การบริหารจัดการความเสี่ยงจากการเปิดรับภัยคุกคามอย่างต่อเนื่อง (CTEM)

zcrCTEM

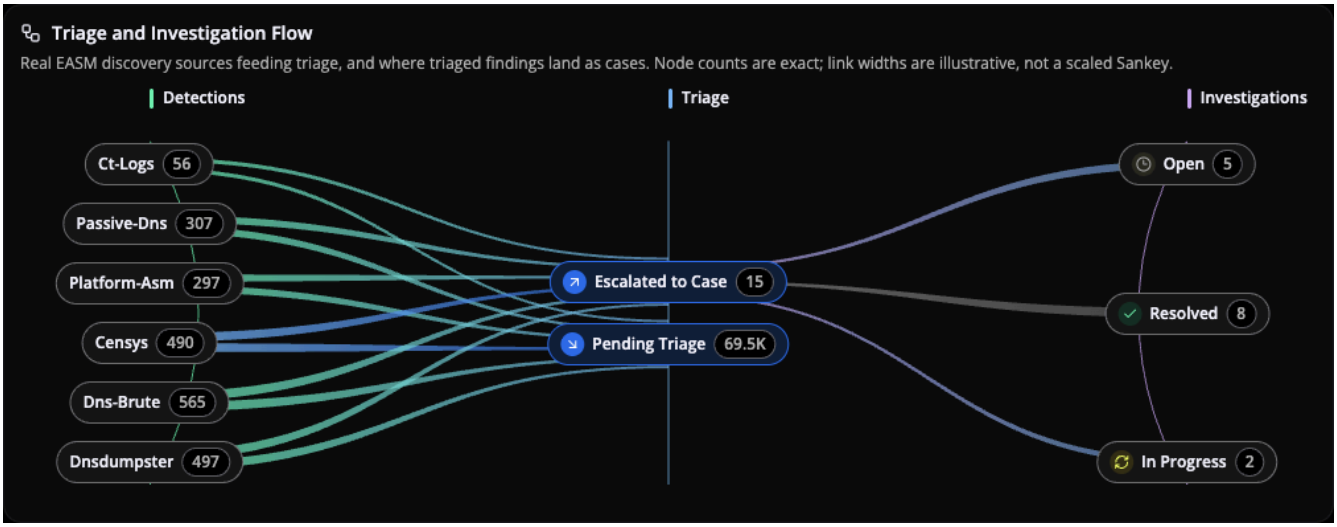
จากสัญญาณสู่การดำเนินการที่ได้รับอนุมัติ

รวมข้อมูลการเปิดรับภัยจากภายนอก ช่องว่างความครอบคลุมของเครื่องมือ และข้อมูลจากดาร์กเว็บไว้ในคอนโซลเดียว ปัญญาประดิษฐ์ (AI) เสนองานให้นักวิเคราะห์ตัดสินใจก่อนดำเนินการ

EASM	ค้นหาสินทรัพย์ที่เปิดรับภัยจากภายนอก External Attack Surface Management
CAASM	ตรวจช่องว่างความครอบคลุมของเครื่องมือ Cyber Asset Attack Surface Management
DRP	ติดตามความเสี่ยงและข้อมูลบนดาร์กเว็บ Digital Risk Protection

รูปแบบการใช้งาน · ซอฟต์แวร์ Cloud / Software as a Service (SaaS) หรือ on-premises โดยยืนยันในแบบออกแบบโซลูชัน

ติดตามข้อมูลตั้งแต่ค้นพบจนถึงการสอบสวน



แดชบอร์ดศูนย์ปฏิบัติการความปลอดภัย (SOC): แหล่งค้นพบ → รอคัดกรองหรือส่งต่อเป็นเคส → สถานะการสอบสวน ความกว้างของเส้นเป็นภาพประกอบ ไม่ใช่ตัวชี้วัดประสิทธิภาพ เปิดภาพต้นฉบับ ↗

ภาพหน้าจอจริงจากเดโมสาธารณะ · เทนแนนต์และค่าเป็นข้อมูลตัวอย่าง · คง UI ภาษาอังกฤษ

