ซอฟต์แวร์วิเคราะห์ความปลอดภัย · ประเมินผ่านพาร์ทเนอร์

zcrSIEM

เลือกแหล่งข้อมูล เวิร์กโฟลว์ และแพ็กเกจให้ตรงกับทีม

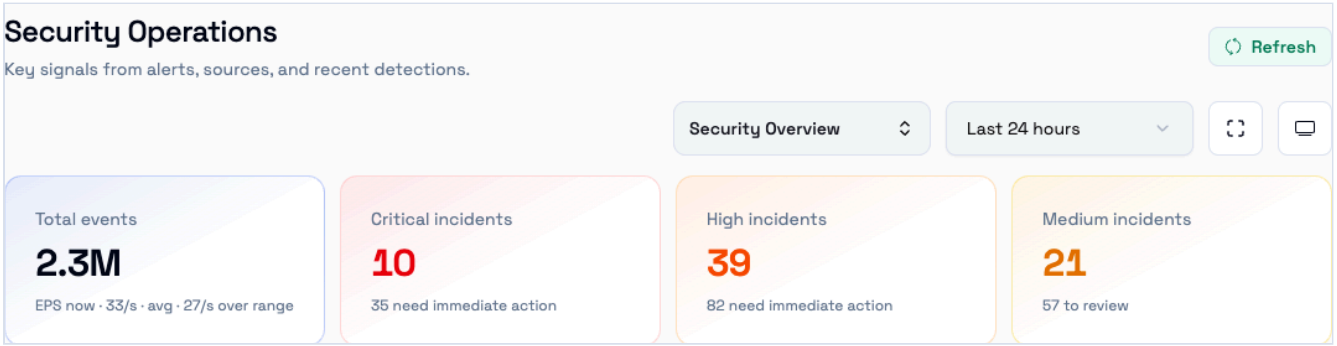
ตรวจจับ สืบสวน และเชื่อมโยงเหตุการณ์ความปลอดภัยไว้ในเวิร์กโฟลว์เดียวของนักวิเคราะห์

ทีม SOC, MDR, MSSP, CISO และทีมความปลอดภัยองค์กร

> zcrSIEM รับข้อมูลจากแหล่งต่าง ๆ ได้เอง ไม่ต้องมี zcrLog บริการเฝ้าระวังและตอบสนองเหตุการณ์แยกสัญญาจากซอฟต์แวร์ ส่วน playbook อัตโนมัติเป็นผลิตภัณฑ์ zcrSOAR ที่จัดหาแยก

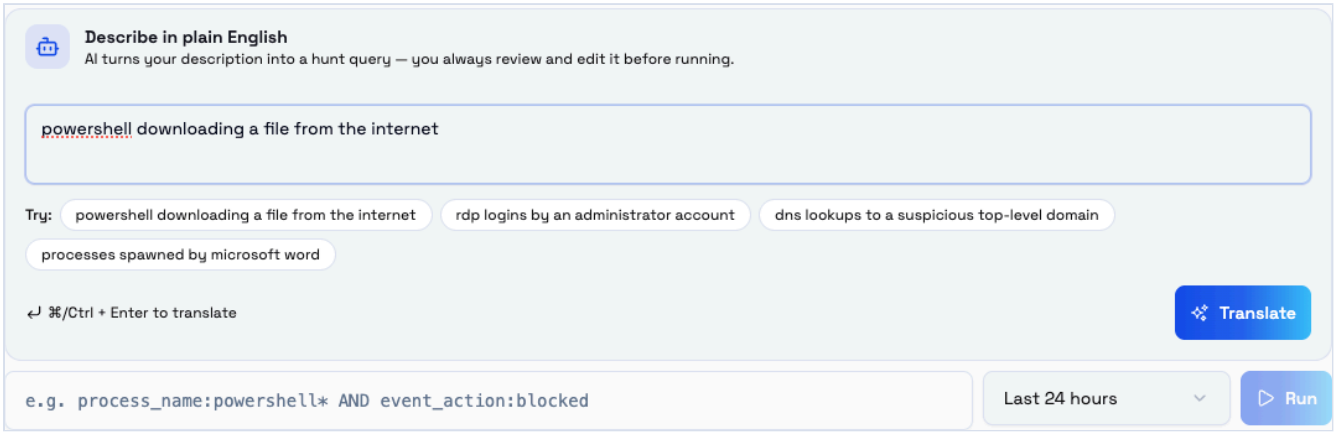
แหล่งข้อมูลและการเชื่อมต่อ

กลุ่มแหล่งข้อมูล	อุปกรณ์ Network · Firewall · IDS/IPS · Windows และ Linux · ระบบ Identity · Endpoint Security · Email Security · Cloud Platform · Container และ Kubernetes · EDR, NDR และ Network Sensor
Cloud Platform	AWS · Azure · Google Cloud · Huawei Cloud · GDCC Cloud · GDCC OpenData เชื่อมต่อผ่าน API, Webhook, Syslog หรือ Native Connector
Endpoint, Email และ Network	สัญญาณ Endpoint จาก Windows, Linux และ macOS · Microsoft Defender for Office 365 · NDR, Network Sensor และ IDS/IPS
Threat Intelligence	แหล่งข้อมูลแบบ Open Source และเชิงพาณิชย์ ผ่าน API, Feed และ STIX/TAXII
การรับข้อมูล	zcrSIEM รับ log จากแหล่งข้อมูลได้เองโดยตรง ทุกแพ็กเกจมีความจุรับข้อมูลต่อวันของตัวเอง จึงไม่ต้องมี zcrLog มาก่อน

