CONTINUOUS THREAT EXPOSURE MANAGEMENT

zcrCTEM

มองเห็นความเสี่ยง จัดลำดับการรับมือให้ชัด

zcrCTEM เป็นแพลตฟอร์ม CTEM ที่รวม EASM สำหรับค้นหา attack surface, CAASM สำหรับหาช่องว่างที่เครื่องมือ security ยังครอบคลุมไม่ถึง และ DRP สำหรับติดตามข้อมูลบน dark web ไว้ในคอนโซลเดียว งานที่ AI เสนอจะดำเนินการได้เมื่อนักวิเคราะห์อนุมัติแล้ว

EASM · CAASM · DRP · Threat Intel · Takedown · AI เสนอ นักวิเคราะห์ตัดสินใจ

รูปแบบติดตั้ง

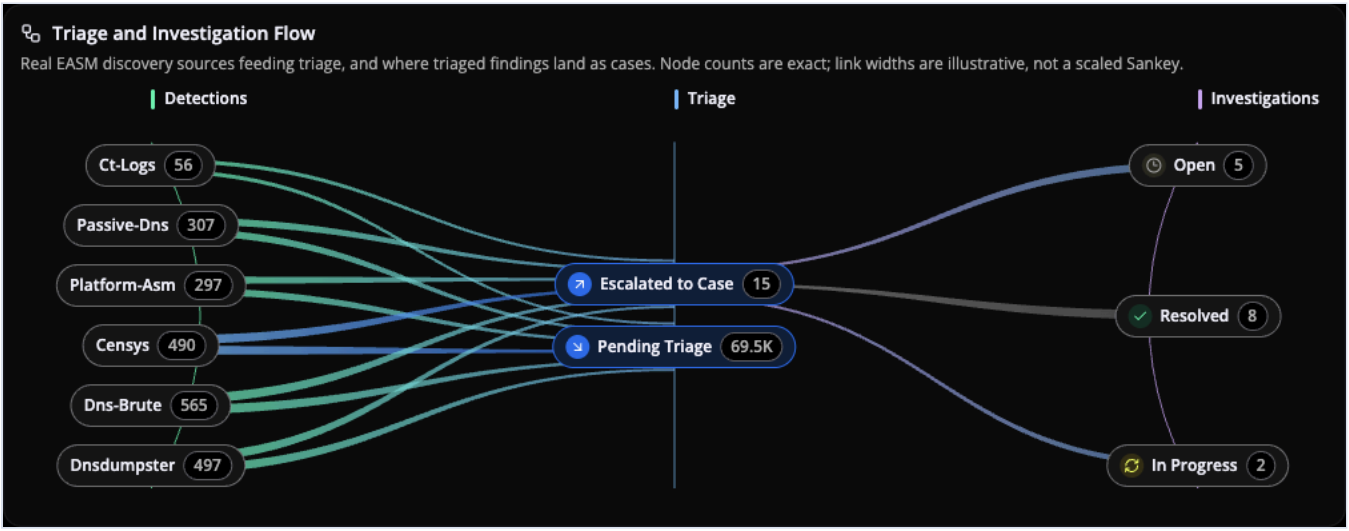
Cloud / SaaS

ซอฟต์แวร์ On-premises

01	02	03	04
ค้นหา	**จัดลำดับ**	**ตรวจสอบ**	**อนุมัติการดำเนินการ**

กระบวนการแนวคิด ไม่ใช่ภาพสถาปัตยกรรมติดตั้งจริง

แดชบอร์ด Agentic SOC



ติดตามแหล่ง discovery ของ tenant ตัวอย่าง ตั้งแต่ขั้นรอคัดกรองหรือส่งต่อเป็นเคส ไปจนถึงสถานะการสอบสวน ความกว้างของเส้นเป็นเพียงภาพประกอบ ไม่ใช่ตัวชี้วัดผลการทำงาน ภาพหน้าจอจริงจากเดโมออนไลน์ ตัวเลขบนหน้าจอเป็นข้อมูลตัวอย่าง

