ความปลอดภัย OT / เอกสารข้อมูลทางเทคนิค

zcrOT

เห็นการสื่อสาร OT ตรวจสอบเหตุการณ์อย่างมีบริบท

zcrOT รวมการมองเห็นเครือข่ายแบบพาสซีฟ การตรวจจับที่รองรับโปรโตคอล Modbus และข้อมูลพลังงานไว้ในมุมมองเดียว สำหรับทีมอุตสาหกรรมและพลังงาน

รูปแบบให้บริการ

- Cloud / SaaS
- เครื่องเสมือน (VM)
- ฮาร์ดแวร์แอปพลายแอนซ์

1 **รับข้อมูล** — TAP / SPAN และ telemetry

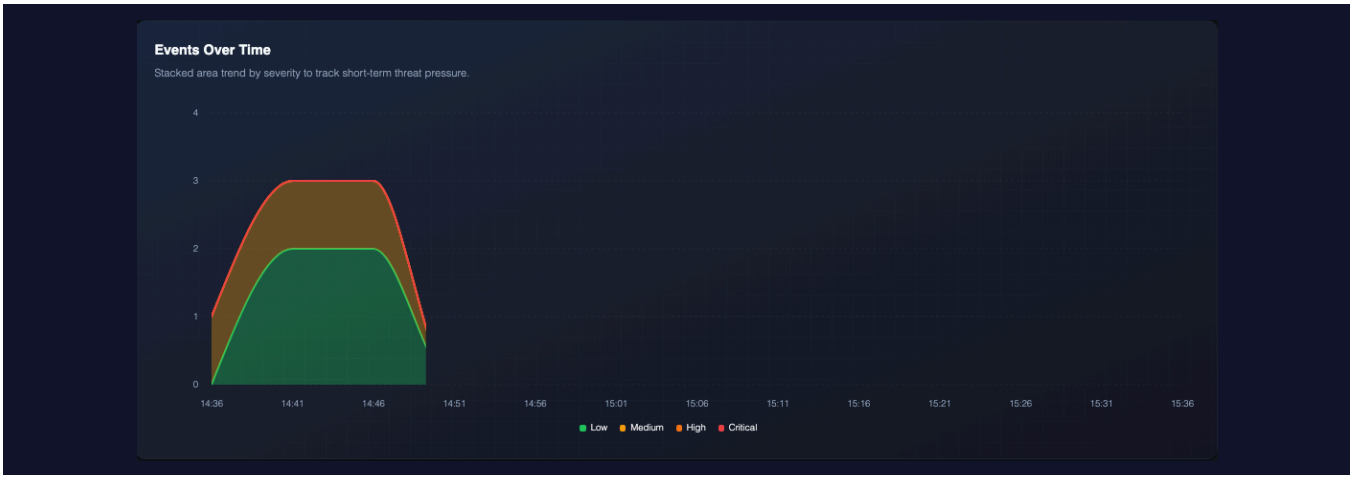
2 **สร้างบริบท** — อุปกรณ์ เส้นทาง ค่าฐาน

3 **ตรวจสอบ** — ความเสี่ยงและคัดแยกเหตุ

4 **รายงาน** — ทบทวนรายสัปดาห์ / เดือน

แผนภาพแนวคิดของงานปฏิบัติการ ไม่ใช่ผังติดตั้งจริง และไม่ได้หมายถึงการสั่งควบคุมหรือบล็อกอุปกรณ์

ตรวจสอบแนวโน้มเหตุการณ์



Security Exposure → Events Over Time: จำนวนเหตุการณ์แยกตามระดับความรุนแรงในช่วงเวลาที่เลือก เป็นข้อมูลเดโมเพื่อประกอบคำอธิบาย ตัวเลขไม่ใช่ผลลัพธ์ของลูกค้า ขีดจำกัดของระบบ หรือค่าความแม่นยำ หน้าจอผลิตภัณฑ์ในภาพเป็นภาษาอังกฤษ เปิดภาพต้นฉบับขนาดเต็ม

