📄 Page 2 – MITRE ATT&CK Mapping + Detection Engineering

By: Kim Lien Chu

Title: MITRE ATT&CK Mapping: Step-by-Step Cheat Sheet for SOC Analysts
Focus Area: Translating threat intel into actionable defense for healthcare SOCs

---

🔍 Summary

This artifact is a hands-on guide for mapping raw adversary behaviors to MITRE ATT&CK techniques, contextualizing them for healthcare environments, and aligning them with federal cybersecurity frameworks. It empowers SOC analysts to operationalize threat intelligence, build detection logic, and support defense planning in clinical settings.

🧠 Skills Demonstrated

- Threat intelligence parsing and technique mapping
- MITRE ATT&CK fluency and sector contextualization
- Detection logic development for SIEM/XDR platforms
- Risk alignment with HHS 405(d), CISA SRMA, and NIST CSF
- Scenario design for tabletop exercises and staff training

🧰 Tools & Frameworks Used

- MITRE ATT&CK Navigator
- CrowdStrike, Mandiant, CISA threat reports
- Splunk/Sysmon detection logic references
- HHS 405(d) Practices #4, #9, #10
- CISA SRMA Sector Risk Profiles

🧩 Artifact Walkthrough

Step 1: Extract Adversary Behaviors

Start with threat intel and pull out raw actions:

- “Fake IT candidates gaining insider access”
- “Use of ORB networks to mask infrastructure”
- “Abuse of AnyDesk for persistence”
- “Callback phishing targeting help desk”

Step 2: Identify the MITRE Technique

Use MITRE ATT&CK Navigator to map each behavior to a technique.

Behavior	**Mapped Technique**	**Technique ID**
Fake IT candidates gaining insider access	Valid Accounts	T1078
Abuse of AnyDesk for persistence	Remote Access Software	T1219
Use of ORB networks to mask infrastructure	Acquire Infrastructure: Domains	T1583.001
Callback phishing targeting help desk	Phishing: Spearphishing via Service	T1566.001

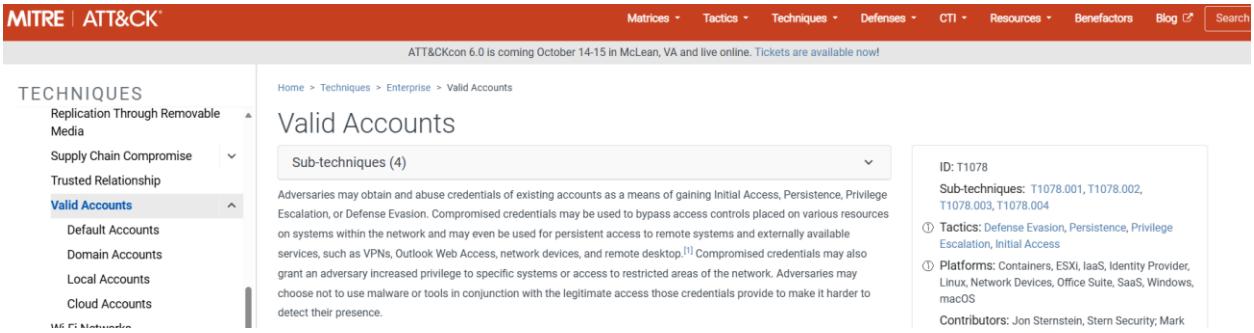

Figure 1: MITRE ATT&CK technique T1078 – Valid Accounts, confirming mapping for insider access via fake IT hires.

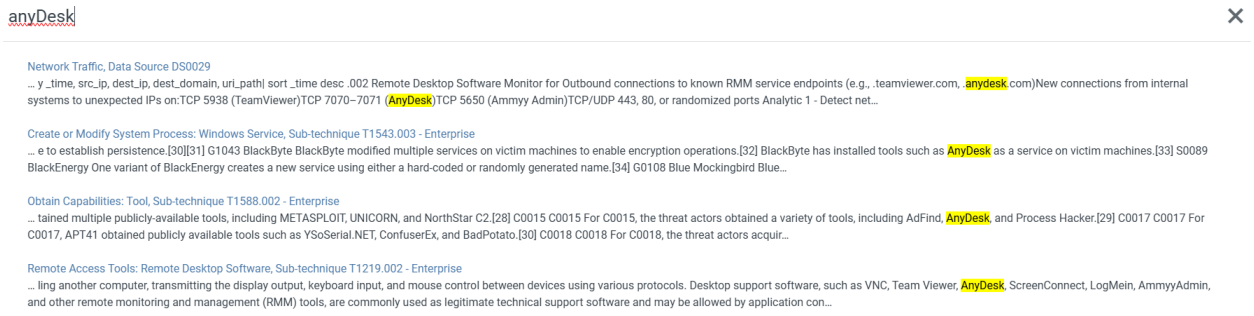

Figure 2: MITRE search results for "AnyDesk" confirming technique T1219 – Remote Access Software.

