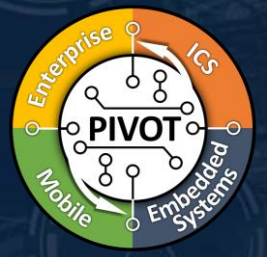
# Platform Independent Vectors of Techniques (PIVOT) Overview




Mario F. Zuniga
Capability Area Lead for Weapon System & Defensive Critical Infrastructure
Cyber Infrastructure Protection Innovation Center, MITRE Labs

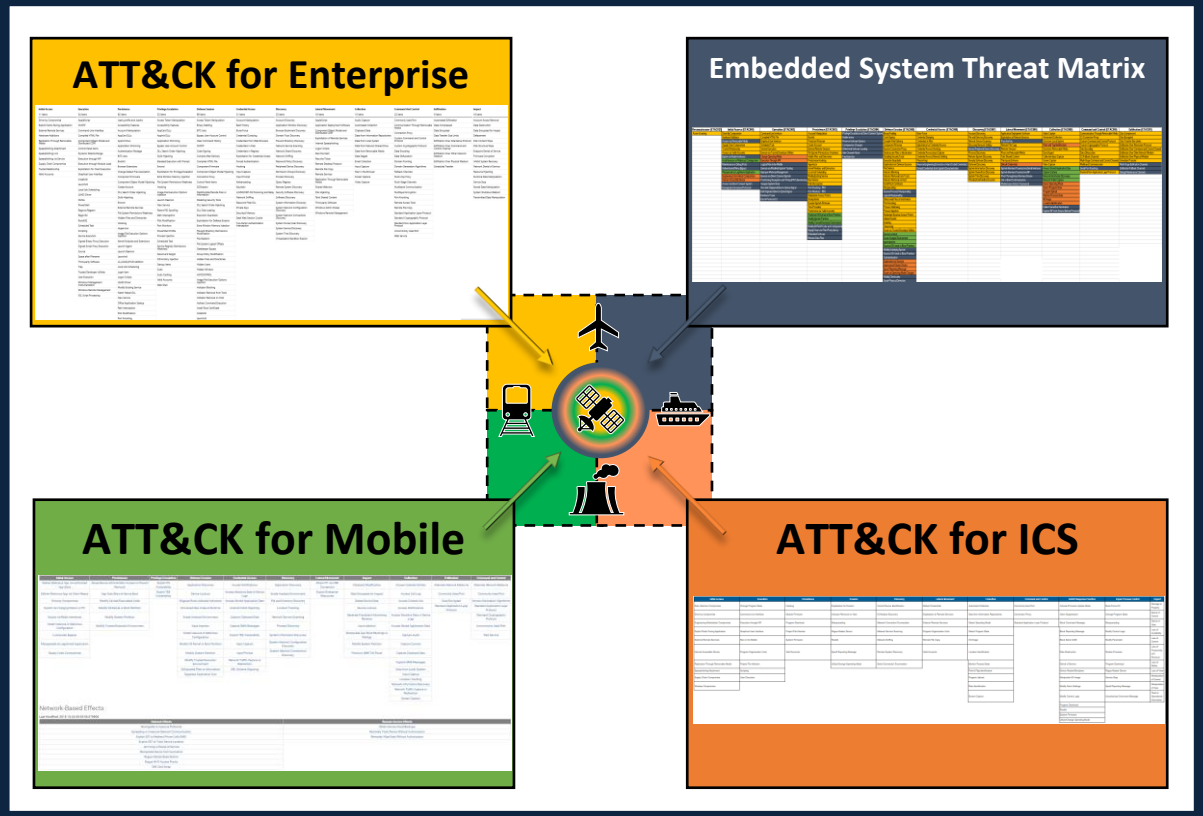
MITRE

# PIVOT Background

- Traditional risk analysis focuses on well-defined boundaries, while systems-of-systems (SoS) involve complex, hyperconnected environments with diverse architectures, protocols, and embedded technologies, making cyber risk assessment more challenging.

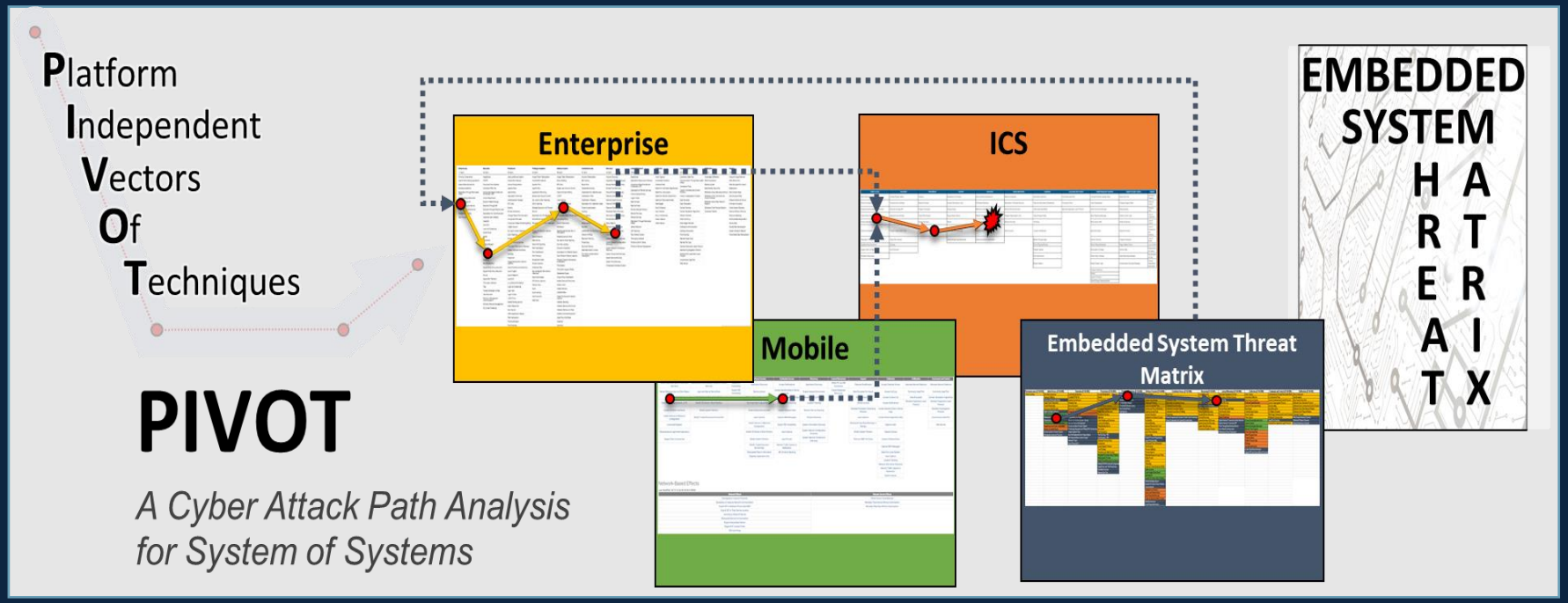
- MITRE developed the PIVOT concept to connect multiple threat matrices, identify critical PIVOT points (e.g., gateway components), and address gaps in SoS cyber assessments, enabling better detection of adversary lateral movements across technology domains (i.e., IT to OT).

Concept to depict the blending of multiple technologies commonly found within a SoS and to correlate the corresponding threat matrix such as, MITRE ATT&CK® and ESTM.