ตัวอย่างจาก demo จริง ข้อมูลและความกว้างของเส้นเป็นข้อมูลประกอบ ไม่ใช่ผลทดสอบสมรรถนะ

ประเมินขอบเขตและโมดูลกับพาร์ทเนอร์

ดูระบบ demo ↗ ปรึกษาพาร์ทเนอร์ ↗

รายละเอียดผลิตภัณฑ์

กระบวนการทำงาน

02

เหมาะสำหรับ

ทีม Security Operations · ทีม Vulnerability Management · ทีม Risk และ Third-Party Risk · MSSP ที่ดูแลหลาย tenant · CISO

ปัญหาที่ทีมเจอ

ผลสแกนจากภายนอก คอนโซล EDR กับ vulnerability scanner, feed จาก dark web และแบบประเมิน vendor ต่างเก็บข้อมูลไว้คนละส่วน ถ้า connector ตัวไหนหยุด sync ไปเงียบ ๆ ก็ไม่มีใครรู้ ทีมก็เลยจัดลำดับงานต่อไปจากข้อมูลที่ไม่เป็นปัจจุบัน

รูปแบบการใช้งาน

ซอฟต์แวร์แบบ Cloud / SaaS หรือ on-premises โดยยืนยันใน solution design

ขั้นตอนการทำงาน

ค้นหา จัดลำดับ และตรวจสอบ แล้วจบที่การดำเนินการที่มีคนอนุมัติ

01 / ค้นหา
กำหนด seed domain และ scope rule แล้ว EASM จะค้นหาต่อเนื่อง CAASM ดึง asset จากเครื่องมือที่เชื่อมไว้ และ Sync Health จะเตือนเมื่อแหล่งข้อมูลไหนเงียบไป

02 / จัดลำดับ
เรียง finding ตาม risk score, EPSS และระดับความสำคัญทางธุรกิจที่ทีมกำหนด เพื่อให้ asset สำคัญที่สุดได้รับการดูแลก่อน

03 / ตรวจสอบ
เปิด finding หรือสัญญาณจาก dark web เพื่อดูหลักฐาน ค่าความเชื่อมั่น การ map กับ MITRE ATT&CK และ asset ที่ตรงกัน

04 / ลงมือเมื่อได้รับอนุมัติ
Agent และผู้ช่วย AI ร่าง ticket และคำขอ takedown ไว้ให้นักวิเคราะห์อนุมัติหรือปฏิเสธทีละรายการ และทุกการตัดสินใจจะบันทึกไว้ใน Audit trail

รายละเอียดผลิตภัณฑ์

ขีดความสามารถหลัก

03

ความสามารถหลัก

แดชบอร์ด Agentic SOC ติดตามแหล่ง discovery ตั้งแต่ขั้นคัดกรองหรือส่งต่อเป็นเคส ไปจนถึงสถานะการสอบสวน

EASM ค้นหา asset จาก seed domain พร้อม scope rule แบบ include/exclude ตาม subdomain, CIDR หรือ ASN

Finding ด้านช่องโหว่, certificate และ open port พร้อม risk score, EPSS ของ CVE และหลักฐานที่ปกปิดข้อมูลอ่อนไหวแล้ว

Priority tier ที่องค์กรกำหนดเองตามความสำคัญทางธุรกิจ เช่น crown jewels แยกจาก severity ทางเทคนิค

CAASM inventory บอก coverage ของ EDR, vulnerability scan และ cloud posture ราย asset และ Sync Health เตือนเมื่อ source หยุดส่งข้อมูล

Threat Intelligence สำหรับ finding จาก dark web พร้อมคะแนน confidence, การ map กับ MITRE ATT&CK และการเชื่อมโยงกับ asset ขององค์กร

DRP กำหนด policy การ takedown ติดตาม incident case และส่ง security questionnaire ให้ third party

Agentic workflow และผู้ช่วย AI ช่วยร่างงานไว้ให้ทีมตรวจทาน ทุกคำตอบและทุกร่างมีบันทึกใน Audit trail และ ticket หรือ takedown ที่ AI เสนอจะเริ่มดำเนินการได้ก็ต่อเมื่อนักวิเคราะห์อนุมัติ