เหมาะสำหรับ · ทีมปฏิบัติการความปลอดภัยและจัดการช่องโหว่ ทีมความเสี่ยงและความเสี่ยงบุคคลที่สาม ผู้ให้บริการความปลอดภัยแบบบริหารจัดการ (MSSP) ที่ดูแลหลายเทนแนนต์ และผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (CISO)

ลำดับงานเดียว โดยมีคนอนุมัติก่อนดำเนินการ

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

ลำดับงานเชิงแนวคิดเพื่ออธิบายการใช้งาน ไม่ใช่แผนผังการเชื่อมต่อระบบ

01 ค้นหา

กำหนดโดเมนตั้งต้นและกฎรวม/ยกเว้นตามซับโดเมน ช่วงเครือข่าย (CIDR) หรือหมายเลขระบบอิสระ (ASN) ให้ EASM ค้นหาต่อเนื่อง CAASM ดึงสินทรัพย์จากเครื่องมือที่เชื่อมไว้ แสดงความครอบคลุมรายสินทรัพย์ของEDR การสแกนช่องโหว่ และสถานะความปลอดภัยคลาวด์ ส่วน Sync Health เตือนเมื่อแหล่งข้อมูลหยุดส่ง

ผลลัพธ์: รายการสินทรัพย์ตามขอบเขตและช่องว่างความครอบคลุม

02 จัดลำดับ

เรียงสิ่งที่ตรวจพบตามคะแนนความเสี่ยง EPSS (Exploit Prediction Scoring System) และระดับความสำคัญทางธุรกิจที่ทีมกำหนด เพื่อดูแลสินทรัพย์สำคัญก่อน

ผลลัพธ์: รายการที่จัดลำดับพร้อมตรวจทาน

03 ตรวจสอบ

เปิดสิ่งที่ตรวจพบหรือสัญญาณจากดาร์กเว็บ เพื่อดูหลักฐาน คะแนนความเชื่อมั่น สินทรัพย์ที่สัมพันธ์กันในรายการ EASM และการเทียบกับ MITRE ATT&CK ซึ่งเป็นฐานความรู้กลยุทธ์และเทคนิคของผู้โจมตี โดย Threat Intelligence จำหน่ายแยก

ผลลัพธ์: หลักฐานที่เชื่อมโยงกับสินทรัพย์ที่ได้รับผลกระทบ

04 ลงมือเมื่อได้รับอนุมัติ

เอเจนต์และผู้ช่วย AI ร่างทิกเก็ตและคำขอ takedown ให้นักวิเคราะห์อนุมัติหรือปฏิเสธทีละรายการก่อนดำเนินการ ทุกคำตอบ ร่างงาน และการตัดสินใจบันทึกไว้ใน Audit trail

จุดตัดสินใจของคน: อนุมัติหรือปฏิเสธ → บันทึกที่ตรวจย้อนกลับได้

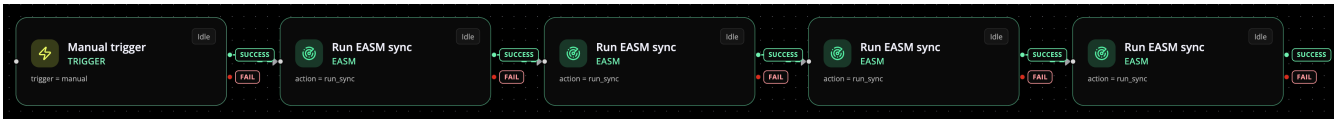
EPSS ของ FIRST ประเมินโอกาสที่ช่องโหว่ซึ่งเผยแพร่แล้วจะถูกใช้โจมตีใน 30 วันข้างหน้า ไม่ใช่หลักฐานว่าถูกโจมตีแล้ว

FIRST · EPSS ↗

CIDR = Classless Inter-Domain Routing (การระบุช่วงเครือข่าย); ASN = Autonomous System Number (หมายเลขระบบอิสระ)