MITRE

# Addressing Utilization of Multiple Threat Matrices

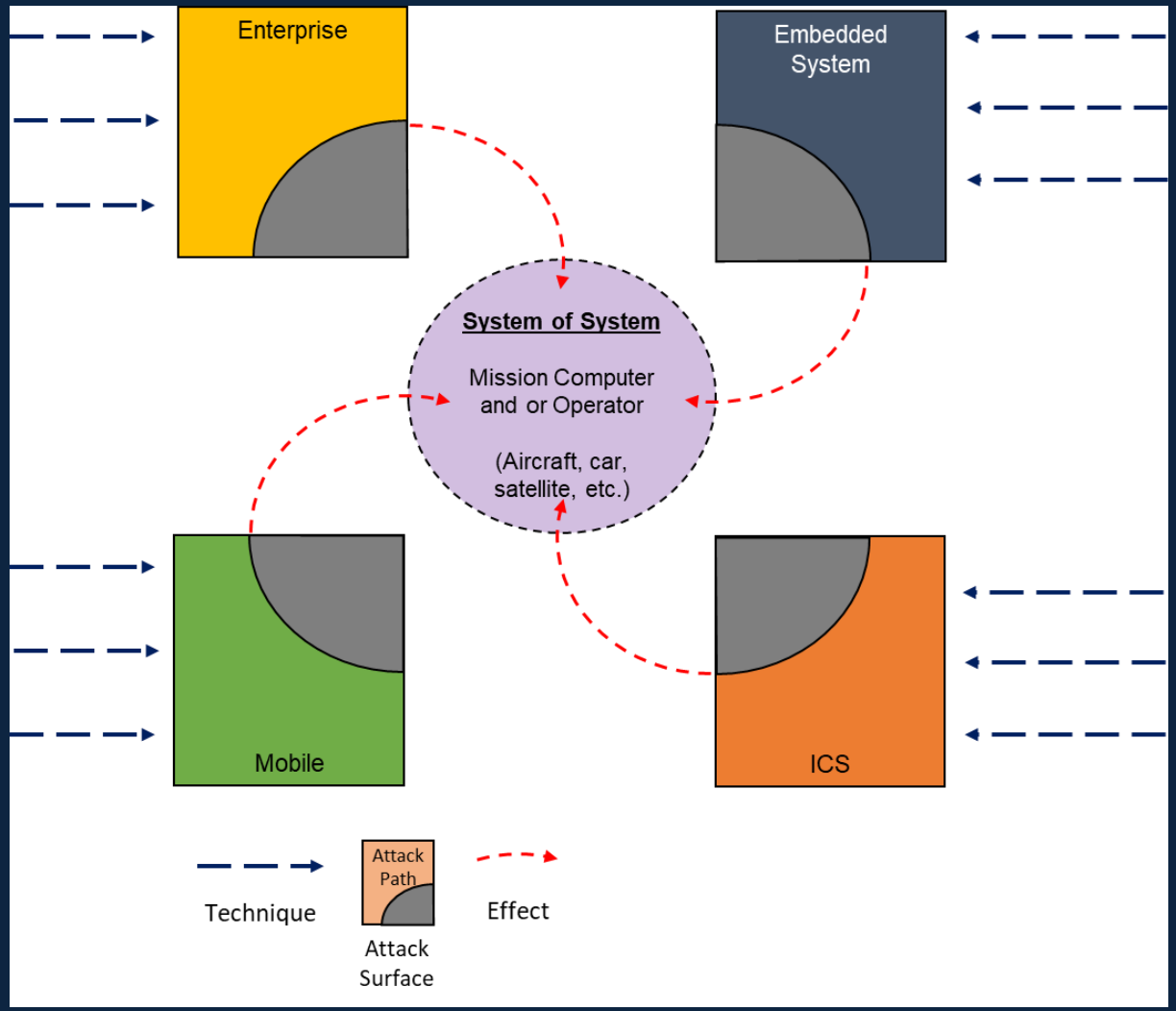



Attack path across a system-of-systems requires use of multiple threat matrices to observe how an adversary must conform their behavior to the environment they seek to effect.

MITRE

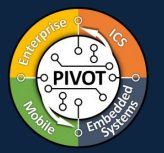
# PIVOT Defined

- A methodology that identifies or discovers the points in a system-of-systems that could be used to bridge between technology stacks, and the associated techniques an attacker would use to cross those bridges.
- Used in combination with digital engineering tools, adversary technique knowledge bases like ATT&CK, and system architecture diagrams.
- Applicability for analysts, system defenders, acquisition community, system owners.
- Integrate with CTI, TTP Based Hunting, and risk assessment to build a synergistic and comprehensive analysis.




