บริการดูแลความปลอดภัย · ส่งมอบผ่านพาร์ทเนอร์ที่ได้รับอนุมัติ

zcrSOC

SOC-as-a-Service

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

องค์กรที่ต้องการการประสานงานตอบสนองแบบ managed · ทีม security operations และ IT · MSP และ MSSP · ลูกค้าที่มีเวลาทำการยาวนาน

เมื่อยืนยัน Incident แล้ว ทีมต้องมีการยกระดับเหตุ การประสานงานตอบสนองที่ชัดเจน และบันทึกสิ่งที่เกิดขึ้น

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

MDR หรือ SOC: เลือกจากขอบเขตงาน

ทั้งสองบริการดูแลการแจ้งเตือนและรายงาน ร่วมกำหนดขอบเขตกับพาร์ทเนอร์ที่ได้รับอนุมัติเพื่อเลี่ยงงานซ้ำซ้อน

	ขอบเขตบริการ	แพลตฟอร์มที่ต้องใช้	สิ่งที่ส่งมอบ
zcrMDR	คัดกรองการแจ้งเตือนและรายงาน; Complete เพิ่มการตอบสนองทางไกลโดยพาร์ทเนอร์ หลังลูกค้าอนุมัติ	zcrSIEM	รายงานรายเดือน · ติดตามเคสผ่าน FWTicket
zcrSOC	เฝ้าระวังและคัดกรอง; Response เพิ่มการประสานตอบสนอง ยกระดับเหตุ และสนับสนุนการรับมือเหตุการณ์	Essential: zcrSIEM · Response: zcrSIEM + zcrSOAR	รายงานรายเดือน · รายงานส่งเวรรายสัปดาห์ · FWTicket

เลือก tier การปฏิบัติการของ zcrSOC

พื้นฐานบริการ zcr	Essential: ต้องใช้ zcrSIEM · Response: ต้องใช้ zcrSIEM + zcrSOAR
สิ่งที่ต้องมี	zcrSOC Essential ทำงานบน zcrSIEM ส่วน zcrSOC Response ทำงานบน zcrSIEM + zcrSOAR ระยะเวลาเก็บข้อมูลเหตุการณ์เป็นไปตามแพ็กเกจ zcrSIEM ของลูกค้า (แพ็กเกจ zcrSIEM แบบ SaaS เก็บ 90 วัน ส่วนแพ็กเกจ zcrSIEM แบบ On-Premises เก็บไม่จำกัด ตามพื้นที่จัดเก็บของคุณเอง) ใบเสนอราคาของพาร์ทเนอร์จะระบุว่าบริการรวมไลเซนส์แพลตฟอร์มใดไว้บ้าง

ใบเสนอราคาของพาร์ทเนอร์ระบุชัดว่ารวมไลเซนส์แพลตฟอร์มใดบ้าง

Essential ครอบคลุมการเฝ้าระวังและคัดกรองโดยนักวิเคราะห์ ส่วน Response เพิ่มการประสานตอบสนอง 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

> Response ประสานการตอบสนองตาม SOW; ผู้อนุมัติ ผู้มีสิทธิ์ดำเนินการ และผู้ยืนยันปิดเคสต้องตกลงกับพาร์ทเนอร์

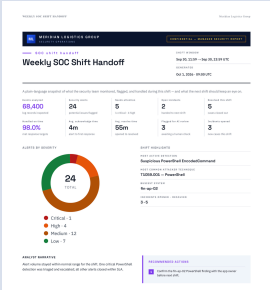
ช่วงเวลาการให้บริการ

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

ส่งต่องานพร้อมบันทึก

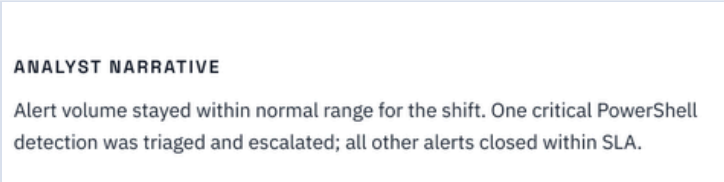
ตัวอย่างประกอบ ไม่ใช่ข้อมูลลูกค้าจริง



ตัวอย่างประกอบ ไม่ใช่ข้อมูลลูกค้าจริง ขยายบันทึกผู้วิเคราะห์และข้อเสนอแนะภาษาอังกฤษเดิม พร้อมคำอธิบายภาษาไทย เปิดภาพต้นฉบับ ↗

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

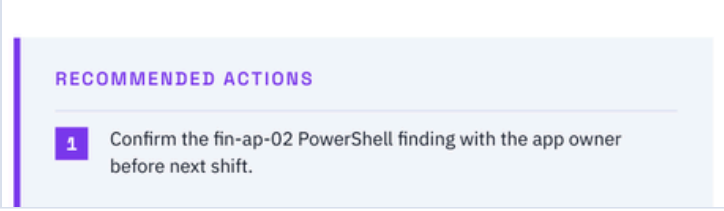
การติดตามเคสใช้ FWTicket customer portal ซึ่ง zcr เป็นผู้ดูแลและรวมอยู่ในบริการ



