ซอฟต์แวร์วิเคราะห์ความปลอดภัย · ประเมินผ่านพาร์ทเนอร์

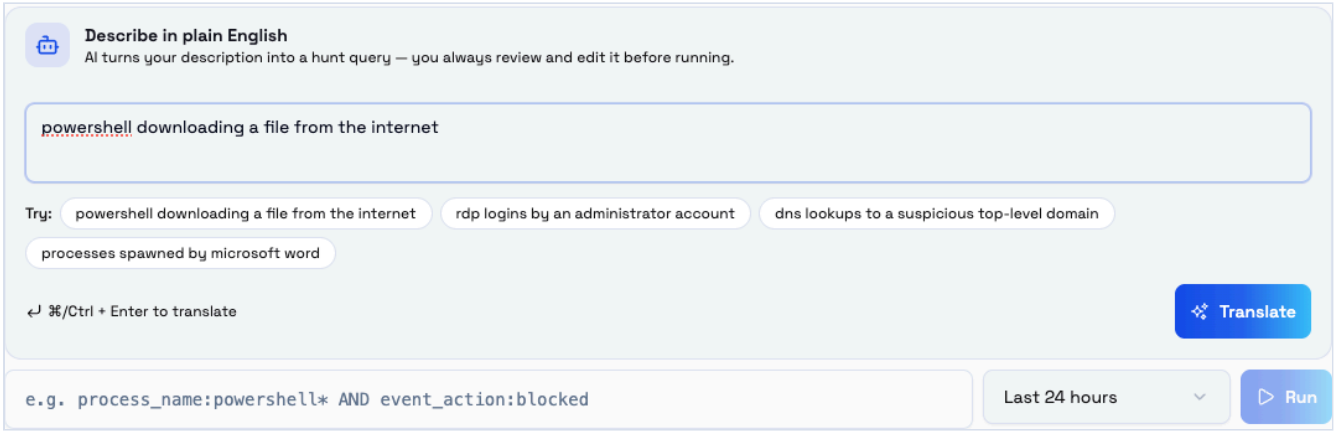
zcrSIEM

เปลี่ยนสัญญาณความปลอดภัย ให้เป็นงานสืบสวนที่ตรวจสอบได้

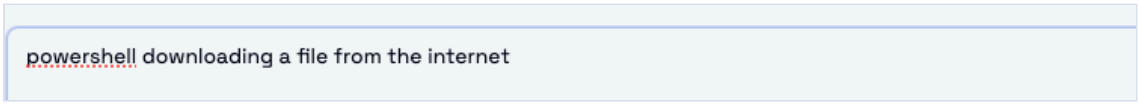
ตรวจจับ สืบสวน และเชื่อมโยงเหตุการณ์ความปลอดภัยไว้ในเวิร์กโฟลว์เดียวของนักวิเคราะห์

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

ตั้งคำถาม ตรวจคิวรี แล้วเลือกเวลารัน



Threat Hunting — ส่วนกรอกคำถามและควบคุมคิวรีในหน้าจอตัวอย่าง ก่อนแปลงคำถามหรือรันคิวรี ข้อมูลเดโมประกอบคำอธิบาย หน้าจอภาษาอังกฤษ ไม่ใช่งานสืบสวนหรือผลตรวจจับของลูกค้า เปิดภาพต้นฉบับ ↗



ภาพขยายคำถามตัวอย่างที่พิมพ์ไว้ ช่องกรอกจริงยาวต่อออกไปนอกภาพตัดนี้ แต่ข้อความคำถามอยู่ครบ เปิดภาพต้นฉบับ ↗

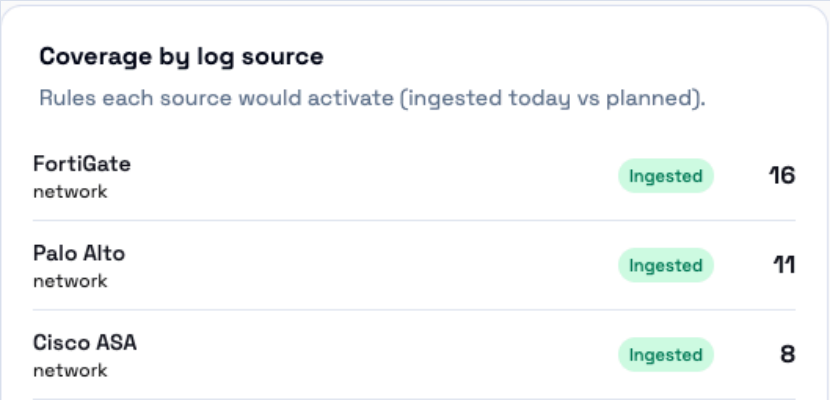
01
ตั้งคำถาม
ระบุโจทย์ที่ต้องการสืบสวน

02
ตรวจคิวรี
ตรวจและแก้คิวรีที่สร้างขึ้นก่อนรัน

03
เลือกให้รัน
นักวิเคราะห์เป็นผู้สั่งรันคิวรีที่ตรวจแล้ว

หน้าจอตัวอย่างขอให้กรอกภาษาอังกฤษ ควรยืนยันภาษาที่ทีมต้องใช้ในเดโมทางเทคนิคร่วมกับพาร์ทเนอร์

