

บริการแบบ managed

zcrMDR

Managed Detection & Response

บริการ MDR สำหรับทีม security ในไทยและอาเซียน เปลี่ยนสัญญาณจากแพลตฟอร์ม zcr ให้เป็น Alert ที่ดำเนินการต่อได้ พร้อมการทบทวนโดยผู้เชี่ยวชาญและรายงานที่ชัดเจน

เหมาะสำหรับ	องค์กรที่เริ่มใช้ managed detection · ทีม IT และความปลอดภัย · MSP และ MSSP · ลูกค้าที่ต้องการรายงานประจำเดือนชัดเจน
โจทย์ที่ต้องแก้	หลายทีมมีข้อมูลอยู่แล้วแต่ไม่มีเวลาตรวจสอบ Alert อย่างต่อเนื่อง จัดลำดับความสำคัญและอธิบายเหตุการณ์ให้ผู้เกี่ยวข้องเข้าใจ
พื้นฐานบริการ zcr	zcrSIEM
สิ่งที่ต้องมี	zcrMDR ทำงานบน zcrSIEM ระยะเวลาเก็บหลักฐานเหตุการณ์เป็นไปตามแพ็คเกจ zcrSIEM ของลูกค้า (แพ็คเกจ zcrSIEM แบบ SaaS เก็บ 90 วัน ส่วนแพ็คเกจ zcrSIEM แบบ On-Premises เก็บไม่จำกัด ตามพื้นที่จัดเก็บของตนเอง) ใบเสนอราคาของพาร์กเนอร์จะระบุว่าบริการรวมไลเซนส์แพลตฟอร์มใดบ้าง
การติดตามเคส	การติดตามเคสใช้ FWTicket customer portal ซึ่ง zcr เป็นผู้ดูแลและรวมอยู่ในบริการ
การให้บริการ	ให้บริการโดย channel partner ที่ได้รับอนุมัติจาก zcr.ai ช่วงเวลาดูแลและระดับบริการกำหนดไว้ในสัญญาบริการของพาร์กเนอร์รายนั้น

ความสามารถหลัก

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

zcrMDR: จากการตรวจจับสู่การดำเนินการที่มีหลักฐาน

วงจรที่เปลี่ยนสัญญาณความปลอดภัยที่รวบรวมใน zcrSIEM เป็นการคัดกรอง การตอบสนอง และบันทึกที่พร้อมส่งให้ลูกค้า

01 ตรวจสอบ

สัญญาณความปลอดภัยที่รวบรวมใน zcrSIEM กลายเป็น Alert ที่ดำเนินการต่อได้

02 คัดกรอง

MDR ตรวจสอบความรุนแรง ขอบเขต และขั้นตอนถัดไป

03 ตอบสนอง

เฉพาะ zcrMDR Complete

Complete ประสาน active response และการสนับสนุน IR (incident response)

