Bruce Large

SESSION 11A

# AN ANALYSIS OF THE INTEGRATION OF SABSA AND MITRE PROJECTS

COSAC

## /whois @beLarge

*A cyber security architecture enthusiast, infrastructure tourist and "cyber hype guy"*

βLARGE
MISSION CRITICAL CYBER SECURITY

- Director and Principal Cyber Security Architect at BLARGE
- Worked in IT and OT in Network & System Engineering and Cyber Security roles for over 15 years
- Proud member of Professionals Australia
  The Union for STEM Workers – join your #STEMUNION
- Experience in Electricity Generation & Transmission, Railway, Aviation, Emergency Services and Consulting industries
- Bach Eng (Telecomms) QUT First Class Honours and Master Business (Applied Finance) with Distinction QUT

# Why *this* presentation?

# Agenda

1. An introduction to MITRE
2. Integrations on a page
3. Deepdive per Project
4. Q&A

# INTRODUCTION TO MITRE

# WHAT IS MITRE?

- Established to Advance National Security in new ways and serve the public interest as an independent advisor
- MITRE was founded in 1958 as an alignment of Industry and Academia and originally sponsored by the US Airforce to Architect the Semi-Automatic Ground Environment (SAGE) system for Air Defense
- MITRE today operates Six Federal Funded Research & Development Centres (FFRDCs)
  - **National Cybersecurity FFRDC**
  - National Security Engineering Centre
  - Centre for Advanced Aviation System Development
  - Centre for Enterprise Modernisation
  - Homeland Security Systems Engineering and Development Institute™
  - The Health FFRDC

Ref - https://www.mitre.org/who-we-are/our-story

# MITRE & CYBER SECURITY

- Cyber Operations & Effects Innovation Centre
  - Cyber Adversary Emulation
  - Cyber Deception and adversary engagement
  - Cyber effects and reverse engineering
  - Cyber forensics
  - Cyber threat intelligence
- Cyber Solutions Innovation Centre
  - Engineering and architecting safe, secure and resilient systems
  - Advancing critical cyber technologies
- Cyber Infrastructure Protection Innovation Centre

Timeline of Cyber Projects

**1999** – CVE
2013 – ATT&CK®
2024 – EMB3D™
ATLAS™
ENGAGE™

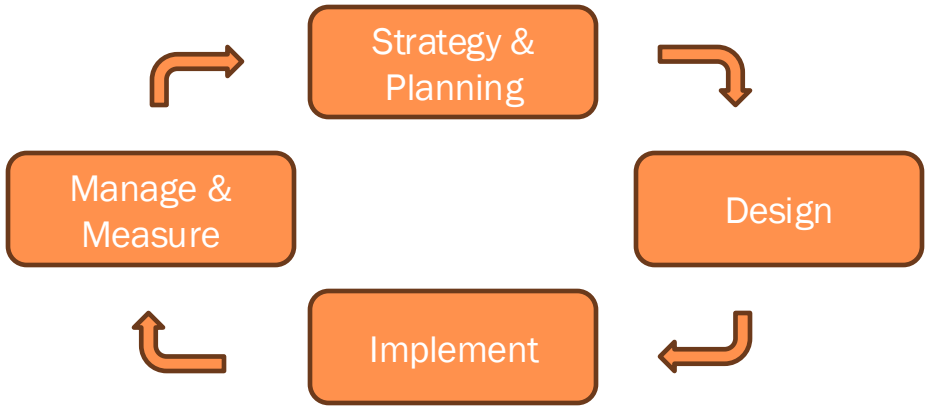
MITRE was the first organisation to register a .org domain in 1985!

Ref - https://www.mitre.org/our-impact/rd-centers/national-cybersecurity-ffrdc

# INTEGRATION ON A PAGE

# HOW THE PROJECTS CAN BE USED IN THE SABSA LIFECYCLE

ATT&CK®




DEFEND™

MITRE | EMB3D

MITRE | ATLAS

# DEEP DIVE PER MITRE PROJECT

# OVERVIEW OF MITRE ATT&CK®

- Developed by MITRE to define the Tactics, Techniques and Procedures that Adversaries use
- Suggested Use Cases for ATT&CK are:
  - Detection & Analytics
  - Threat Intelligence
  - Adversary Emulation & Red Teaming
  - **Assessment & Engineering**
- Initially considered Enterprise but now consider Industrial Control Systems (ICS) and Mobile
- Has become a well recognised common language for cyber professionals to describe cyber security intrusions and to understand adversary behaviour
- This is a great taxonomy for Architects to use to ensure we are using a common language in cyber