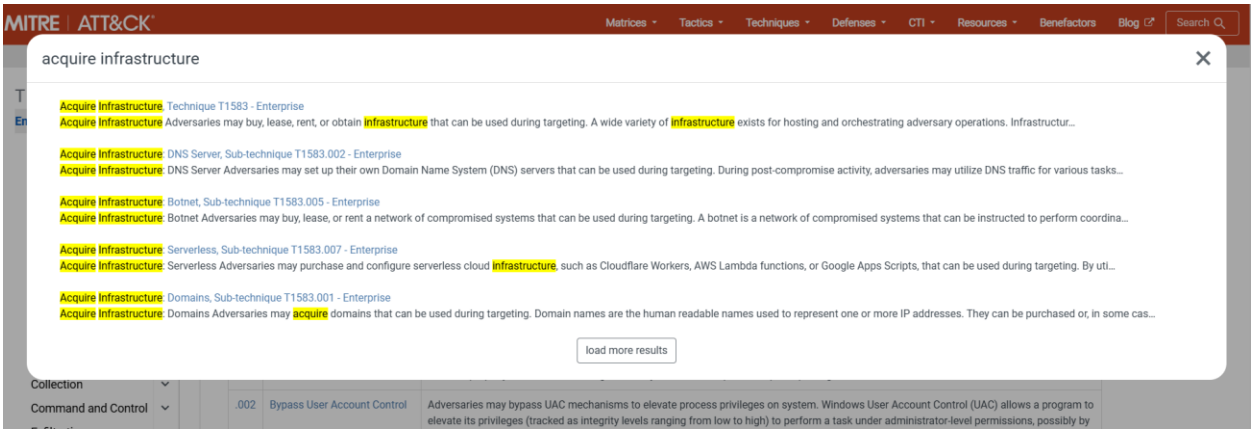

Figure 3: MITRE sub-technique T1583.001 – Domains, used to mask C2 infrastructure via ORB networks.

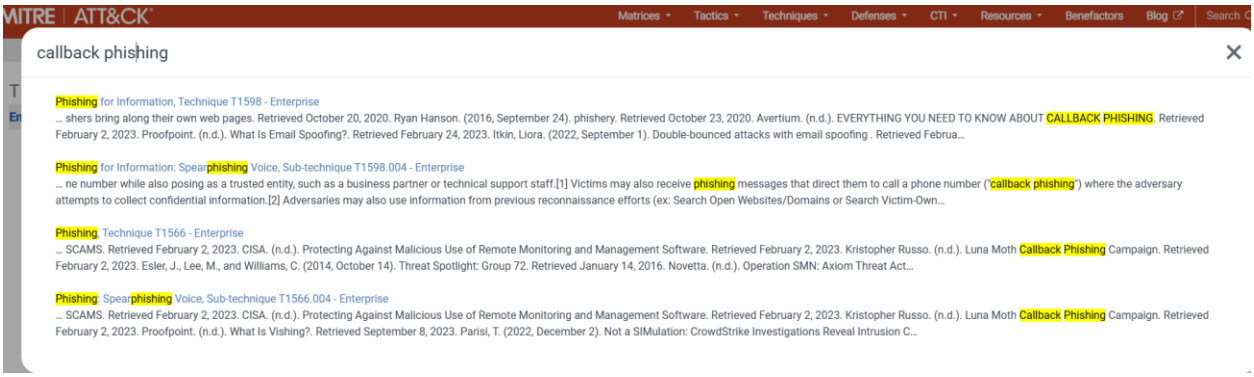

Figure 4: MITRE technique T1566.001 – Phishing via Service, used in callback phishing targeting help desks.