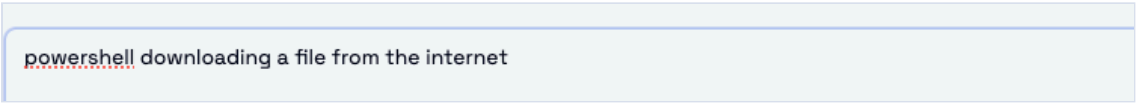


Security Operations — หน้าสรุปแยกเหตุการณ์และ incident ตัวอย่างตามความรุนแรง ข้อมูลเดโม ไม่ใช่ปริมาณงานลูกค้า ขีดจำกัด หรือหลักฐานประสิทธิภาพ หน้าจอภาษาอังกฤษ เปิดภาพต้นฉบับ ↗

ตั้งคำถาม ตรวจคิวรี แล้วเลือกเวลารัน



Threat Hunting — ส่วนกรอกคำถามและควบคุมคิวรีในหน้าจอตัวอย่าง ก่อนแปลงคำถามหรือรันคิวรี ข้อมูลเดโมประกอบคำอธิบาย หน้าจอภาษาอังกฤษ ไม่ใช่งานสืบสวนหรือผลตรวจจับของลูกค้า เปิดภาพต้นฉบับ ↗



ภาพขยายคำถามตัวอย่างที่พิมพ์ไว้ ช่องกรอกจริงยาวต่อออกไปนอกภาพตัดนี้ แต่ข้อความคำถามอยู่ครบ เปิดภาพต้นฉบับ ↗

01
ตั้งคำถาม
ระบุโจทย์ที่ต้องการสืบสวน

02
ตรวจคิวรี
ตรวจและแก้คิวรีที่สร้างขึ้นก่อนรัน

03
เลือกให้รัน
นักวิเคราะห์เป็นผู้สั่งรันคิวรีที่ตรวจแล้ว

หน้าจอตัวอย่างขอให้กรอกภาษาอังกฤษ ควรยืนยันภาษาที่ทีมต้องใช้ในเดโมทางเทคนิคร่วมกับพาร์ทเนอร์

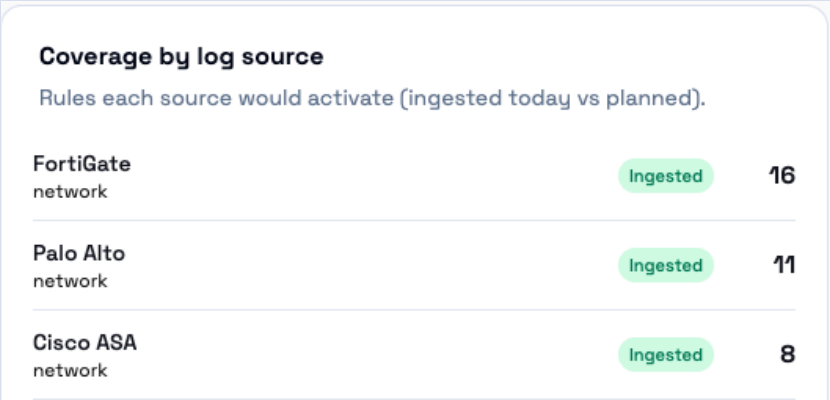
ความสามารถหลัก

- AI ช่วยตรวจจับภัยคุกคามและเชื่อมโยงเหตุการณ์
- ค้นหาภัยคุกคามด้วยภาษาธรรมชาติ ให้ AI แปลงเป็นคำสั่งค้นหาที่ตรวจสอบได้ก่อนรัน
- สืบสวนพร้อมบริบท MITRE ATT&CK และติดตามความครอบคลุมของการตรวจจับ

ความจุ ระยะเก็บข้อมูล การเริ่มใช้งาน การติดตั้ง การเชื่อมต่อระบบ บริการสนับสนุน และ SLA ยืนยันในการออกแบบโซลูชันและใบเสนอราคาที่เกี่ยวข้อง

zcrSIEM Brochure สรุปเส้นทางการสืบสวนแบบกระชับ ส่วนเอกสารนี้ใช้ประเมินรายละเอียดทางเทคนิคและแพ็กเกจ