เนื้อหาในเอกสาร

2 ความสามารถทางเทคนิค
3 เงื่อนไขการค้าและรูปแบบติดตั้ง
4 ขอบเขตการติดตั้งและการทำงาน
5 ตรวจสอบหลักฐานก่อนนำไปใช้งาน
6 อุปกรณ์และเมทาดาทาโปรโตคอล
7 การตรวจจับและความเชื่อถือได้ของระบบควบคุม
8 หลักฐานแพ็กเก็ตและการส่งออก
9 การเชื่อมโยงเหตุ การบริหาร และรายงาน

ขอบเขตทางเทคนิค

ความสามารถทางเทคนิค

02

ใช้บริบทเครือข่าย โปรโตคอล และข้อมูลที่ตรวจพบ เพื่อเลือกอุปกรณ์หรือเหตุการณ์ที่ควรตรวจสอบต่อ

ความสามารถ	ขอบเขตทางเทคนิค
ค้นพบอุปกรณ์แบบพาสซีฟ	มองเห็นทราฟฟิก OT และจุดเชื่อมต่อ IT/OT ผ่าน network TAP, SPAN / mirror port หรือข้อมูลจากเซนเซอร์ ขอบเขตขึ้นอยู่กับจุดรับทราฟฟิก
แผนที่การสื่อสาร	แสดงต้นทาง ปลายทาง โปรโตคอล พอร์ต และทิศทาง เชื่อมบริบทของ OT gateway และ logical unit เข้ากับเส้นทางที่ตรวจพบ
ตรวจจับ Modbus	จำแนกคำสั่ง read, write, error และ malformed ต้องทดสอบเวอร์ชันโปรโตคอลและทราฟฟิกของไซต์ที่ต้องการใช้งาน
ตัวตนและความเสี่ยง	แท็กอุปกรณ์ที่รู้จัก/ไม่รู้จัก ใช้บริบทตัวตน คะแนนความเสี่ยง และผลประเมินโอกาสถูกโจมตีเพื่อจัดลำดับตรวจสอบ ไม่ใช่หลักฐานยืนยันว่าถูกโจมตีแล้ว
ค่าฐานพฤติกรรม	วิเคราะห์ทราฟฟิกเซนเซอร์แบบเรียลไทม์หรือใกล้เคียง เทียบพฤติกรรมกับค่าฐานและตรวจการเปลี่ยนแปลง ไม่ใช่การรับประกันค่า latency ตลอดเส้นทาง
ข้อมูลพลังงาน	เก็บและวิเคราะห์ข้อมูลปัจจุบัน/ย้อนหลัง รวมถึงกำลังผลิตโซลาร์ สถานะเครื่องชาร์จรถยนต์ไฟฟ้า (EV) และไฟฟ้าโรงงาน เมื่อมีแหล่งข้อมูลที่ต้องใช้
การรับข้อมูลต้นทาง	พอร์ต syslog แยกตามแหล่งข้อมูลและตัวนับทราฟฟิกแบบเรียลไทม์ ช่วยตรวจว่าข้อมูลที่คาดหวังส่งเข้ามาหรือไม่
คัดแยกเหตุและรายงาน	ตรวจสอบเหตุการณ์ผ่านขั้นตอน triage และสร้างรายงานการมองเห็น/ความปลอดภัย OT รายสัปดาห์หรือรายเดือน เพื่อการทบทวนภายใน ไม่ใช่การรับรองมาตรฐาน
เชื่อมต่อผ่าน API	อินเทอร์เฟซสำหรับเชื่อมระบบ (API) และเฟรมเวิร์กเชื่อมต่อระบบ รองรับงานร่วมกับศูนย์ปฏิบัติการความปลอดภัย (SOC), ระบบรวมและวิเคราะห์เหตุการณ์ (SIEM) และระบบมอนิเตอร์หรือวิเคราะห์ข้อมูล โดยต้องยืนยันอินเทอร์เฟซและฟิลด์ที่จะใช้ก่อน