Risk scenario แสดงโอกาสเกิดเทียบกับขนาดความเสียหาย พร้อมมูลค่าความเสียหายต่อปีและลิงก์ไปยังหลักฐาน

โมดูล AI & Compliance: เตรียมพร้อม PDPA/CII ร่างหนังสือแจ้งเหตุข้อมูลรั่วไหล และช่วยจัดทำรายงาน compliance ด้วย AI

รายละเอียด Finding

เปิดแต่ละ finding เพื่อดู risk score, ค่า EPSS กรณีที่มี CVE, port ที่ตรวจพบ, หลักฐานที่ปกปิดข้อมูลอ่อนไหวแล้ว และ investigation path ก่อนส่งต่อเป็น ticket ภาพหน้าจอจริงจากเดโมออนไลน์ ตัวเลขบนหน้าจอเป็นข้อมูลตัวอย่าง

เปิดภาพต้นฉบับ ↗

รายละเอียดผลิตภัณฑ์

EASM และ CAASM

04

EASM

รู้ว่าองค์กรเปิดอะไรสู่อินเทอร์เน็ตบ้าง โดยเริ่มค้นจาก root domain ขององค์กรเอง

- ค้นหา asset จาก seed domain นำเข้าหลายรายการพร้อมกันได้ และกำหนด rule include/exclude ตาม subdomain, CIDR หรือ ASN
- Finding ด้านช่องโหว่, certificate และ open port พร้อม risk score และค่า EPSS ของ CVE
- จัด priority tier เช่น crown jewels แยกจาก severity ทางเทคนิค และใช้ auto-assign ตาม severity ได้
- บันทึกว่าใครเปิดใช้หรือแก้ seed domain และ scope rule

CAASM

รู้ว่า asset ตัวไหนมีเครื่องมือ security ดูแลอยู่จริง

- รวม host, device และ cloud resource จากหลาย source เป็น inventory ชุดเดียว
- ดู coverage ราย asset ทั้ง EDR, vulnerability scan และ cloud posture ว่ามี ขาด หรือยังยืนยันไม่ได้
- Risk score และสถานะ internet safety ของแต่ละ asset
- Sync Health เตือนว่าอาจมีจุดบอดเมื่อ source ขาดการเชื่อมต่อ ทำงานผิดปกติ หรือหยุดส่งข้อมูล

Scope & Discovery

กำหนด seed domain, rule include/exclude และ discovery source ที่ EASM จะใช้ในรอบ sync ถัดไป ภาพหน้าจอจริงจากเดโมออนไลน์ ตัวเลขบนหน้าจอเป็นข้อมูลตัวอย่าง

เปิดภาพต้นฉบับ ↗

Asset Inventory

ดู coverage ของ EDR, vulnerability scan และ cloud posture รวมถึง risk score และ priority tier ของทุก asset ใน CAASM inventory เดียว ภาพหน้าจอจริงจากเดโมออนไลน์ ตัวเลขบนหน้าจอเป็นข้อมูลตัวอย่าง

เปิดภาพต้นฉบับ ↗

รายละเอียดผลิตภัณฑ์

DRP, Threat Intelligence

05

DRP

จัดการการแอบอ้างแบรนด์และความเสี่ยงจาก third party โดยมี policy คุม takedown

- ตรวจพบ domain เลียนแบบ แอปมือถือปลอม และช่องทาง messaging ที่เผยข้อมูลองค์กร
- Policy ของ protected asset กำหนดว่าทำ takedown ได้หรือไม่ ต้องมีผู้อนุมัติกี่คน และต้องมี rollback หรือไม่
- Incident case รวม finding ที่เกี่ยวข้องกันไว้ด้วยกัน พร้อม severity, สถานะ, SLA และผู้รับผิดชอบ
- ทะเบียน vendor ที่ส่ง security questionnaire ได้ และมี template ให้ใช้ซ้ำ

