บริการดูแลความปลอดภัย · ส่งมอบผ่านพาร์ทเนอร์ที่ได้รับอนุมัติ

zcrMDR

Managed Detection & Response

บริการ MDR สำหรับทีม security ในไทยและอาเซียน เปลี่ยนสัญญาณจากแพลตฟอร์ม zcr ให้เป็น Alert ที่ดำเนินการต่อได้ พร้อมการทบทวนโดยผู้เชี่ยวชาญและรายงานที่ชัดเจน

องค์กรที่เริ่มใช้ managed detection · ทีม IT และความปลอดภัย · MSP และ MSSP · ลูกค้าที่ต้องการรายงานประจำเดือนชัดเจน

หลายทีมมีข้อมูลอยู่แล้วแต่ไม่มีเวลาตรวจสอบ Alert อย่างต่อเนื่อง จัดลำดับความสำคัญ และอธิบายเหตุการณ์ให้ผู้เกี่ยวข้องเข้าใจ

มีผู้คัดกรองการแจ้งเตือน

คัดกรองการแจ้งเตือนจากสัญญาณใน zcrSIEM ให้ทีมใช้พิจารณาขั้นตอนถัดไป

ติดตามเคสได้ผ่านพอร์ทัล

ติดตามเคสผ่าน FWTicket พอร์ทัลของ zcr ที่รวมอยู่ในบริการ

มีบันทึกสำหรับทบทวนบริการ

ใช้รายงานรายเดือนอัตโนมัติเป็นข้อมูลประกอบการทบทวนงานกับพาร์ทเนอร์

MDR หรือ SOC: เลือกจากขอบเขตงาน

ทั้งสองบริการดูแลการแจ้งเตือนและรายงาน ร่วมกำหนดขอบเขตกับพาร์ทเนอร์ที่ได้รับอนุมัติเพื่อเลี่ยงงานซ้ำซ้อน

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

เลือก edition ของ zcrMDR

พื้นฐานบริการ zcr	zcrMDR ทำงานบน zcrSIEM โดยไม่ต้องมี EDR ของลูกค้าเอง
สิ่งที่ต้องมี	zcrMDR ทำงานบน zcrSIEM ระยะเวลาเก็บหลักฐานเหตุการณ์เป็นไปตามแพ็กเกจ zcrSIEM ของลูกค้า (แพ็กเกจ zcrSIEM แบบ SaaS เก็บ 90 วัน ส่วนแพ็กเกจ zcrSIEM แบบ On-Premises เก็บไม่จำกัด ตามพื้นที่จัดเก็บของคุณเอง) ใบเสนอราคาของพาร์ทเนอร์จะระบุว่าบริการรวมไลเซนส์แพลตฟอร์มใดไว้บ้าง

ใบเสนอราคาของพาร์ทเนอร์ระบุชัดว่ารวมไลเซนส์แพลตฟอร์มใดบ้าง

สองระดับบริการแยกงาน Alert และรายงานออกจาก active response และการสนับสนุน incident response

	zcrMDR Essential MDR · ESSENTIAL	zcrMDR Complete MDR · COMPLETE +IR
จุดเน้น	การตรวจจับและรายงาน	Essential พร้อม active response
สิ่งที่รวมอยู่	• คัดกรอง Alert และรายงานประจำเดือนอัตโนมัติ • FWTicket customer portal • ไม่รวม SOCRadar หรือขอบเขต CVE-check บน portal	• รวมบริการ Alert และรายงานของ Essential • active response และการสนับสนุน incident response • ข้อตกลงการตอบสนองตาม SLA ที่เลือก เฉพาะ Complete: ดำเนินการทางไกลโดยพาร์ทเนอร์ที่ได้รับอนุมัติ หลังลูกค้าอนุมัติเท่านั้น ไม่รวมการเข้าหน้างาน
แพลตฟอร์ม	zcrSIEM: รวมสัญญาณจาก zcr ไว้ใน zcrSIEM ก่อนที่นักวิเคราะห์ MDR จะคัดกรองและดำเนินการ ระยะเวลาเก็บหลักฐานเหตุการณ์เป็นไปตามแพ็กเกจ zcrSIEM ของลูกค้า (แพ็กเกจ zcrSIEM แบบ SaaS เก็บ 90 วัน ส่วนแพ็กเกจ zcrSIEM แบบ On-Premises เก็บไม่จำกัด ตามพื้นที่จัดเก็บของคุณเอง)	