MITRE

# PIVOT Defined



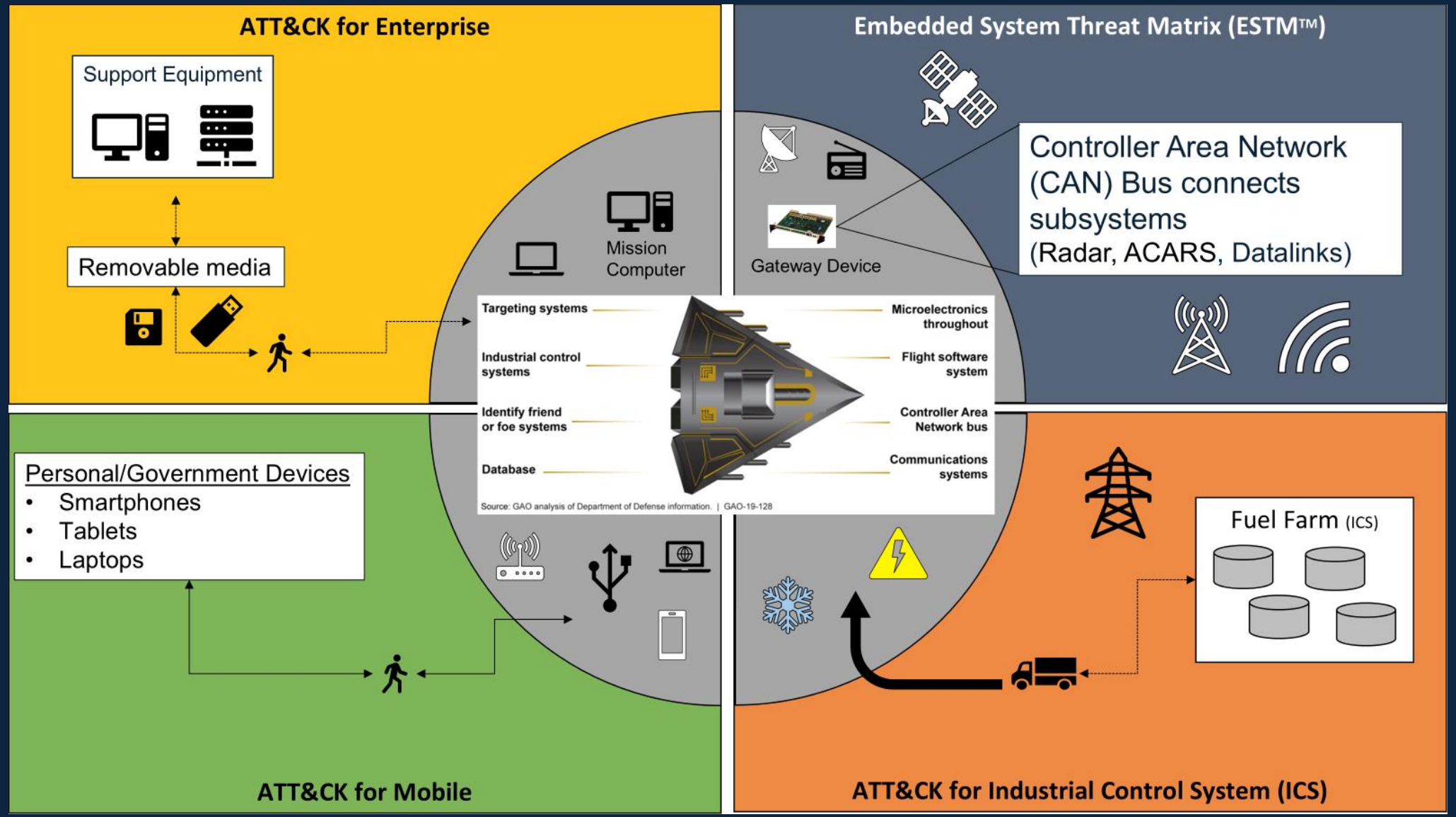

1. Conduct mission decomposition to identify mission critical functions (i.e., MRAP-C, FMA-C, STPA-Sec).
2. Conduct system decomposition (i.e., ASSURANT, MRAP-C, CMTA).
3. Identify mission critical components that if affected, would impact the system's ability to execute its mission.
   - Identify terrain or components that act as "PIVOT points" or bridge technology boundaries.
4. Map Attack Paths from Mission Critical Component to Entry Access Point.
   - For each cyber action that could cause mission failure:
     a) Analyze and identify the techniques an adversary could use to accomplish that action
     b) For each technique, determine prerequisites for techniques on that system (e.g., Access, Credentials, Information)
     c) If all pre-requisites are now outside the system boundaries (e.g., internet access, no credentials)
        - Attack path is complete, repeat process for next mission failure scenario
     d) If not,
        - For each pre-requisite, return to (a) and repeat.
5. Determine what steps could be taken to block or mitigate effects, tactics, and techniques along the attack path.

**Core Principles**

PIVOT Points  Multiple Technologies  "Z to A" Attack Path Analysis

MITRE

# PIVOT Storyboard: Notional Aircraft




MITRE

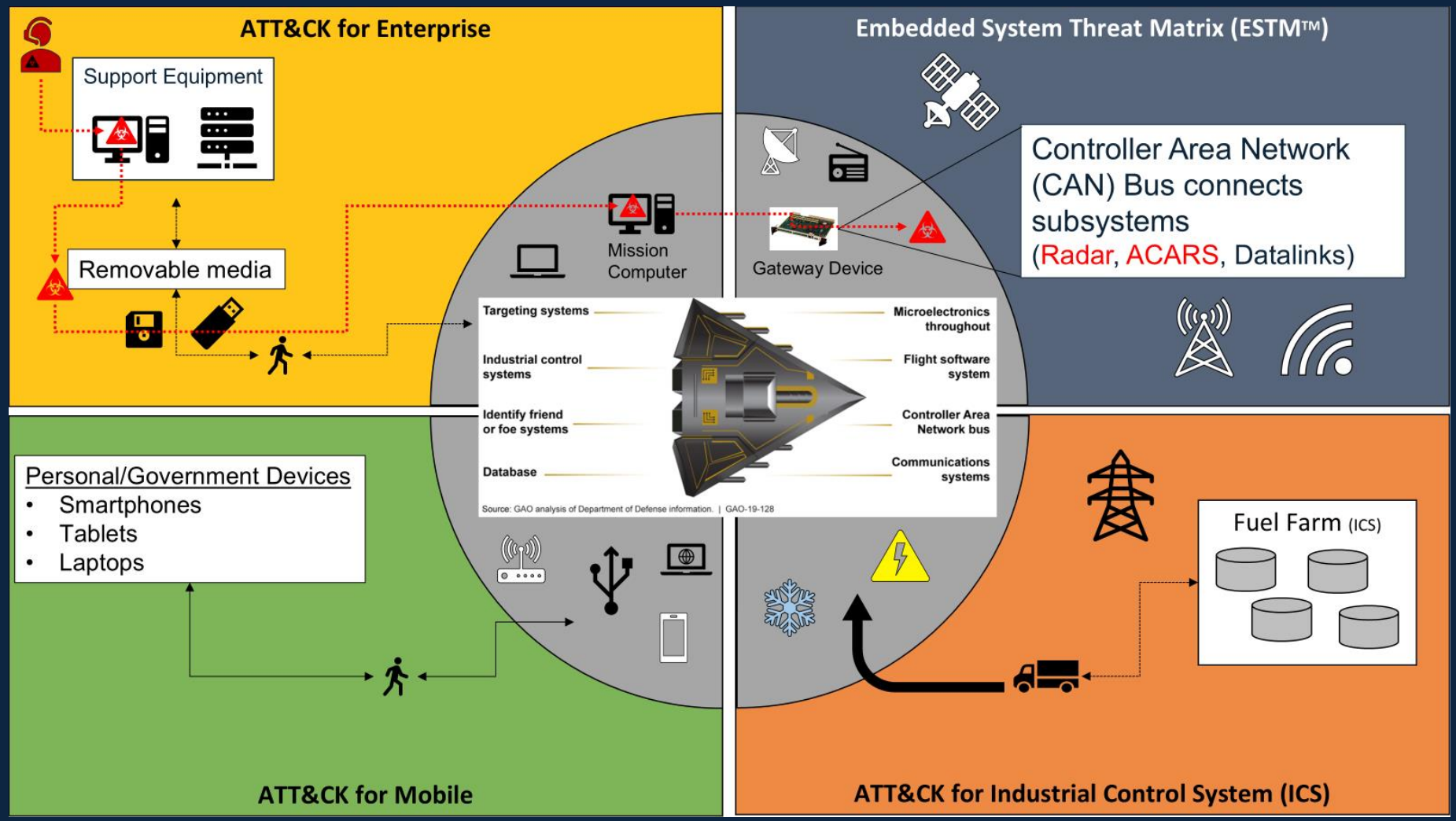
# PIVOT Storyboard: Notional Aircraft Attack Scenario

ATT&CK TTPs

T1195: Supply Chain Compromise

T1091: Replication Through Removable Media

T1570: Lateral Tool Transfer




ESTM TTPs

EST000140: System Interface Traversal via Serial Interface

EST000204: Impair Process via Modified System Tasking

MITRE

# The Fusion of Technology for Aviation

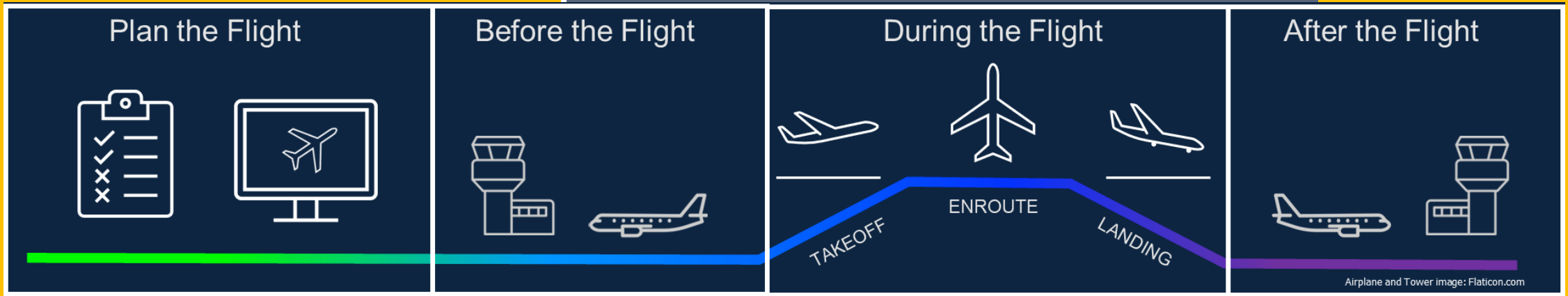
- Complex environments such as an airport require the fusion of multiple technologies, connections and data pathways.