สำหรับทีมเทคโนโลยีปฏิบัติการ (OT) ระบบควบคุมอุตสาหกรรม (ICS) โรงงาน เครือข่าย และความปลอดภัย รวมถึงพาร์ทเนอร์ผู้ให้บริการดูแลความปลอดภัย

ขอบเขตทางเทคนิค

เงื่อนไขการค้าและรูปแบบติดตั้ง

03

มีทั้ง SaaS, VM และ Hardware Appliance เลือกรูปแบบติดตั้งและขอบเขตข้อมูลร่วมกับพาร์ทเนอร์ที่ได้รับอนุมัติ ก่อนกำหนดโครงสร้างพื้นฐาน

รูปแบบติดตั้ง	แพ็กเกจและเงื่อนไขการค้า
zcrOT-Appliance	ซื้อขาด ฿3,200,000 รวมปีแรก ยังไม่รวม VAT ประกอบด้วย security collector 1 เครื่อง, zcrLog server 1 เครื่อง และชุดซอฟต์แวร์ zcrOT 1 ชุด ตั้งแต่ปีที่ 2 คิดค่าบำรุงรักษา (MA) รายปี 30% ของราคาแพ็กเกจสุทธิ หรือ ฿960,000/ปี บวก VAT
Cloud / SaaS	฿1,500,000/ปี ยังไม่รวม VAT ประกอบด้วย security collector 1 เครื่อง, zcrLog SaaS 1 ปี และชุดซอฟต์แวร์ zcrOT 1 ชุด
เครื่องเสมือน (VM)	ยังรองรับ VM แบบติดตั้งภายในองค์กรบนระบบที่ลูกค้าดูแล พาร์ทเนอร์ที่ได้รับอนุมัติเสนอราคาตามการกำหนดค่า โครงสร้างพื้นฐาน และขอบเขตงาน แหล่งราคาแพ็กเกจนี้ไม่ได้กำหนดราคา VM แยกไว้

สิ่งที่รวมในทั้งสองแพ็กเกจ

การเชื่อมระบบและทดสอบส่งมอบ โมเดลตรวจจับด้วย AI ข้อมูลภัยคุกคามและการอัปเดต การมอนิเตอร์ผ่าน Cloud API และการสนับสนุน ต้องตกลงสเปกฮาร์ดแวร์ เกณฑ์รับมอบงาน ขอบเขตต่ออายุ เวลาสนับสนุน และ SLA กับพาร์ทเนอร์ที่ได้รับอนุมัติ

> ข้อมูล ณ วันที่ 31 ตุลาคม 2026 ราคาทั้งหมดยังไม่รวม VAT โดยคิด VAT เพิ่มจากราคา Appliance, SaaS และ MA รายปี ค่าบำรุงรักษา Appliance เริ่มปีที่ 2 ในอัตรา 30% ของราคาแพ็กเกจสุทธิ พาร์ทเนอร์ยืนยันใบเสนอราคาและระยะเวลาที่ใช้ได้จริง

กำหนดขนาดจากไซต์ ไม่ใช่ตัวเลขในเดโม

กำหนดขนาดจาก segment, collector, ปริมาณทราฟฟิก แหล่ง telemetry ระยะเก็บข้อมูล และรอบรายงาน จำนวนเครื่องหรือชุดที่รวมในแพ็กเกจไม่ใช่จำนวน segment ที่ได้รับสิทธิ์หรือขีดความสามารถของระบบ ต้องตกลง CPU, RAM, storage, throughput, ขีดจำกัดเซนเซอร์ จุดรับข้อมูลเพิ่ม ราคา VM รายการฮาร์ดแวร์ และ SLA ในข้อเสนอของพาร์ทเนอร์ โดยไม่ได้กำหนดขีดความสามารถเริ่มต้นไว้

