

Managed service

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.

BUILT FOR	Organisations starting managed detection · IT and security teams · MSPs and MSSPs · Customers needing clear monthly reporting
THE OPERATING GAP	Teams often have the data but lack time to continuously review alerts, prioritise activity, and explain security events to stakeholders.
ZCR SERVICE FOUNDATION	zcrSIEM
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.
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

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

zcrMDR: detection to documented action

The operating loop that turns security signals collected in zcrSIEM into triage, response, and a customer-ready record.

01 Detect

Security signals collected in zcrSIEM become actionable alerts.

02 Triage

MDR validates severity, scope, and next action.

03 Respond zcrMDR Complete only

Complete coordinates active response and IR (incident response) support.

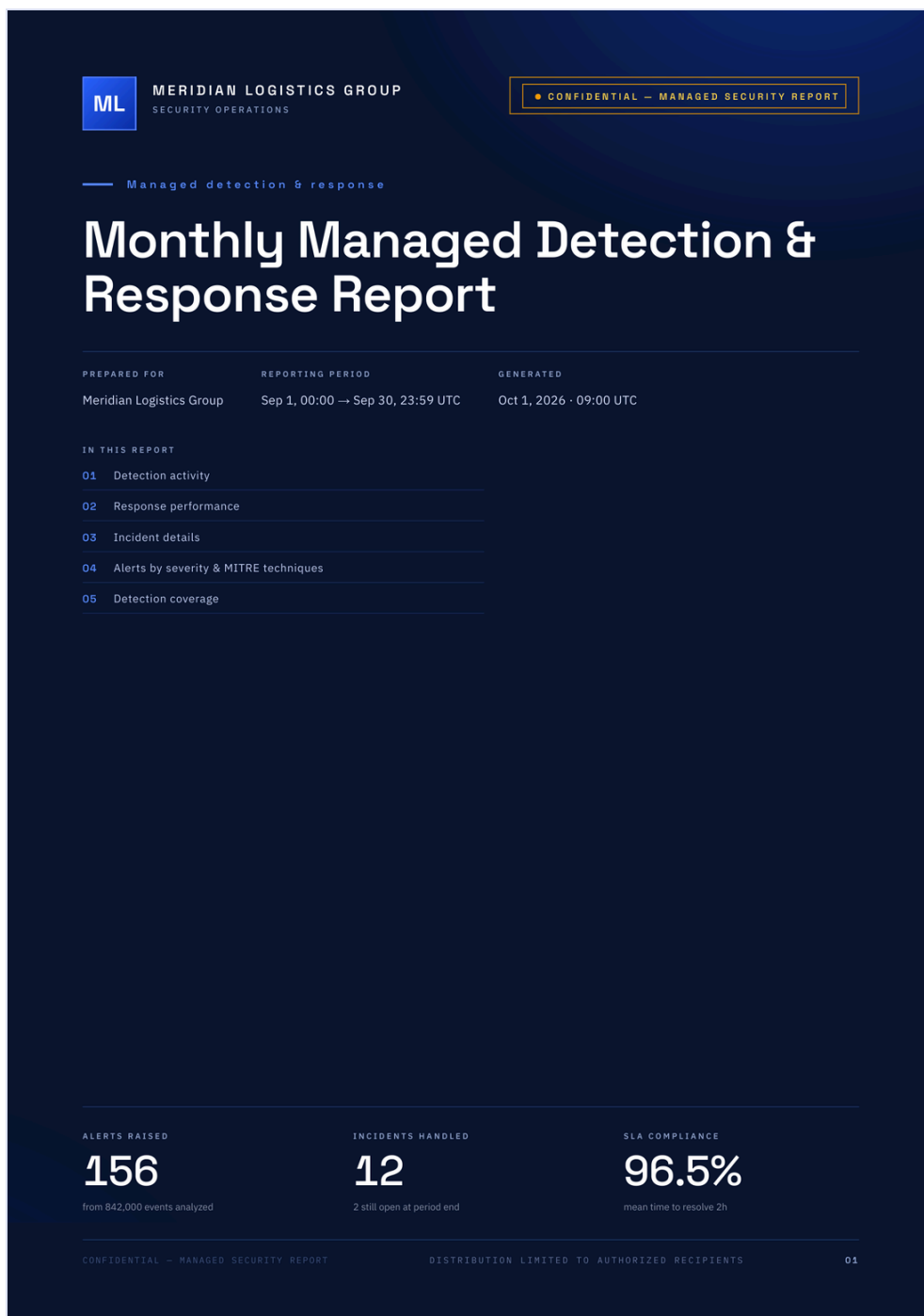
04 Report

FWTicket and monthly reports close the operating loop.

Choose the zcrMDR edition

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
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).	



Monthly service report. A sample managed detection & response report — showing the shape of SLA performance, incident counts, and response-time reporting. (Illustrative sample, not customer data)

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.

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.

Detection with a clear operating record

zcrMDR helps teams retain event context, review alerts, and communicate service activity through consistent reporting.

Talk to a zcr.ai channel partner

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

Contact a channel partner ↗

zcr.ai/contact/?lng=en