## Embedded Systems



Radar and radio tower images: Wikipedia.com

- Leverage the appropriate threat matrix to analyze cyber risk to a system or component.




Information Technology

Critical Infrastructure

- Fuse together an attack path that crosses technology stacks.

MITRE

# PIVOT Use Case: 2017 TRITON ICS ATTACK

- **Engineered for Destruction**: TRITON is one of most dangerous threat activity publicly known.
  - The malware was intentionally developed to compromise and disrupt industrial safety instrumented systems (SIS), which are designed to prevent loss of life and environmental damage.

- **Danger Lies in TRITON Potential:** The malware framework was highly tailored, and while challenging to scale, it provides a blueprint of how to target SIS and similar systems.
  - The *tradecraft* is scalable and publicly available, even if the malware code changes.

- **Currently Active**: The Russian threat actor XENOTIME/TEMP.Veles remains active.
  - Evidence indicates that the threat actors are using some of the same digital tradecraft to target victims in North America.

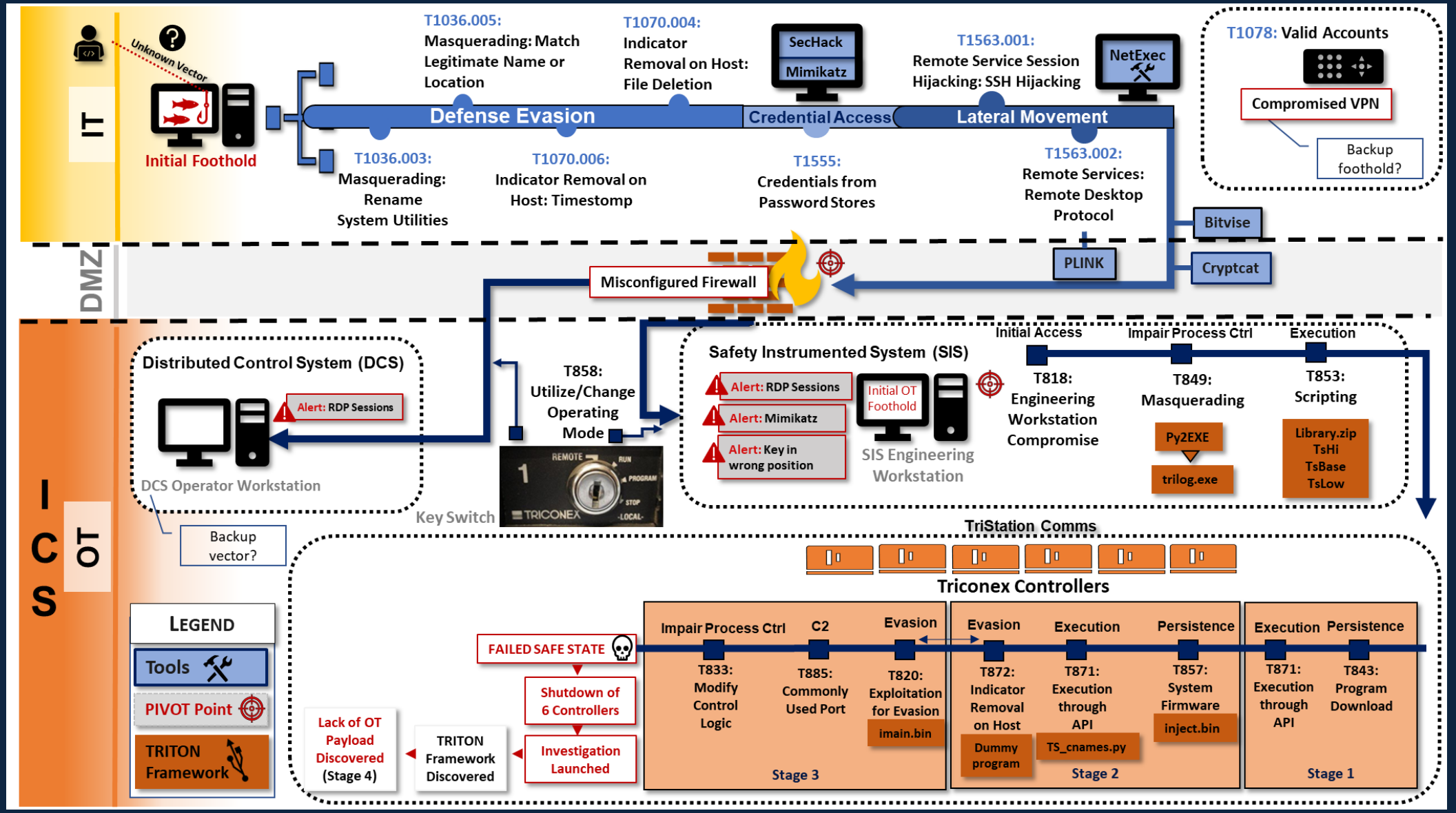
MITRE

# TRITON Campaign Overview

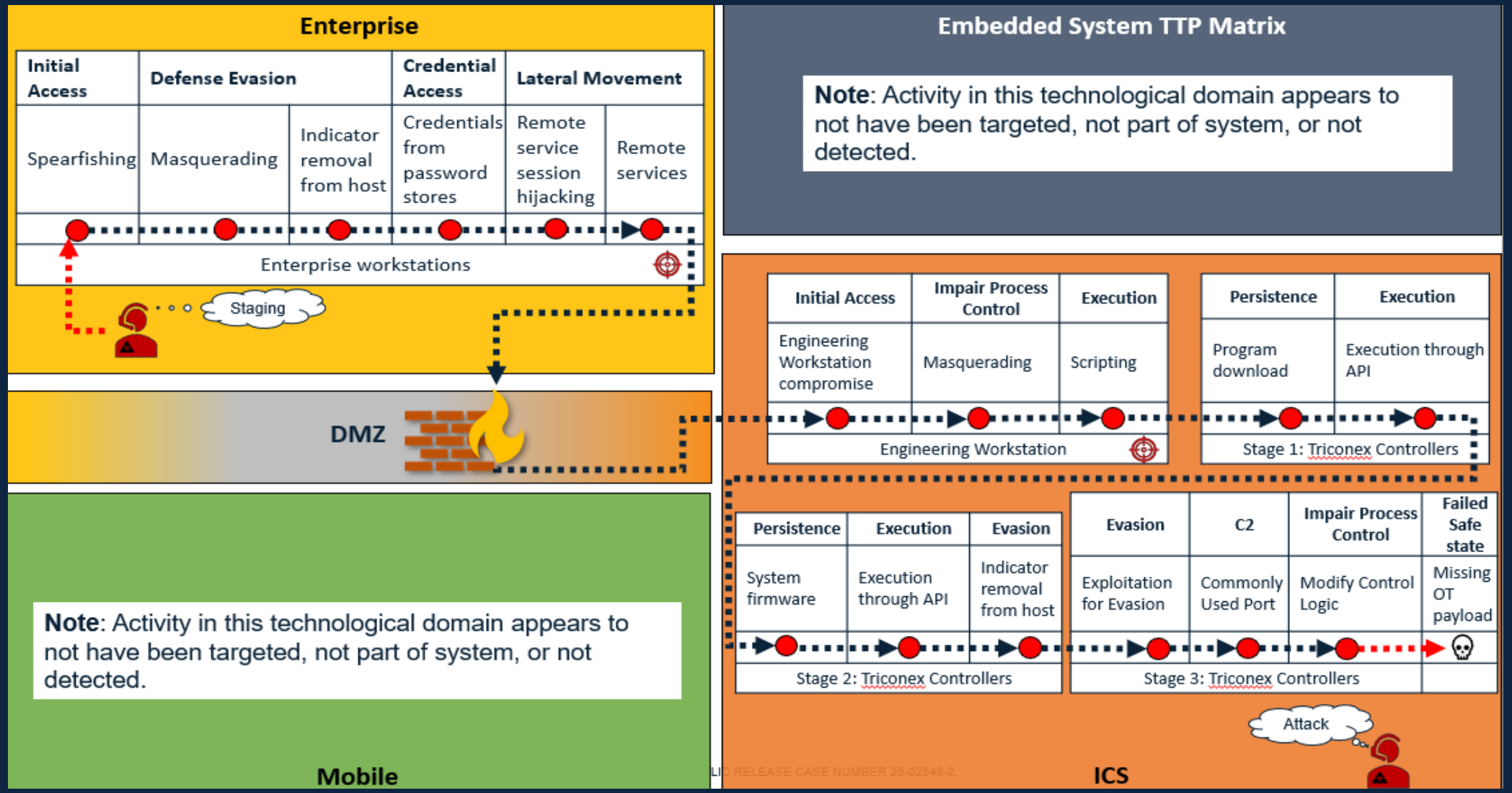

