

■ Bruce Large

SESSION 11A

AN ANALYSIS OF THE INTEGRATION OF SABSA AND MITRE PROJECTS

**/whois
@beLarge**

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



- 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

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™

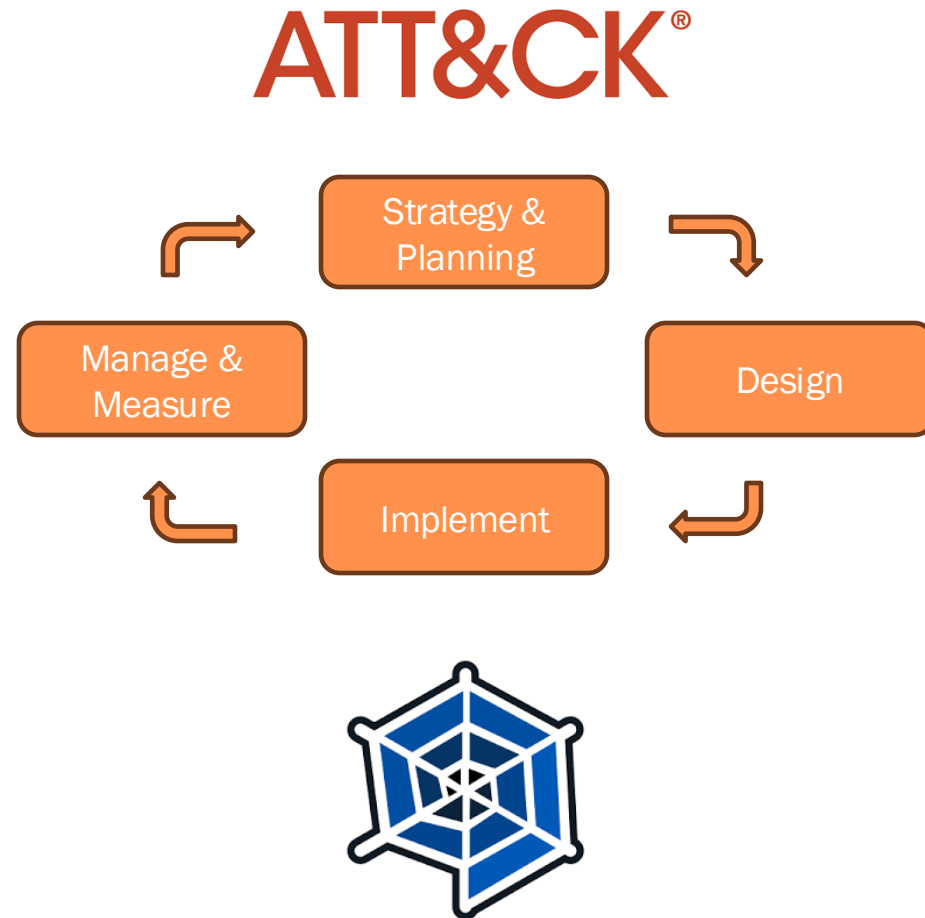
MITRE was the first
organisation to register a
.org domain in 1985!



INTEGRATION ON A PAGE



HOW THE PROJECTS CAN BE USED IN THE SABSA LIFECYCLE



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.)

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)								
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Exploit Public-Facing Application	Command and Scripting Interpreter (0/9)	BITS Jobs	Access Token Manipulation (0/5)								
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)								
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)								
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Phishing (0/3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (0/4)								
Phishing for Information (0/3)	Establish Accounts (0/3)	Replication Through Removable Media	Inter-Process Communication (0/3)	Compromise Client Software Binary	Domain Policy Modification (0/2)								
Search Closed Sources (0/2)	Obtain Capabilities (0/6)	Supply Chain Compromise (0/3)	Native API	Create Account (0/3)	Escape to Host								
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Trusted Relationship	Scheduled Task/Job (0/5)	Create or Modify System Process (0/4)	Event Triggered Execution (0/16)								
Search Open Websites/Domains (0/3)		Valid Accounts (0/4)	Serverless Execution	Event Triggered	Exploitation for								
Search Victim-Owned Websites			Shared Modules										

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.

