LOG MANAGEMENT

zcrLog

เก็บ Log ให้พร้อมค้นหา และตรวจสอบย้อนหลัง

zcrLog รวบรวม เก็บรักษา ค้นหา และจัดทำรายงานจาก Log สำหรับทีม IT และทีมที่ดูแลการปฏิบัติตามกฎหมาย เลือกใช้งานแบบ Cloud, Dedicated VM หรือ Hardware Appliance ผ่านพาร์ทเนอร์ที่ได้รับอนุมัติ

รูปแบบติดตั้ง

- Cloud / SaaS
- Dedicated VM
- Hardware Appliance

1 **รวบรวม**
รับข้อมูลผ่าน Syslog UDP/TCP และ API ที่รองรับ

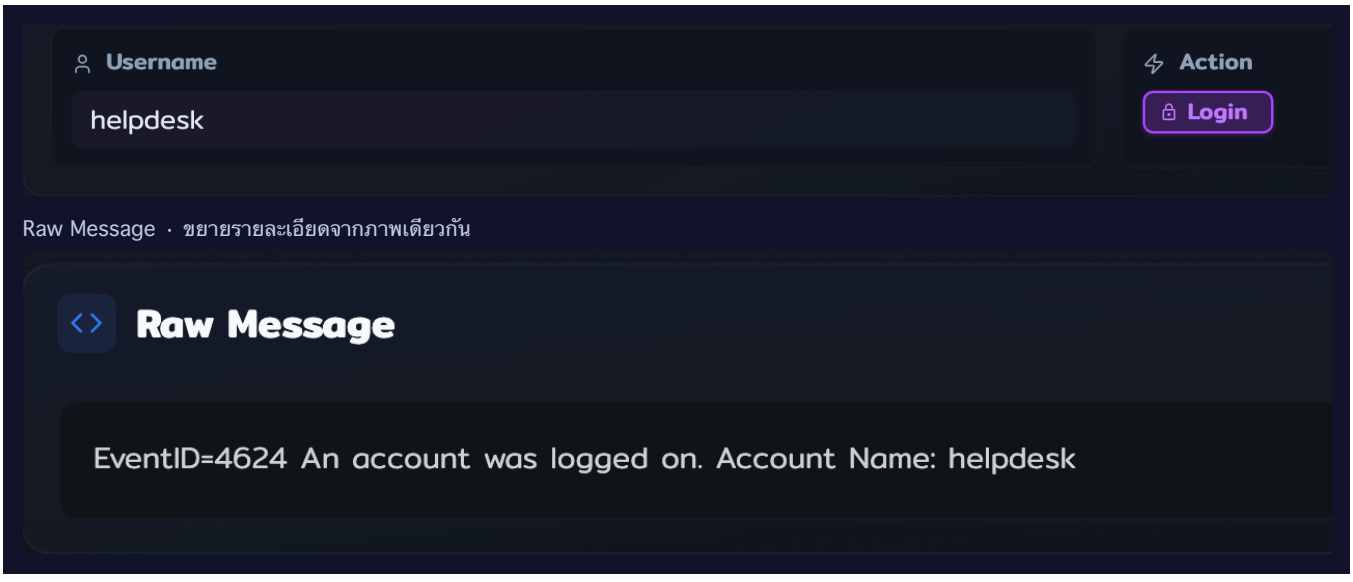
2 **เก็บรักษา**
กำหนดระยะเก็บตามแพ็กเกจ ปริมาณข้อมูล และพื้นที่จัดเก็บ

3 **ค้นหาและรายงาน**
กรองตามเวลา แหล่งข้อมูล ผู้ใช้ และ Event ID

แผนภาพแนวคิดการใช้งาน ไม่ใช่สถาปัตยกรรมติดตั้งจริง

จากเหตุการณ์ สู่หลักฐานที่ตรวจสอบได้

DEMO / 4624



ภาพตัดจาก demo จริง ข้อมูลเหตุการณ์เป็นตัวอย่าง ไม่ใช่ข้อมูลลูกค้าหรือผลทดสอบสมรรถนะ

ระบบต้นทาง: **Windows Server** ผู้ใช้: **helpdesk** การกระทำ: **Login**

ประเมินแหล่ง Log และรูปแบบติดตั้งกับพาร์ทเนอร์

ดูระบบ demo ↗ ปรึกษาพาร์ทเนอร์ ↗

รายละเอียดผลิตภัณฑ์

การรับและเก็บข้อมูล

02

ขนาดระบบขึ้นกับชนิด Log วิธีส่งข้อมูล และระยะเวลาที่ต้องเก็บ ตัวเลขบน dashboard แสดงปริมาณการใช้งาน ไม่ใช่ผลทดสอบสมรรถนะ