- The multi-stage malware campaign was extremely stealthy and was only uncovered because the attackers made a mistake that triggered the safety system, shutting down the plant.
  - Following the initial compromise of the IT system, the threat actor ***harvested credentials*** to aid with lateral movement across the DMZ to reach the SIS engineering workstation (OT system).
  - Exploited a ***buffer overflow*** vulnerability to install a Remote Access Trojan (RAT).
  - Using the RAT, they exploited a zero-day ***privilege escalation*** to elevate read, write, and execute privileges.
  - The threat actors had planned to manipulate the speed of the components to cause an explosion but triggered a failed safe state and shut down the plant.

MITRE

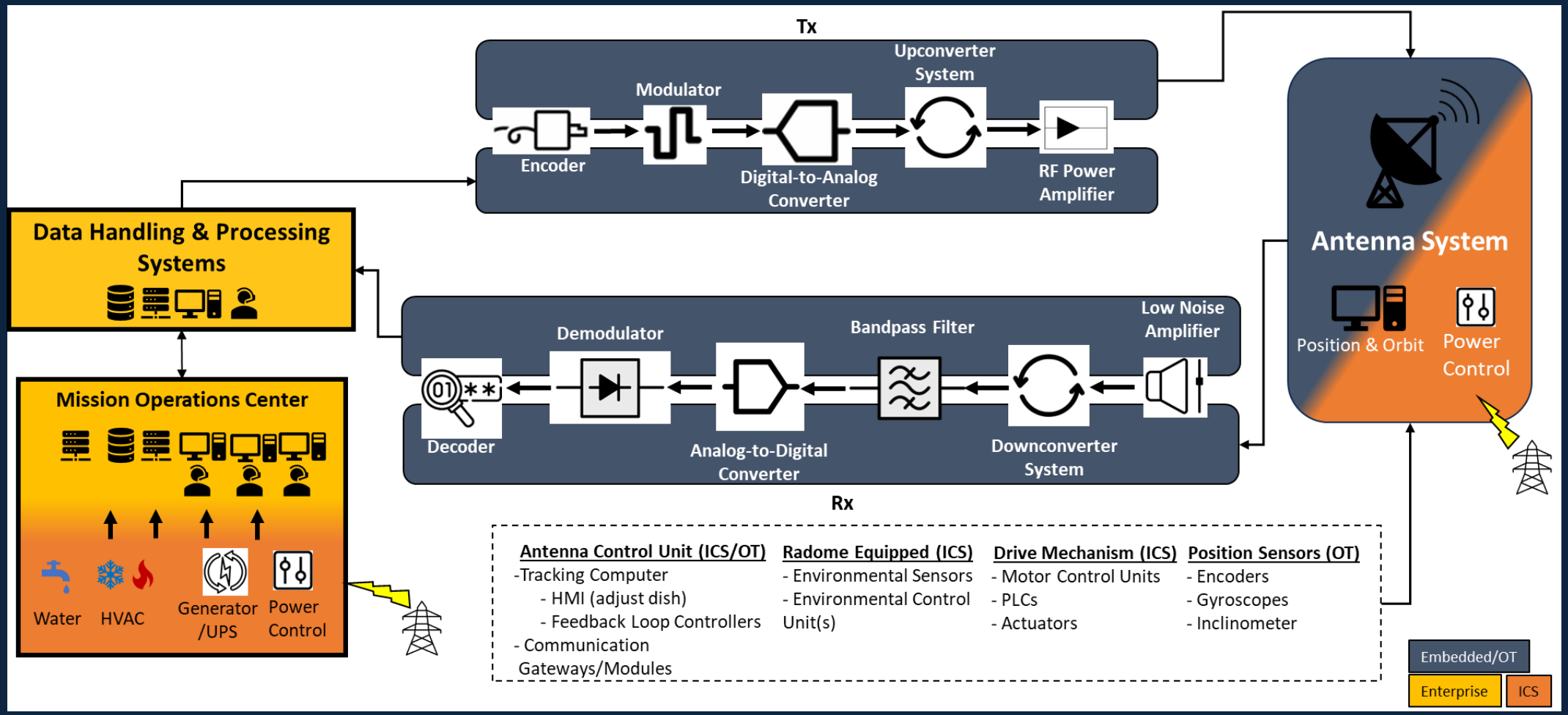
# PIVOT Storyboard (Detailed): TRITON



# PIVOT Storyboard (Simple): TRITON



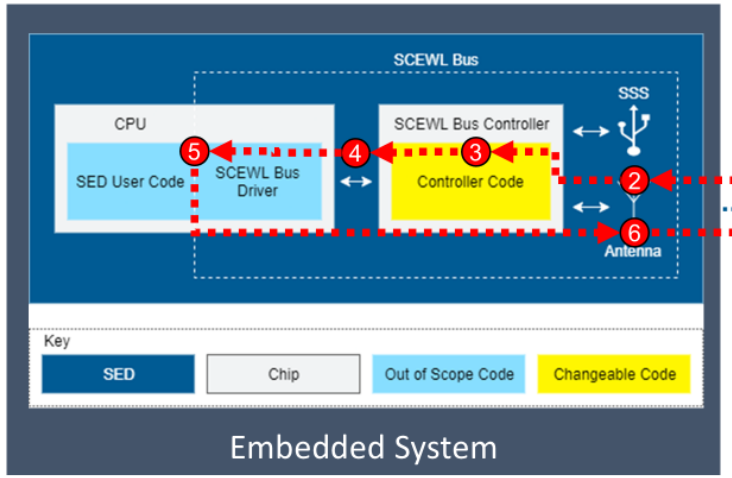
# PIVOT Storyboard: Generic Space System



# PIVOT Storyboard: MITRE eCTF 2021

- Teams were challenged during this capture the flag with preventing an adversary from reading, modifying, or replaying transmissions and prevent spoofing against UAV.
- Storyboard depicts the use of PIVOT, ATT&CK and ESTM in conjunction with a threat actor's attack path.

