R0Cyber

MITRE ATT&CK FOR DEFENDERS · ตอนที่ 1

รู้จัก MITRE ATT&CK

ภาษากลางที่ทีมป้องกันทั่วโลกใช้อธิบายพฤติกรรมของผู้โจมตี — จากรายงานภัยคุกคาม สู่การตรวจจับที่วัดผลได้

TTPs | v20 · ต.ค. 2569 | Blue Team

01 RECON	02 RESOURCE	03 INITIAL
04 EXECUTION	05 PERSIST	06 PRIV-ESC
07 STEALTH	08 DEF-IMPAIR	09 CRED
10 DISCOVERY	11 LATERAL	12 COLLECT
13 C2	14 EXFIL	15 IMPACT

ENTERPRISE · 15 TACTICS · v20

อ้างอิง MITRE ATT&CK® v20 (ต.ค. 2569) · ATT&CK® เป็นเครื่องหมายการค้าของ The MITRE Corporation · เนื้อหาเพื่อการศึกษาฝ่ายป้องกัน

R0Cyber

ตอนนี้มี 5 หัวข้อ

01	ATT&CK คืออะไร	ที่มา · ทำไมต้องดูพฤติกรรม · Pyramid of Pain
02	โครงสร้างข้อมูล	Tactic · Technique · Sub-technique · Procedure
03	วัตถุอื่นในฐานความรู้	Groups · Software · Campaigns · Mitigations · Detection
04	โดเมนและเวอร์ชัน	Enterprise · Mobile · ICS · v20 · เส้นทางหลักสูตร
05	ทบทวนและสรุป	Quick check · สรุปตอน

R0Cyber

ATT&CK = ฐานความรู้พฤติกรรมผู้โจมตีจากเหตุการณ์จริง

Adversarial

มองจากมุมผู้โจมตี

Tactics

เป้าหมาย: ทำไปเพื่ออะไร

Techniques

วิธีการ: ทำอย่างไร

Common Knowledge

รวบรวมจากเหตุจริงที่เปิดเผย

ใครดูแล

MITRE องค์กรไม่แสวงกำไร เริ่มพัฒนาราวปี 2013 และเปิดสาธารณะปี 2015 — ใช้ฟรี

อัปเดตปีละ 2 ครั้ง

เมษายนและตุลาคม · ล่าสุด v20 (ต.ค. 2569)

ไม่ใช่มาตรฐานบังคับ

เป็นกรอบอ้างอิงที่ทั้งโลกใช้ร่วมกัน — ผู้ขาย SOC ผู้ตรวจสอบ ใช้ภาษาเดียวกัน

ไม่ใช่ checklist

ไม่ได้หมายความว่าต้องป้องกันครบทุกเทคนิค แต่ช่วยเลือกสิ่งที่สำคัญ

R0Cyber

ทำไมต้องดูพฤติกรรม ไม่ใช่แค่ IOC



ATT&CK

อยู่ชั้นบนสุด — อธิบาย TTP

หลักคิด: บล็อก IP หรือแฮช ผู้โจมตีเปลี่ยนได้ในไม่กี่นาที · ตรวจจับ "พฤติกรรม" ได้ ผู้โจมตีต้องเปลี่ยนวิธีทำงานทั้งหมด

STRUCTURE

R0Cyber

โครงสร้าง 4 ระดับของ ATT&CK

Tactic TA0001	ทำไม — เป้าหมายทางยุทธวิธี เช่น Initial Access: "พยายามเข้ามาในเครือข่าย"
Technique T1566	อย่างไร — วิธีการบรรลุเป้าหมาย เช่น Phishing
Sub-technique T1566.001	รายละเอียดเจาะจงขึ้น เช่น Spearphishing Attachment
Procedure	ผู้โจมตีรายหนึ่ง "ทำจริง" อย่างไร เช่น กลุ่ม X ส่งไฟล์แนบเอกสารปลอมเรื่องภาษี

รูปแบบรหัส: TAxxxx = Tactic · Txxxx = Technique · Txxxx.xxx = Sub-technique — ใช้รหัสอ้างอิงแทนชื่อ ช่วยให้สื่อสารตรงกัน

R0Cyber

วัตถุอื่นในฐานความรู้ ATT&CK

Groups G0xxx

กลุ่มผู้โจมตีที่ติดตาม และเทคนิคที่ใช้

Software S0xxx

มัลแวร์และเครื่องมือที่ถูกใช้

Campaigns C0xxx

ชุดปฏิบัติการในช่วงเวลาหนึ่ง

Mitigations M1xxx

มาตรการลดความเสี่ยง เช่น MFA (M1032)

Detection Strategies

แนวทางตรวจจับต่อเทคนิค (ใหม่ตั้งแต่ v18)

Analytics + Data Components

ตรรกะตรวจจับ และข้อมูล/log ที่ต้องมี

ทุกอย่างเชื่อมกัน: กลุ่ม ⟶ ใช้ซอฟต์แวร์ ⟶ ใช้เทคนิค ⟶ ป้องกันด้วย mitigation ⟶ ตรวจจับด้วย detection strategy