ขอบเขตทางเทคนิค

ขอบเขตการติดตั้งและการทำงาน

04

มองเห็นแบบพาสซีฟ แยกจากเส้นทางควบคุม

งานมอนิเตอร์เครือข่ายแบบพาสซีฟใช้สำเนาทราฟฟิก ไม่ติดตั้งแบบ inline ในเส้นทางควบคุม ไม่ต้องใช้ agent บนปลายทางสำหรับงานนี้ และไม่ควบคุมอุปกรณ์ OT โดยตรง ต้องตกลงการปรับจุดรับข้อมูลและช่วงเวลาเปลี่ยนแปลงกับเจ้าของโรงงาน คำว่า “พาสซีฟ” ไม่ใช่การรับประกันว่าการติดตั้งไม่มีความเสี่ยง

เครือข่ายที่แยกขาดและการใช้งานออฟไลน์

หากเสนอการมอนิเตอร์ด้วย appliance แบบออฟไลน์ ต้องตรวจสอบ licensing, การอัปเดต, ช่องทางสนับสนุน, การเทียบเวลา และการส่งออกข้อมูลในเครือข่ายที่แยกขาด ไม่ควรถือว่า integration ทุกชนิดใช้งานออฟไลน์ได้

กำหนดขอบเขตการเชื่อมระบบ

ระบุเส้นทางต้นทาง → ตัวรวบรวม → แพลตฟอร์ม → ระบบปลายทาง ยืนยันรูปแบบ syslog/API, การยืนยันตัวตน, ทิศทางข้อมูล และผู้รับผิดชอบ เอกสารนี้ไม่ได้รับรอง connector รายยี่ห้อหรือการตอบสนองอัตโนมัติ

> พาร์ทเนอร์ดูแลการสนับสนุนด่านแรก โดย zcr สนับสนุนพาร์ทเนอร์อีกชั้น เวลาบริการ การยกระดับปัญหา SLA ขอบเขตติดตั้ง และหน้าที่บำรุงรักษาต้องตกลงในข้อเสนอ

ในเครือข่าย OT ของคุณกำลังเกิดอะไรขึ้น?

ทำแผนที่อุปกรณ์และเส้นทางการสื่อสารที่ตรวจพบ แยกอุปกรณ์ที่รู้จักกับไม่รู้จัก และใช้บริบทของโปรโตคอลตรวจสอบกิจกรรมผิดปกติ ขอบเขตการมองเห็นขึ้นอยู่กับทราฟฟิกและข้อมูลที่ส่งให้แพลตฟอร์ม

ขอบเขตทางเทคนิค

ตรวจสอบหลักฐานก่อนนำไปใช้งาน

05

การประเมินที่ดีควรจบด้วยขอบเขตการมองเห็นและแนวทางส่งมอบงานที่ตกลงร่วมกัน มากกว่าแค่ภาพหน้าจอ dashboard

หัวข้อประเมิน	สิ่งที่ต้องตรวจสอบ
ขอบเขตรับข้อมูล	ระบุ segment, จุดรับทราฟฟิก, interface และส่วนที่ระบบมองไม่เห็น
โปรโตคอลและอุปกรณ์	ตรวจตัวอย่าง Modbus read/write/error, gateway และแท็กอุปกรณ์ที่รู้จัก/ไม่รู้จัก
ข้อมูลและเหตุการณ์	ตรวจตัวนับข้อมูล เวลา หน่วยพลังงาน และบริบทเหตุการณ์ด้วยข้อมูลทดสอบที่ไซต์อนุมัติ
การปฏิบัติการ	ตกลงระยะเก็บข้อมูล รอบรายงาน ผู้ดูแลสิทธิ์ และความรับผิดชอบด้านสนับสนุน/บำรุงรักษา

