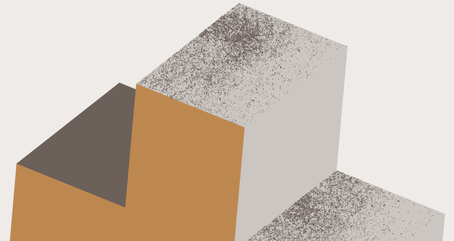
Understanding MITRE ATT&CK

Framework for Cybersecurity Assessment

- **MITRE ATT&CK is a matrix of tactics and techniques used to assess and classify cyber threats.**
- **It helps threat hunters identify and address risks, while red teamers simulate attacks to test security defenses.**
- **It’s objective is to strengthen the steps taken after an organization has been comprised.**

Delve into the mind-bending world of MITRE ATT&CK Types!



1. Reconnaissance(10 techniques): Gathering information about the target organization to plan future adversary operations.

2. Resource Development(8 techniques): Establishing resources they can use to support operations.

3. Initial Access(10 techniques): Getting into your network, that is spear phishing.

4. Execution(14 techniques): Running malicious code, for example, running a remote access tool.

5. Persistence(20 techniques): Maintaining their foothold by changing configurations.

6. Privilege Escalation(14 techniques): Trying to gain higher-level permissions, that is, leveraging a vulnerability to elevate access.

7. Defense Evasion(43 techniques): Avoiding being detected by using trusted processes to hide malware.

8. Credential Access(17 techniques): Stealing accounts passwords and names.

9. Discovery(32 techniques): Figuring out your environment and exploring what they can control.

10. Lateral Movement(9 techniques): Moving through your environment by using legitimate credentials to pivot through several systems.

11. Collection(17 techniques): Gathering data of interest to their goal by accessing data in cloud storage.

12. Command and Control(18 techniques): Communicating with compromised network systems to control them by imitating normal web traffic to communicate with a victim network.

13. Exfiltration(9 techniques): Stealing data and transferring it to a cloud account.

14. Impact(14 techniques): Manipulating, interrupting, or destroying your systems and data.

"Where on Earth and Why is Mitre Att&ck making waves?"

MITRE ATT&CK's Popular Hangouts

1. **Government Agencies**:
   - **Spotlight**: Government bigwigs in defense, intelligence, and cybersecurity swear by MITRE ATT&CK to shield national secrets and vital infrastructure.
   - **Why the Fuss?**: With sneaky nation-state foes lurking, these agencies need to crack the code on potential threats to stay one step ahead.
2. **Financial Fortresses**:
   - **Spotlight**: Banks and money maestros rely on MITRE ATT&CK to lock down cash vaults and financial info from cyber crooks.
   - **Why the Craze?**: Money talks, and so do cyber bandits eyeing a slice. Knowing the attack playbook helps keep data safe from breaches and financial hanky-panky.
3. **Healthcare Heroes**:
   - **Spotlight**: Hospitals and health wizards use MITRE ATT&CK to guard patient records and lifesaving gadgets.
   - **Why the Buzz?**: Health secrets are the holy grail, and uninterrupted care is a must, making healthcare a bullseye for digital bad guys.
4. **Tech Titans**:
   - **Spotlight**: Tech gurus crafting software, hardware, and security gems weave MITRE ATT&CK into their shields and innovation quests.
   - **Why the Hype?**: Innovation is a treasure trove for thieves, pushing tech wizards to fortify defenses and keep creativity safe.
5. **Power Protectors**:
   - **Spotlight**: Energy giants harness MITRE ATT&CK to armor up power grids and oil rigs.
   - **Why the Heat?**: Power plants and pipelines are the lifelines of a nation, making them prime targets for cyber mischief-makers.
6. **Watchful Guardians (SOCs)**:
   - **Spotlight**: Security superheroes in SOCs flex MITRE ATT&CK for spotting, fighting, and hunting threats.
   - **Why the Spark?**: It's like having X-ray vision for cyber threats, making SOCs faster and deadlier at thwarting digital baddies.
7. **Brainy Campuses**:
   - **Spotlight**: Universities and research hubs wave the MITRE ATT&CK flag for securing brainy data and ideas.
   - **Why the Applause?**: With spies snooping around for juicy research bits, these institutions need a shield for their intellectual treasures.

MITRE ATT&CK's Cool Factor

#Threat Buffet: MITRE ATT&CK serves up a feast of cyber threat tactics, giving a 360-degree view of what's lurking in the digital shadows.
#Lingo Love: It's the secret security language that unites cyber defenders, making battle plans clearer and teamwork smoother.
#Real Deal: Based on real-world baddie moves, MITRE ATT&CK is as legit as it gets for tackling actual threats head-on.
#Spot-On Defense: By linking security strategies to MITRE ATT&CK tactics, organizations can sniff out, fight off, and squash attacks like never before.
#Stay Ahead: With MITRE ATT&CK, it's all about being the hunter, not the hunted. Spot vulnerabilities before the baddies do, and sleep easier at night.
#Always Fresh: MITRE ATT&CK stays in the loop with the latest threat tricks, keeping organizations one step ahead in the digital cat-and-mouse game.
#Rulebook Gold: Many cybersecurity rules and guides nod to MITRE ATT&CK, making it a must-have for playing by the book and staying secure.

THANK YOU

By Aradhana Baranwal