MITRE

Who is MITRE?
- Non-for-profit private company operating in the public interest.
- Created after the 2nd WORLD WAR and rising on the Cold War.
- Focuses on R+D for EE.UU. Nation Security working on Federally Funded Research and Development Center(FFRDC)
- From Air Defense System in the Cold War to GPS, Air Traffic Collision Avoidance Systems and others.
- Holds +200 patents and +670 technologies licenses transferred to industry and universities
- 1.800.000$ revenue / 8.200 employees / 60 locations in EEUU.
- Operates in different segments (Security, Healthcare, etc)

CENTERS

Others. | *HEALTHCARE* | **CYBERSECURITY** | *AVIATION* | *MODERNIZATION*

MITRE | ATT&CK

Knowledge Database of Adversary Tactics & Techniques

FROM: Looking at attacker methods and behaviors

TO: Applying active defense methods

Active Defense Knowledge Database

MITRE | Shield

TACTICS (TA00xx)
- **TECNICS (T1xxx)**
  - Subtecnics (T1xxx.0xx)
- Mitigation (M10xx)
- Group (string name)

MAPPING

DEFENSIVE TACTICS (DTA000x)
- **DEFENSIVE TECNICS (DTE00xx)**
  - Defen.Opportunities (DOS0xxx)
  - Defen.Use Cases (DUC0xxx)
  - Defen.Procedure (DPR000x)

Definitions:
- TActics: Adversary "High-Level" technical goal / target
- Tecnics - Subtecnics: How the goal is achieved
- Mitigations:the action of reducing the severity, seriousness, or painfulness of the attack
- Groups: Sets of related intrusion activity that are tracked by a common name in the security community
- Defense Opportunity: What to learn or achieve
- Use Case: What can be done or executed
- Procedure: Take action!!

ATT&CK Technique	Opportunity Space	AD Technique	Use Case
T1001 - Data Obfuscation	There is an opportunity to detect adversary activity that uses obfuscated communication.	DTE0028 - PCAP Collection	A defender can capture network traffic for a compromised system and look for abnormal network traffic that may signal data obfuscation.
T1001 - Data Obfuscation	There is an opportunity to reveal data that the adversary has tried to protect from defenders	DTE0031 - Protocol Decoder	Defenders can develop protocol decoders that can decrypt network capture data and expose an adversary's command and control traffic as well as their exfiltration activity.
T1003 - OS Credential Dumping	There is an opportunity to deploy a tripwire that triggers an alert when an adversary touches a network resource or uses a specific technique.	DTE0012 - Decoy Credentials	A defender can seed systems with decoy credentials in a variety of locations and establish alerting that will trigger if an adversary harvests the credentials and attempts to use them.