# ATT&CK – ASSESSMENT AND ENGINEERING USE CASE

# OVERVIEW OF ATT&CK (CONT.)


## Summary

***Note:*** *This Activity Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) framework. See the MITRE ATT&CK for Enterprise and ATT&CK for Industrial Control Systems (ICS) frameworks for all referenced threat actor techniques and mitigations.*

The Cybersecurity and Infrastructure Security Agency (CISA) encourages asset owner operators across all critical infrastructure sectors to review the below threat actor techniques and ensure the corresponding mitigations are applied.

CISA responded to a cyberattack affecting control and communication assets on the operational technology (OT) network of a natural gas compression facility. A cyber threat actor used a *Spearphishing Link* [T1192] to obtain initial access to the organization's information technology (IT) network before pivoting to its OT network. The threat actor then deployed commodity ransomware to *Encrypt Data for Impact* [T1486] on both networks. Specific assets experiencing a *Loss of Availability* [T826] on the OT network included human machine interfaces (HMIs), data historians, and polling servers. Impacted assets were no longer able to read and aggregate real-time operational data reported from low-level OT devices, resulting in a partial *Loss of View* [T829] for human operators. The attack did not impact any programmable logic controllers (PLCs) and at no point did the victim lose control of operations. Although the victim's emergency response plan did not specifically consider cyberattacks, the decision was made to implement a deliberate and controlled shutdown to operations. This lasted approximately two days, resulting in a *Loss of Productivity and Revenue* [T828], after which normal operations resumed. CISA is providing this Alert to help administrators and network defenders protect their organizations against this and similar ransomware attacks.

Ref - https://mitre-attack.github.io/attack-navigator/ & https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-049a

# HOW ATT&CK CAN INTEGRATE WITH SABSA

- ATT&CK can be used to understand evolving threat behaviour and capabilities and what assets are being targeted