Threat Intelligence

แยกให้ออกว่า finding จาก dark web เกี่ยวข้องกับองค์กรคุณจริงหรือไม่

- Finding จาก dark web ทั้ง credential ที่รั่ว, stealer log, โพสต์บน ransomware leak site และ source code ที่หลุด
- คะแนน confidence ที่บอกว่าตรวจหลักฐานอะไรแล้ว และยังขาดอะไร
- Map กับเทคนิคใน MITRE ATT&CK, เชื่อมโยงกับ inventory ของ EASM และอ้างอิงกรณีโจมตีที่มีการเปิดเผยต่อสาธารณะ ซึ่งมีสัญญาณคล้ายกัน
- แยกมุมมอง Darkweb, Email Security และ Briefs พร้อม triage และสร้าง ticket จาก finding บน dark web ได้

Threat Assessment

ประเมิน finding จาก dark web โดยดูคะแนน confidence, หลักฐานที่ยังขาด, เทคนิค MITRE ATT&CK และ asset ที่ตรงกัน ก่อนตัดสินใจ triage หรือสร้าง ticket ภาพหน้าจอจริงจากเดโมออนไลน์ ตัวเลขบนหน้าจอเป็นข้อมูลตัวอย่าง

เปิดภาพต้นฉบับ ↗

รายละเอียดผลิตภัณฑ์

AI & Compliance

06

01

เตรียมความพร้อม

PDPA / CII

02

ร่างแจ้งเหตุ

Breach notification

03

ช่วยจัดทำรายงาน

AI-assisted reporting

โมดูลคิดราคาแยกสำหรับการเตรียมความพร้อมและจัดทำรายงาน

- เตรียมพร้อม PDPA/CII และร่างหนังสือแจ้งเหตุข้อมูลรั่วไหล
- ช่วยจัดทำรายงาน compliance ด้วย AI
- ยืนยันกรอบที่ใช้ หลักฐาน และ workflow กับพาร์ทเนอร์ที่ได้รับอนุมัติ เอกสารนี้ไม่ใช่ใบรับรองหรือข้อยืนยันว่าปฏิบัติตามกฎหมายแล้ว

เดโมออนไลน์

เดโมออนไลน์ใช้ข้อมูลตัวอย่าง และครอบคลุม EASM, CAASM, DRP, Threat Intelligence, Agentic Workflow และ Audit trail ส่วนโมดูล Compliance ไม่ได้อยู่ในเดโม ขอการสาธิตผ่านพาร์ทเนอร์ที่ได้รับอนุมัติจาก zcr

> Threat Intelligence เสนอราคาแยก ไม่รวมอัตโนมัติใน 4 โมดูลที่แสดงราคาในเอกสารนี้ และไม่รวมในส่วนลด bundle ของ 4 โมดูล

ประเมินขอบเขตและโมดูลกับพาร์ทเนอร์

ยืนยันขอบเขตสินทรัพย์ โมดูล การเชื่อมต่อ และความรับผิดชอบกับพาร์ทเนอร์

ปรึกษาพาร์ทเนอร์ ↗

รายละเอียดผลิตภัณฑ์

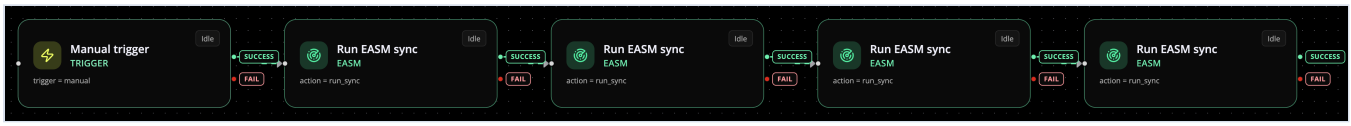
Agentic Workflow

07

แคนวาสออกแบบ Agent Workflow

สร้าง agent จากขั้นตอน trigger และ action ที่ต่อกันเป็นลำดับ แยกเส้นทางกรณีสำเร็จกับล้มเหลว แล้วเปิดใช้งานหรือสั่งรันเมื่อต้องการ ภาพหน้าจอจริงจากเดโมออนไลน์ ตัวเลขบนหน้าจอเป็นข้อมูลตัวอย่าง

