ARAK
Data Protection and Sovereignty

PRODUCT DATASHEET

ARAK Respond Center

แพลตฟอร์ม EDR · XDR · CTEM ในศูนย์กลางเดียว

ARAK Respond Center รวมการเฝ้าระวังเครื่องปลายทาง การเชื่อมโยงข้อมูลภัยคุกคามข้ามทั้งองค์กร และการประเมินความเสี่ยงอย่างต่อเนื่องไว้บนหน้าจอเดียว ทำงานร่วมกับ ARAK Agent ขนาดเล็กที่ติดตั้งได้ด้วยคำสั่งเดียว ไม่ต้องใช้ไดรเวอร์ และจัดเก็บข้อมูลทั้งหมดบนเซิร์ฟเวอร์ขององค์กรเอง

EDR · XDR · CTEM · TLS 1.3 + Hybrid PQC · NIST CSF 2.0 Mapping

~8 MB	< 1%	10–15 MB	0	1 คำสั่ง	< 3 วินาที
ขนาดไฟล์ agent ไฟล์เดียว	การใช้ CPU โดยเฉลี่ย	หน่วยความจำ บน Linux	ไม่ต้องติดตั้ง driver / Npcap / eBPF	ติดตั้งและลงทะเบียน โดยอัตโนมัติ	ตรวจประเมิน การบุกรุกทั้งเครื่อง

สามความสามารถในแพลตฟอร์มเดียว

Endpoint Detection & Response

EDR

เฝ้าระวังกิจกรรมของโปรแกรมบนเครื่องปลายทาง ตรวจหามัลแวร์ backdoor rootkit และกลไกการฝังตัว พร้อมตอบสนองด้วยการบล็อกการเชื่อมต่อและแยกเครื่องออกจากเครือข่าย

Extended Detection & Response

XDR

เชื่อมโยงข้อมูลการเชื่อมต่อเครือข่าย DNS และ TLS SNI จากทุกเครื่องเข้ากับ Threat Intelligence เพื่อตรวจจับ C2, beacon, DNS tunnel และการลักลอบนำข้อมูลออกในระดับองค์กร

Continuous Threat Exposure Management

CTEM

ประเมินความเสี่ยงของทุกเครื่องอย่างต่อเนื่อง จากแพตช์ความปลอดภัยที่ยังไม่ได้ติดตั้ง บริการที่เปิดสู่อินเทอร์เน็ต ผลการตรวจประเมินการบุกรุก และการแจ้งเตือนที่ยังไม่ได้รับการแก้ไข

ความสามารถหลัก

มองเห็นการเชื่อมต่อทั้งองค์กร

- ทุกการเชื่อมต่อผูกกับ process, path, ผู้ใช้ และค่า SHA-256
- ชื่อโดเมนจาก DNS / TLS SNI พร้อมประเทศและ ASN
- แผนที่โลกสามมิติและหน้าจอติดตามแบบเรียลไทม์

Compromise Assessment

- backdoor, spyware, keylogger, rootkit และ RAT
- การฝังตัว process ปลอมแปลง และการปิด Defender
- สรุปผล COMPROMISED / SUSPICIOUS / CLEAN

ตรวจแพตช์และช่องโหว่ (CTEM)

- Linux: เทียบแพ็กเกจกับฐานข้อมูลช่องโหว่ OSV
- Windows: cumulative update ตาม MSRC และเบราว์เซอร์
- จัดลำดับด้วย CISA KEV, EPSS และการเปิดบริการจริง

ตรวจจับภัยคุกคาม

- Threat Intelligence ในตัว ปรับปรุงทุก 6 ชั่วโมง
- C2 beacon, DNS tunnel, การนำข้อมูลออก และ LOLBin
- อ้างอิง MITRE ATT&CK พร้อมคำแนะนำภาษาไทย

ARAK Protect — ตอบสนองอัตโนมัติ

- Fleet Blocklist บล็อก IP อันตรายบนทุกเครื่อง
- พอร์ตกับดัก (Decoy) และ LOLBin Egress Lock
- Network Isolation ด้วยคำสั่งที่ลงนาม Ed25519

สุขภาพเครื่องและทรัพยากร

- CPU หน่วยความจำ ดิสก์ และ top process
- แจ้งเตือน crypto miner และดิสก์ใกล้เต็ม
- คะแนนความเสี่ยงรายเครื่องและ Security Grade

พร้อมสำหรับยุคควอนตัม — ช่องทางสื่อสารระหว่าง agent กับศูนย์กลางเข้ารหัสด้วย **TLS 1.3** แบบ **Hybrid Post-Quantum Cryptography** (X25519 + ML-KEM-768 ตามมาตรฐาน NIST FIPS 203) ป้องกันการดักเก็บข้อมูลไว้ถอดรหัสในอนาคต (harvest now, decrypt later) พร้อมตรึงกุญแจของเซิร์ฟเวอร์ (certificate pinning)

