Response

zcrSOAR

การประสานงาน การทำงานอัตโนมัติ และการตอบสนองภัยคุกคาม

zcrSOAR เปลี่ยนการคัดกรองให้เป็นคิวกลางที่ดึงเคสไปทำ รัน Playbook ภายใต้ gating รายขั้นตอนแบบ Autonomous, Approval หรือ Blocked ติดตาม SLA ของ Notify กับ Respond แยกกันตาม severity พร้อมส่ง Approval และ Response Action ผ่านคิวเดียวที่กำหนดสิทธิ์ตามบทบาท

เหมาะสำหรับ	ทีม SOC ที่ต้องคัดกรอง Alert ปริมาณสูง · MSSP และผู้ให้บริการ MDR · ทีมที่ต้องการมาตรฐาน Playbook พร้อมการดูแล · ทีมที่ต้องพิสูจน์ SLA compliance ได้
โจทย์ที่ต้องแก้	ถ้าไม่มีคิวกลาง นักวิเคราะห์อาจทำงานซ้ำกับ Alert เดียวกัน Playbook ที่รันแบบไม่มีใครดูแลเลยมีความเสี่ยง ส่วน Playbook ที่ต้องรอคนทุกขั้นตอนก็ช้าเกินจะขยายได้ และ SLA มักถูกติดตามย้อนหลัง แทนที่จะเห็นแบบ Real-time
เชื่อมต่อกับ	zcrSIEM (Bidirectional Bridge) · SentinelOne EDR (Isolate, Scan) · MISP Threat Intelligence (Sync Indicator) · AI Assistant แบบ OpenAI-compatible
รูปแบบการติดตั้ง	SaaS (คลาวด์) หรือซอฟต์แวร์ติดตั้งในองค์กร เลือกได้ในขั้นออกแบบโซลูชัน

ความสามารถหลัก

- Triage Board: คิวแบบดึงไปทำ — หยิบเคสไปแล้วหลุดจากคิวสำหรับคนอื่น
- Playbook Library พร้อม Version, ขั้นตอนอนุมัติ และ Dry-Run
- ร่าง Playbook ใหม่ด้วย AI จาก Prompt หรือ Import เป็นไฟล์ YAML/JSON
- Gating รายขั้นตอน — Autonomous, Approval หรือ Blocked
- Approvals & Tasks: คิวเดียวตามสิทธิ์ เวลาแตกต่างตามประเภทงาน และ Revision ไม่มีกำหนดเวลา
- ติดตาม SLA ของ Notify และ Respond แยกกันตาม Severity พร้อมรายการที่ Breach
- Attack Flows: Timeline ต่อเคสที่ Map กับ MITRE ATT&CK
- IOC Library สำหรับ IP, Domain, Hash, URL และอีเมล พร้อม Sync กับ MISP
- เก็บประวัติการรัน Playbook ไว้เป็นหลักฐาน รวมถึง Dry-Run

จากสัญญาณสู่การดำเนินการที่ตรวจสอบได้

คิวเดียว Playbook ที่มีระดับการดูแลที่พอดี

zcrSOAR รับ Incident จากแหล่งที่เชื่อมต่อไว้ รวมถึง Bidirectional Bridge กับ zcrSIEM แล้วนำเข้าคิว Triage Board แบบดึงไปทำ — นักวิเคราะห์หยิบเคสไป เคสนั้นก็หลุดจากคิวสำหรับคนอื่นทันที Playbook รันด้วย Gating รายขั้นตอน (Autonomous, Approval หรือ Blocked) ส่วนการอนุมัติของเคส การอนุมัติของ Playbook แต่ละขั้นตอน และ Response Action ทั้งหมดผ่านคิว Approvals & Tasks เดียว โดยติดตาม SLA ของ Notify และ Respond แยกกันตาม Severity

ตรวจคำขอให้ชัดก่อนตัดสินใจ

Ransomware indicators on WKS-0774 `CASE-00000005`

TRANSITION: CONTAINED → CLOSED

Closure requested after containment was confirmed on Ransomware indicators on WKS-0774.