รายการ	ขอบเขตและเงื่อนไข
แหล่งข้อมูล	Firewall, Active Directory, Endpoint Security (เช่น CrowdStrike Falcon), Microsoft 365, Microsoft Entra ID, AWS CloudTrail, Google Cloud audit log และอุปกรณ์เครือข่ายที่ส่ง Syslog ได้ ส่วน parser และสิทธิ์ API ของแต่ละแหล่งจะยืนยันกันในขั้นออกแบบระบบ
รับและส่งต่อ	รับข้อมูลผ่าน Syslog UDP/TCP และ API ที่รองรับ และส่งต่อไปยัง Syslog Server หรือ Log Receiver โดยกำหนด source, destination และ port
เวลาอ้างอิง	ตั้งค่า NTP และ time zone ให้สอดคล้องกันก่อนเทียบเหตุการณ์จากหลายระบบ
ระยะเก็บ	เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามมาตรา 26 ของ พ.ร.บ. คอมพิวเตอร์ฯ ได้ตั้งแต่ 90 วันถึง 2 ปี ระยะเก็บจริงขึ้นกับแพ็กเกจ ปริมาณข้อมูล และพื้นที่จัดเก็บ และไม่ใช่ทุกแพ็กเกจที่รวมการเก็บ 2 ปี
ความถูกต้องของข้อมูล	ตรวจสอบความถูกต้องของข้อมูลด้วย MD5, SHA-1 และ SHA-256 และเข้ารหัส Log ด้วย AES-128
Archive / Export	รองรับ archive, JSON, CSV, Parquet และการสำรองข้อมูลแบบ incremental หรือ full
การกู้คืน	กู้ข้อมูลจาก archive/backup ตรวจพื้นที่ใช้จริง และกำหนดเวลา auto archive / cleanup ตามนโยบาย
ปลายทางสำรอง	Cloud/SaaS สำรองข้อมูลผ่าน HTTPS ไปยังบริการ Cloud ส่วน Hardware Appliance และ Dedicated VM ใช้ external disk, FTP/TFTP และ manual download ได้ด้วย ปลายทางและวิธีป้องกันข้อมูลจะกำหนดในขั้นออกแบบระบบ
การจัดเก็บซ้ำซ้อน	รองรับ redundant storage ตามสถาปัตยกรรมที่ออกแบบ ต้องแยกจากการสำรองข้อมูลและการทดสอบ restore

Microsoft 365, Entra ID และแหล่งข้อมูลบน Cloud

zcrLog เก็บ audit log ของ Microsoft 365 (Exchange, SharePoint และ Teams) ผ่าน Office 365 Management API และเก็บ sign-in log กับ audit log ของ Microsoft Entra ID นอกจากนี้ยังเก็บ AWS CloudTrail, Google Cloud audit log และ Log จาก CrowdStrike Falcon ได้ด้วย

รายละเอียดผลิตภัณฑ์

การค้นหาและการปฏิบัติงาน

03

เริ่มจากคำถามปฏิบัติงาน: ข้อมูลเข้าอยู่หรือไม่ เหตุการณ์เกิดเมื่อใด และส่งหลักฐานให้ผู้รับผิดชอบได้อย่างไร