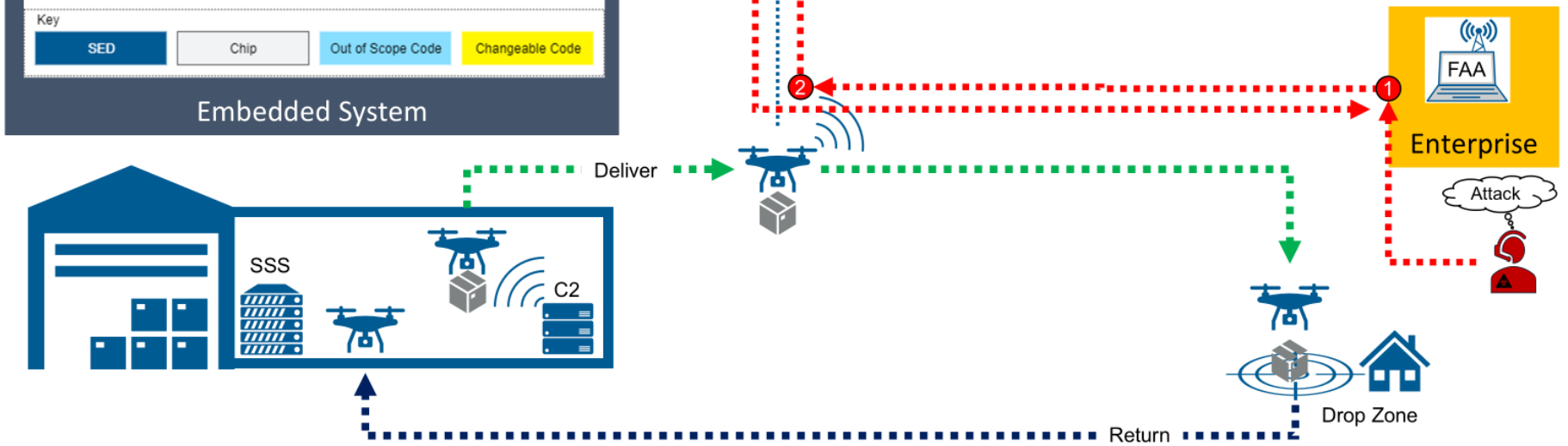
## Example eCTF PIVOT Storyboard




**Vignette**

- **Reading the content of SCEWL Transmissions**

| Step 1 | Step 2 | Step 3 | Step 4 | Step 5 | Step 6 |
|---|---|---|---|---|---|
| **Initial Access** | **Initial Access** | **Execution** | **Lateral Movement** | **Execution** | **Exfiltration** |
| FAA Receiver | Antenna | Controller | SCEWL Bus | CPU | Controller / Antenna |
| Multiple Enterprise TTPs | Exploit via Radio Interface | Improper Memory Management | System interface traversal via serial interfaces | Service Execution | Exfil data over FAA Channel |
| **Enterprise** | Embedded | Embedded | Embedded | Embedded | Enterprise |



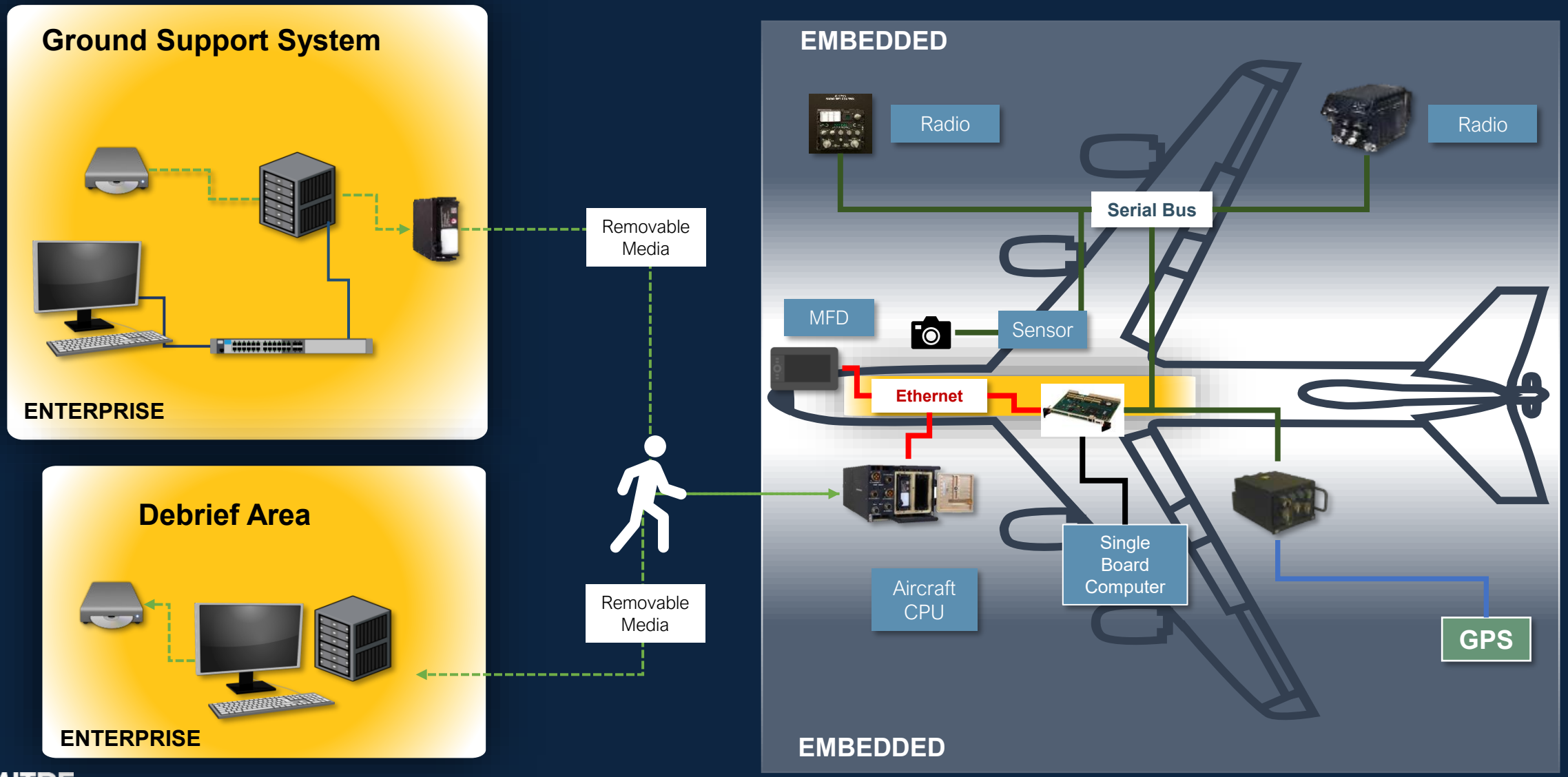

MITRE



9

MITRE

# PIVOT Storyboard: Generic Aircraft Platform




MITRE

# Combined Storyboard: PIVOT (ATT&CK & ESTM) + D3FEND

1 **Initial Access**
**T1133:** External Remote Services – Remote service gateway