ออกแบบให้เบาและไม่รบกวนผู้ใช้

Agent น้ำหนักเบา

- Windows ใช้ ETW · Linux ใช้ netlink + kernel BPF filter
- ลำดับความสำคัญต่ำ (EcoQoS / nice 10) และจำกัดทรัพยากร
- Resource Governor ลดภาระตนเองเมื่อใช้ CPU เกินงบ

ทำงานต่อเนื่องแม้เครือข่ายขัดข้อง

- พักข้อมูลบนดิสก์สูงสุด 50 MB แล้วส่งย้อนหลัง
- แจ้งเตือนเมื่อ agent หยุดส่งข้อมูลผิดปกติ

ความมั่นคงปลอดภัยและความเป็นส่วนตัว

ข้อมูลอยู่ในการควบคุมขององค์กร

- ส่งเฉพาะ metadata ไม่จัดเก็บเนื้อหาข้อมูลหรือ pcap
- ศูนย์กลางติดตั้ง on-premises หรือ private cloud
- TLS 1.3 + Hybrid PQC และ certificate pinning
- คำสั่งตอบสนองลงลายมือชื่อดิจิทัล Ed25519
- สิทธิ์ admin / viewer และ audit log

NIST Cybersecurity Framework 2.0 Mapping

Function	Category	ความสามารถใน ARAK Respond Center	ระดับการรองรับ
Govern	GV.RR	สิทธิ์ผู้ใช้ admin / viewer และ audit log	บางส่วน
Identify	ID.AM · ID.RA	ทะเบียนเครื่องและซอฟต์แวร์ แพตช์ที่ขาด (KEV / EPSS) และคะแนนความเสี่ยง	ครอบคลุม
Protect	PR.DS · PR.IR	TLS 1.3 + Hybrid PQC · Fleet Blocklist, LOLBin Lock, Decoy	ครอบคลุม / บางส่วน
Detect	DE.CM · DE.AE	เฝ้าระวังต่อเนื่อง Threat Intelligence และ MITRE ATT&CK	ครอบคลุม
Respond	RS.MA·RS.AN·RS.MI	แจ้งเตือนตามความรุนแรง สืบสวนเหตุ Isolation และ Auto-block	ครอบคลุม
Respond	RS.CO	แจ้งเตือนแบบเรียลไทม์บน Dashboard พร้อมคำแนะนำภาษาไทย	บางส่วน
Recover	RC.RP	ยกเลิกการแยกเครื่อง/บล็อกด้วยคลิกเดียว และตรวจประเมินซ้ำ	ใช้ร่วมกับระบบอื่น

สถาปัตยกรรม

ARAK Agent
Windows · Linux
flow · DNS · SNI · scan · แพตช์

→ TLS 1.3 PQC

ARAK Respond Center
Threat Intel · Detection · Risk Score
Response · ไฟล์เดียว ฐานข้อมูลในตัว

→ HTTPS

SOC / ผู้ดูแลระบบ
Dashboard บนเว็บ
SEE · LEARN · RESPOND

ระบบปฏิบัติการที่รองรับ

ระบบปฏิบัติการ	CPU	หมายเหตุ
Windows 10 / 11 Server 2016+	x64	ครบทุกความสามารถ
Linux (systemd)	x64 · ARM64	Protect อยู่ในแผนพัฒนา
macOS เร็ว ๆ นี้	Apple silicon · Intel	อยู่ระหว่างพัฒนา

การติดตั้งและความต้องการของระบบ

ศูนย์กลาง	Linux x64 · ไฟล์เดียว · RAM ระดับหลักสิบ MB
เครือข่าย	agent ใช้ขาออกพอร์ต 8444 เท่านั้น
ติดตั้ง agent	คำสั่งเดียว ลงทะเบียนด้วย enroll key
ส่งข้อมูล	เป็นชุดทุก 20–60 วินาที บีบอัดและเข้ารหัส

ทดลองใช้ ARAK Respond Center ในองค์กรของคุณ

ติดต่อทีมงานเพื่อขอสาธิตการใช้งาน ติดตั้งระบบทดลองภายในองค์กร หรือขอคำปรึกษาด้านการเฝ้าระวังและตอบสนองต่อภัยคุกคาม

สนใจบริการ ติดต่อ

บริษัท ทูนาเบิล โปรเจค จำกัด
info@tunableproject.com

SRAN Cyber Tech
info@gbtech.co.th

ตัวเลขด้านประสิทธิภาพวัดจากระบบที่ใช้งานจริง ผลลัพธ์อาจแตกต่างกันตามปริมาณการใช้งานของแต่ละเครื่อง · การเทียบเคียงกับ NIST CSF 2.0 จัดทำโดย ARAK เพื่อใช้อ้างอิงประกอบการพิจารณา มิใช่การรับรองจาก NIST · ชื่อผลิตภัณฑ์และเครื่องหมายการค้าอื่นเป็นของเจ้าของแต่ละราย · ข้อมูลอาจเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบล่วงหน้า