กำหนดขนาดจากไซต์ ไม่ใช่ตัวเลขในเดโม

กำหนดขนาดจาก segment, collector, ปริมาณทราฟฟิก แหล่ง telemetry ระยะเก็บข้อมูล และรอบรายงาน จำนวนเครื่องหรือชุดที่รวมในแพ็กเกจไม่ใช่จำนวน segment ที่ได้รับสิทธิ์หรือขีดความสามารถของระบบ ต้องตกลง CPU, RAM, storage, throughput, ขีดจำกัดเซนเซอร์ จุดรับข้อมูลเพิ่ม ราคา VM รายการฮาร์ดแวร์ และ SLA ในข้อเสนอของพาร์ทเนอร์ โดยไม่ได้กำหนดขีดความสามารถเริ่มต้นไว้

วางแผนประเมินร่วมกับพาร์ทเนอร์ที่ได้รับอนุมัติ

เตรียมผังเครือข่าย จำนวน segment และเซนเซอร์โดยประมาณ แหล่งข้อมูล และข้อจำกัดการติดตั้ง ข้อเสนอเชิงพาณิชย์ สัญญา และการส่งมอบงานให้ลูกค้าดำเนินการผ่าน distributor, reseller/SI หรือ MSP/MSSP ที่ได้รับอนุมัติ ส่วน zcr.ai ช่วยแนะนำพาร์ทเนอร์ให้คุณได้

ประสานพาร์ทเนอร์ / หารือขอบเขต ↗ ดูข้อมูล zcrOT ↗ ลองใช้เดโมสาธารณะ ↗

zcr.ai/contact/ · zcr.ai/product/zcrot/ · demo.ot.zcr.ai

ขอบเขตทางเทคนิค · รูปแบบติดตั้งที่ตกลง

อุปกรณ์และเมทาดาทาโปรโตคอล

06

ทดสอบฟิลด์ ขอบเขตโปรโตคอล และตัวกรองกับทราฟฟิกตัวแทนจากไซต์จริง

ขอบเขตทางเทคนิค · รูปแบบติดตั้งที่ตกลง

ความสามารถต่อไปนี้พร้อมส่งมอบตามรูปแบบติดตั้งที่ตกลง กำหนดเกณฑ์รับมอบร่วมกับพาร์ทเนอร์ที่ได้รับอนุมัติให้ครอบคลุมแหล่งข้อมูล เวอร์ชันโปรโตคอล อินเทอร์เฟซ สิทธิ์เข้าถึง ระยะเก็บข้อมูล และเงื่อนไขปฏิบัติงาน ทดสอบการทำงานร่วมกันและขั้นตอนในเครือข่ายแยกขาดที่ต้องใช้ก่อนนำไปใช้งานจริง ขอบเขตนี้ไม่ได้กำหนดขีดความสามารถ ประสิทธิภาพ การรับรอง หรือ SLA

ความสามารถ	ขอบเขตทางเทคนิค
รายละเอียดอุปกรณ์	IP และ MAC, โปรโตคอล พอร์ต ประเภทอุปกรณ์ logical unit ทิศทางสื่อสาร และสถานะ mapping ตั้งชื่อ เพิ่มรายละเอียด และจัดกลุ่มอุปกรณ์ที่รู้จัก/ไม่รู้จัก engineering workstation โครงสร้างพื้นฐานเครือข่าย industrial gateway และอุปกรณ์ OT อื่น
เส้นทางและตัวกรอง	เส้นทางภายใน ภายนอก เส้นทางที่ติดต่อมาก และเส้นทางใหม่ พร้อมปริมาณการติดต่อ กรองตามเวลา อุปกรณ์ โปรโตคอล ความเสี่ยง และทิศทาง เทียบค่าฐานเพื่อตรวจอุปกรณ์ไม่รู้จัก ปลายทางภายนอก เส้นทางเปลี่ยน และพฤติกรรมที่อาจเป็น lateral movement หรือ command and control
บริบทเกตเวย์	แยกอุปกรณ์ที่พบโดยตรงผ่าน Ethernet/IP ออกจาก logical OT unit ที่ระบุด้วย gateway telemetry เพราะ IP เพียงอย่างเดียวอาจระบุแต่ละ unit ไม่ได้
ฟิลด์เมทาดาทา	Timestamp, source IP/MAC, destination IP/MAC, protocol, port, direction, session context, classification และสถานะผิดปกติที่เกี่ยวข้อง สืบค้นและเชื่อมโยงเมทาดาทาเพื่อลดความจำเป็นในการเปิด raw packet ทุกครั้ง
รายการโปรโตคอล	HTTP, DNS, SMB, HTTPS, TLS, TCP, UDP, ICMP, SNMP, Modbus TCP และ EtherNet/IP ต้องทดสอบเวอร์ชัน parser และฟิลด์ที่รองรับ รายการนี้ไม่ใช่การรับรองการทำงานร่วมกัน
ฟิลด์ระดับแอปพลิเคชัน	HTTP: method, host, URI, status code, user agent และทิศทาง DNS: query, response, record type, resolved IP และพฤติกรรมผิดปกติ SMB: session, user, share, file operation และกิจกรรมที่เกี่ยวกับ lateral movement

