Managed security service · Delivered through approved partners

zcrMDR

Managed Detection & Response

zcrMDR is a Managed Detection and Response service for Thailand and ASEAN teams, turning zcr platform signals into actionable, human-reviewed alerts.

Organisations starting managed detection · IT and security teams · MSPs and MSSPs · Customers needing clear monthly reporting

Teams often have the data but lack time to continuously review alerts, prioritise activity, and explain security events to stakeholders.

Alerts reviewed for your team

Triage alerts from signals collected in zcrSIEM so your team can review the next step.

Follow service cases

Track cases through FWTicket, zcr's customer portal included in the service.

A record for service reviews

Use automated monthly reports to review service activity with your partner.

MDR or SOC: choose by operating scope

Both cover alert operations and reporting. Agree the scope with your approved partner to avoid overlapping work.

	Service scope	Required platform	Delivered records
zcrMDR	Alert triage and reporting; Complete adds remote response by the partner after customer approval.	zcrSIEM	Monthly reports · FWTicket case tracking
zcrSOC	Monitoring and triage; Response adds response coordination, escalation and incident-response support.	Essential: zcrSIEM · Response: zcrSIEM + zcrSOAR	Monthly reports · weekly shift handoff · FWTicket

Choose the zcrMDR edition

ZCR SERVICE FOUNDATION	zcrMDR runs on zcrSIEM; customer-owned EDR is not required.
PREREQUISITES	zcrMDR runs on zcrSIEM. Event retention follows the customer's zcrSIEM plan (90 days on zcrSIEM SaaS tiers; unlimited on zcrSIEM on-premises tiers, on your own storage). Your partner's quotation lists which platform licences the service includes.

The partner's quotation explicitly lists which platform licences are included.

Two service levels separate alert-and-report operations from active response and incident-response support.

	zcrMDR Essential MDR · ESSENTIAL	**zcrMDR Complete** MDR · COMPLETE +IR
Focus	Detection and reporting	Essential plus active response
Includes	• Alert triage and automated monthly report • FWTicket customer portal • No SOCRadar or CVE-check portal scope	• All Essential alert and reporting services • Active response and incident-response support • Response commitments aligned to selected SLA > Complete only: remote actions by the approved partner after customer approval only; no on-site component.
Platform	zcrSIEM: Centralise zcr signals in zcrSIEM before MDR analysts triage and act. Event retention follows the customer's zcrSIEM plan (90 days on zcrSIEM SaaS tiers; unlimited on zcrSIEM on-premises tiers, on your own storage).	

SERVICE COVERAGE

The same zcrMDR service can be contracted for 8×5, 16×5, or 24×7 coverage.

8×5 coverage	Business-hours managed detection, alerting, and monthly reporting.
16×5 coverage	Extended weekday coverage for organisations with longer operating hours.
24×7 coverage	Round-the-clock coverage aligned to the agreed service scope.

Conceptual map: signals to service records

01
Security signals in zcrSIEM

02
Alert triage

03
FWTicket case tracking + automated monthly reports

Conceptual map of confirmed service scope, not a report excerpt or system architecture. Delivery details follow the partner SOW.

Illustrative sample, not customer data



Sample report cover for format context; not customer data or evidence of service results. Open original capture ↗

- zcr-powered detection and alerting
- Automated monthly reporting
- FWTicket customer portal
- 8×5, 16×5, or 24×7 SLA coverage

Case tracking uses the FWTicket customer portal, run by zcr and included in the service.

zcrMDR: detection to documented action

01 Detect
Security signals collected in zcrSIEM become actionable alerts.

02 Triage
MDR validates severity, scope, and next action.

03
Respond · Complete only
Your approved partner provides remote response and incident-response support after customer approval, within the agreed scope.

04 Report
FWTicket and monthly reports close the operating loop.

> Complete only: remote actions by the approved partner after customer approval only; no on-site component.

zcrMDR FAQ

What is included in zcrMDR Essential?

It includes zcr-powered detection and alerting, automated monthly reporting, the FWTicket customer portal, and zcrSIEM event retention on the customer's zcrSIEM plan (90 days on zcrSIEM SaaS tiers; unlimited on zcrSIEM on-premises tiers, on your own storage).

Which service hours are available?

Choose 8×5, 16×5, or 24×7 coverage in the applicable SLA and statement of work.

What does zcrMDR Complete's active response cover?

Response actions are remote. Your channel partner takes them only after you approve, and zcrMDR Complete has no on-site component.

Conceptual responsibility handoff

01

Platform · zcrSIEM

Collect security signals for detection and alerting.

02

Approved partner · triage and case tracking

Triage alerts; track cases through the included FWTicket portal.

03

Customer + partner · scope agreement

Define approvers, access, execution, escalation and closure duties in the SOW.

Conceptual roles, not an execution sequence. Agree responsibilities and permissions in the SOW before service starts.

Coverage, service levels (SLA), scope and execution permissions follow the partner's agreement and SOW.

Your approved channel partner provides first-line support; zcr provides product support to that partner.

Delivered by an approved zcr.ai channel partner. Coverage hours and service levels are set in that partner's service agreement.

Prepare a scoped service evaluation

Source inventory and current or planned zcrSIEM plan. · Preferred service edition and coverage hours. · Incident contacts, approvers and access boundaries to discuss.

Quotation: service edition, platform plan and explicitly included licences.

SOW: scope, coverage, SLA, responsibilities, approvals, execution permissions, escalation and closure.

Review your scope with an approved zcr.ai channel partner ↗