ตั้งแต่ v18 (ต.ค. 2568) MITRE เปลี่ยนส่วน Detection เป็น Detection Strategies + Analytics และเลิกใช้ Data Sources แบบเดิม

EXAMPLE

R0Cyber

ตัวอย่าง: อ่านเหตุการณ์ด้วยภาษา ATT&CK

อีเมลแนบไฟล์หลอกลวง

Initial Access

T1566.001

→

ผู้ใช้เปิด มาโครรัน PowerShell

Execution

T1059.001

→

ใช้บัญชีพนักงานที่ขโมยได้

Privilege Esc. / Persistence

T1078

→

เข้ารหัสไฟล์เรียกค่าไถ่

Impact

T1486

ประโยชน์: SOC ผู้บริหาร ผู้ให้บริการ และผู้ตรวจสอบ คุยกันรู้เรื่องด้วยรหัสเดียวกัน และถามต่อได้ทันทีว่า "เราตรวจจับ T1059.001 ได้หรือยัง"

หนึ่งเทคนิคอาจอยู่ได้หลาย tactic เช่น Valid Accounts ใช้ได้ทั้งเข้าระบบ คงอยู่ และยกระดับสิทธิ์

R0Cyber

3 โดเมนของ ATT&CK (ข้อมูล v20 ต.ค. 2569)

โดเมน	ครอบคลุม	Tactics	Techniques	Sub-techniques
Enterprise	Windows · macOS · Linux · Cloud · SaaS · Identity · Network · Containers	15	227	479
Mobile	Android · iOS	12	78	47
ICS	ระบบควบคุมอุตสาหกรรม (เชื่อมกับหลักสูตร OT/IoT)	12	78	26

v18 (ต.ค. 2568)

ปรับระบบ Detection ใหม่ทั้งหมด: Detection Strategies + Analytics

v19 (เม.ย. 2569)

แยก Defense Evasion ⟶ Stealth + Defense Impairment · ICS มี sub-technique

v20 (ต.ค. 2569)

เทคนิคด้าน AI (prompt injection · AI result poisoning) · แคมเปญใหม่

ทำไมต้องรู้

เครื่องมือและรายงานเก่าอาจอ้าง ID/ชื่อที่เปลี่ยนแล้ว — ระบุเวอร์ชันทุกครั้ง

R0Cyber

เส้นทางหลักสูตร 7 ตอน

ตอน 1
รู้จัก ATT&CK

ตอน 2
15 Tactics

ตอน 3
Techniques และการอ่านหน้า

ตอน 4
Threat Intelligence + Navigator

ตอน 5
Detection Engineering + Coverage

ตอน 6
Emulation · Purple Team · Frameworks

ตอน 7
Workshop: map เหตุจริง

วัดผล: แบบทดสอบก่อนเรียน · ควิซท้ายตอน · Workshop mapping · แบบทดสอบหลังเรียน · ใบรับรอง

เหมาะกับ: นักวิเคราะห์ SOC · Threat hunter · Detection engineer · ทีม IR · ผู้บริหารความปลอดภัย

QUICK CHECK

R0Cyber

ทบทวนสั้น ๆ: จริงหรือไม่จริง?

1. Technique ตอบคำถามว่า "ผู้โจมตีทำไปเพื่ออะไร"	✗ ไม่จริง	นั่นคือ Tactic
2. T1566.001 เป็นรหัสของ Sub-technique	✓ จริง	มีจุดตามด้วยเลข
3. ตรวจจับพฤติกรรม (TTP) ทำให้ผู้โจมตีเปลี่ยนตัวได้ยากกว่า IOC	✓ จริง	Pyramid of Pain
4. ATT&CK เป็น checklist ที่ต้องป้องกันครบทุกเทคนิค	✗ ไม่จริง	ใช้จัดลำดับความสำคัญ

SUMMARY · ตอนที่ 1

สรุป: รู้จัก MITRE ATT&CK

- ✓ ฐานความรู้พฤติกรรมผู้โจมตีจากเหตุจริง · ใช้ฟรี
- ✓ TTP อยู่บนสุดของ Pyramid of Pain
- ✓ Tactic (ทำไม) ⟶ Technique (อย่างไร) ⟶ Sub-technique ⟶ Procedure
- ✓ Groups · Software · Mitigations · Detection Strategies
- ✓ 3 โดเมน · Enterprise v20 มี 15 tactics

ทำแบบทดสอบท้ายตอน แล้วพบกันในตอนถัดไป

R0Cyber

MITRE ATT&CK · learn.r0cyber.com

ตอนถัดไป

ตอนที่ 2

15 Tactics ของ Enterprise

- จาก Reconnaissance ถึง Impact
- Stealth + Defense Impairment (v19)
- ไม่จำเป็นต้องเรียงตามลำดับ
- มุมมองฝ่ายป้องกันในแต่ละ tactic