

SIEM ที่ขับเคลื่อนด้วย AI

zcrSIEM

ระบบจัดการข้อมูลและเหตุการณ์ความปลอดภัยที่ใช้ AI ช่วยวิเคราะห์

ตรวจจับ สืบสวน และเชื่อมโยงเหตุการณ์ความปลอดภัยไว้ในเวิร์กโฟลว์เดียวของนักวิเคราะห์

เหมาะสำหรับ	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

ความสามารถหลัก

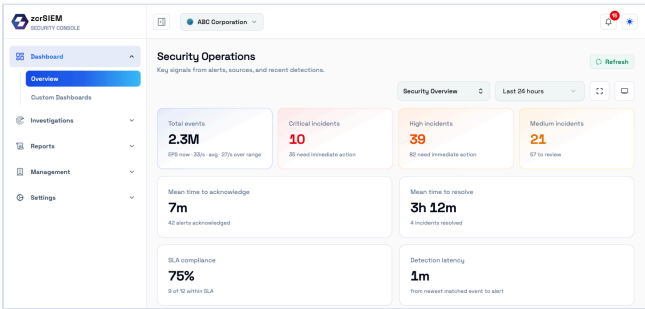
- AI ช่วยตรวจจับภัยคุกคามและเชื่อมโยงเหตุการณ์
- ค้นหาภัยคุกคามด้วยภาษาธรรมชาติ ให้ AI แปลงเป็นคำสั่งค้นหาที่ตรวจสอบได้ก่อนรับ
- สืบสวนพร้อมบริบท MITRE ATT&CK และติดตามความครอบคลุมของการตรวจจับ
- ซิงค์กฎจาก Sigma และ Elastic พร้อมดู coverage ตาม tactic และแหล่งข้อมูล
- แดชบอร์ด การแจ้งเตือน และภาพรวมการตอบสนองแบบเรียลไทม์
- ต่อยอดจากการแจ้งเตือนไปสู่ incident workflow รายงาน MDR และการสื่อสารกับผู้บริหาร
- รองรับหลาย tenant โดยแยกข้อมูลและนโยบายของแต่ละ tenant ใช้ได้ทั้งบนคลาวด์และติดตั้งในองค์กร ทุกแพ็คเกจ ไม่จำกัดจำนวน tenant และผู้ใช้

แหล่งข้อมูลและการเชื่อมต่อ

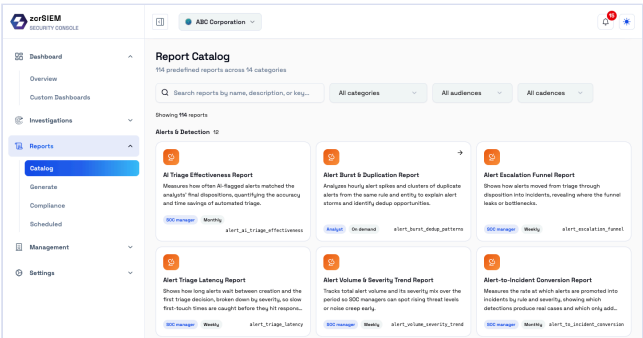
กลุ่มแหล่งข้อมูล	อุปกรณ์ Network · Firewall · IDS/IPS · Windows และ Linux · ระบบ Identity · Endpoint Security · Email Security · Cloud Platform · Container และ Kubernetes · EDR, NDR และ Network Sensor
Cloud Platform	AWS · Azure · Google Cloud · Huawei Cloud · GDCC Cloud · GDCC OpenData เชื่อมต่อผ่าน 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 ทุกแพ็คเกจมีความจุรับข้อมูลต่อวันของตัวเอง จึงไม่ต้องมี zcrLog มาก่อน

จากสัญญาณเตือนสู่การตอบสนองที่มีผู้รับผิดชอบชัดเจน

01 / ตรวจสอบ	เชื่อมโยงเหตุการณ์และค้นหาพฤติกรรมน่าสงสัย
02 / สืบสวน	ไล่ดูเหตุการณ์ที่เกี่ยวข้องด้วยคำสั่งค้นหาที่ตรวจสอบได้
03 / ตอบสนอง	ติดตามเหตุการณ์ ผู้รับผิดชอบ และความคืบหน้าการแก้ไข
04 / รายงาน	รวบรวมหลักฐานจากการปฏิบัติงานเป็นรายงาน MDR และรายงานสำหรับผู้บริหาร



แดชบอร์ดปฏิบัติการความปลอดภัย — ตัวอย่างจากสภาพแวดล้อมโม ไม่ใช้ตัวเลขจริง



แคตตาล็อกรายงาน — ตัวอย่างจากสภาพแวดล้อมโม ไม่ใช้ตัวเลขจริง

ภาพจากคอนโซล

zcrSIEM SECURITY CONSOLE

ABC Corporation

Threat Hunting

Search normalized telemetry, investigate patterns, and save repeatable hunts.

