Risk Radar – คู่มือผู้ใช้งาน (User Manual)

แพลตฟอร์มบริหารความเสี่ยงและช่องโหว่แบบต่อเนื่อง (Continuous Vulnerability & Risk Management)

---

1. Risk Radar คืออะไร

Risk Radar ช่วยให้ทีม Security และเจ้าของระบบ สแกนหาช่องโหว่ ประเมินความเสี่ยง และติดตามการแก้ไขได้เองแบบ Real-time โดยไม่ต้องรอรอบ pentest ประจำปี – ครอบคลุมตั้งแต่ค้นหา asset, สแกนด้วยหลายเครื่องมือ, ให้คะแนนความเสี่ยง, แจ้งเตือน, ออกรายงาน ไปจนถึงแนะนำวิธีแก้และปิดช่องโหว่

นอกจากตอบว่า "เว็บนี้ถูกเจาะได้ไหม" (ช่องโหว่) ระบบยังตรวจได้ว่า "เว็บนี้ถูกยึด/ฝังของไปแล้วหรือยัง" (มัลแวร์และการถูกยึด – ดูหัวข้อ 7–8)

2. การเข้าใช้งาน

1. เปิดเบราว์เซอร์ไปที่ URL ของระบบ (เช่น https://riskradar.example.com)
2. ระบบจะพาไปหน้าล็อกอิน (Single Sign-On)
3. กรอก username / password ขององค์กร แล้วเข้าสู่ระบบ
4. การเข้าใช้งานครั้งแรก ระบบจะแสดง "ข้อตกลงการใช้งาน" (Acceptable Use) – ต้องกด ยอมรับ ก่อนจึงเข้าใช้งานได้ (ยืนยันว่าจะสแกนเฉพาะระบบที่คุณเป็นเจ้าของหรือได้รับอนุญาตเท่านั้น) ระบบจะจำการยอมรับไว้ ไม่ถามซ้ำ
5. มุมขวาบนจะแสดงชื่อผู้ใช้ และปุ่ม logout

3. หน้า Dashboard

หน้าหลักแสดงภาพรวมความเสี่ยงทั้งองค์กรแบบ Real-time:

- แถบแดง "การถูกยึดที่ต้องจัดการ" (บนสุด): โผล่เฉพาะเมื่อมีการถูกยึด – สรุป asset + finding ที่ต้องจัดการก่อน พร้อมปุ่ม "เปิดเคส" (ดูหัวข้อ 12)
- Org risk score (จอเรดาร์): คะแนนความเสี่ยงรวม 0–100 พร้อมแนวโน้ม 7 วัน และจุด (blip) แสดง asset เสี่ยงสูงสุด
- Open findings by severity (spider chart): จำนวนช่องโหว่ที่เปิดอยู่ แยกตามระดับ
- Overview: สรุปจำนวน assets, ที่จัดการแล้ว, และช่องโหว่แต่ละระดับ
- Organizational risk trend: กราฟแนวโน้มคะแนนความเสี่ยงตามเวลา
- การวิเคราะห์การแก้ไข (Remediation analytics): MTTR + open/managed/compromise + กราฟแท่งรายสัปดาห์ (ดูหัวข้อ 13)
- Asset risk heatmap: ช่องสีตามความเสี่ยงของแต่ละ asset – คลิกช่องเพื่อสั่งสแกน
- ผลการสแกนแยกตาม Asset / Live event feed

4. การเพิ่ม Asset

ที่การ์ด "Assets" ด้านล่าง:

1. พิมพ์ค่า asset (เช่น https://www.example.com)
2. เลือกประเภท: url / api / domain / ip / cidr / host
3. เลือกความสำคัญ (criticality) และ environment (production/staging/dev)
4. กด Add

หมายเหตุ: ใส่ hostname ที่ resolve ได้จริง (ปกติมี www หรือใส่ https:// เต็ม) – ถ้าใส่ apex ที่ไม่มี DNS record ระบบจะแจ้งว่าเชื่อมต่อเป้าหมายไม่ได้

5. ยืนยันความเป็นเจ้าของโดเมน

สำหรับ asset ที่เป็น url/api/domain จะมีลิงก์ "ยืนยันโดเมน" ข้างชื่อ (หรือ " ยืนยันแล้ว" ถ้าทำแล้ว):

1. คลิก "ยืนยันโดเมน" ระบบแสดง DNS TXT record ที่ต้องเพิ่ม (กดคัดลอก)
2. นำ TXT record ไปเพิ่มที่ DNS ของโดเมน รอ DNS กระจาย
3. กด "ตรวจสอบ DNS" เมื่อพบ record ที่ถูกต้อง asset จะขึ้น " ยืนยันแล้ว"