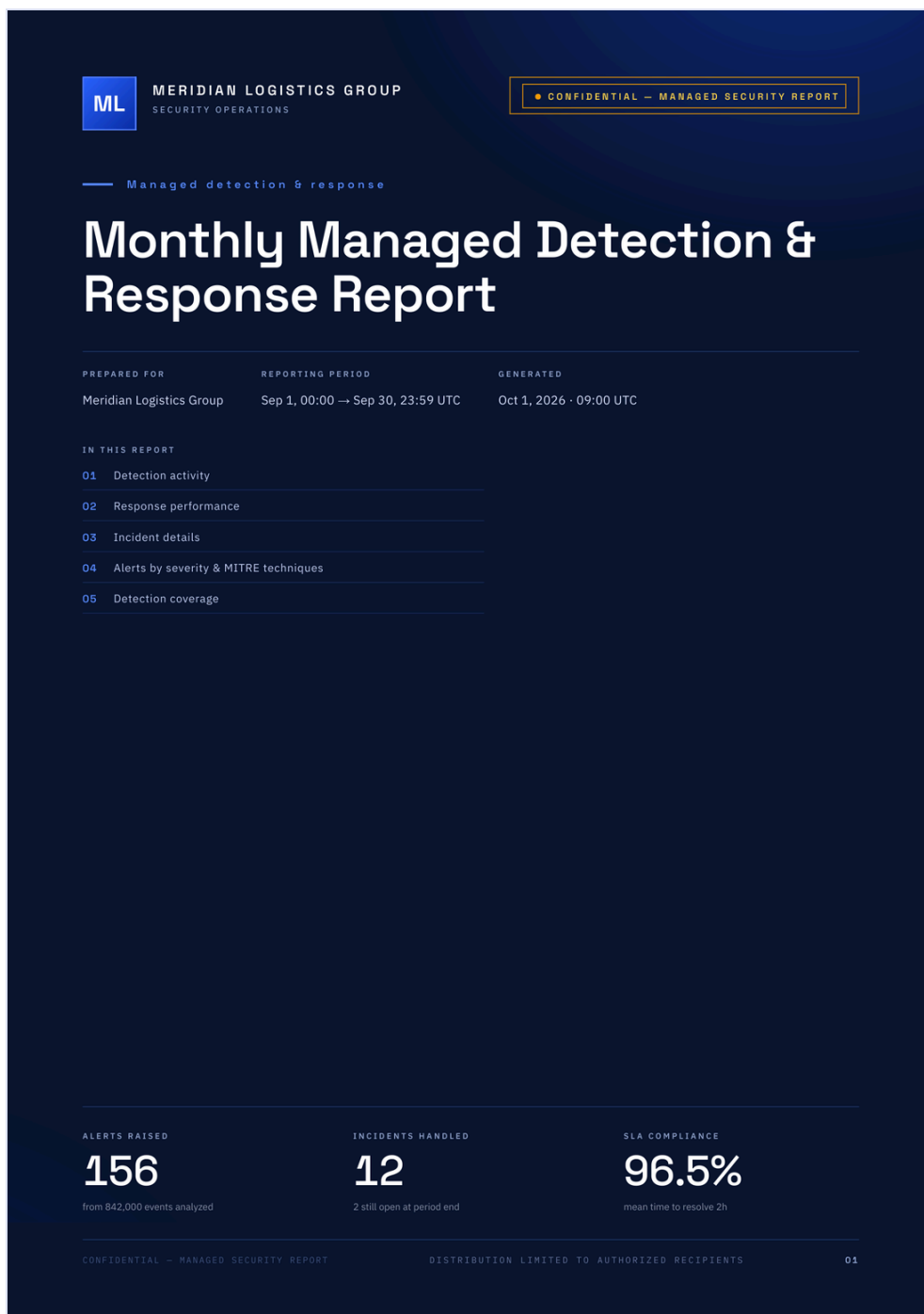
04 รายงาน

FWTicket และรายงานรายเดือนทำให้วงจรการปฏิบัติงานครบถ้วน

เลือก edition ของ zcrMDR

สองระดับบริการแยกงาน Alert และรายงานออกจาก active response และการสนับสนุน incident response

	zcrMDR Essential MDR · ESSENTIAL	zcrMDR Complete MDR · COMPLETE +IR
จุดเน้น	การตรวจจับและรายงาน	Essential พร้อม active response
สิ่งที่มีอยู่	- คัดกรอง Alert และรายงานประจำเดือนอัตโนมัติ - FWTicket customer portal - ไม่รวม SOCRadar หรือขอบเขต CVE-check uu portal	- รวมบริการ Alert และรายงานของ Essential - active response และการสนับสนุน incident response - ข้อตกลงการตอบสนองตาม SLA ที่เลือก
แพลตฟอร์ม	zcrSIEM: รวมสัญญาณจาก zcr ไว้ใน zcrSIEM ก่อนที่นักวิเคราะห์ MDR จะคัดกรองและดำเนินการระยะเวลาเก็บหลักฐานเหตุการณ์เป็นไปตามแพ็คเกจ zcrSIEM ของลูกค้า (แพ็คเกจ zcrSIEM แบบ SaaS เก็บ 90 วัน ส่วนแพ็คเกจ zcrSIEM แบบ On-Premises เก็บไม่จำกัด ตามพื้นที่จัดเก็บของคุณเอง)	



รายงานบริการรายเดือน: ตัวอย่างรูปแบบรายงาน MDR — แสดงโครงสร้างการรายงาน SLA จำนวน incident และเวลาตอบสนอง (ตัวอย่างประกอบ ไม่ใช่ข้อมูลลูกค้าจริง)

คำถามที่พบบ่อย zcrMDR

zcrMDR Essential มีอะไรบ้าง?

ประกอบด้วย การตรวจจับและแจ้งเตือนด้วย zcr รายงานประจำเดือนอัตโนมัติ FWTicket customer portal และการเก็บข้อมูลใน zcrSIEM ตามแพ็คเกจ zcrSIEM ของลูกค้า (แพ็คเกจ zcrSIEM แบบ SaaS เก็บ 90 วัน ส่วนแพ็คเกจ 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?

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

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

ตรวจจับพร้อมบันทึกการปฏิบัติงานที่ชัดเจน

zcrMDR ช่วยให้ทีมเก็บบริบทเหตุการณ์ ตรวจสอบ Alert และสื่อสารกิจกรรมบริการผ่านรายงานที่สม่ำเสมอ

คุยกับ channel partner ของ zcr.ai

คุยกับ channel partner ของ zcr.ai เพื่อเลือกระดับบริการและ SLA ที่ตรงกับเวลาทำการขององค์กร

ติดต่อ channel partner ↗

zcr.ai/contact/