

บริการแบบ managed

zcrSOC

SOC-as-a-Service

บริการจัดการ security operations แบบครบถ้วนสำหรับทีม security ในไทยและอาเซียน รับทราบ Alert คัดกรอง ประสานการตอบสนอง และรายงาน Incident ประจำเดือนอัตโนมัติ

เหมาะสำหรับ	องค์กรที่ต้องการการประสานงานตอบสนองแบบ managed · ทีม security operations และ IT · MSP และ MSSP · ลูกค้าที่มีเวลาทำการยาวนาน
โจทย์ที่ต้องแก้	เมื่อยืนยัน Incident แล้ว ทีมต้องมีการยกระดับเหตุ การประสานงานตอบสนองที่ชัดเจน และบันทึกสิ่งที่เกิดขึ้น
พื้นฐานบริการ zcr	zcrSIEM + zcrSOAR
สิ่งที่ต้องมี	zcrSOC Essential ทำงานบน zcrSIEM ส่วน zcrSOC Response ทำงานบน zcrSIEM + zcrSOAR ระยะเวลาเก็บข้อมูลเหตุการณ์เป็นไปตามแพ็คเกจ zcrSIEM ของลูกค้า (แพ็คเกจ zcrSIEM แบบ SaaS เก็บ 90 วัน ส่วนแพ็คเกจ zcrSIEM แบบ On-Premises เก็บไม่จำกัด ตามพื้นที่จัดเก็บของคุณเอง) ใบเสนอราคาของพาร์กเนอร์จะระบุค่าบริการรวมไลเซนส์แพลตฟอร์มได้ไว้บ้าง
การติดตามเคส	การติดตามเคสใช้ FWTicket customer portal ซึ่ง zcr เป็นผู้ดูแลและรวมอยู่ในบริการ
การให้บริการ	ให้บริการโดย channel partner ที่ได้รับอนุมัติจาก zcr.ai ช่วงเวลาดูแลและระดับบริการกำหนดไว้ในสัญญาบริการของพาร์กเนอร์รายนั้น

ความสามารถหลัก

- รับทราบและคัดกรอง Alert
- ประสานการตอบสนองและยกระดับเหตุ (เฉพาะ zcrSOC Response)
- รายงาน Incident ประจำเดือนอัตโนมัติ
- SLA 8 × 5, 16 × 5 หรือ 24 × 7

zcrSOC: การปฏิบัติการแบบ managed จากสัญญาณสู่การแก้ไข

วงจรที่เปลี่ยนข้อมูลความปลอดภัยเป็นการคัดกรอง การยกระดับเหตุ การตอบสนอง และการปรับปรุงที่มี
เจ้าภาพ

01 เฝ้าระวัง

zcrSIEM เปลี่ยนข้อมูลความปลอดภัยเป็น Alert

02 สืบสวน

SOC ตรวจสอบความรุนแรง ขอบเขต และผู้รับผิดชอบ

03 ประสานงาน เฉพาะ zcrSOC Response

Response ยกระดับเหตุและประสาน IR ตาม SLA

04 ปรับปรุง

FWTicket และรายงานรายเดือนทำให้วงจรการปฏิบัติงานครบถ้วน

เลือก tier การปฏิบัติการของ zcrSOC

Essential ครอบคลุมการเฝ้าระวังและคัดกรองโดยนักวิเคราะห์ ส่วน Response เพิ่มการประสานตอบ
สนอง การยกระดับเหตุ และการสนับสนุน IR

	zcrSOC Essential SOC · ESSENTIAL	zcrSOC Response SOC · RESPONSE
จุดเน้น	การเฝ้าระวังและคัดกรอง	response workflow แบบประสานงาน
สิ่งที่รวมอยู่	- เฝ้าระวัง คัดกรอง Alert และรายงานประจำเดือน - คิดตามขนาด 1 / 3 / 5 / 10 GB ต่อวันบน zcrSIEM SaaS (เก็บข้อมูล 90 วัน) หรือ 20 GB ต่อวันบน zcrSIEM แบบ On-Premises (เก็บข้อมูลไม่จำกัด ตามพื้นที่จัดเก็บของคุณเอง) - รายงานส่งเวรรายสัปดาห์	- การเฝ้าระวัง Essential พร้อมการประสานตอบสนอง - ยกระดับเหตุ สนับสนุน IR และรายงานสำหรับผู้บริหาร - คิดตามขนาดเดียวกับ Essential คือ 1 / 3 / 5 / 10 / 20 GB ต่อวัน - รายงานส่งเวรรายสัปดาห์
แพลตฟอร์ม	ต้องใช้ zcrSIEM เป็นพื้นฐานการตรวจจับ	ต้องใช้ zcrSIEM + zcrSOAR