เปิดภาพต้นฉบับ ↗



มุมมองครบทั้งสายงาน: ทริกเกอร์แบบสั่งเอง → งานซิงก์ EASM สี่ขั้น เห็นขั้วสำเร็จ/ล้มเหลวและปลายทั้งสองด้าน โหนดอยู่ในสถานะ Idle ภาพนี้ไม่ใช่หลักฐานการรันทิกเก็ตหรือ takedown เปิดภาพต้นฉบับ ↗

ภาพหน้าจอจริงจากเดโมสาธารณะ · เทนแนนต์และค่าเป็นข้อมูลตัวอย่าง · คง UI ภาษาอังกฤษ



ภาพขยายช่วงต้นจากสายงานเดียวกัน สร้างเอเจนต์ด้วยทริกเกอร์และแอ็กชัน แยกทางสำเร็จ/ล้มเหลว แล้วเปิดใช้หรือสั่งรันตามต้องการ ในตัวอย่างแบบอ่านอย่างเดียวนี้ ขั้วล้มเหลวยังไม่ได้เชื่อมต่อ เปิดภาพต้นฉบับ ↗

ภาพหน้าจอจริงจากเดโมสาธารณะ · เทนแนนต์และค่าเป็นข้อมูลตัวอย่าง · คง UI ภาษาอังกฤษ

ภาพ Workflow และ Audit trail เป็นคนละมุมมองของข้อมูลตัวอย่าง ไม่ใช่หลักฐานการดำเนินเคสเดียวกันครบวงจร