ตรวจข้อเสนอก่อนเริ่มดำเนินการ

01 / แคนวาสออกแบบ Agent Workflow



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

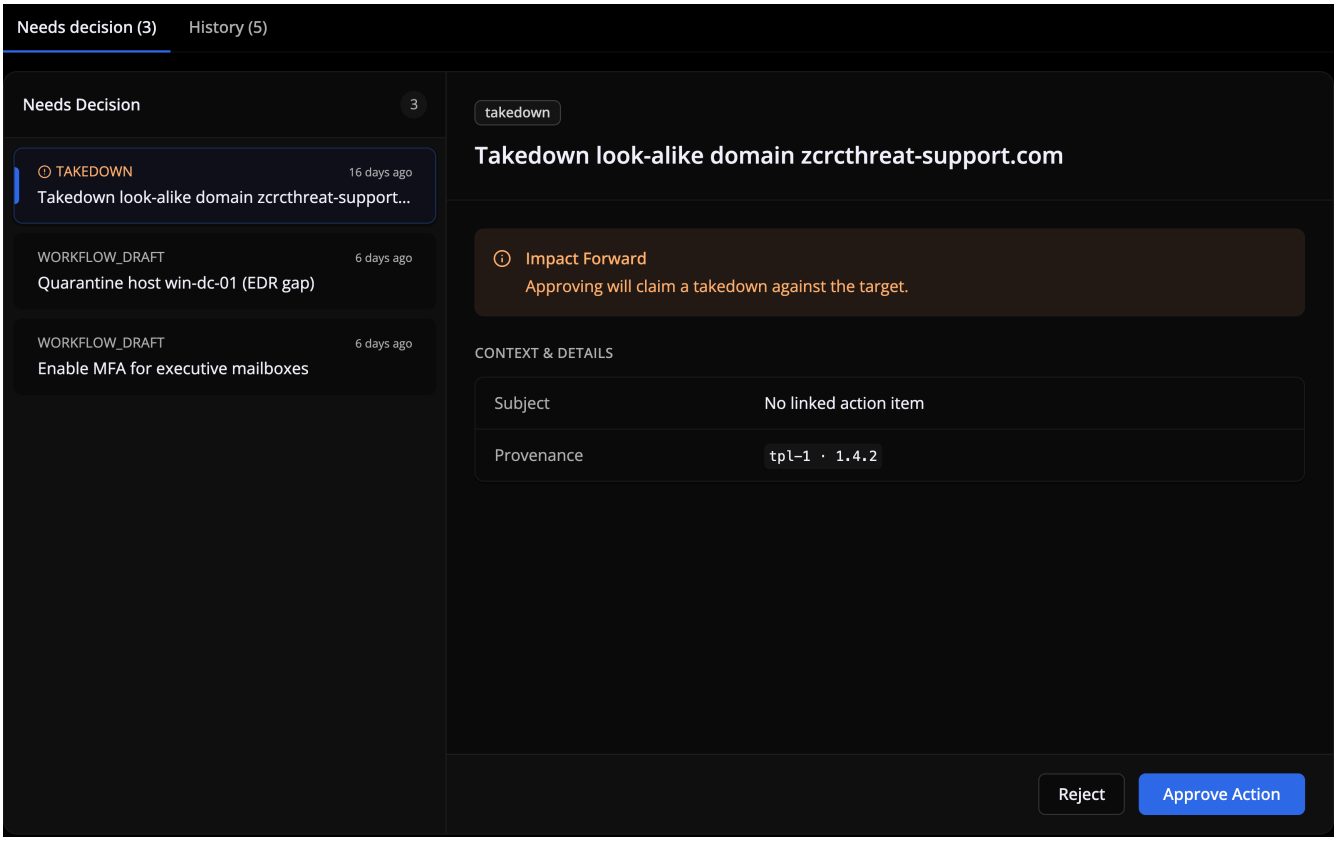
ภาพหน้าจอจริงจากเดโมสาธารณะ · เทนแนนต์และค่าเป็นข้อมูลตัวอย่าง · คง UI ภาษาอังกฤษ