รายการ	ขอบเขตและเงื่อนไข
ค้นหาและกรอง	ค้นหา Log ที่เก็บไว้ และกรองตามช่วงเวลา, source/device, IP, user, event, application, protocol และ severity
แดชบอร์ด	จำนวน Log, Top-N ของแหล่งข้อมูล, EPS, storage, retention, เหตุการณ์ล่าสุด และ audit trail ตามมุมมองของ console
บริบทเหตุการณ์	Incident grouping, MITRE ATT&CK mapping, risk score, attack map และ IP intelligence เป็นเครื่องมือประกอบการตรวจสอบ ไม่ใช่คำรับรองว่าจะตรวจพบทุกการโจมตี
กฎการตรวจจับ	สร้าง rule ได้ทั้งแบบ custom, ใช้ AI ช่วย, Sigma และ template ควรตรวจและทดสอบ rule กับข้อมูลจริงในระบบของคุณก่อนใช้งาน
รายงาน	เลือกช่วงเวลาและหลักฐานเพื่อจัดทำรายงาน executive summary ได้ ส่วนรายงาน MDR (สรุปความรุนแรง แนวโน้มการโจมตี Incident ที่ต้องติดตาม รายละเอียดทางเทคนิค และคำแนะนำจาก AI) เป็นส่วนหนึ่งของบริการ zcrMDR ไม่ใช่สิทธิ์การใช้งานเดี่ยวของ zcrLog และงาน SIEM เต็มรูปแบบอยู่ใน zcrSIEM ซึ่งเป็นผลิตภัณฑ์แยก
แจ้งเตือน	Email, Microsoft Teams และ LINE ตามการตั้งค่า detection/alert rules และสิทธิ์ของช่องทางปลายทาง
สิทธิ์และ Audit	MFA, role-based access control (RBAC), multi-tenant, ประวัติ login/logout, access, configuration changes และข้อผิดพลาดของระบบ
ตรวจสุขภาพระบบ	CPU, memory, disk, network, filesystem และ services ตาม deployment โดย threshold ของ CPU/RAM/storage ระดับเครื่องใช้เฉพาะการติดตั้งแบบ on-premises

ฟีเจอร์ของผลิตภัณฑ์กับงานบริการ

หน้าจอ incident และรายงานเป็นฟีเจอร์ของผลิตภัณฑ์ ส่วนการเฝ้าระวังโดยนักวิเคราะห์ การตอบสนองเหตุการณ์ และ SLA เป็นงานบริการที่รวมอยู่ด้วยเฉพาะเมื่อระบุไว้ในสัญญา

ข้อมูลสำหรับเลือกรุ่น

Hardware Appliance

04

สเปกที่เผยแพร่ของรุ่น ICT ค่า EPS (อีเวนต์ต่อวินาที) เป็นค่าที่ประกาศไว้ของแต่ละรุ่น พาร์ทเนอร์จะช่วยเลือกรุ่นให้เหมาะกับปริมาณงานจริงและยืนยัน BOM ก่อนสั่งซื้อ

รายการ	ICT1	ICT2	ICT3
CPU	8 Core	8 Core	16 Core
หน่วยความจำ	16 GB	32 GB	64 GB
SSD	1 TB	2 × 480 GB	2 × 480 GB
HDD	—	2 × 4 TB	2 × 8 TB
Network	1 × 1 GE RJ45	2 × 1 GE RJ45	2 × 1 GE RJ45
Form factor	Mini PC	1 RU	1 RU
EPS ตามรุ่น	1,000	7,000	20,000
อุปกรณ์แนะนำ	3–5	6–15	16–30
Retention ตั้งต้น	90 วัน[1]	90 วัน[1]	90 วัน[1]

Retention

[1] ระยะเก็บขึ้นกับปริมาณข้อมูลและพื้นที่ที่ใช้งานได้จริง ต้องรวมผลของ RAID และพื้นที่สำรองในการคำนวณ

RAID / BOM

รองรับ RAID 0/1/5/10 ตาม configuration โดยค่าเริ่มต้นเป็น RAID 1 สำหรับรุ่นที่รองรับ ต้องยืนยัน BOM ที่จัดส่งจริงกับพาร์ทเนอร์

Power

เอกสารนี้ไม่ระบุค่ากำลังไฟ พาร์ทเนอร์จะยืนยันข้อกำหนดด้านไฟฟ้าและ BOM ของรุ่นที่จัดส่งก่อนสั่งซื้อ

สิ่งที่รวมอยู่ในทุกแพ็กเกจ

ทุกแพ็กเกจของ zcrLog มีการรับ Syslog, dashboard, MITRE ATT&CK mapping, rule ที่ใช้ AI ช่วย, executive summary, การแจ้งเตือน, backup และ archive, ความปลอดภัยของบัญชี และ multi-tenant ส่วน onboarding, HA/DR และ SLA จะรวมอยู่ด้วยเฉพาะเมื่อระบุไว้ในข้อเสนอ ส่วนรายงาน MDR เป็นส่วนหนึ่งของบริการ zcrMDR ไม่ใช่สิทธิ์ของแพ็กเกจ zcrLog

