Response

zcrSOAR

Security Orchestration, Automation & Response

zcrSOAR turns triage into a pull queue, runs playbooks under per-step Autonomous, Approval, or Blocked gating, and tracks Notify and Respond SLA separately by severity, with approvals and response actions routed through one role-gated queue.

BUILT FOR	SOC teams triaging high alert volume · MSSPs and MDR providers · Teams standardizing playbooks with oversight · Teams that must prove SLA compliance
THE OPERATING GAP	Without a shared queue, analysts duplicate work on the same alert. Fully unsupervised playbooks are risky, playbooks that need a person for every step don't scale, and SLA is often tracked only after the fact, not in real time.
CONNECTS WITH	zcrSIEM (bidirectional bridge) · SentinelOne EDR (isolate, scan) · MISP Threat Intelligence (sync indicators) · OpenAI-compatible AI assistant
DELIVERY OPTIONS	SaaS (cloud) or on-premises software, chosen in solution design

CORE CAPABILITIES

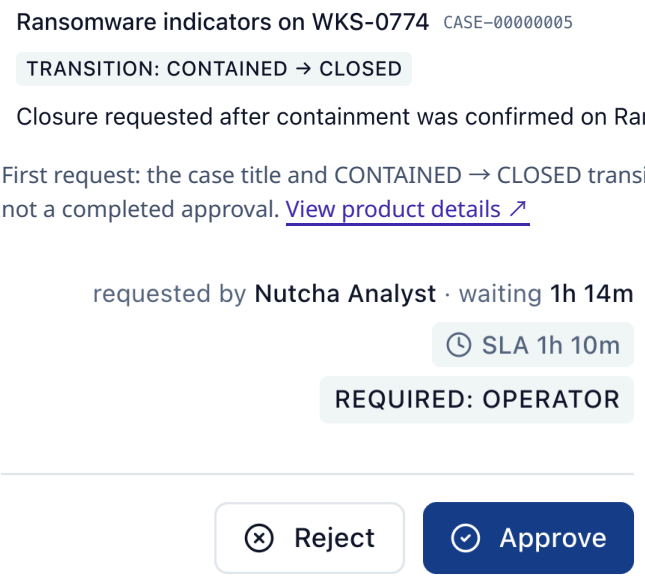
- Triage board: a pull queue — taking a case removes it for other analysts
- Playbook library with versioning, approval, and dry-runs
- AI-assisted playbook drafting from a prompt, or import as YAML/JSON
- Per-step gating — Autonomous, Approval, or Blocked
- Approvals & tasks: one role-gated queue; timing depends on item type, and revisions have no deadline
- Notify and Respond SLA tracked separately by severity, with a breach list
- Attack flows: MITRE ATT&CK-mapped timeline per case
- IOC library for IPs, domains, hashes, URLs and email, with MISP sync
- Run history retained as evidence, including dry-runs

FROM SIGNAL TO ACCOUNTABLE ACTION

One queue, playbooks with the right amount of oversight

zcrSOAR receives incidents from connected sources, including a bidirectional bridge to zcrSIEM, and places them in a pull-queue triage board — an analyst takes a case and it leaves the queue for everyone else. Playbooks run with per-step gating (Autonomous, Approval, or Blocked), and case approvals, playbook-step approvals, and response actions route through one Approvals & tasks queue, with Notify and Respond SLA tracked separately by severity.

Inspect the request before deciding



First request: the case title and CONTAINED → CLOSED transition identify what is being requested. This is a pending request, not a completed approval. View product details ↗

The same first pending request: REQUIRED: OPERATOR, elapsed waiting time, the demo SLA indicator, and Reject / Approve controls. This UI example is not a contractual support SLA. View product details ↗

01 · Request

Review the case transition and its stated context.

02 · Role

Identify the required role before choosing an action.

03 · Decision

Approve or reject within the authorized workflow; this still does not prove execution.

> Illustrative demo data, not customer results, capacity or performance evidence. English UI retained.

One response path across tools

Isolate or release an endpoint and trigger a scan through SentinelOne, or search, publish, and sync indicators through MISP — triggered from a case or a playbook step.