คำขอแรก: ชื่อเคสและการเปลี่ยนสถานะ CONTAINED → CLOSED ระบุสิ่งที่ขออนุมัติ ภาพนี้เป็นคำขอที่รอพิจารณา ไม่ใช่ผลอนุมัติสำเร็จ ดูรายละเอียดผลิตภัณฑ์ ↗

requested by **Nutcha Analyst** · waiting **1h 14m**

SLA 1h 10m

REQUIRED: OPERATOR

Reject | Approve

รายละเอียดจากคำขอแรกเดียวกัน: REQUIRED: OPERATOR เวลาที่รอ ค่า SLA ที่แสดงในเดโม และปุ่ม Reject / Approve ภาพนี้ยังเป็นคำขอรอพิจารณา ไม่ใช่คำรับรอง SLA ตามสัญญา ดูรายละเอียดผลิตภัณฑ์ ↗

01 · คำขอ

ตรวจการเปลี่ยนสถานะและบริบทที่ระบุในเคส

02 · บทบาท

ตรวจบทบาทที่มีสิทธิ์ก่อนเลือกดำเนินการ

03 · การตัดสินใจ

อนุมัติหรือปฏิเสธตามสิทธิ์ใน workflow ภาพนิ่งนี้ยังไม่ยืนยันการดำเนินการจริง

> ข้อมูลเดโมเพื่อประกอบคำอธิบาย ไม่ใช่ผลลัพธ์ลูกค้า ขีดความสามารถ หรือหลักฐานประสิทธิภาพ คง UI ภาษาอังกฤษตามต้นฉบับ

เส้นทางตอบสนองเดียวข้ามหลายเครื่องมือ

Isolate หรือ Release Endpoint และสั่ง Scan ผ่าน SentinelOne หรือค้นหา Publish และ Sync Indicator ผ่าน MISP ได้จาก Case หรือขั้นตอนของ Playbook โดยตรง

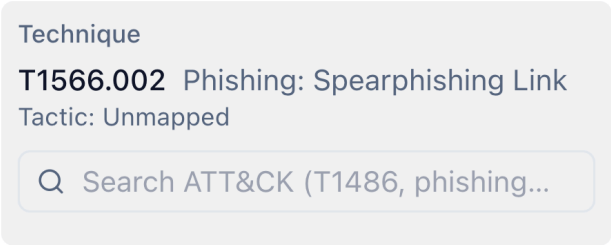
Playbook Automation

เริ่มต้นด้วย Playbook สำเร็จรูปสำหรับ Phishing, Malware, Brute-Force และ C2 Isolation จัดกลุ่มตาม NIST Category หรือให้ AI Assistant ร่าง Playbook ใหม่จาก Prompt ก็ได้

แยกแท็กเทคนิคออกจากความครบของ tactic



MITRE ATT&CK v14.1 · สามขั้นตอนแสดง T1566.002, T1204.002 และ T1486 พร้อม Tactic: Unmapped ทุกขั้น ชื่อขั้นแรกถูกย่อใน UI โดยอ่านชื่อเต็มได้จากแผงรายละเอียด ตัวอย่างนี้ยังจับคู่ tactic ไม่ครบ ดูรายละเอียดผลิตภัณฑ์ ↗



แผงรายละเอียดของขั้นตอนแรกแสดง T1566.002 — Phishing: Spearphishing Link และ Tactic: Unmapped เป็นข้อมูลของ node ที่เลือก ไม่ใช่คะแนนความครอบคลุมทั้ง flow ดูรายละเอียดผลิตภัณฑ์ ↗

เปิดใช้ใน Production อย่างปลอดภัย

Playbook ที่ยังไม่อนุมัติจะอยู่ใน Draft, Test, Dry-run หรือ Simulation Mode จนกว่าองค์กรจะอนุญาตให้ทำงานจริง

ภาพรวมการปฏิบัติการ: ปริมาณเคส Mean Time to Acknowledge และ Close และสถานะการทำงานของ Automation ในหน้าเดียว อัปเดตแบบเรียลไทม์ (ตัวอย่างจากสภาพแวดล้อมเดโม ไม่ใช่ตัวเลขจริง)

ขั้นตอนอนุมัติตามสิทธิ์บทบาท: ส่งคำขออนุมัติปิดเคสตามบทบาทที่กำหนด (operator หรือ admin) พร้อมนับถอยหลัง SLA แบบเรียลไทม์ (ตัวอย่างจากสภาพแวดล้อมเดโม ไม่ใช่ตัวเลขจริง)

> ข้อมูลเดโมเพื่อประกอบคำอธิบาย ไม่ใช่ผลลัพธ์ลูกค้า ขีดความสามารถ หรือหลักฐานประสิทธิภาพ คง UI ภาษาอังกฤษตามต้นฉบับ

เปรียบเทียบแพ็กเกจตาม production run

SaaS และซอฟต์แวร์ on-premises มีราคาเท่ากันที่ขนาดเดียวกัน ตารางนี้ใช้เงินบาท เรียกเก็บรายเดือนตามสัญญา 12 เดือน รวม VAT