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

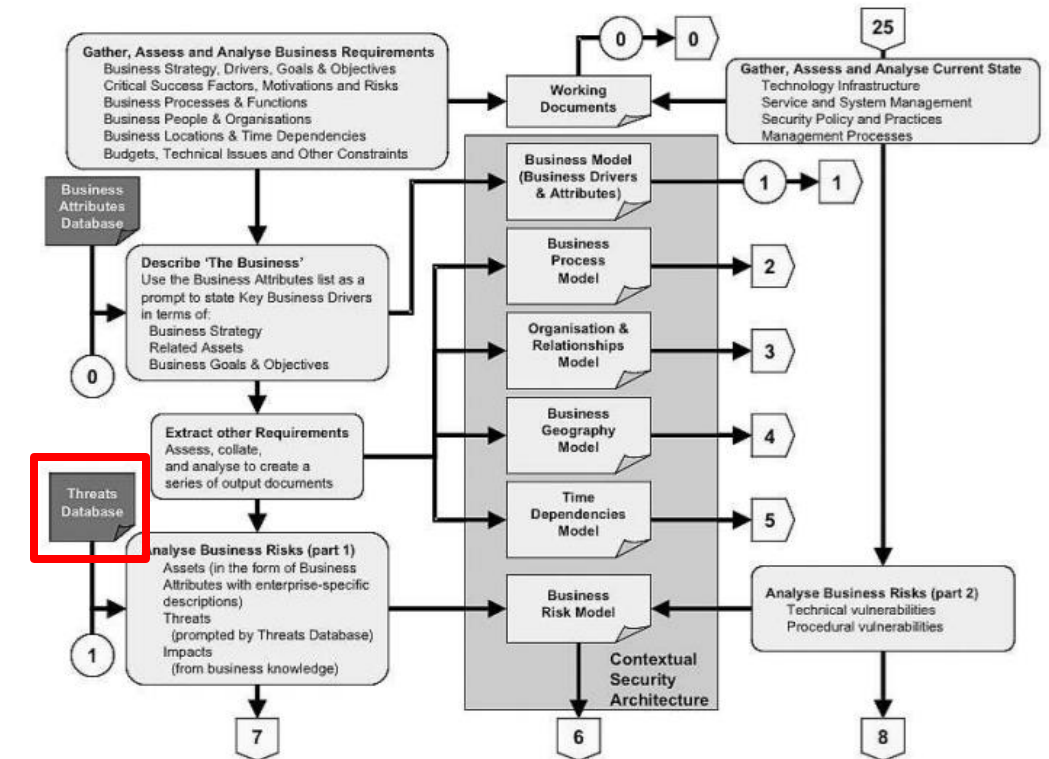
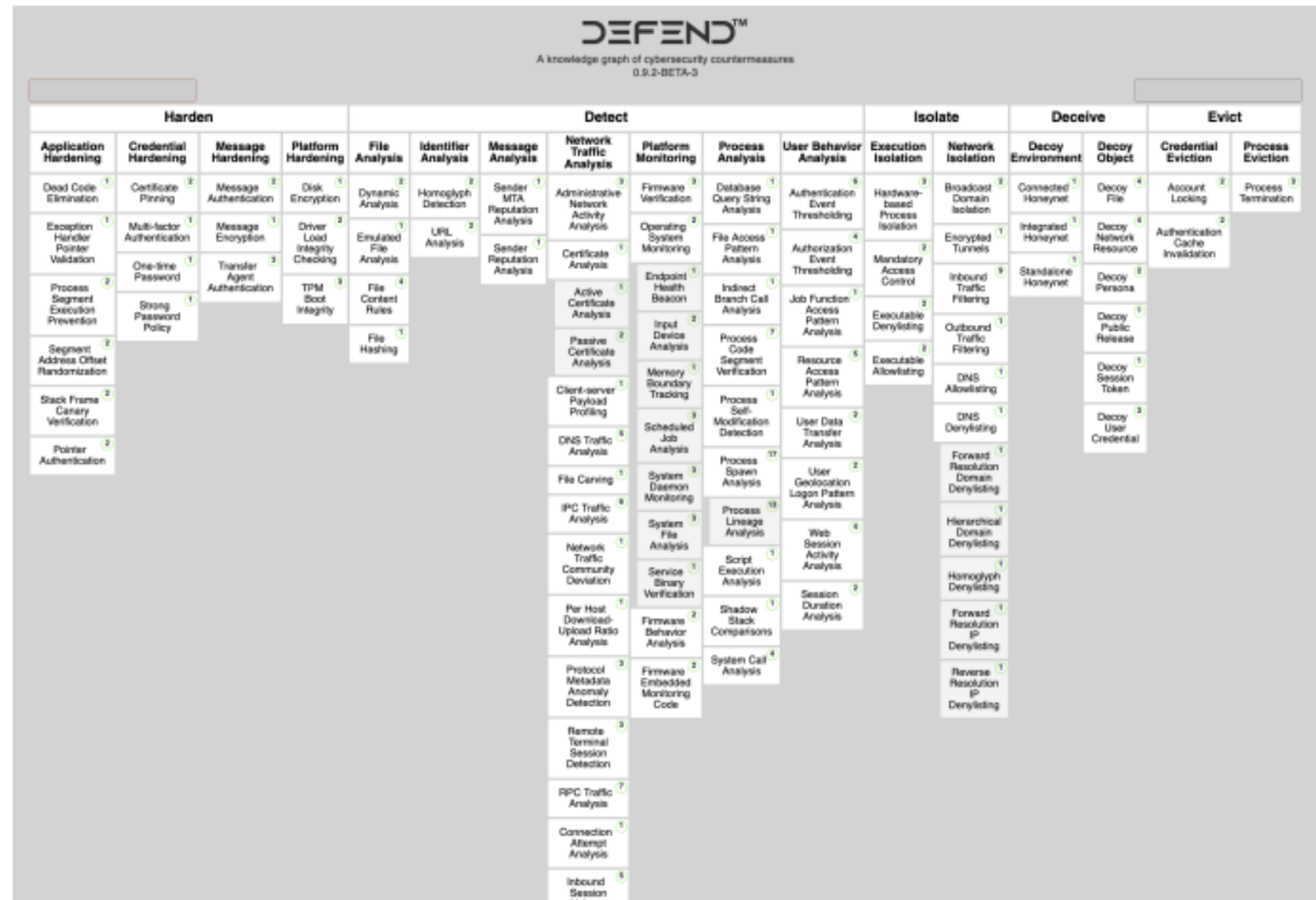


