Managed security service · Delivered through approved partners

zcrSOC

SOC-as-a-Service

zcrSOC is a complete managed security operations service for alert triage, response coordination, and monthly incident reporting for Thai and ASEAN teams.

Organisations needing managed response coordination · Security and IT operations teams · MSPs and MSSPs · Customers with extended operating hours

When an incident is confirmed, teams need clear escalation, accountable response coordination, and a record of what happened.

01 Monitor
zcrSIEM turns security telemetry into alerts.

02 Investigate
SOC validates severity, scope, and ownership.

03 Coordinate
zcrSOC
Response only
Response escalates and coordinates IR support under the SLA.

04 Improve
FWTicket and monthly reporting close the operating loop.

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 zcrSOC operating tier

ZCR SERVICE FOUNDATION	Essential: requires zcrSIEM · Response: requires zcrSIEM + zcrSOAR
PREREQUISITES	zcrSOC Essential runs on zcrSIEM; zcrSOC Response runs on zcrSIEM + zcrSOAR. 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.

Essential covers analyst monitoring and triage; Response adds coordinated response, escalation, and IR support.

	zcrSOC Essential SOC · ESSENTIAL	**zcrSOC Response** SOC · RESPONSE
Focus	Monitoring and triage	Coordinated response workflow
Includes	• Continuous monitoring, alert triage, and monthly report • Sized by 1 / 3 / 5 / 10 GB per day on zcrSIEM SaaS (90-day retention), or 20 GB per day on zcrSIEM On-premises (unlimited retention on your own storage) • Weekly shift handoff report	• Essential monitoring plus coordinated response • Escalation, IR support, and executive-ready reporting • Sized by the same 1 / 3 / 5 / 10 / 20 GB/day ladder as Essential • Weekly shift handoff report
Platform	Requires zcrSIEM as the detection foundation	Requires zcrSIEM + zcrSOAR

> Response coordinates within the SOW; agree approvers, execution permissions and closure duties with your partner.

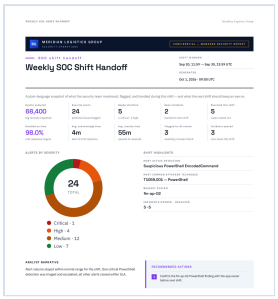
SERVICE COVERAGE

Workload-sized SOC operations can be aligned to 8×5, 16×5, or 24×7 coverage.

8×5 coverage	Business-hours security operations coverage.
16×5 coverage	Extended weekday security operations coverage.
24×7 coverage	Round-the-clock managed operations aligned to the agreed service scope.

Carry context into the next shift

Illustrative sample, not customer data



Illustrative sample, not customer data. Enlarged original English analyst notes and recommendation, with explanatory callouts. Open original capture ↗

- Alert acknowledgement and triage
- Response coordination and escalation (zcrSOC Response only)
- Automated monthly incident reporting
- 8×5, 16×5, or 24×7 SLA coverage

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

ANALYST NARRATIVE

Alert volume stayed within normal range for the shift. One critical PowerShell detection was triaged and escalated; all other alerts closed within SLA.

Original sample text (English)

Alert volume stayed within normal range for the shift. One critical PowerShell detection was triaged and escalated; all other alerts closed within SLA.

Analyst notes explain what was triaged and escalated. Illustrative sample, not customer data Open original capture ↗

RECOMMENDED ACTIONS

1 Confirm the fin-ap-02 PowerShell finding with the app owner before next shift.

Original sample text (English)

Confirm the fin-ap-02 PowerShell finding with the app owner before next shift.

Next-shift follow-up: confirm the finding with the app owner. Illustrative sample, not customer data Open original capture ↗

> Response coordinates within the SOW; agree approvers, execution permissions and closure duties with your partner.

zcrSOC FAQ

What's the difference between zcrSOC Essential and Response?

Essential covers alert acknowledgement, triage, and monthly reporting on top of zcrSIEM. Response adds coordinated response, escalation, and IR support on top of zcrSIEM + zcrSOAR. In both, event retention follows the customer's zcrSIEM plan (90 days on zcrSIEM SaaS tiers; unlimited on zcrSIEM on-premises tiers, on your own storage).

Can zcrSOC support 24×7 operations?

Yes. 8×5, 16×5, and 24×7 service coverage are available under the applicable SLA and statement of work.

Is zcrSOC available through partners?

Yes. zcrSOC is delivered only by an approved zcr.ai channel partner; coverage hours and service levels are set in that partner's service agreement.

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 ↗