ML

MERIDIAN LOGISTICS GROUP

SECURITY OPERATIONS

CONFIDENTIAL — MANAGED SECURITY REPORT

SOC shift handoff

Weekly SOC Shift Handoff

SHIFT WINDOW

Sep 30, 11:59 → Sep 30, 23:59 UTC

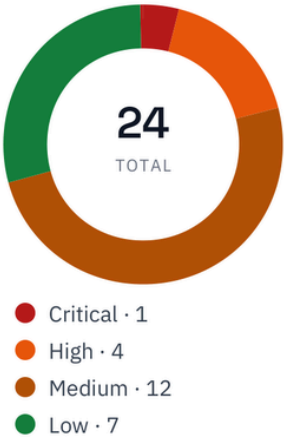
GENERATED

Oct 1, 2026 · 09:00 UTC

A plain-language snapshot of what the security team monitored, flagged, and handled during this shift — and what the next shift should keep an eye on.

Events analyzed 68,400 log records inspected	Security alerts 24 potential issues flagged	Needs attention 5 1 critical · 4 high	Open incidents 2 handed to next shift	Resolved this shift 5 cases closed out
Handled on time 98.0% met response targets	Avg. acknowledge time 4m alert to first response	Avg. resolve time 55m opened to resolved	Flagged for AI review 3 awaiting a human check	Incidents opened 3 new cases this shift

ALERTS BY SEVERITY



SHIFT HIGHLIGHTS

MOST ACTIVE DETECTION	Suspicious PowerShell EncodedCommand
MOST COMMON ATTACKER TECHNIQUE	T1059.001 — PowerShell
BUSIEST SYSTEM	fin-ap-02
INCIDENTS OPENED · RESOLVED	3 · 5

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.

RECOMMENDED ACTIONS

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

รายงานส่งต่อจะ: ตัวอย่างรายงานส่งต่อของทีม SOC — สรุประดับความรุนแรงของ alert ตัวชี้วัดการตอบสนอง และบันทึกส่งต่อให้กะถัดไป (ตัวอย่างประกอบ ไม่ใช่ข้อมูลลูกค้าจริง)

คำถามที่พบบ่อย zcrSOC

zcrSOC Essential กับ Response ต่างกันอย่างไร?

Essential ครอบคลุมการรับทราบ คัดกรอง Alert และรายงานประจำเดือนบน zcrSIEM ส่วน Response เพิ่มการประสานตอบสนอง ยกระดับเหตุ และสนับสนุน IR บน zcrSIEM + zcrSOAR ทั้งสองระดับมีระยะเวลาเก็บข้อมูลเหตุการณ์เป็นไปตามแพ็คเกจ zcrSIEM ของลูกค้า (แพ็คเกจ zcrSIEM แบบ SaaS เก็บ 90 วัน ส่วนแพ็คเกจ zcrSIEM แบบ On-Premises เก็บไม่จำกัด ตามพื้นที่จัดเก็บของตนเอง)

zcrSOC รองรับการทำงาน 24 × 7 หรือไม่?

รองรับ โดยเลือกความครอบคลุม 8 × 5, 16 × 5 หรือ 24 × 7 ตาม SLA และ statement of work ที่เกี่ยวข้อง

zcrSOC ให้บริการผ่าน partner หรือไม่?

ใช่ zcrSOC ให้บริการผ่าน channel partner ที่ได้รับอนุมัติจาก zcr.ai เท่านั้น โดยช่วงเวลาดูแลและระดับบริการกำหนดไว้ในสัญญาบริการของพาร์ตเนอร์รายนั้น

ช่วงเวลาการให้บริการ

การปฏิบัติการ SOC ที่คิดตาม workload ปรับให้ตรงกับความครอบคลุม 8 × 5, 16 × 5 หรือ 24 × 7 ได้

ช่วงเวลาดูแล 8 × 5	ความครอบคลุม security operations ในเวลาทำการ
ช่วงเวลาดูแล 16 × 5	ความครอบคลุม security operations แบบขยายเวลาในวันทำงาน
ช่วงเวลาดูแล 24 × 7	Managed operations ตลอดเวลาตามขอบเขตบริการที่ตกลงกัน

ตอบสนองด้วยความรับผิดชอบที่ชัดเจน

zcrSOC รวมการดูแล Alert การยกระดับเหตุ และรายงาน Incident ไว้ในรูปแบบการปฏิบัติงานแบบ managed

คุยกับ channel partner ของ zcr.ai

คุยกับ channel partner ของ zcr.ai เพื่อเลือกระดับบริการและ SLA ที่เหมาะกับองค์กร

ติดต่อ channel partner ↗

zcr.ai/contact/