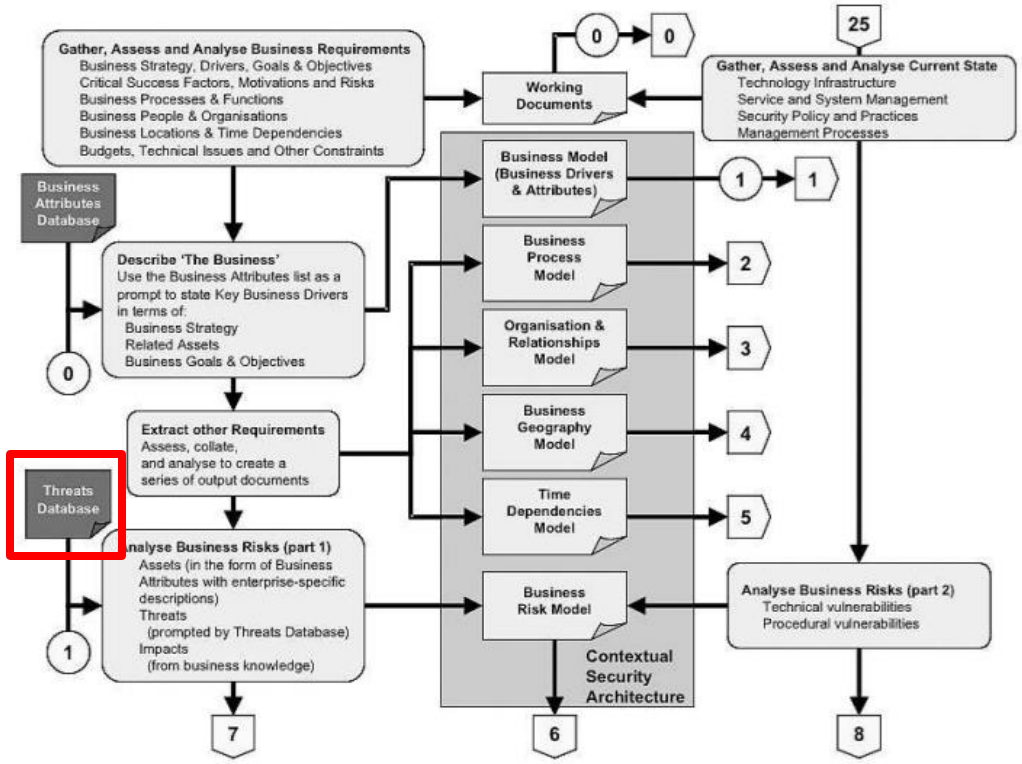
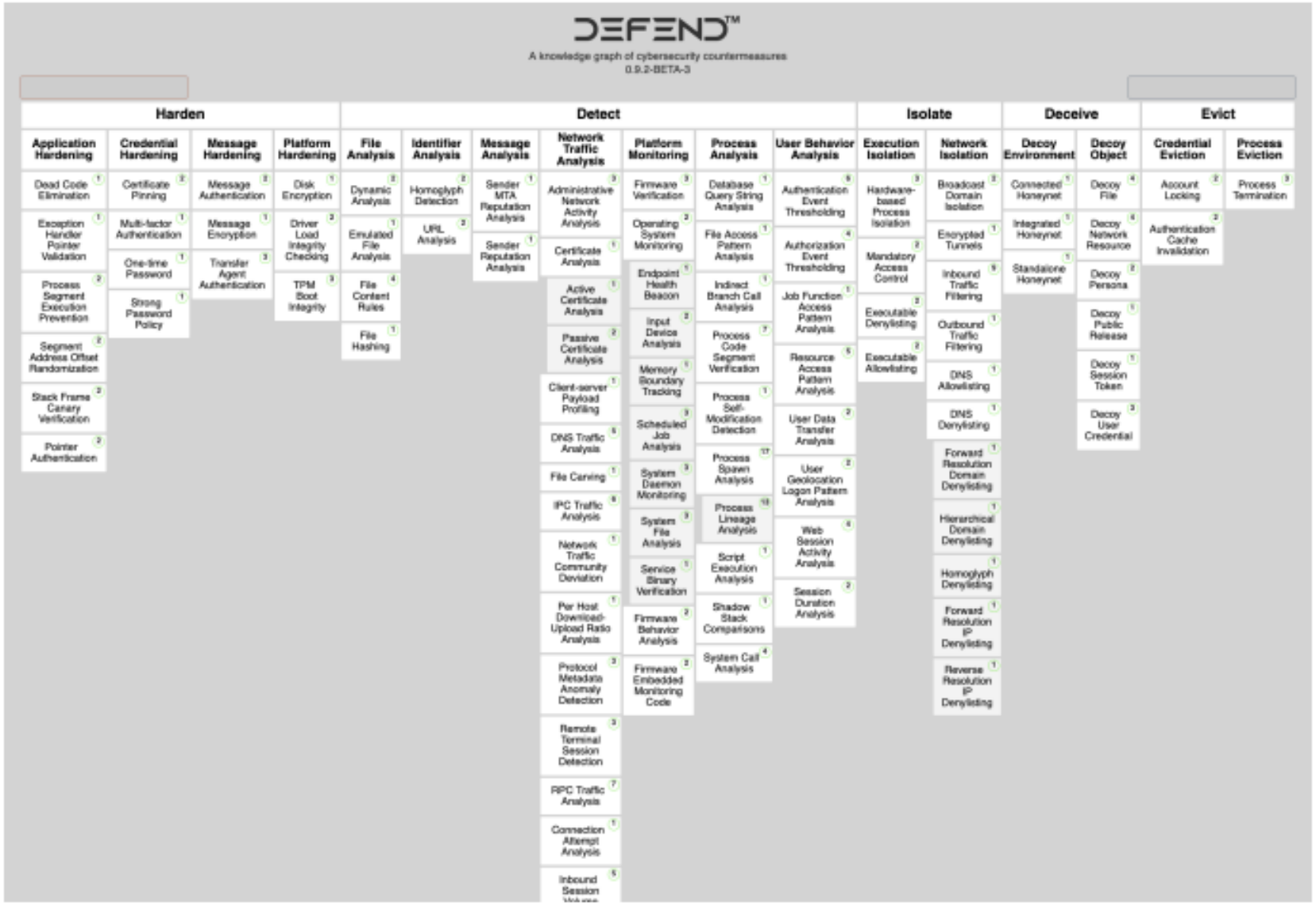