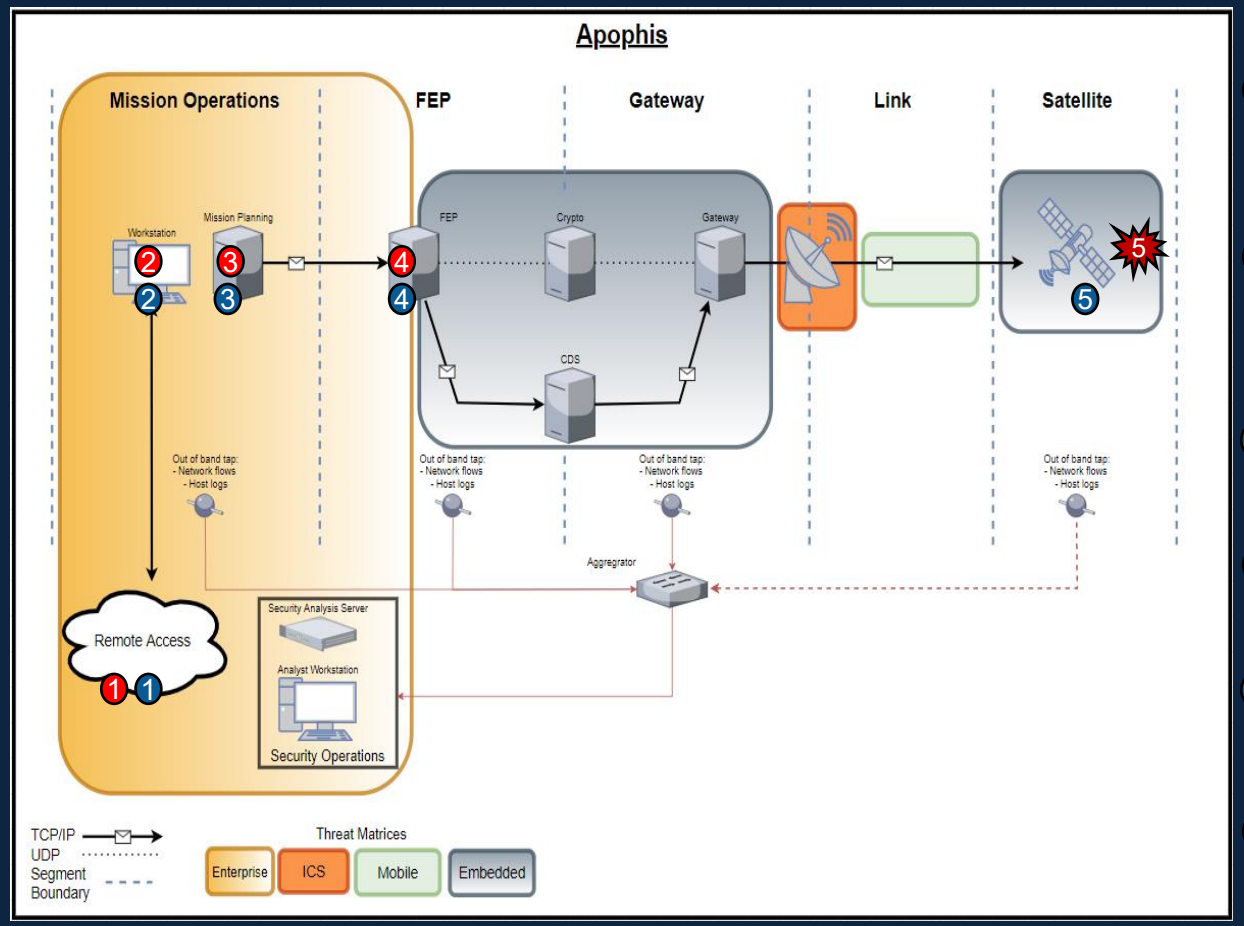
2 **Lateral Movement**
**T1078:** Valid Accounts – leveraging valid accounts to access workstation
**T1021:** Remote Services – leveraging access to space planning software (COSMOS)

2 **Defense Evasion**
**T1036:** Masquerading – adversary blends in with normal space software artifacts

3 **C2**
**T1090:** Proxy – adversary leverages trusted connection to dispatch commands to target component

4 **Collection**
**T1557:** Adversary-in-Middle – adversary profiles C2 communications to FEP

5 **Impact**
**T1565:** Data Manipulation – adversary manipulates data in transit to send malicious commands from FEP to satellite




1 **Initial Access**
**T1133:** External Remote Services
**D3-UGLPA**: User Geolocation Logon Pattern Analysis

2 **Lateral Movement**
**T1078:** Valid Accounts
**D3-DAM:** Domain Account Monitoring
**T1021:** Remote Services
**D3-RTSD:** Remote Terminal Session Detection