Query Workspace Run ad-hoc searches across telemetry

Hunt Library Browse saved hunts and coverage gaps

Describe in plain English

Describe in plain English AI turns your description into a hunt query — you always review and edit it before running.

powershell downloading a file from the internet

Try: powershell downloading a file from the internet rdp logins by an administrator account dns lookups to a suspicious top-level domain processes spawned by microsoft word

⌘/Ctrl + Enter to translate

Translate

e.g. process_name:powershell* AND event_action:blocked

Last 24 hours

Run

field:value · combine with AND OR NOT · wildcard * · numeric > < >= <= · quote values with spaces

ค้นหาภัยคุกคามด้วย AI — ตัวอย่างจากสภาพแวดล้อมเดโม ไม่ใช่ตัวจริง

zcrSIEM SECURITY CONSOLE

ABC Corporation

Detection Coverage

Measure source and MITRE ATT&CK coverage to expose detection blind spots.

Rule Catalog Manage and synchronize detection logic

Coverage Source and MITRE ATT&CK coverage

Engine Health Workers, queues, and runtime performance

Live 39 Rules a log source feeds today

Ready 15 Activate when a planned source...

Uncovered 0 No planned source provides their...

ATT&CK techniques 35/35 24 live · 100% covered · v1.1

Coverage by log source Rules each source would activate (Ingested today vs planned).

FortiGate network	Ingested	16
Palo Alto network	Ingested	11
Cisco ASA network	Ingested	8
Sangfor NGAF network	Ingested	6
Sangfor Proxy proxy	Ingested	7
CrowdStrike Falcon endpoint	Ingested	12

MITRE ATT&CK coverage by tactic Base techniques with a rule — the live portion fires on currently-ingest...

Reconnaissance	100%
Initial Access	100%
Execution	100%
Persistence	100%
Privilege Escalation	100%
Defense Evasion	100%
Credential Access	100%
Discovery	100%

ความครอบคลุม MITRE ATT&CK — ตัวอย่างจากสภาพแวดล้อมเดโม ไม่ใช่ตัวจริง

แพ็คเกจและราคา

แพ็คเกจ	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

ทุกแพ็คเกจชำระรายเดือน สัญญา 12 เดือน ราคารวม VAT และไม่จำกัดจำนวน tenant และผู้ใช้ แพ็คเกจ On-premises เป็นซอฟต์แวร์อย่างเดียว ติดตั้งบนเครื่องหรือ VM ของลูกค้าเอง

ความจุ ระยะเก็บข้อมูล การเริ่มใช้งาน การติดตั้ง การเชื่อมต่อระบบ บริการสนับสนุน และ SLA ยืนยันในการออกแบบโซลูชันและใบเสนอราคาที่เกี่ยวข้อง zcrSIEM เป็นซอฟต์แวร์ การที่ระบบแสดง incident แดชบอร์ด รายงาน MDR หรือรายงานผู้บริหาร ไม่ได้แปลว่ารวมบริการเฟิร์มแวร์โดยนักวิเคราะห์หรือบริการตอบสนองเหตุการณ์ไว้ด้วย บริการเหล่านี้แยกต่างหาก

ติดต่อพาร์ทเนอร์ของ zcr เพื่อนัดสาธิตระบบและพูดคุยว่าโซลูชันเหมาะกับองค์กรของคุณหรือไม่

พาร์ทเนอร์จะสาธิตระบบให้คุณ ช่วยประเมินขนาดระบบร่วมกับทีมของคุณ แล้วจัดทำการออกแบบโซลูชันและใบเสนอราคา

ประเมินผ่านพาร์ทเนอร์ ↗

zcr.ai/contact/