ขอบเขตทางเทคนิค · รูปแบบติดตั้งที่ตกลง

การตรวจจับและความเชื่อถือได้ของระบบควบคุม

07

ทดสอบกฎและสัญญาณการทำงาน โดยไม่ตีความเป็นการรับประกันการป้องกันหรือความแม่นยำ

ขอบเขตทางเทคนิค · รูปแบบติดตั้งที่ตกลง

ความสามารถต่อไปนี้พร้อมส่งมอบตามรูปแบบติดตั้งที่ตกลง กำหนดเกณฑ์รับมอบร่วมกับพาร์ทเนอร์ที่ได้รับอนุมัติให้ครอบคลุมแหล่งข้อมูล เวอร์ชันโปรโตคอล อินเทอร์เฟซ สิทธิ์เข้าถึง ระยะเก็บข้อมูล และเงื่อนไขปฏิบัติงาน ทดสอบการทำงานร่วมกันและขั้นตอนในเครือข่ายแยกขาดที่ต้องใช้ก่อนนำไปใช้งานจริง ขอบเขตนี้ไม่ได้กำหนดขีดความสามารถ ประสิทธิภาพ การรับรอง หรือ SLA

ความสามารถ	ขอบเขตทางเทคนิค
ความเชื่อถือได้ของ Modbus	ระดับ unit/operation: request volume, error count, response time, slow poll, success rate และสถานะ logical unit เปรียบเทียบข้อมูลย้อนหลังเพื่อตรวจการเสื่อมประสิทธิภาพและผลกระทบที่อาจเกิดกับการผลิต โดยไม่ได้ระบุค่า throughput หรือ latency
ความผิดปกติในการทำงาน	Request ผิดปกติ function ที่ไม่เคยพบ การเข้าถึง unit ที่ไม่ได้รับอนุญาต error เพิ่มขึ้น response time ผิดปกติ และกิจกรรมนอกเวลาปฏิบัติงาน
ข้อมูลสำหรับกฎ	กฎมาตรฐานและกฎกำหนดเองใช้ traffic, protocol metadata, asset context และ operational telemetry เงื่อนไขประกอบด้วย source, destination, protocol, port, direction, asset, time window, baseline, severity และ event classification
ตัวอย่างการตรวจจับ	Unknown client เส้นทางใหม่ การติดต่อภายนอก กิจกรรมนอกเวลางาน โปรโตคอลที่ไม่ได้รับอนุญาต พอร์ตน่าสงสัย Modbus disruption ปริมาณ request ผิดปกติ error ซ้ำ slow poll และพฤติกรรมต่างจากค่าฐาน
จัดลำดับและปรับแต่ง	Severity, risk score, verdict และ classification รวมถึง allowlist กิจกรรมที่อนุมัติ และการปรับกฎ ต้องทดสอบผลต่อ false positive ไม่ถือว่ารับประกันการลดลง
ภาพรวมและวงจรเหตุการณ์	Security event, high/critical event, unknown client, likely-attack verdict แนวโน้ม การกระจาย verdict และแหล่งความเสี่ยงสูง พร้อมเจาะดูรายละเอียดและหลักฐาน Incident ที่เกี่ยวข้องประกอบด้วย asset, alert, protocol, source/destination, severity, timeline และหลักฐาน ตั้งแต่เริ่มพบจนปิดเหตุ