2 **Defense Evasion**
**T1036:** Masquerading
**D3-FA**: File Analysis

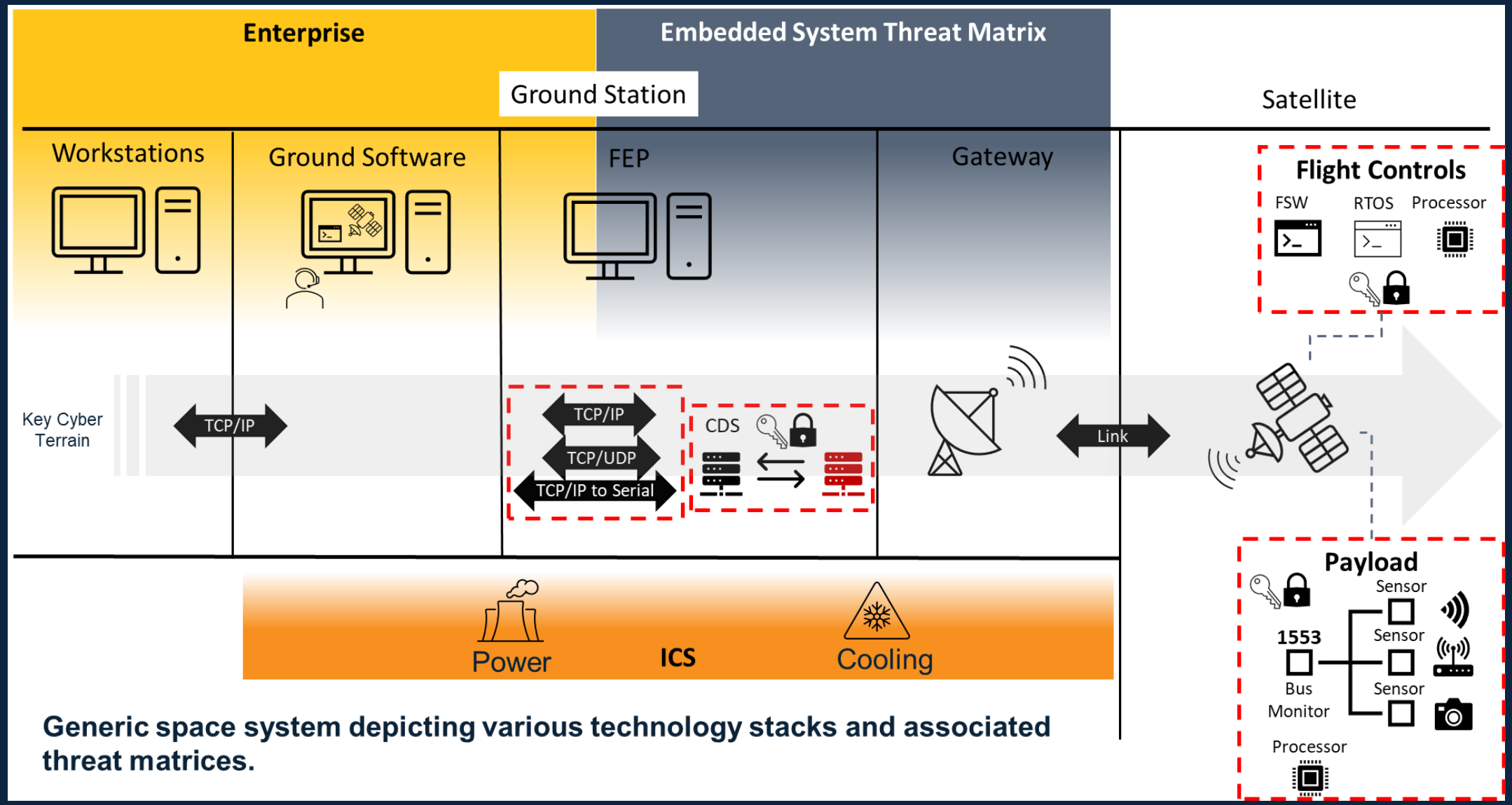
3 **C2**
**T1090:** Proxy
**D3-NTCD:** Network Traffic Community Deviation

4 **Collection**
**T1557:** Adversary-in-Middle
**D3-NTCD:** Network Traffic Community Deviation

5 **Impact**
**T1565:** Data Manipulation
**D3-CSPP**: Client-server Payload Profiling

MITRE

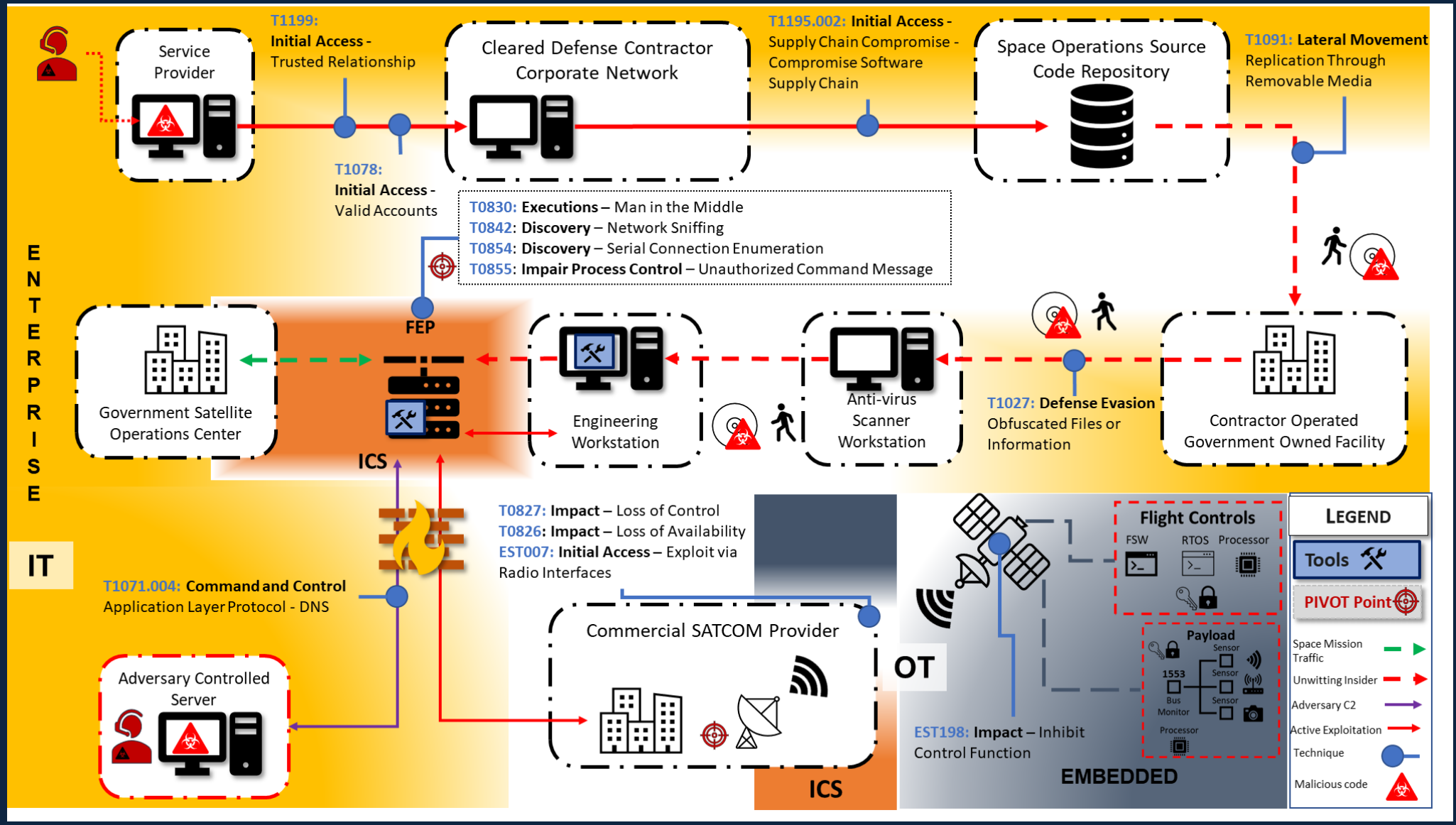
# PIVOT Storyboard (Simple): Notional Space System




**Generic space system depicting various technology stacks and associated threat matrices.**

MITRE

# PIVOT Storyboard (Detailed): Notional Space System




MITRE

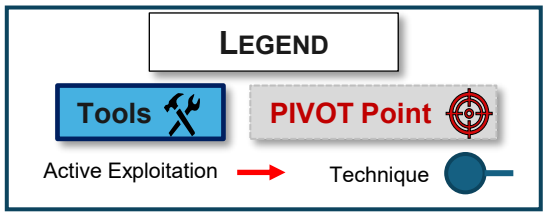
# PIVOT Cyber Threat & Countermeasure Storyboard Template

Threat Actor TTPs

Cyber Risk Scenario
or
Attack Path

Countermeasures

ENTERPRISE | MOBILE | ESTM | ICS




For more information email the PIVOT team at: pivot@mitre.org