SKU SaaS / ส่วนท้าย on-prem	Production run / เดือน	บาท / เดือน รวม VAT	การติดตั้ง
zcrSOAR-500 **OP-500**	500	125,000	SaaS / On-premises
zcrSOAR-2K **OP-2K**	2,000	250,000	SaaS / On-premises
zcrSOAR-10K **OP-10K**	10,000	450,000	SaaS / On-premises
zcrSOAR-50K **OP-50K**	50,000	580,000	SaaS / On-premises

SKU ซอฟต์แวร์ On-premises: zcrSOAR-OP-500 / zcrSOAR-OP-2K / zcrSOAR-OP-10K / zcrSOAR-OP-50K

กำหนดปริมาณและขอบเขตร่วมกับพาร์ทเนอร์

1 run คือการรัน automation จริงใน production 1 ครั้ง ทุกแพ็กเกจไม่จำกัด playbook, integration, tenant และผู้ใช้

หากต้องการจำนวน run ระหว่างแพ็กเกจ ให้พาร์ทเนอร์ที่ได้รับอนุมัติจัดทำใบเสนอราคาตามขอบเขต ไม่ใช้อัตราต่อ run คำนวณราคาโดยอัตโนมัติ

> ใบเสนอราคา/SOW ระบุวิธีนับปริมาณ เงื่อนไขใช้งานเกินแพ็กเกจ การปรับแพ็กเกจ และเวลาให้บริการสนับสนุนที่ตกลงกัน

พาร์ทเนอร์เป็นผู้เสนอราคา ทำสัญญา ส่งมอบ และสนับสนุนชั้นแรก โดย zcr สนับสนุนพาร์ทเนอร์ งานติดตั้งและตั้งค่าเสนอราคาแยกตามขอบเขต

แพ็กเกจปัจจุบัน ↗

เตรียมรูปแบบติดตั้งและความรับผิดชอบ

On-premises เป็นซอฟต์แวร์บนฮาร์ดแวร์หรือ VM ของคุณ ไม่มี appliance ของ zcrSOAR งานติดตั้งและตั้งค่าเสนอราคาแยกจากค่าสมัครตามขอบเขต ราคาเท่ากันเพราะไม่มีต้นทุน hosted storage ให้หักลด และยังมีงานสนับสนุนอัปเกรด/connector ในระบบที่ดูแลเอง

> ซื้อ zcrSOAR แยกได้ โดยไม่ต้องมี zcrSIEM หรือ zcrLog

คำถามที่พบบ่อย zcrSOAR

zcrSOAR ตัดสินใจอย่างไรว่า Action ไหนใน Playbook รันอัตโนมัติ?

แต่ละขั้นตอนของ Playbook กำหนดเป็น Autonomous, Approval หรือ Blocked ขั้นตอน Autonomous รันทันที ขั้นตอน Approval รอการอนุมัติตามสิทธิ์บทบาท ส่วนขั้นตอน Blocked จะไม่ทำงานจนกว่าจะเปลี่ยน Gating

zcrSOAR สร้าง Playbook ใหม่ได้ไหม?

ได้ — AI Assistant ร่าง Playbook จาก Prompt ให้ตรวจสอบก่อนใช้งาน และยัง Import นิยาม Playbook เป็นไฟล์ YAML หรือ JSON ได้โดยตรง

zcrSOAR ต้องมี zcrSIEM ไหม?

ไม่จำเป็น zcrSOAR เชื่อมกับ zcrSIEM แบบ Bidirectional Bridge เมื่อติดตั้งทั้งคู่ และยังรับข้อมูลจากแหล่งอื่นที่เชื่อมต่อไว้ เช่นแพลตฟอร์ม EDR ได้ด้วย ไม่ได้จำกัดแค่ zcrSIEM อย่างเดียว

zcrSOAR ติดตาม SLA compliance อย่างไร?

SLA ของ Notify และ Respond ติดตามแยกกันตาม Severity ของเคส เทียบกับเป้าหมาย compliance พร้อม Mean Time to Acknowledge และ Mean Time to Respond รวมถึงรายการเคสที่พลาด SLA

ประเมินระบบผ่านพาร์ทเนอร์ที่ได้รับอนุมัติ

เตรียมจำนวน production run รายเดือน ระบบต้นทาง เจ้าของสิทธิ์อนุมัติ และรูปแบบติดตั้ง ให้พาร์ทเนอร์กำหนดแพ็กเกจ นิยามการนับ เวลาให้บริการสนับสนุน และผู้รับผิดชอบการติดตั้งในข้อเสนอ

พาร์ทเนอร์ที่ได้รับอนุมัติเป็นผู้วางขอบเขตข้อเสนอ เสนอราคา ทำสัญญา และส่งมอบงาน

ติดต่อพาร์ทเนอร์ ↗ แพ็กเกจปัจจุบัน ↗ เอกสารผลิตภัณฑ์ ↗