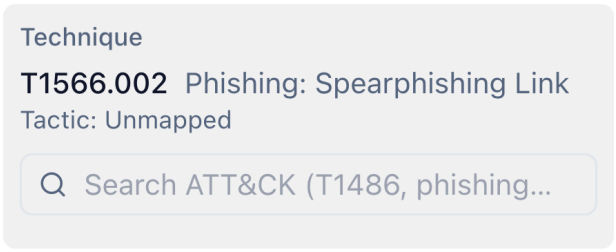
Playbook Automation

Start with out-of-the-box playbooks for phishing, malware, brute-force, and C2 isolation, organized by NIST category, or generate a new one from a prompt with an AI assistant.

Read technique tags and tactic coverage separately



MITRE ATT&CK v14.1 · The three steps show T1566.002, T1204.002 and T1486, all with Tactic: Unmapped. The UI abbreviates the first action title; its full name is available in the inspector. Tactic mapping is unfinished in this example. View product details ↗



The first selected node's inspector shows T1566.002 — Phishing: Spearphishing Link and Tactic: Unmapped. This describes one node, not a flow-wide coverage score. View product details ↗

Safe production activation

Unapproved playbooks remain in Draft, Test, Dry-run, or Simulation Mode until the organization authorizes production execution.

Operations Overview. Case volume, mean time to acknowledge and close, and automation run health in one dashboard, refreshed in real time. (Illustrative demo data, not live figures)

Role-Based Approval Workflow. Case-closure approvals routed by required role (operator vs. admin) with live SLA countdowns. (Illustrative demo data, not live figures)

> Illustrative demo data, not customer results, capacity or performance evidence. English UI retained.

Compare production-run packages

SaaS and on-premises software have the same prices at equal capacity. THB is the currency of record here; monthly billing on a 12-month term, VAT included.

SaaS SKU / on-prem suffix	Production runs / month	THB / month, VAT incl.	Deployment
zcrSOAR-500 **OP-500**	500	125,000	SaaS / On-premises
zcrSOAR-2K **OP-2K**	2,000	250,000	SaaS / On-premises
zcrSOAR-10K **OP-10K**	10,000	450,000	SaaS / On-premises
zcrSOAR-50K **OP-50K**	50,000	580,000	SaaS / On-premises

On-premises SKU: zcrSOAR-OP-500 / zcrSOAR-OP-2K / zcrSOAR-OP-10K / zcrSOAR-OP-50K

Size the deployment with your partner

One run is one production execution of an automation. Playbooks, integrations, tenants and users are unlimited on every package.

For volumes between the listed packages, an approved partner prepares a scope-based quotation. Do not calculate a binding price from a marginal per-run rate.

> The quotation/SOW defines metering, usage above the package, package changes and the agreed support coverage.

An approved partner provides the quotation, contract, delivery and first-line support; zcr supports the partner. Installation and configuration are quoted separately by scope.

Current packages ↗

Plan deployment and ownership

On-premises is software on your own hardware or VMs; there is no zcrSOAR appliance. Installation and configuration are quoted separately from the subscription, by scope. Equal pricing reflects no hosted-storage discount and the upgrade/connector support work of self-managed deployment.

> zcrSOAR can be bought independently; neither zcrSIEM nor zcrLog is required.

zcrSOAR FAQ

How does zcrSOAR decide which playbook actions run automatically?

Each playbook step is set to Autonomous, Approval, or Blocked. Autonomous steps run immediately; Approval steps wait for a role-gated sign-off; Blocked steps never run until the gating changes.

Can zcrSOAR generate new playbooks?

Yes — an AI assistant can draft a playbook from a prompt for review, and a playbook definition can also be imported directly as YAML or JSON.

Does zcrSOAR require zcrSIEM?

No. zcrSOAR connects to zcrSIEM as a bidirectional bridge when both are deployed, and it can also ingest from other connected sources such as an EDR platform — it is not limited to zcrSIEM alone.

How does zcrSOAR track SLA compliance?

Notify and Respond SLA are tracked separately, by case severity, against a compliance target, with mean time to acknowledge and mean time to respond, plus a breach list for cases that missed SLA.

Evaluate with an approved partner

Bring monthly production-run volumes, connected source tools, approval owners and the intended deployment. Ask the partner for package sizing, metering definitions, support coverage and implementation responsibilities.

Your approved partner scopes the proposal, quotation, contract and delivery.

Contact a partner ↗ Current packages ↗ Product resources ↗