→ **ประเมินแหล่ง Log และรูปแบบติดตั้งกับพาร์ทเนอร์**

ยืนยันปริมาณ Log ระยะเก็บ พื้นที่ใช้งานได้จริง และ BOM กับพาร์ทเนอร์ก่อนสั่งซื้อ · ปรึกษาพาร์ทเนอร์ ↗

ข้อมูลสำหรับเลือกรุ่น

Dedicated VM และ Cloud

05

แพ็กเกจ Dedicated VM กำหนดตามทรัพยากรขั้นต่ำและพื้นที่จัดเก็บ ส่วนแพ็กเกจ Cloud กำหนดตามปริมาณข้อมูลต่อวัน (GB/วัน) ค่า EPS และจำนวนอุปกรณ์เป็นค่าอ้างอิง นำมาใช้แทนกันเป็นขีดจำกัดความจุไม่ได้

Dedicated VM · ICTC

รายการ	ICTC1	ICTC2	ICTC3
CPU ขั้นต่ำ	4 vCore	4 vCore	4 vCore
RAM ขั้นต่ำ	4 GB	4 GB	4 GB
Storage	1 TB	2 TB	3 TB
อุปกรณ์อ้างอิง	3	5	10
Retention ตั้งต้น	90 วัน	90 วัน	90 วัน

แพ็กเกจ Dedicated VM ไม่กำหนด EPS เป็นขีดจำกัด แต่ throughput จริงขึ้นกับทรัพยากรที่จัดสรรให้ VM ค่าในตารางเป็นสเปกขั้นต่ำ หากปริมาณงานสูงควรเพิ่มทรัพยากร

Cloud / SaaS · ปริมาณรับข้อมูลต่อวัน

แพ็กเกจ	Cloud1	Cloud2	Cloud3	Cloud4
GB / วัน	1	3	5	10
Retention ตั้งต้น	90 วัน	90 วัน	90 วัน	90 วัน
จำนวนอุปกรณ์	ไม่จำกัด	ไม่จำกัด	ไม่จำกัด	ไม่จำกัด

SaaS คิดแพ็กเกจตาม GB/วัน ไม่จำกัดจำนวนอุปกรณ์หรือ EPS เพื่อคิดราคา ตารางแสดง Cloud1–4; แพ็กเกจรับข้อมูลพื้นฐานขยายได้ถึง 50 GB/วัน ส่วน retention add-on 180 วัน, 365 วัน และ 2 ปีเสนอเฉพาะระดับไม่เกิน 10 GB/วัน ไม่เสนอ add-on เหล่านี้เมื่อรับข้อมูลเกิน 10 GB/วัน

ขอบเขตผลิตภัณฑ์ เอกสารนี้อธิบาย zcrLog สำหรับการเก็บ Log และหลักฐาน ไม่ใช่ข้อเสนอ SIEM หรือบริการ MDR แบบครบวงจร zcrSIEM เป็นผลิตภัณฑ์แยกและไม่จำเป็นต้องติดตั้ง zcrLog ก่อน

รายละเอียดผลิตภัณฑ์

การประเมินผ่านพาร์ทเนอร์

06

พาร์ทเนอร์จะไล่ตรวจรายการเหล่านี้ร่วมกับคุณตอนออกแบบระบบและทำใบเสนอราคา เพื่อให้การติดตั้งตรงกับข้อมูลจริงและผู้รับผิดชอบในองค์กร

รายการประเมิน	สิ่งที่ต้องยืนยัน
ข้อมูลเข้า	รายการแหล่ง Log, protocol, parser, API permissions, GB/วัน และช่วง peak
นโยบายข้อมูล	ระยะเก็บ ตำแหน่งจัดเก็บ สิทธิ์เข้าถึง NTP และแผน archive/backup
การทดสอบรับมอบ	ตรวจ event จากต้นทาง เทียบเวลา ค้นหาข้อมูล ทดสอบแจ้งเตือน และทดลอง restore
ผู้รับผิดชอบ	ระบุเจ้าของ source, platform, channel partner และเส้นทาง escalation
ขอบเขตบริการ	ยืนยัน integration, onboarding, HA/DR, support, SLA และงานนอกขอบเขตเป็นลายลักษณ์อักษร

มาตรฐานและเอกสารสำหรับจัดซื้อ

อ้างอิงมาตรฐาน มศอ. 4003.1-2560 สำหรับระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ให้พาร์ทเนอร์ยืนยันใบรับรองผลิตภัณฑ์ที่ตรงกับรุ่นซอฟต์แวร์และรูปแบบติดตั้งที่เสนอ