ขอบเขตทางเทคนิค · รูปแบบติดตั้งที่ตกลง

หลักฐานแพ็กเก็ตและการส่งออก

08

ทดสอบการบันทึก อายุเก็บข้อมูล สิทธิ์เข้าถึง และการส่งออก ก่อนใช้แพ็กเก็ตเป็นหลักฐาน

ขอบเขตทางเทคนิค · รูปแบบติดตั้งที่ตกลง

ความสามารถต่อไปนี้พร้อมส่งมอบตามรูปแบบติดตั้งที่ตกลง กำหนดเกณฑ์รับมอบร่วมกับพาร์ทเนอร์ที่ได้รับอนุมัติให้ครอบคลุมแหล่งข้อมูล เวอร์ชันโปรโตคอล อินเทอร์เฟซ สิทธิ์เข้าถึง ระยะเก็บข้อมูล และเงื่อนไขปฏิบัติงาน ทดสอบการทำงานร่วมกันและขั้นตอนในเครือข่ายแยกขาดที่ต้องใช้ก่อนนำไปใช้งานจริง ขอบเขตนี้ไม่ได้กำหนดขีดความสามารถ ประสิทธิภาพ การรับรอง หรือ SLA

ความสามารถ	ขอบเขตทางเทคนิค
รูปแบบการบันทึก	Full packet capture ผ่าน network sensor ในไซต์ จัดเก็บหลักฐาน PCAP หรือ PCAPNG สำหรับตรวจสอบเครือข่ายและ OT ต้องยืนยัน interface ขีดความสามารถ พื้นที่ และอายุเก็บข้อมูล เอกสารนี้ไม่ระบุตัวเลขเหล่านั้น
นโยบายการบันทึก	กำหนดตาม sensor, network segment, protocol, asset, time window, detection rule และ severity เพื่อควบคุมขอบเขตและปริมาณแพ็กเก็ต โดยให้ความสำคัญกับระบบและทรัพย์สินสำคัญ
หลักฐานตามเงื่อนไข	เมื่อ IDS signature ตรงเงื่อนไข ให้บันทึก PCAP ที่เกี่ยวข้องอัตโนมัติก่อน ระหว่าง และหลังตรวจพบ พร้อมเชื่อมกับ alert หรือ incident ต้องทดสอบ buffer เวลา trigger และพฤติกรรมในรูปแบบติดตั้งที่เสนอ
ข้อมูลอ้างอิงเหตุการณ์	Sensor, capture time, source IP, destination IP, protocol, file size, file hash และ incident reference ในพื้นที่ตรวจสอบเหตุ การแสดง hash เพียงอย่างเดียวไม่ใช่การรับรองห่วงโซ่การควบคุมหลักฐาน
ส่งออกตามสิทธิ์	ผู้ได้รับสิทธิ์คัดลอก ดาวน์โหลด หรือส่งออก PCAP ที่เกี่ยวข้องผ่านช่องทางปลอดภัย เพื่อวิเคราะห์ต่อด้วย Wireshark หรือเครื่องมือนิติวิทยาศาสตร์เครือข่ายภายนอก
ความต่อเนื่องของหลักฐาน	คง timestamp, capture metadata, incident reference และข้อมูลตรวจสอบย้อนหลังที่จำเป็น เพื่อให้ทีม SOC ตอบสนองเหตุ และนิติวิทยาศาสตร์ดิจิทัลวิเคราะห์ต่อภายนอกแพลตฟอร์ม ต้องยืนยันสิทธิ์ วิธีส่ง และฟิลด์ที่คงไว้