Figure 7-4: Developing the Contextual Security Architecture

# MITRE D3FEND™

- D3FEND is a Knowledge Graph of Cyber Security Counter Measures
- Assigns Countermeasures to the below Categories:
  - Model
  - Harden
  - Detect
  - Isolate
  - Deceive
  - Evict
  - Restore
- It includes sub-techniques and maps back into the ATT&CK knowledge base

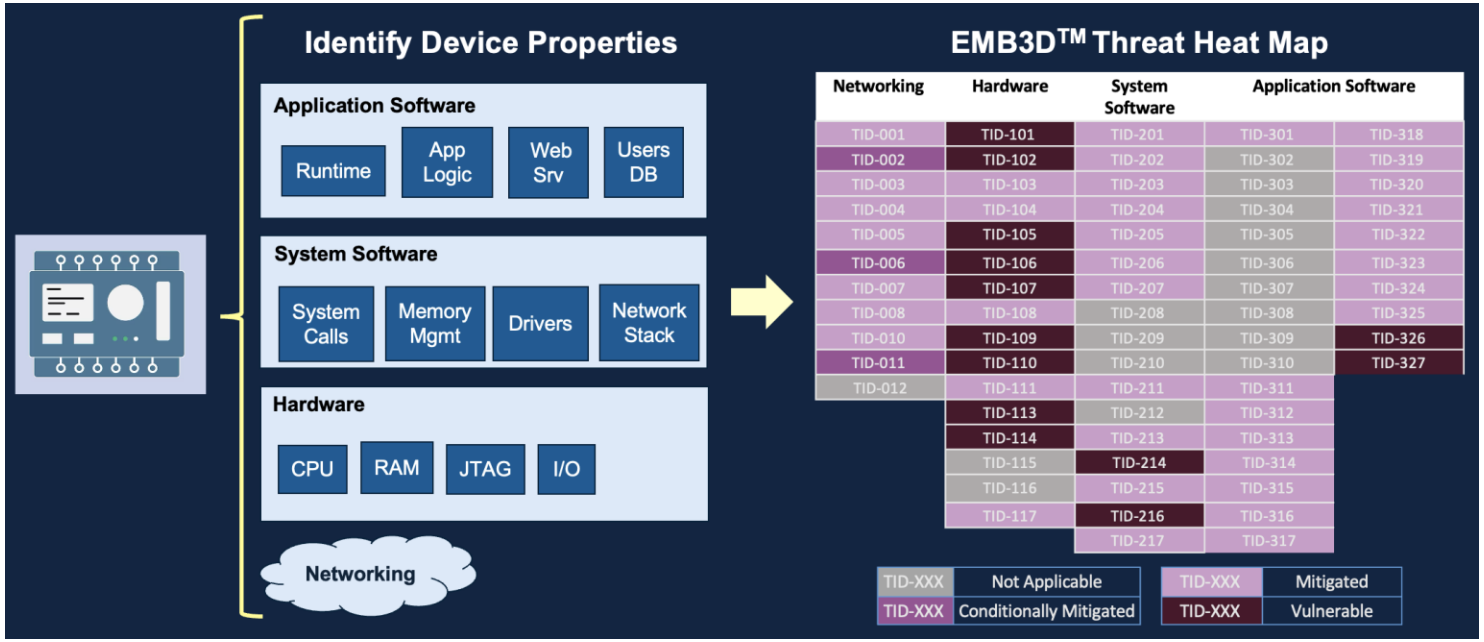
# D3FEND (CONT.)