Step 3: Contextualize the Mapping

Technique ID	Name	Use Case
T1078	Valid Accounts	Insider access via fake IT hires in healthcare SOC
T1219	Remote Access Software	RMM abuse during callback phishing to maintain persistence
T1583.001	Acquire Infrastructure: Domains	ORB networks used to mask C2 targeting hospital help desks
T1566.001	Phishing: Spearphishing via Service	Callback phishing targeting help desk to reset credentials

---

Step 4: Align to Sector Risks

Risk Vector	Technique	Mitigation Strategy
Insider Threat	T1078	Enhanced vetting, behavioral analytics
Remote Access Abuse	T1219	Restrict RMM usage, monitor anomalies

Infrastructure Obfuscation	T1583.001	Threat hunting, DNS anomaly detection
Social Engineering	T1566.001	Training, MFA, call-back verification

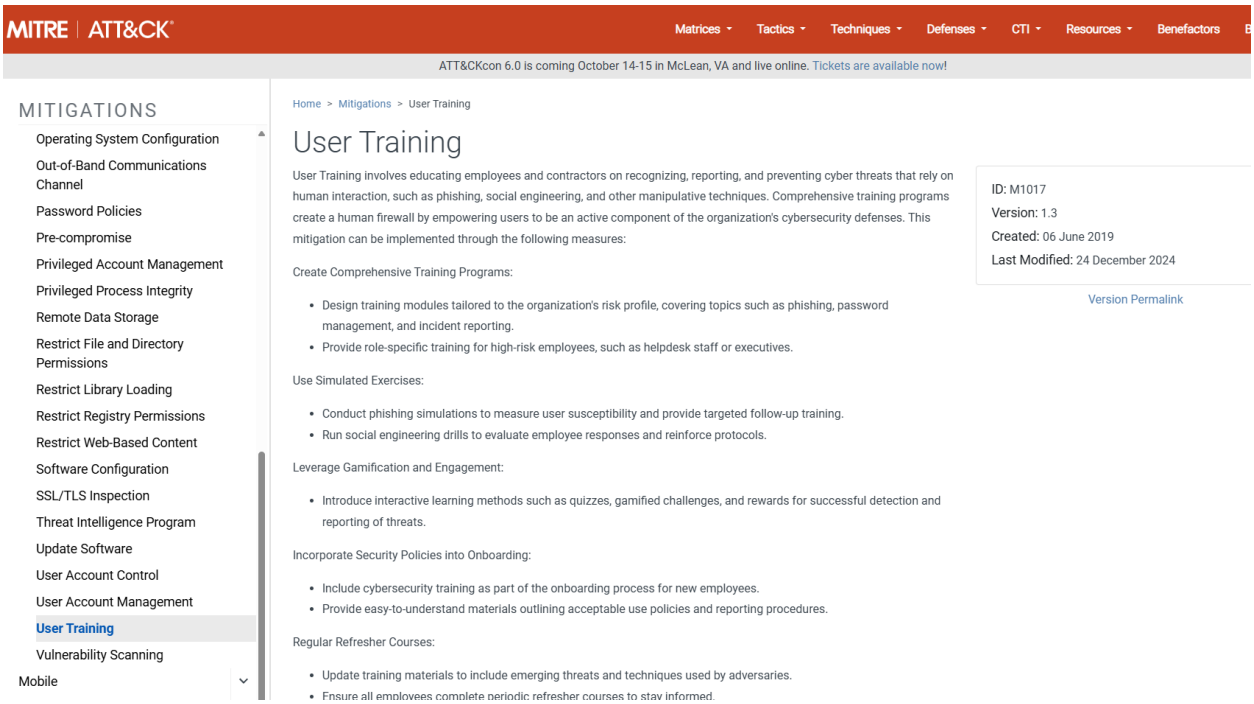

Figure 5: MITRE M1017 – User Training mitigation strategy for phishing and social engineering.

Step 5: Apply in Defense Planning

Use these mappings to:

- Build SIEM/XDR detection rules
- Create tabletop scenarios for SOC teams
- Train staff on specific TTPs and red flags
- Align with HHS 405(d), CISA SRMA, and NIST CSF practices

🏥 Use Case Scenario

During a simulated callback phishing attack at a regional hospital, analysts used this cheat sheet to rapidly identify RMM abuse, map it to T1219, and deploy detection logic in Splunk. The artifact also supported tabletop planning and staff training aligned with HHS 405(d) Practice #10.

✍️ Reflection

This artifact reflects my commitment to bridging the gap between threat intelligence and operational defense. By translating raw behaviors into standardized techniques and aligning them with healthcare-specific risks, I help SOC teams move faster, smarter, and in sync with national guidance.

📚 References

1. MITRE ATT&CK Framework – https://attack.mitre.org
2. MITRE M1017: User Training – https://attack.mitre.org/mitigations/M1017
3. HHS 405(d) Cybersecurity Practices – https://405d.hhs.gov
4. CISA Sector Risk Management Agency Guidance – https://www.cisa.gov/srma
5. CrowdStrike 2025 Threat Hunting Report – Referenced for adversary behaviors and technique validation
6. Mandiant Threat Intelligence Briefs – Used for mapping callback phishing and infrastructure tactics
7. Sysmon + Splunk Detection Logic – Applied in simulation context for T1219 and T1078