เห็นว่าแหล่งข้อมูลใดทำให้กฎตรวจจับทำงานได้



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

ความสามารถหลัก

- AI ช่วยตรวจจับภัยคุกคามและเชื่อมโยงเหตุการณ์
- ค้นหาภัยคุกคามด้วยภาษาธรรมชาติ ให้ AI แปลงเป็นคำสั่งค้นหาที่ตรวจสอบได้ก่อนรัน
- สืบสวนพร้อมบริบท MITRE ATT&CK และติดตามความครอบคลุมของการตรวจจับ
- ซิงก์กฎจาก Sigma และ Elastic พร้อมดู coverage ตาม tactic และแหล่งข้อมูล

จากสัญญาณเตือนสู่การตอบสนองที่มีผู้รับผิดชอบชัดเจน

01 / ตรวจจับ
เชื่อมโยงเหตุการณ์และค้นหาพฤติกรรมน่าสงสัย

02 / สืบสวน
ไล่ดูเหตุการณ์ที่เกี่ยวข้องด้วยคำสั่งค้นหาที่ตรวจสอบได้

03 / ตอบสนอง
ติดตามเหตุการณ์ ผู้รับผิดชอบ และความคืบหน้าการแก้ไข

04 / รายงาน
รวบรวมหลักฐานจากการปฏิบัติงานเป็นรายงาน MDR และรายงานสำหรับผู้บริหาร

เลือกซอฟต์แวร์ให้ตรงกับรูปแบบการทำงาน

ทีม SOC, MDR, MSSP, CISO และทีมความปลอดภัยองค์กร

ช่องว่างในการปฏิบัติงาน	ข้อมูลความปลอดภัย เครื่องมือที่แยกกัน และการแจ้งเตือนจำนวนมาก ทำให้ยากจะสรุปว่าเกิดอะไรขึ้นและควรทำอะไรต่อ
แหล่งข้อมูลความปลอดภัย	ไฟร์วอลล์ · Active Directory · เครื่องปลายทาง · เครือข่าย · Microsoft 365 · บริการคลาวด์
รูปแบบการใช้งาน	Cloud / SaaS หรือซอฟต์แวร์ติดตั้งในองค์กร (on-premises) โดยยืนยันในการออกแบบโซลูชัน
การรับข้อมูล	zcrSIEM รับ log จากแหล่งข้อมูลได้เองโดยตรง ทุกแพ็กเกจมีความจุรับข้อมูลต่อวันของตัวเอง จึงไม่ต้องมี zcrLog มาก่อน

- แดชบอร์ด การแจ้งเตือน และภาพรวมการตอบสนองแบบเรียลไทม์
- ต่อยอดจากการแจ้งเตือนไปสู่ incident workflow รายงาน MDR และการสื่อสารกับผู้บริหาร
- รองรับหลาย tenant โดยแยกข้อมูลและนโยบายของแต่ละ tenant ใช้ได้ทั้งบนคลาวด์และติดตั้งในองค์กร ทุกแพ็กเกจไม่จำกัดจำนวน tenant และผู้ใช้

zcrSIEM เป็นซอฟต์แวร์ การที่ระบบแสดง incident แดชบอร์ด รายงาน MDR หรือรายงานผู้บริหาร ไม่ได้แปลว่ารวมบริการเฝ้าระวังโดยนักวิเคราะห์หรือบริการตอบสนองเหตุการณ์ไว้ด้วย บริการเหล่านี้แยกต่างหาก

ความจุ ระยะเก็บข้อมูล การเริ่มใช้งาน การติดตั้ง การเชื่อมต่อระบบ บริการสนับสนุน และ SLA ยืนยันในการออกแบบโซลูชันและใบเสนอราคาที่เกี่ยวข้อง

พาร์ทเนอร์ที่ได้รับอนุมัติให้การสนับสนุนด่านแรก และ zcr สนับสนุนด้านผลิตภัณฑ์ให้พาร์ทเนอร์ โดยกำหนดเงื่อนไขการสนับสนุนในสัญญาที่เกี่ยวข้อง

อ่าน zcrSIEM Product Overview ต่อสำหรับกลุ่มแหล่งข้อมูล รูปแบบติดตั้ง แพ็กเกจ และขอบเขตการประเมิน

วางแผนประเมินทางเทคนิคกับพาร์ทเนอร์ที่ได้รับอนุมัติ

เตรียมรายการแหล่งข้อมูล ปริมาณรับเข้ารายวันโดยประมาณ ระยะเวลาเก็บ และรูปแบบติดตั้งที่ต้องการ พาร์ทเนอร์จะยืนยันขอบเขต ออกแบบโซลูชัน และจัดทำใบเสนอราคา

หารือการประเมินกับพาร์ทเนอร์ ↗ **เอกสารผลิตภัณฑ์ ↗**