Ref - https://d3fend.mitre.org/resources/D3FEND.pdf

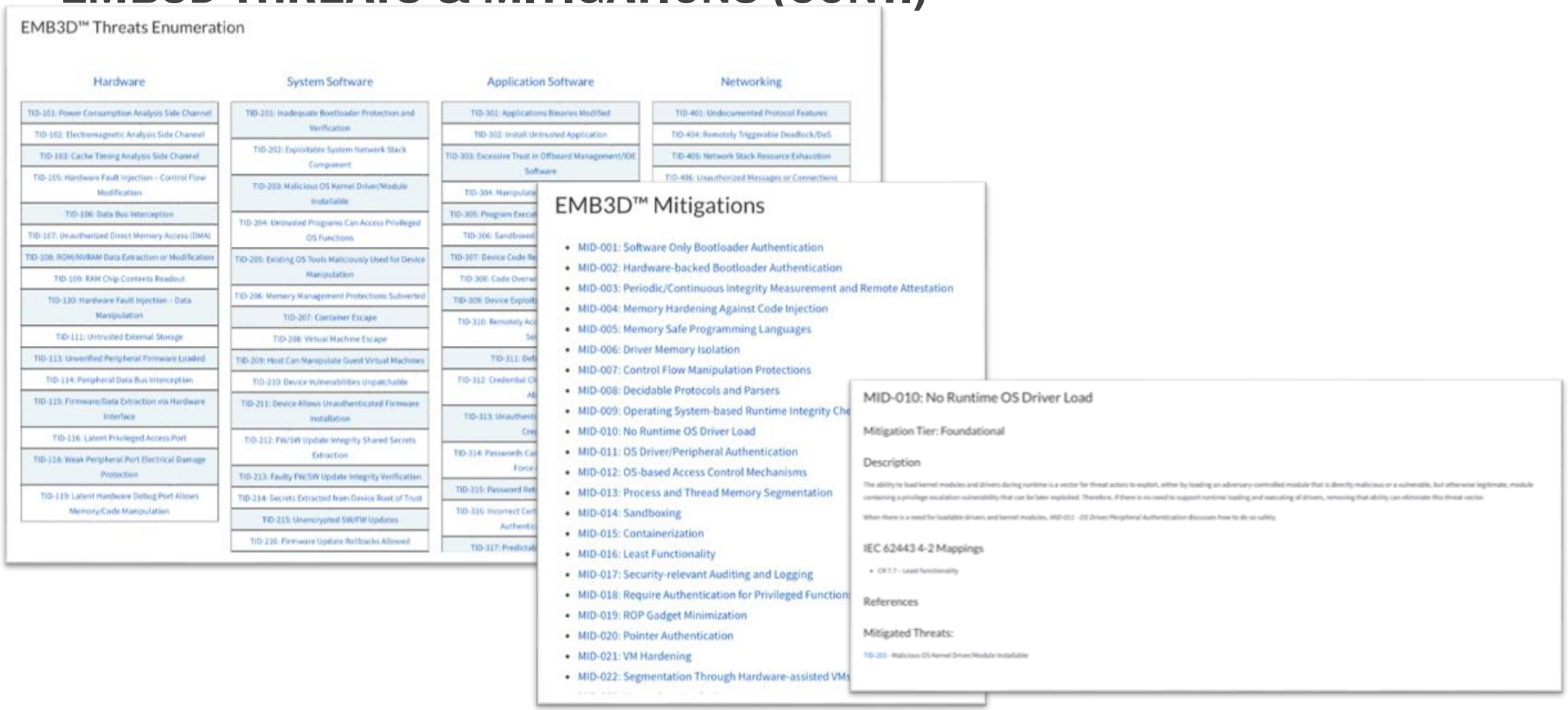
# MITRE EMB3D™

- Threat Model for Embedded Systems to support Critical Infrastructure, IoT and Medical Sectors etc.
- Identifies Threats and Mitigations depending on Device Properties