ลิงก์ NECTEC เป็นเอกสารเกณฑ์มาตรฐาน สำหรับการจัดซื้อให้ตรวจสอบใบรับรองฉบับจริง เลขที่ หน่วยงานผู้ออก วันที่ออกและสิ้นอายุ รวมถึงขอบเขตที่ใช้กับโครงการ

การใช้ระบบที่ได้รับการรับรองไม่ทดแทนหน้าที่ขององค์กรตามกฎหมาย

อ่านมาตรฐาน NECTEC ↗ ขอเอกสารประกอบผ่านพาร์ทเนอร์ ↗

นัดประเมินกับพาร์ทเนอร์ zcr

การเสนอราคา ทำสัญญา และส่งมอบให้ลูกค้าดำเนินผ่าน distributor, reseller/SI หรือ MSP/MSSP ที่ได้รับอนุมัติ

ติดต่อพาร์ทเนอร์ ↗ ดูแพ็กเกจปัจจุบัน ↗ เปิดหน้า Demo ↗

สเปกและแพ็กเกจอาจเปลี่ยนแปลงได้ สอบถามรายละเอียดล่าสุดสำหรับข้อเสนอของคุณได้จากพาร์ทเนอร์

7 · รายละเอียดสำหรับการออกแบบระบบ

รายละเอียดผลิตภัณฑ์

รายละเอียดสำหรับการออกแบบระบบ

07

รายละเอียดทางวิศวกรรมที่ต้องตกลงร่วมกับพาร์ทเนอร์ตอนออกแบบระบบ ไม่ใช่คำรับรอง SLA

รายการ	ขอบเขตและเงื่อนไข
การส่งต่อ Log	การส่งต่อ Log ไม่เปลี่ยนแปลงข้อมูลต้นทาง และเลือก source, destination, port และช่วงเวลาได้ ตรวจสอบความครบถ้วนของ payload และเวลาที่ปลายทางระหว่างการทดสอบรับมอบ
Archive และการบีบอัด	การบีบอัด Archive สูงสุดได้ถึง 15 เท่า ขึ้นอยู่กับเนื้อหา Log วัดอัตราจริงจาก Log ของคุณเอง อย่าใช้ค่าสูงสุดเป็นตัวรับประกันพื้นที่จัดเก็บ
Backup และการกู้คืน	ปลายทาง backup ขึ้นกับรูปแบบการติดตั้ง (ดูหน้า 2) ควรทดสอบกู้คืนข้อมูลจากปลายทางที่เลือกไว้ในการทดสอบรับมอบด้วย
พื้นที่เก็บ	ตั้งเวลา auto archive / cleanup และลบ Log ตามนโยบายเมื่อใช้พื้นที่ถึงเกณฑ์ ขยาย storage ของ VM ได้ตามแพ็กเกจและข้อเสนอที่เลือก
Monitoring แบบ on-premises	การติดตาม CPU, memory, disk, network, filesystem และ service ระดับ host ใช้กับการติดตั้งแบบ on-premises threshold เหล่านี้ไม่ใช่สิทธิ์ที่รับประกันให้ทุก SaaS tenant
Network threshold	มี threshold สำหรับ network utilization, error packet และ discard packet ตรวจสอบ interface ที่ติดตามและข้อมูลที่เก็บได้จริงในสภาพแวดล้อมของคุณ
Role และ Audit	กำหนด role/privilege เพิ่มเติมได้; บันทึก login/logout, access, system status changes, failures/errors และ system structure/configuration changes
Reports และ Ingestion	เลือกช่วงรายงานได้ 1, 3, 5, 7, 30, 60 หรือ 90 วัน หรือกำหนดเอง ส่วนการรับข้อมูลมี Syslog UDP/TCP, Office 365 Management API สำหรับ Microsoft 365, EDR API key, custom integration และ per-device analytics โดย connector ของแต่ละแหล่งข้อมูลจะยืนยันกันในขั้นออกแบบระบบ
MSSP และขอบเขตบริการ	การจัดการแบบ multi-tenant ไม่ได้มาพร้อมสิทธิ์ขายต่อแบบ MSSP หรือบริการ MDR โดยอัตโนมัติ สิทธิ์ใช้งาน ความรับผิดชอบ และขอบเขตการสนับสนุนจะระบุไว้ในสัญญากับพาร์ทเนอร์