รายละเอียดผลิตภัณฑ์

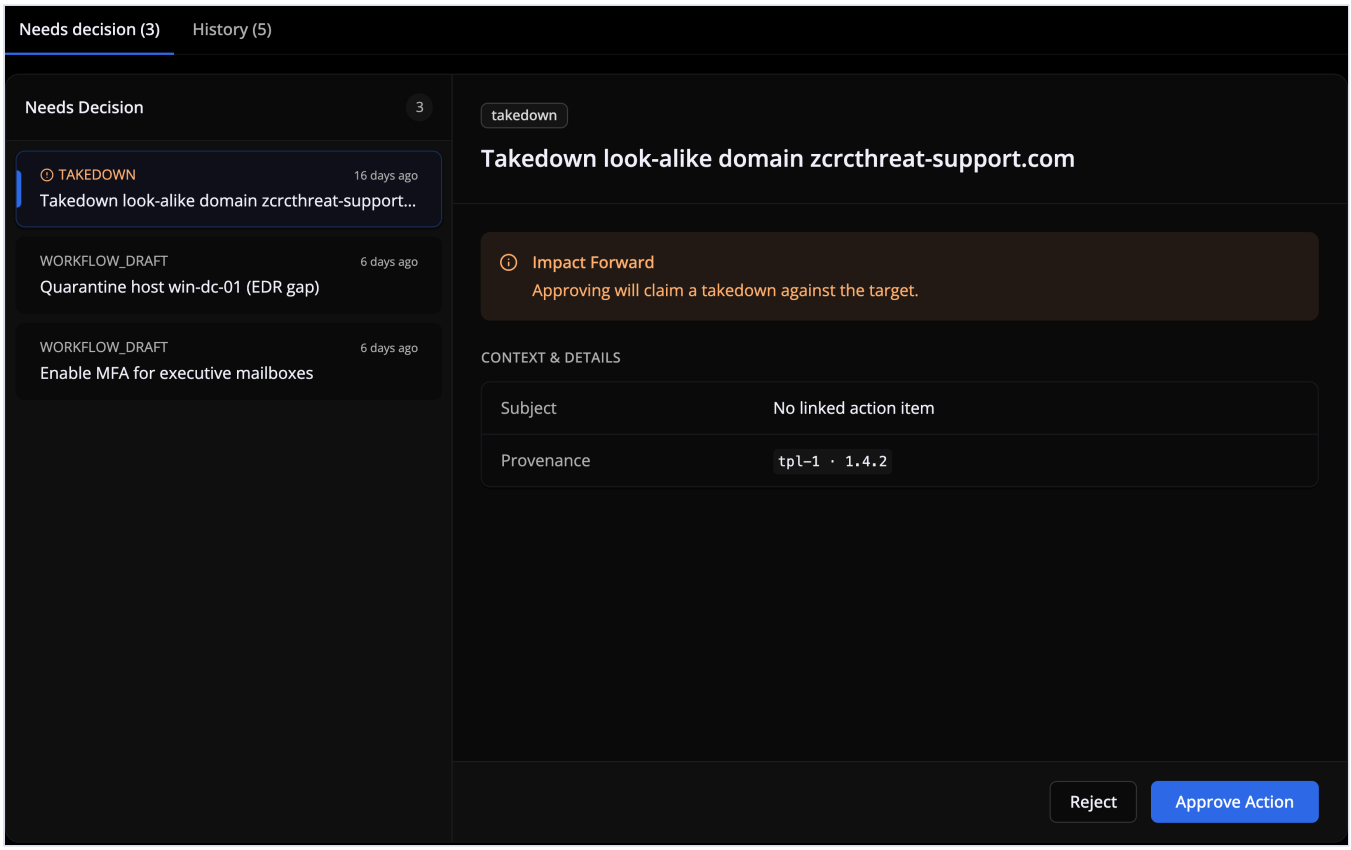
หลักฐานและการอนุมัติ

08

บันทึกการตรวจสอบ (Audit trail)

อนุมัติหรือปฏิเสธ ticket และ takedown ที่ AI ร่างไว้ โดยตรวจย้อนได้ว่าแต่ละร่างมาจาก template และเวอร์ชันใด ภาพหน้าจอจริงจากเดโมออนไลน์ ตัวเลขบนหน้าจอเป็นข้อมูลตัวอย่าง

เปิดภาพต้นฉบับ ↗



ข้อเสนอ takedown ที่เห็นเนื้อหาครบ พร้อมเทมเพลต tpl-1 เวอร์ชัน 1.4.2 และปุ่ม Approve / Reject สถานะยังรอการตัดสินใจ ไม่มีการอนุมัติหรือ takedown เพื่อจัดทำโบรชัวร์นี้ เปิดภาพต้นฉบับ ↗

ภาพหน้าจอจริงจากเดโมสาธารณะ · เทนแนนต์และค่าเป็นข้อมูลตัวอย่าง · คง UI ภาษาอังกฤษ

ภาพ Workflow และ Audit trail เป็นคนละมุมมองของข้อมูลตัวอย่าง ไม่ใช่หลักฐานการดำเนินเคสเดียวกันครบวงจร

รายละเอียดผลิตภัณฑ์

แพ็กเกจและหน่วยคิดราคา

09

แพ็กเกจ

EASM — เริ่มต้น ฿10,600/เดือน	ค้นหา External Attack Surface 5 ระดับ CTEM1-5 สูงสุด 2,000 asset (฿10,600-85,500/เดือน) เกินคิดเพิ่ม ฿21/asset/เดือน คิดราคาตาม asset ที่นับได้ — domain, subdomain, public IP, SSL/TLS cert คิดค่าบริการรายเดือน สัญญา 12 เดือน ราคารวม VAT
CAASM — เริ่มต้น ฿10,600/เดือน	รวบรวมสินทรัพย์คลาวด์และภายในองค์กร (AWS/Azure/GCP/M365/OT) 5 ระดับ สูงสุด 20,000 asset (฿10,600-85,500/เดือน ราคาเท่ากับ EASM ทุกระดับ) เกินคิดเพิ่ม ฿2.35/asset/เดือน คิดค่าบริการรายเดือน สัญญา 12 เดือน ราคารวม VAT
DRP + Dark Web — เริ่มต้น ฿21,300/เดือน	เฝ้าระวังความเสี่ยงดิจิทัลและ Dark Web พร้อมบริการ Takedown มี 5 ระดับ สูงสุด 100 keyword ที่มอนิเตอร์ (฿21,300-160,400/เดือน) เกินคิดเพิ่ม ฿856/keyword/เดือน รวมคำขอ takedown ปีละ 3-60 ครั้งตามระดับ คิดค่าบริการรายเดือน สัญญา 12 เดือน ราคารวม VAT
AI & Compliance — เริ่มต้น ฿10,600/เดือน	เตรียมพร้อม PDPA/CII แจ้งเหตุข้อมูลรั่วไหล รายงาน Compliance โดย AI มี 5 ระดับ สูงสุด 10,000 พนักงาน (฿10,600-96,200/เดือน) เกินคิดเพิ่ม ฿5.35/พนักงาน/เดือน คิดค่าบริการรายเดือน สัญญา 12 เดือน ราคารวม VAT