ขอบเขตทางเทคนิค · รูปแบบติดตั้งที่ตกลง

การเชื่อมโยงเหตุ การบริหาร และรายงาน

09

ทดสอบความสัมพันธ์ข้ามระบบ การบริหาร และเนื้อหารายงานในรุ่นที่เสนอ

ขอบเขตทางเทคนิค · รูปแบบติดตั้งที่ตกลง

ความสามารถต่อไปนี้พร้อมส่งมอบตามรูปแบบติดตั้งที่ตกลง กำหนดเกณฑ์รับมอบร่วมกับพาร์ทเนอร์ที่ได้รับอนุมัติให้ครอบคลุมแหล่งข้อมูล เวอร์ชันโปรโตคอล อินเทอร์เฟซ สิทธิ์เข้าถึง ระยะเก็บข้อมูล และเงื่อนไขปฏิบัติงาน ทดสอบการทำงานร่วมกันและขั้นตอนในเครือข่ายแยกขาดที่ต้องใช้ก่อนนำไปใช้งานจริง ขอบเขตนี้ไม่ได้กำหนดขีดความสามารถ ประสิทธิภาพ การรับรอง หรือ SLA

ความสามารถ	ขอบเขตทางเทคนิค
เชื่อมโยงข้ามระบบ	จัดกลุ่มเหตุจาก network, endpoint, identity/user, cloud และระบบควบคุมความปลอดภัยอื่นลงใน case/incident เดียวอัตโนมัติ ต้องยืนยันตรรกะจับคู่ แหล่งข้อมูล และรุ่น ไม่ได้หมายถึงการตอบสนองอัตโนมัติ
ความสัมพันธ์และต้นเหตุ	ความสัมพันธ์ alert, entity, host, user, IP, asset, process, file และ network session พร้อม timeline/kill chain ติดตาม initial activity, lateral movement, command and control, data access และ impact จากเหตุ network/endpoint/identity/cloud/control, metadata, detection และ PCAP
EDR และแหล่งภายนอก	API, Webhook, Syslog และ integration framework รวมบริบท endpoint alert, process, command line, file, hash, user, network connection และ mitigation action ต้องทดสอบ EDR, SIEM, identity, cloud, firewall, IDS/IPS, ticketing และ monitoring โดยยังไม่ยืนยัน connector รายยี่ห้อหรือการสั่ง mitigation
การบริหาร	ภาพรวม asset เส้นทาง exposure incident พลังงาน พอร์ต สิทธิ์ผู้ใช้ และสุขภาพข้อมูล กำหนดชื่อ/ประเภท/รายละเอียดจาก IP, MAC หรือ Modbus Unit ID บริหาร syslog port แยกแหล่ง sensor input และ telemetry โดยต้องยืนยัน last activity ตัวนับ และการเพิ่ม/ปิด/แก้ไข
รายงาน	Executive Summary และ OT Visibility & Security Report ระบุอุปกรณ์ที่พบ อุปกรณ์รู้จัก/ไม่รู้จัก เส้นทาง เหตุการณ์ เหตุ high/critical incident แหล่งความเสี่ยงสูง control reliability และภาพรวมความเสี่ยง ต้องทดสอบช่วงเวลา แนวโน้ม สรุปเหตุสำคัญ และการส่งออกสำหรับผู้บริหาร OT ความปลอดภัย และการทบทวนภายใน
ระบบแยกเครือข่าย	วางแผน VM/appliance แบบ on-premises สำหรับ offline หรือ isolated network ที่ตกลง ต้องยืนยันที่ตั้งข้อมูล licensing การอัปเดต เวลา การสนับสนุน และการส่งออก ไม่ถือว่าทุก integration ใช้แบบ offline ได้