> บางการติดตั้ง (โหมดสาธารณะ) จะ บังคับยืนยันโดเมนก่อนจึงจะสแกนได้ – ป้องกันการสแกนระบบที่ไม่ได้เป็นเจ้าของ

6. การสั่งสแกน

ที่แถว asset ให้ เลือกโปรไฟล์จาก dropdown ข้างปุ่ม Scan แล้วกด Scan (หรือคลิกช่องใน heatmap เพื่อสแกนด้วยโปรไฟล์เริ่มต้น)

Profile	ตรวจอะไร	เหมาะกับ
recon	port/service ที่เปิด (Nmap)	asset ประเภท ip/host
web	ช่องโหว่เว็บ/API (Nuclei + ZAP)	ประเมินช่องโหว่เว็บ
malware	การถูกยึด/ฝังมัลแวร์ (หัวข้อ 7)	มอนิเตอร์รายวัน (เบา, ปลอดภัยกับ production)
full	ครบทุกชั้น (ช่องโหว่ + มัลแวร์)	สแกนครบในครั้งเดียว
deep	full + การทดสอบเชิงรุก (active)	staging/dev เท่านั้น (ห้ามใช้กับ production)

ระหว่างสแกนจะเห็น จอเรดาร์ + pipeline แสดงความคืบหน้าทีละขั้น พร้อมบอกว่ากำลังตรวจด้วยเครื่องมืออะไร (ไม่ต้องกดซ้ำ ผลขึ้นเองเมื่อเสร็จ)

7. การตรวจจับมัลแวร์และการถูกยึด (Malware & Compromise Detection)

เลือกโปรไฟล์ malware (หรือ full/deep) เพื่อตรวจว่าเว็บถูกยึดหรือฝังของไม่ดีหรือยัง การตรวจทั้งหมด อ่านอย่างเดียว (HTTP) – ไม่รันไฟล์ จึงปลอดภัยกับ production

ตรวจ 4 อย่าง: (1) Web shell / backdoor (2) Injected / obfuscated JS + redirect (3) Blocklist reputation (URLhaus / Google Safe Browsing) (4) Defacement / SEO spam

เฝ้าระวังการเปลี่ยนแปลง (Integrity monitoring):
ระบบจำรายการสคริปต์ภายนอกของหน้าเว็บ แล้วเทียบทุกครั้ง – ถ้ามีสคริปต์จากโดเมนภายนอกใหม่ (เช่น Magecart) จะแจ้งเตือน ส่วนการเปลี่ยนสคริปต์โดเมนเดิม (deploy) จะไม่เตือน

IOC correlation: ระบบดึงรายชื่อ IOC (โดเมน/IP ที่รู้ว่าเป็นอันตราย) จาก feed สาธารณะทุกวัน แล้วเทียบกับ asset + สคริปต์ของคุณ – ถ้าตรง จะแจ้งเป็น finding "มัลแวร์"

> รายละเอียดดู MALWARE_DETECTION.md

8. วิเคราะห์ไฟล์ (Static File Analysis)

การ์ด "วิเคราะห์ไฟล์" (เหนือตาราง Assets) – ตรวจไฟล์ต้องสงสัยโดย ไม่รันไฟล์:

1. กดเลือกไฟล์ ระบบคำนวณ hash + ตรวจ

2. ผลแสดงเป็น 3 ระดับ: ปลอดภัย / น่าสงสัย / อันตราย พร้อม hash, ชนิดไฟล์, และสัญญาณที่พบ

ตรวจด้วย: hash reputation (MalwareBazaar / VirusTotal) + heuristics (web shell, macro, PowerShell, base64, packer) –
ไฟล์ที่วิเคราะห์ล่าสุดแสดงเป็นรายการด้านล่าง

9. ตั้งเวลาสแกนอัตโนมัติ

ที่ตาราง Assets คอลัมน์ "Daily scan": ติ๊ก checkbox เลือกชั่วโมง เลือกโปรไฟล์ ระบบจะสแกนเองทุกวัน

แนะนำ: ตั้งโปรไฟล์ malware รันทุกวัน (เบา, ปลอดภัย) เพื่อจับการถูกยึดเร็ว; web/full ตั้งถี่น้อยกว่า

10. ดูผล + วิธีแก้ไข

ที่ "ผลการสแกนแยกตาม Asset": คลิก asset เพื่อกาง คลิกช่องโหว่เพื่อดู ผลกระทบ / วิธีแก้ไข (พร้อมตัวอย่างโค้ด) / อ้างอิง

รายการที่เป็นการถูกยึดจะมี badge สีแดง ถูกยึด / มัลแวร์ ข้างระดับความรุนแรง (จัดการก่อนเป็นลำดับแรก)