ภาพขยายช่วงต้นจากสายงานเดียวกัน สร้างเอเจนต์ด้วยทริกเกอร์และแอ็กชัน แยกทางสำเร็จ/ล้มเหลว แล้วเปิดใช้หรือสั่งรันตามต้องการ ในตัวอย่างแบบอ่านอย่างเดียวนี้ ขั้วล้มเหลวยังไม่ได้เชื่อมต่อ เปิดหน้าจอเดโม ↗

ภาพหน้าจอจริงจากเดโมสาธารณะ · เทนแนนต์และค่าเป็นข้อมูลตัวอย่าง · คง UI ภาษาอังกฤษ

02 / ข้อเสนอรออนุมัติและที่มา



ข้อเสนอ takedown ของ zcrcthreat-support.com ยังรอตัดสินใจ ที่มา tpl-1 / 1.4.2 และ Subject: No linked action item คำเตือน Impact Forward ระบุว่าการอนุมัติจะอ้างการ takedown ต่อเป้าหมาย คงปุ่ม Reject / Approve Action โดยไม่ได้กดอนุมัติหรือดำเนินการเพื่อจัดทำโบรชัวร์นี้ เปิดหน้าจอเดโม ↗

ภาพหน้าจอจริงจากเดโมสาธารณะ · เทนแนนต์และค่าเป็นข้อมูลตัวอย่าง · คง UI ภาษาอังกฤษ

> ภาพ Workflow และ Audit trail เป็นคนละมุมมองของข้อมูลตัวอย่าง ไม่ใช่หลักฐานการดำเนินเคสเดียวกันครบวงจร

กำหนดขอบเขตร่วมกับพาร์ทเนอร์

โมดูลและเงื่อนไขเชิงพาณิชย์

EASM · CAASM · DRP	เลือกขอบเขตสินทรัพย์และโมดูลกับพาร์ทเนอร์ที่ได้รับอนุมัติ การเห็นฟังก์ชันในเดโมไม่ได้ยืนยันสิทธิ์ที่ซื้อ
Threat Intelligence	จำหน่ายแยกและเสนอราคาโดยพาร์ทเนอร์ที่ได้รับอนุมัติจาก zcr ไม่รวมในโมดูลที่มีราคาทั้งสี่หรือส่วนลดแบบซื้อครบ
AI & Compliance	คิดราคาแยก: เตรียมพร้อมตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ร่างหนังสือแจ้งเหตุข้อมูลรั่วไหล และช่วยจัดทำรายงานการปฏิบัติตามข้อกำหนดด้วย AI

ขอบเขตด้านการปฏิบัติตามข้อกำหนด · ยืนยันกรอบที่ใช้ หลักฐาน และ workflow กับพาร์ทเนอร์ที่ได้รับอนุมัติ เอกสารนี้ไม่ใช่ใบรับรองหรือข้อยืนยันว่าปฏิบัติตามกฎหมายแล้ว

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

ไม่การันตีผลสำเร็จของการ takedown — ขึ้นกับความร่วมมือของผู้ให้บริการ/registrar ที่เกี่ยวข้อง

ขอประเมินระบบผ่านพาร์ทเนอร์ที่ได้รับอนุมัติจาก zcr

เตรียมโดเมนตั้งต้น ขอบเขตสินทรัพย์และระดับความสำคัญ เครื่องมือและตัวเชื่อมต่อที่ใช้ รูปแบบ SaaS หรือ on-premises ที่ต้องการ ผู้มีสิทธิ์อนุมัติ และความต้องการด้านหลักฐาน

พาร์ทเนอร์ที่ได้รับอนุมัติจะใช้ข้อมูลนี้เพื่อยืนยันโมดูล การเริ่มใช้งาน การติดตั้ง การเชื่อมต่อ การซัพพอร์ต ข้อตกลงระดับการให้บริการ (SLA) และราคาในแบบออกแบบโซลูชันและใบเสนอราคา

ลองเดโมzcrCTEM ได้เลย ไม่ต้องล็อกอิน

ประเมินระบบผ่านพาร์ทเนอร์ ↗ แพ็กเกจปัจจุบัน ↗ เปิดเดโม↗

พาร์ทเนอร์เป็นผู้ให้การสนับสนุนด่านแรก โดย zcr สนับสนุนพาร์ทเนอร์