แต่ละโมดูลคิดราคาตามหน่วยของตัวเอง ชำระรายเดือน สัญญา 12 เดือน ราคารวม VAT ดูทุกระดับราคาและส่วนลดเมื่อซื้อครบ 4 โมดูลได้ที่ zcr.ai/pricing/

ราคาอ้างอิงเป็นเงินบาท (THB) รวม VAT คิดรายเดือนภายใต้สัญญา 12 เดือน พาร์ทเนอร์ยืนยันข้อเสนอและขอบเขตก่อนสั่งซื้อ

> Threat Intelligence เสนอราคาแยก ไม่รวมอัตโนมัติใน 4 โมดูลที่แสดงราคาในเอกสารนี้ และไม่รวมในส่วนลด bundle ของ 4 โมดูล

ขอบเขตการให้บริการ

ไม่การันตีผลสำเร็จของการ takedown — ขึ้นกับความร่วมมือของผู้ให้บริการ/registrar ที่เกี่ยวข้อง

รายละเอียดผลิตภัณฑ์

การประเมินผ่านพาร์ทเนอร์

10

คำถามที่พบบ่อย

zcrCTEM ครอบคลุมอะไรบ้าง?

ครอบคลุม attack surface ภายนอก (EASM), coverage ของ asset ภายในและบน cloud (CAASM), การป้องกันความเสี่ยงดิจิทัล (DRP) และ threat intelligence ในคอนโซลเดียว ส่วนรายงาน Compliance สำหรับ PDPA และ CII อยู่ในโมดูล AI & Compliance ที่คิดราคาแยก

AI ดำเนินการเองได้หรือไม่?

ได้เฉพาะขั้นตอนประจำที่ตั้งค่าไว้ เช่น สั่ง sync ข้อมูล ส่วน ticket หรือ takedown ที่ AI ร่างขึ้นจะยังเป็นแค่ข้อเสนอ จนกว่านักวิเคราะห์จะกดอนุมัติหรือปฏิเสธ ทุกคำตอบและทุกร่างที่ AI สร้างจะบันทึกไว้ใน Audit trail พร้อมระบุ template และเวอร์ชันที่ใช้

เดโมออนไลน์มีส่วน Compliance ไหม?

ไม่มี เดโมออนไลน์แสดงเฉพาะงานด้าน exposure ได้แก่ EASM, CAASM, DRP, threat intelligence และ agentic workflow ส่วนการเตรียมพร้อม PDPA/CII, การร่างหนังสือแจ้งเหตุข้อมูลรั่วไหล และรายงาน Compliance โดย AI อยู่ในโมดูล AI & Compliance หากต้องการดูส่วนนี้ ขอการสาธิตผ่านพาร์ทเนอร์ที่ได้รับอนุมัติจาก zcr

ขอบเขตที่ต้องยืนยัน

ขอบเขตของ asset โมดูล การเริ่มใช้งาน การติดตั้ง การเชื่อมต่อ การซัพพอร์ต SLA และราคา จะยืนยันใน solution design และใบเสนอราคา

ขอประเมินระบบผ่านพาร์ทเนอร์ที่ได้รับอนุมัติจาก zcr

ลองเดโม zcrCTEM ได้เลย ไม่ต้องล็อกอิน

ประเมินระบบผ่านพาร์ทเนอร์ ↗ zcr.ai/contact/ · แพ็กเกจปัจจุบัน ↗ zcr.ai/pricing/ · เปิดเดโม ↗ demo.zcrctem.zcr.ai/dashboards