Ref - https://emb3d.mitre.org/

# EMB3D THREATS & MITIGATIONS (CONT.)

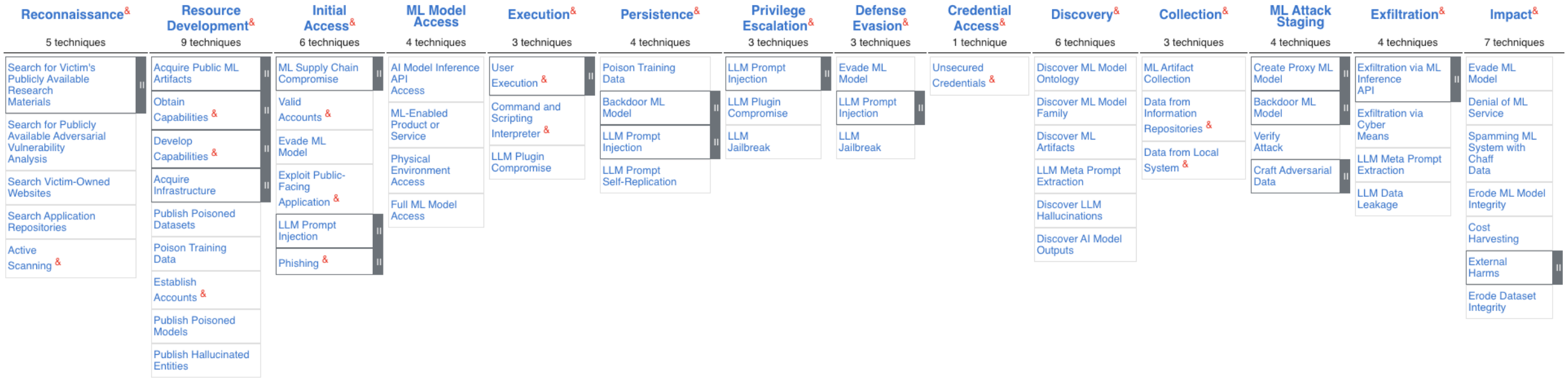



Ref - https://emb3d.mitre.org/threats/, https://emb3d.mitre.org/mitigations/, https://emb3d.mitre.org/mitigations/MID-010.html

# MITRE ATLAS™

- The Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS) is a knowledge base to describe adversary Tactics, Techniques and Procedures when attacking AI Systems
- ATLAS also defines mitigations https://atlas.mitre.org/mitigations/