ข้อความจากต้นฉบับตัวอย่าง (ภาษาอังกฤษ)

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

บันทึกผู้วิเคราะห์สรุปสิ่งที่คัดกรองและยกระดับเหตุ ตัวอย่างประกอบ ไม่ใช่ข้อมูลลูกค้าจริง เปิดภาพต้นฉบับ ↗



ข้อความจากต้นฉบับตัวอย่าง (ภาษาอังกฤษ)

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

งานต่อกะถัดไป: ยืนยันสิ่งที่ตรวจพบกับเจ้าของแอปพลิเคชัน ตัวอย่างประกอบ ไม่ใช่ข้อมูลลูกค้าจริง เปิดภาพต้นฉบับ ↗

> Response ประสานการตอบสนองตาม SOW; ผู้อนุมัติ ผู้มีสิทธิ์ดำเนินการ และผู้ยืนยันปิดเคสต้องตกลงกับพาร์ทเนอร์

คำถามที่พบบ่อย zcrSOC

zcrSOC Essential กับ Response ต่างกันอย่างไร?

Essential ครอบคลุมการรับทราบ คัดกรอง Alert และรายงานประจำเดือนบน zcrSIEM ส่วน Response เพิ่มการประสานตอบสนอง ยกระดับเหตุ และสนับสนุน IR บน zcrSIEM + zcrSOAR ทั้งสองระดับมีระยะเวลาเก็บข้อมูลเหตุการณ์เป็นไปตามแพ็กเกจ zcrSIEM ของลูกค้า (แพ็กเกจ zcrSIEM แบบ SaaS เก็บ 90 วัน ส่วนแพ็กเกจ zcrSIEM แบบ On-Premises เก็บไม่จำกัด ตามพื้นที่จัดเก็บของคุณเอง)

zcrSOC รองรับการดำเนินงาน 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 โดยช่วงเวลาดูแลและระดับบริการกำหนดไว้ในสัญญาบริการของพาร์ทเนอร์รายนั้น

แผนภาพแนวคิด: บทบาทและจุดส่งต่องาน

01

แพลตฟอร์ม · zcrSIEM

รวบรวมสัญญาณความปลอดภัยเพื่อการตรวจจับและแจ้งเตือน

02

พาร์ทเนอร์ที่ได้รับอนุมัติ · คัดกรองและติดตามเคส

คัดกรองการแจ้งเตือน ติดตามเคสผ่าน FWTicket ซึ่งรวมอยู่ในบริการ

03

ลูกค้า + พาร์ทเนอร์ · ข้อตกลงขอบเขตงาน

กำหนดผู้อนุมัติ สิทธิ์เข้าถึง ผู้ดำเนินการ การยกระดับเหตุ และผู้ยืนยันปิดเคสใน SOW

แผนภาพบทบาทเชิงแนวคิด ไม่ใช่ขั้นตอนสั่งดำเนินการ ต้องตกลงหน้าที่และสิทธิ์ใน SOW ก่อนเริ่มบริการ

ช่วงเวลาดูแล ระดับบริการ (SLA) ขอบเขตงาน และสิทธิ์ดำเนินการเป็นไปตามสัญญาและ SOW ของพาร์ทเนอร์

พาร์ทเนอร์ที่ได้รับอนุมัติของคุณเป็นผู้ให้การสนับสนุนด่านแรก โดย zcr สนับสนุนพาร์ทเนอร์ด้านผลิตภัณฑ์

ให้บริการโดย channel partner ที่ได้รับอนุมัติจาก zcr.ai ช่วงเวลาดูแลและระดับบริการกำหนดไว้ในสัญญาบริการของพาร์ทเนอร์รายนั้น

เตรียมข้อมูลเพื่อประเมินขอบเขตบริการ

รายการแหล่งข้อมูลและแพ็กเกจ zcrSIEM ที่ใช้อยู่หรือวางแผนใช้ · รุ่นบริการและช่วงเวลาดูแลที่ต้องการ · ผู้ติดต่อเมื่อเกิดเหตุ ผู้อนุมัติ และขอบเขตสิทธิ์เข้าถึงที่ต้องหารือ

ใบเสนอราคา: รุ่นบริการ แพ็กเกจแพลตฟอร์ม และไลเซนส์ที่รวมอยู่

SOW: ขอบเขต ช่วงเวลาดูแล SLA หน้าที่ การอนุมัติ สิทธิ์ดำเนินการ การยกระดับเหตุ และการปิดเคส

หารือขอบเขตกับพาร์ทเนอร์ที่ได้รับอนุมัติของ zcr.ai ↗