ช่วงเวลาการให้บริการ

บริการ zcrMDR เดียวกันเลือกทำสัญญาความครอบคลุม 8 × 5, 16 × 5 หรือ 24 × 7 ได้

ช่วงเวลาดูแล 8 × 5	Managed detection แจ้งเตือน และรายงานประจำเดือนในเวลาทำการ
ช่วงเวลาดูแล 16 × 5	ครอบคลุมวันทำงานแบบขยายเวลาสำหรับองค์กรที่ทำงานนานขึ้น
ช่วงเวลาดูแล 24 × 7	ความครอบคลุมตลอดเวลาตามขอบเขตบริการที่ตกลงกัน

แผนภาพแนวคิด: จากสัญญาณสู่บันทึกบริการ

01
สัญญาณความปลอดภัยใน zcrSIEM

02
คัดกรองการแจ้งเตือน

03
ติดตามเคสผ่าน FWTicket + รายงานรายเดือนอัตโนมัติ

แผนภาพแนวคิดจากขอบเขตบริการที่ยืนยันแล้ว ไม่ใช่หน้ารายงานหรือสถาปัตยกรรมระบบ รายละเอียดการส่งมอบเป็นไปตาม SOW

ตัวอย่างประกอบ ไม่ใช่ข้อมูลลูกค้าจริง



ปกรายงานตัวอย่างเพื่อแสดงรูปแบบ ไม่ใช่ข้อมูลลูกค้าจริงหรือตัวเลขยืนยันผลบริการ เปิดภาพต้นฉบับ ↗

- การตรวจจับและแจ้งเตือนด้วย zcr
- รายงานประจำเดือนอัตโนมัติ
- FWTicket customer portal
- SLA 8 × 5, 16 × 5 หรือ 24 × 7

การติดตามเคสใช้ FWTicket customer portal ซึ่ง zcr เป็นผู้ดูแลและรวมอยู่ในบริการ

zcrMDR: จากการตรวจจับสู่การดำเนินการที่มีหลักฐาน

01 ตรวจจับ
สัญญาณความปลอดภัยที่รวบรวมใน zcrSIEM กลายเป็น Alert ที่ดำเนินการต่อได้

02 คัดกรอง
MDR ตรวจสอบความรุนแรง ขอบเขต และขั้นตอนถัดไป

03
ตอบสนอง · เฉพาะ Complete
พาร์ทเนอร์ที่ได้รับอนุมัติให้การตอบสนองทางไกลและสนับสนุนการรับมือเหตุการณ์ หลังลูกค้าอนุมัติ ตามขอบเขตที่ตกลงกัน

04 รายงาน
FWTicket และรายงานรายเดือนทำให้วงจรการปฏิบัติงานครบถ้วน

> เฉพาะ Complete: ดำเนินการทางไกลโดยพาร์ทเนอร์ที่ได้รับอนุมัติ หลังลูกค้าอนุมัติเท่านั้น ไม่รวมการเข้าหน้างาน

คำถามที่พบบ่อย zcrMDR

zcrMDR Essential มีอะไรบ้าง?

ประกอบด้วยการตรวจจับและแจ้งเตือนด้วย zcr รายงานประจำเดือนอัตโนมัติ FWTicket customer portal และการเก็บข้อมูลใน zcrSIEM ตามแพ็กเกจ zcrSIEM ของลูกค้า (แพ็กเกจ zcrSIEM แบบ SaaS เก็บ 90 วัน ส่วนแพ็กเกจ zcrSIEM แบบ On-Premises เก็บไม่จำกัด ตามพื้นที่จัดเก็บของคุณเอง)

เลือกเวลาบริการได้อย่างไร?

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

Active response ของ zcrMDR Complete ครอบคลุมอะไรบ้าง?

การดำเนินการตอบสนองทำจากระยะไกลทั้งหมด โดย channel partner ของคุณจะดำเนินการหลังจากที่คุณอนุมัติเท่านั้น zcrMDR Complete ไม่มีองค์ประกอบที่ต้องเข้าไปดำเนินการหน้างาน (on-site)

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 ↗