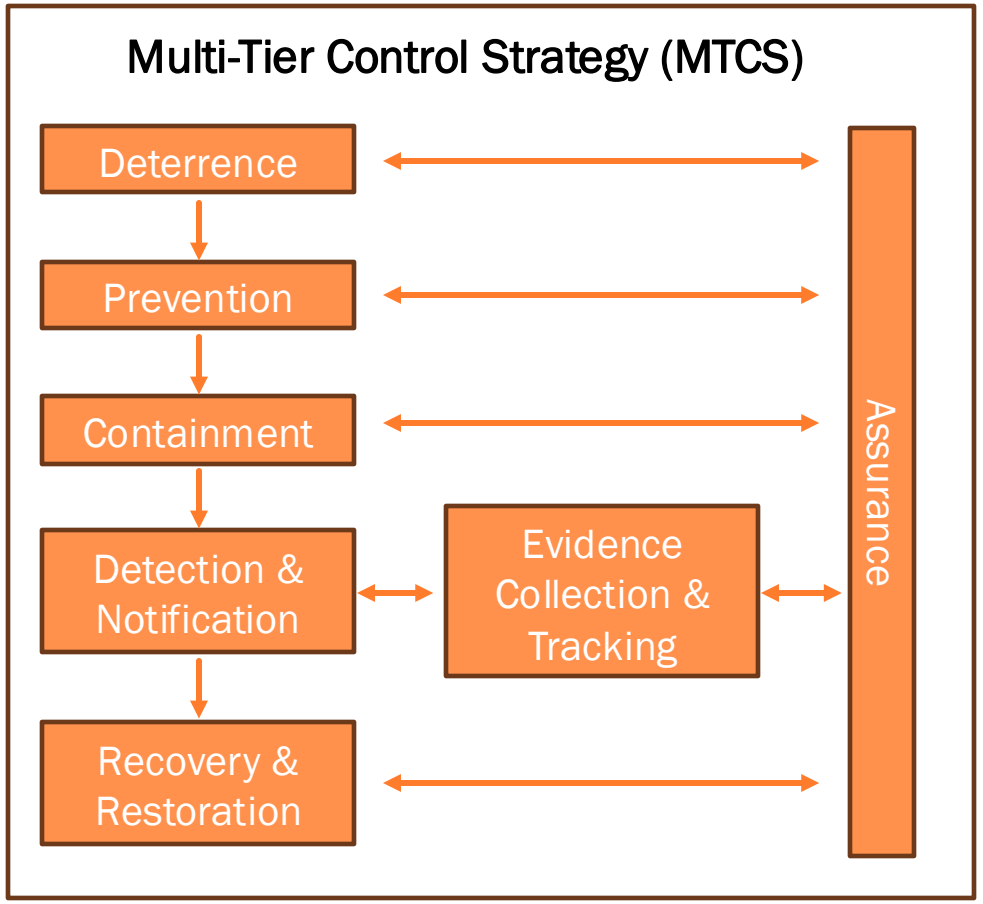
# ATLAS MATRIX




Ref - https://atlas.mitre.org/matrices/ATLAS

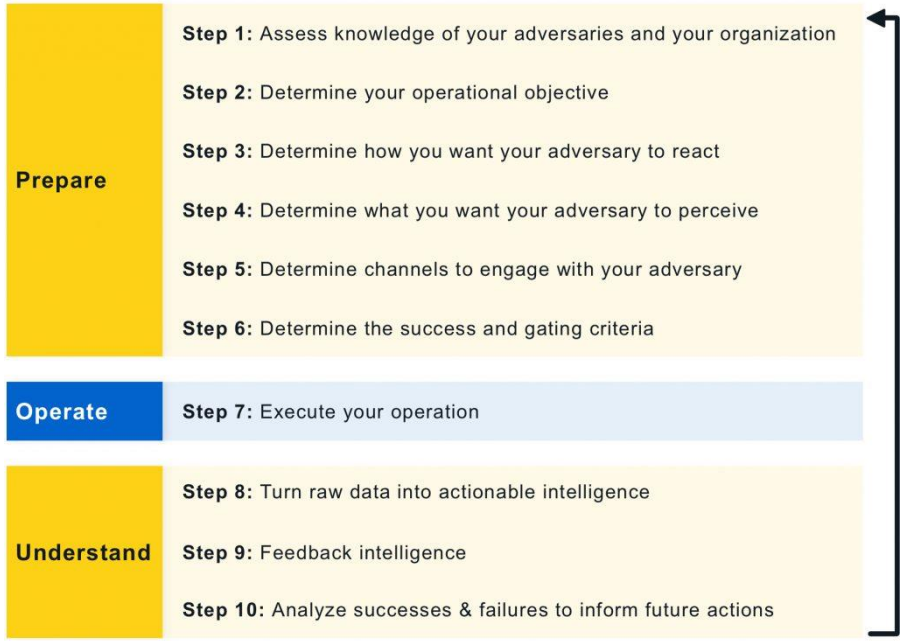
# HOW D3FEND™, EMB3D™ AND ATLAS™ CAN INTEGRATE WITH SABSA

- These MITRE Frameworks represent a control framework that can be used with or replace MTCS
- This integration can tie together modern, maintained and evolving security control Mechanisms and Components with the Enterprise Security Architecture Concepts and Activities in SABSA



# MITRE ENGAGE™

- Use Active Defense techniques in your control strategy – if an adversary breaches your systems introduce ambiguous and misleading information
- Adversary Engagement
  - Narrative
  - Engagement
  - Monitoring
  - Analysis
- Tied together with an Operational Objective




Ref - https://engage.mitre.org/starter-kit/

# ENGAGE MATRIX

| Prepare | Expose | | Affect | | | Elicit | | Understand |
|---|---|---|---|---|---|---|---|---|
| Plan | Collect | Detect | Prevent | Direct | Disrupt | Reassure | Motivate | Analyze |
| Cyber Threat Intelligence | API Monitoring | Introduced Vulnerabilities | Baseline | Attack Vector Migration | Isolation | Application Diversity | Application Diversity | After-Action Review |
| Engagement Environment | Network Monitoring | Lures | Hardware Manipulation | Email Manipulation | Lures | Artifact Diversity | Artifact Diversity | Cyber Threat Intelligence |
| Gating Criteria | Software Manipulation | Malware Detonation | Isolation | Introduced Vulnerabilities | Network Manipulation | Burn-In | Information Manipulation | Threat Model |
| Operational Objective | System Activity Monitoring | Network Analysis | Network Manipulation | Lures | Software Manipulation | Email Manipulation | Introduced Vulnerabilities | |
| Persona Creation | | | Security Controls | Malware Detonation | | Information Manipulation | Malware Detonation | |
| Storyboarding | | | | Network Manipulation | | Network Diversity | Network Diversity | |
| Threat Model | | | | Peripheral Management | | Peripheral Management | Personas | |
| | | | | Security Controls | | Pocket Litter | | |
| | | | | Software Manipulation | | | | |

Ref - https://engage.mitre.org/

# FURTHER RESOURCES

- Getting Started with MITRE ATT&CK® Blog
  - Getting Started with ATT&CK: Assessments & Engineering
- MITRE D3FEND™ White Paper
- MITRE EMB3D™ White Paper
  - Getting Started with EMB3D
- MITRE ATLAS™ Fact Sheet
  - ATLAS Video Resources
- MITRE ENGAGE™ Starter Kit

# THANK YOU, QUESTIONS?


https://linkedin.com/in/blargeau


https://github.com/beLarge


bruce@blarge.io


https://blarge.io

# SESSION FEEDBACK

- Paper feedback forms are available from the front of the room

OR
cosac.bz/feedback