เห็นว่าแหล่งข้อมูลใดทำให้กฎตรวจจับทำงานได้



Detection Coverage — ตัวอย่างแหล่ง log สามแถวที่แสดงครบ พร้อมจำนวนกฎ เป็นเพียงบางแถว ไม่ใช่รายการแหล่งข้อมูลทั้งหมด ข้อมูลเดโมไม่ได้ยืนยันประสิทธิผลการตรวจจับหรือรับประกันความครอบคลุม หน้าจอภาษาอังกฤษ เปิดภาพต้นฉบับ ↗

- ซิงก์กฎจาก Sigma และ Elastic พร้อมดู coverage ตาม tactic และแหล่งข้อมูล
- แดชบอร์ด การแจ้งเตือน และภาพรวมการตอบสนองแบบเรียลไทม์
- ต่อยอดจากการแจ้งเตือนไปสู่ incident workflow รายงาน MDR และการสื่อสารกับผู้บริหาร
- รองรับหลาย tenant โดยแยกข้อมูลและนโยบายของแต่ละ tenant ใช้ได้ทั้งบนคลาวด์และติดตั้งในองค์กร ทุกแพ็กเกจไม่จำกัดจำนวน tenant และผู้ใช้

จากสัญญาณเตือนสู่การตอบสนองที่มีผู้รับผิดชอบชัดเจน

01 / ตรวจจับ
เชื่อมโยงเหตุการณ์และค้นหาพฤติกรรมน่าสงสัย

02 / สืบสวน
ไล่ดูเหตุการณ์ที่เกี่ยวข้องด้วยคำสั่งค้นหาที่ตรวจสอบได้

03 / ตอบสนอง
ติดตามเหตุการณ์ ผู้รับผิดชอบ และความคืบหน้าการแก้ไข

04 / รายงาน
รวบรวมหลักฐานจากการปฏิบัติงานเป็นรายงาน MDR และรายงานสำหรับผู้บริหาร

zcrSIEM เป็นซอฟต์แวร์ การที่ระบบแสดง incident แดชบอร์ด รายงาน MDR หรือรายงานผู้บริหาร ไม่ได้แปลว่ารวมบริการเฝ้าระวังโดยนักวิเคราะห์หรือบริการตอบสนองเหตุการณ์ไว้ด้วย บริการเหล่านี้แยกต่างหาก

แพ็กเกจและราคา

แพ็กเกจ	ข้อมูลต่อวัน	ระยะเก็บข้อมูล	ราคาต่อเดือน (รวม VAT)
SaaS (Cloud)			
zcrSIEM-1	1 GB	90 วัน	฿6,000
zcrSIEM-3	3 GB	90 วัน	฿18,000
zcrSIEM-5	5 GB	90 วัน	฿30,000
zcrSIEM-10	10 GB	90 วัน	฿45,000
On-premises (ซอฟต์แวร์)			
SITE-10	10 GB	ตามพื้นที่จัดเก็บที่ลูกค้าจัดเตรียม	฿31,500
SITE-20	20 GB	ตามพื้นที่จัดเก็บที่ลูกค้าจัดเตรียม	฿52,500
SITE-50	50 GB	ตามพื้นที่จัดเก็บที่ลูกค้าจัดเตรียม	฿92,400
SITE-100	100 GB	ตามพื้นที่จัดเก็บที่ลูกค้าจัดเตรียม	฿158,900

ทุกแพ็กเกจชำระรายเดือน สัญญา 12 เดือน ราคารวม VAT และไม่จำกัดจำนวน tenant และผู้ใช้ แพ็กเกจ On-premises เป็นซอฟต์แวร์อย่างเดียว ติดตั้งบนเครื่องหรือ VM ของลูกค้าเอง

> การติดตั้งและตั้งค่าระบบ on-premises เสนอราคาแยกจากค่าสมาชิกรายเดือนตามขอบเขตงานจริง ผ่านช่องทางเชิงพาณิชย์ของพาร์ทเนอร์ที่ได้รับอนุมัติ

พาร์ทเนอร์ที่ได้รับอนุมัติให้การสนับสนุนด่านแรก และ zcr สนับสนุนด้านผลิตภัณฑ์ให้พาร์ทเนอร์ โดยกำหนดเงื่อนไขการสนับสนุนในสัญญาที่เกี่ยวข้อง

วางแผนประเมินทางเทคนิคกับพาร์ทเนอร์ที่ได้รับอนุมัติ

เตรียมรายการแหล่งข้อมูล ปริมาณรับเข้ารายวันโดยประมาณ ระยะเวลาเก็บ และรูปแบบติดตั้งที่ต้องการ พาร์ทเนอร์จะยืนยันขอบเขต ออกแบบโซลูชัน และจัดทำใบเสนอราคา

หารือการประเมินกับพาร์ทเนอร์ ↗ เอกสารผลิตภัณฑ์ ↗