

Managed service

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.

BUILT FOR	Organisations needing managed response coordination · Security and IT operations teams · MSPs and MSSPs · Customers with extended operating hours
THE OPERATING GAP	When an incident is confirmed, teams need clear escalation, accountable response coordination, and a record of what happened.
ZCR SERVICE FOUNDATION	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.
CASE TRACKING	Case tracking uses the FWTicket customer portal, run by zcr and included in the service.
SERVICE DELIVERY	Delivered by an approved zcr.ai channel partner. Coverage hours and service levels are set in that partner's service agreement.

CORE CAPABILITIES

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

zcrSOC: managed operations from signal to resolution

The operating loop that turns security telemetry into accountable triage, escalation, response, and improvement.

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.

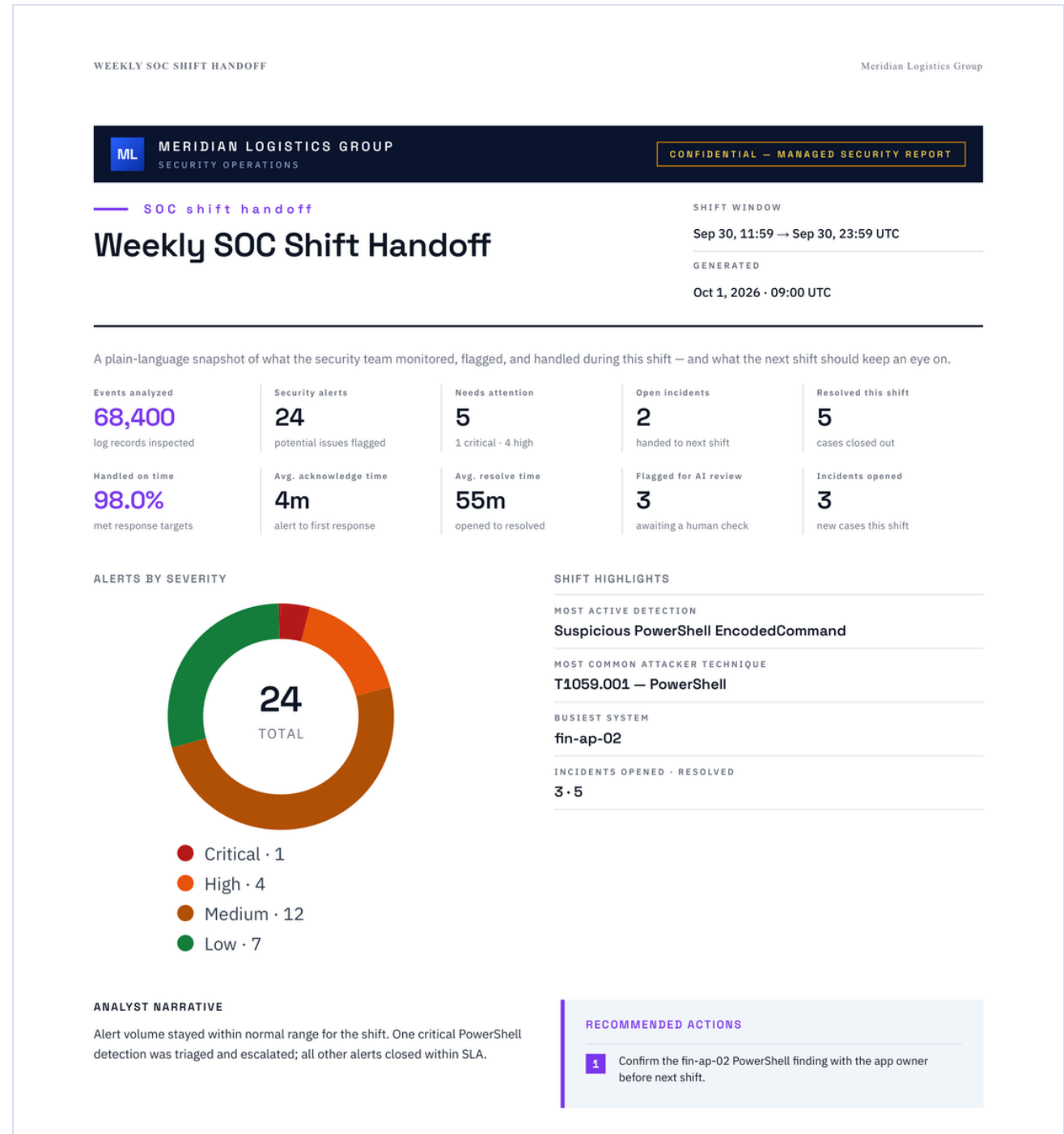
04 Improve

FWTicket and monthly reporting close the operating loop.

Choose the zcrSOC operating tier

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



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.

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.

Response with clear accountability

zcrSOC brings alert handling, escalation, and incident reporting into a managed operating model.

Talk to a zcr.ai channel partner

Talk to a zcr.ai channel partner about the coverage and SLA that fit your organisation.

Contact a channel partner ↗

zcr.ai/contact/?lng=en