11. การจัดการช่องโหว่ (Lifecycle)

แต่ละช่องโหว่มีแถว "ทำเครื่องหมายเป็น:" เลือก แก้แล้ว / ยอมรับความเสี่ยง / False positive

ช่องโหว่ที่จัดการแล้วจะถูกตัดออกจากคะแนน (คะแนนลดทันที) และซ่อนได้ด้วยตัวกรอง "ซ่อนที่จัดการแล้ว" – กด "เลิกทำ" เพื่อย้อนกลับ

12. เคส / Incident cases

เมื่อพบการถูกยึด สร้างเคสเพื่อติดตามการสืบสวน:

1. ที่แถบแดง "การถูกยึดที่ต้องจัดการ" กด "+ เปิดเคส" (ผูก finding การถูกยึดของ asset นั้นเข้าเคสอัตโนมัติ)
2. เคสจะขึ้นในหัวข้อ "เคส / Incident cases" คลิกเพื่อเปิดรายละเอียด
3. ในเคส: เปลี่ยน สถานะ (เปิด กำลังสืบสวน ควบคุมได้ ปิดแล้ว), กด "รับเคสนี้" เพื่อเป็นผู้รับผิดชอบ, และพิมพ์ โน้ต บันทึกการสืบสวน
4. ทุกการกระทำถูกบันทึกใน Timeline พร้อมชื่อผู้ทำและเวลา

13. การวิเคราะห์การแก้ไข (Remediation analytics)

การ์ดใต้กราฟ trend แสดง KPI การจัดการ:

- MTTR – เวลาเฉลี่ยที่ใช้แก้ช่องโหว่ (ขึ้น "–" ถ้ายังไม่มีรายการที่แก้เสร็จ)
- ช่องโหว่ที่เปิดอยู่ / จัดการแล้ว / การถูกยึดที่ยังเปิด
- กราฟแท่งรายสัปดาห์ – เปรียบเทียบช่องโหว่ที่เปิดใหม่ vs ที่แก้/จัดการ (ดู remediation velocity)

14. รายงาน PDF

กดปุ่ม ดาวน์โหลดรายงาน PDF (มุมขวาบน) เพื่อดาวน์โหลดรายงานผู้บริหาร (คะแนนความเสี่ยง, สรุป severity, asset เสี่ยงสูงสุด, ช่องโหว่เด่น)

15. การแจ้งเตือน

เมื่อเจอช่องโหว่ระดับ High/Critical ระบบส่งแจ้งเตือนไป Slack/Teams/Jira/ServiceNow (ตามที่ตั้งค่าไว้) และส่งสรุปภาษาเข้าใจง่ายหลังสแกนเสร็จทุกครั้ง

16. บทบาทผู้ใช้ (RBAC)

- Admin – จัดการได้ทั้งองค์กร
- Security Officer – สแกน/ดู/จัดการช่องโหว่ทุก asset ในองค์กร
- System Owner – สแกนและจัดการเฉพาะ asset ที่ตนเป็นเจ้าของ

17. คำถามที่พบบ่อย

- เข้าใช้งานครั้งแรกมีหน้าให้กดยอมรับ – ข้อตกลงการใช้งาน กดครั้งเดียว
- ยืนยันโดเมนแล้วแต่ยังขึ้นไม่สำเร็จ – DNS ใช้เวลากระจาย 1–30 นาที ลองใหม่ภายหลัง

- เลือกโปรไฟล์ deep ไม่ได้กับ production – ถูกต้อง; deep เป็น active test อนุญาตเฉพาะ staging/dev
- สแกน malware แล้วไม่เจออะไร – ดี แปลว่าไม่พบร่องรอยถูกยึด (ระบบเก็บ baseline ไว้เทียบครั้งถัดไป)
- วิเคราะห์ไฟล์ขึ้น อันตราย – ตรวจ hash/heuristic แล้วพบสัญญาณมัลแวร์ (ไฟล์ไม่ถูกรัน จึงปลอดภัย)
- MTTR ขึ้น "–" – ยังไม่มีช่องโหว่ที่ทำเครื่องหมาย "แก้แล้ว" (remediated); พอมีจะคำนวณให้
- สแกนขึ้น "เชื่อมต่อเป้าหมายไม่ได้" – ตรวจ URL/DNS โดยมากต้องใช้ www.<domain>
- สแกนเว็บภายนอกช้า (2–3 นาที) – ปกติ; ระบบมีตัวบอกความคืบหน้า
- ขึ้นเตือนใบรับรอง (internal) – self-signed cert กดยอมรับครั้งเดียว หรือ trust root CA
