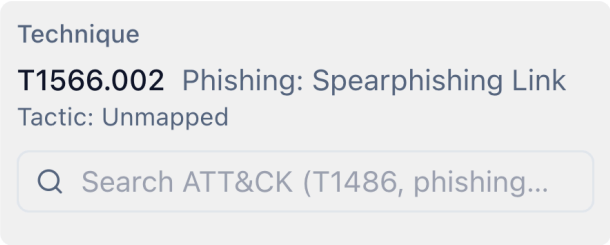
プレイブック自動化

Phishing、Malware、Brute-Force、C2 IsolationなどのPlaybookを標準搭載し、NIST Categoryで分類。AIアシスタントがPromptから新しいPlaybookを生成することもできます。

手法タグと戦術の対応状況を分けて読む



MITRE ATT&CK v14.1 · 3つのステップにT1566.002、T1204.002、T1486が表示され、すべてTactic: Unmappedです。最初の操作名はUI内で省略され、詳細パネルで正式名を確認できます。この例では戦術の対応付けが未完了です。 製品の詳細を見る ↗



最初に選択したノードの詳細にT1566.002 — Phishing: Spearphishing LinkとTactic: Unmappedを表示します。1ノードの情報であり、フロー全体の対応率ではありません。
製品の詳細を見る ↗

本番環境で安全に有効化

承認されていないプレイブックは、組織が本番での実行を許可するまで、Draft、Test、Dry-run、Simulation Modeのいずれかにとどまります。

運用概況：ケース数、平均確認時間・平均クローズ時間、自動化の稼働状況をリアルタイムで一画面に表示します。（デモ環境の例であり、実測値ではありません）

役割ベースの承認ワークフロー：ケースクローズの承認を必要な役割（オペレーター／管理者）に振り分け、SLAのカウントダウンをリアルタイム表示します。（デモ環境の例であり、実測値ではありません）

> 説明用のデモデータです。顧客実績、処理容量、性能の証拠ではありません。元の英語UIを保持しています。

本番実行回数でプランを比較する

同じ容量ではSaaSとオンプレミスソフトウェアは同額です。本表はTHB建て、12か月契約の月額請求、VAT込みです。

SaaS SKU／オンプレミス接尾辞	本番実行回数／月	THB／月・VAT込	導入形態
zcrSOAR-500 **OP-500**	500	125,000	SaaS／オンプレミス
zcrSOAR-2K **OP-2K**	2,000	250,000	SaaS／オンプレミス
zcrSOAR-10K **OP-10K**	10,000	450,000	SaaS／オンプレミス
zcrSOAR-50K **OP-50K**	50,000	580,000	SaaS／オンプレミス

オンプレミスSKU: zcrSOAR-OP-500 / zcrSOAR-OP-2K / zcrSOAR-OP-10K / zcrSOAR-OP-50K

パートナーと必要な容量・範囲を決める

1 runは本番環境でのautomationの実行1回です。全プランでplaybook、連携、テナント、ユーザー数は無制限です。

掲載プランの中間の実行回数については、承認済みパートナーが範囲に応じて見積もります。段階単価から契約価格を自動計算するものではありません。

> 計測方法、プランを超える利用、プラン変更、合意した支援時間帯は見積もり／SOWに明記します。

承認済みパートナーが見積もり、契約、導入と一次支援を担当し、zcrがパートナーを支援します。導入・設定は範囲別に別途見積もります。

現行プラン ↗

導入形態と責任分担を整理する

オンプレミスは自社ハードウェアまたはVMで動作するソフトウェアです。zcrSOAR専用機はありません。導入・設定は契約料とは別に範囲別で見積もります。保管基盤の費用削減がなく、自主管理環境では更新・connector支援が必要なため同額です。

> zcrSOARは単独購入でき、zcrSIEMもzcrLogも必須ではありません。

zcrSOARに関するよくある質問

zcrSOARはPlaybookのどのアクションを自動実行するか、どう決めますか？

Playbookの各ステップは自律・承認待ち・ブロックのいずれかに設定します。自律ステップは即座に実行され、承認ステップは役割に基づく承認を待ち、ブロックステップはゲーティングが変わるまで実行されません。

zcrSOARは新しいPlaybookを生成できますか？

はい。AIアシスタントがプロンプトからPlaybookを下書き生成し、レビューできます。また、Playbook定義をYAMLまたはJSON形式で直接インポートすることもできます。

zcrSOARにはzcrSIEMが必要ですか？

いいえ。zcrSOARは両方を導入している場合にzcrSIEMと双方向ブリッジで連携しますが、EDRプラットフォームなど他の連携元からも取り込めるため、zcrSIEMのみに限定されません。

zcrSOARはSLA遵守をどのように追跡しますか？

通知SLAと対応SLAをケースの深刻度別に分けて追跡し、コンプライアンス目標に対して平均確認時間と平均対応時間を計測します。SLAを満たさなかったケースの一覧も提供します。

承認済みパートナーと評価する

月間本番実行回数、連携元ツール、承認責任者、導入形態を用意してください。パートナーがプラン、計測定義、支援時間帯、導入責任を提案に明記します。

承認済みパートナーが提案範囲、見積もり、契約、導入を担当します。

パートナーに相談 ↗　現行プラン ↗　製品資料 ↗