Figure 7-4: Developing the Contextual Security Architecture

MITRE D3FEND™

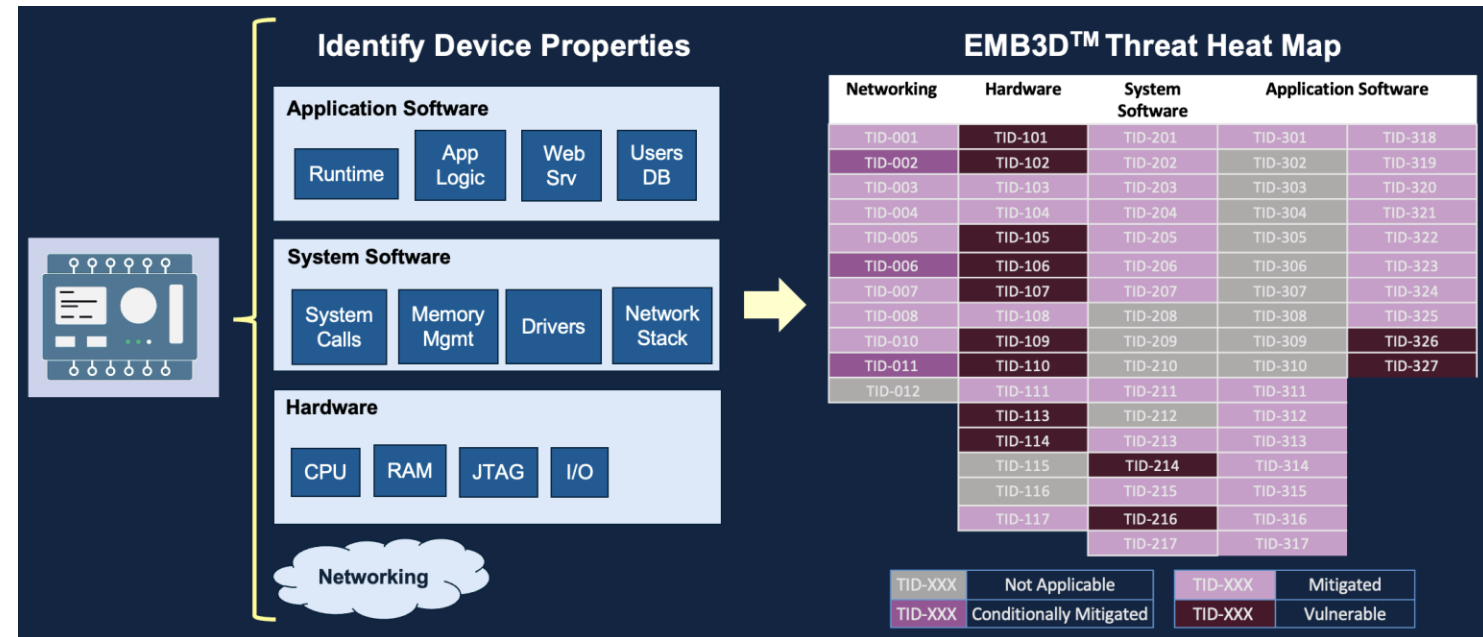
- D3FEND is a Knowledge Graph of Cyber Security Counter Measures
- Assigns Countermeasures to the below Categories:
 - Model
 - Harden
 - Detect
 - Isolate
 - Deceive
 - Evict
 - Restore
- It includes sub-techniques and maps back into the ATT&CK knowledge base

D3FEND (CONT.)



MITRE EMB3D™

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



EMB3D THREATS & MITIGATIONS (CONT.)

EMB3D™ Threats Enumeration

Hardware	System Software	Application Software	Networking
TID-101: Power Consumption Analysis Side Channel	TID-201: Inadequate Bootloader Protection and Verification	TID-301: Applications Binaries Modified	TID-401: Undocumented Protocol Features
TID-102: Electromagnetic Analysis Side Channel	TID-202: Exploitable System Network Stack Component	TID-302: Install Untrusted Application	TID-404: Remotely Triggerable Deadlock/DoS
TID-103: Cache Timing Analysis Side Channel	TID-203: Malicious OS Kernel Driver/Module Installable	TID-303: Excessive Trust in Offboard Management/DOE Software	TID-405: Network Stack Resource Exhaustion
TID-105: Hardware Fault Injection - Control Flow Modification	TID-204: Untrusted Programs Can Access Privileged OS Functions	TID-304: Manipulate	TID-406: Unauthorized Messages or Connections
TID-106: Data Bus Interception	TID-205: Existing OS Tools Maliciously Used for Device Manipulation	TID-305: Program Execut	
TID-107: Unauthorized Direct Memory Access (DMA)	TID-206: Memory Management Protections Subverted	TID-306: Sandboxed	
TID-108: ROM/NVRAM Data Extraction or Modification	TID-207: Container Escape	TID-307: Device Code Re	
TID-109: RAM Chip Contents Readout	TID-208: Virtual Machine Escape	TID-308: Code Overw	
TID-110: Hardware Fault Injection - Data Manipulation	TID-209: Host Can Manipulate Guest Virtual Machines	TID-309: Device Exploib	
TID-111: Untrusted External Storage	TID-210: Device Vulnerabilities Unpatchable	TID-310: Remotely Acc	
TID-113: Unverified Peripheral Firmware Loaded	TID-211: Device Allows Unauthenticated Firmware Installation	TID-311: Defi	
TID-114: Peripheral Data Bus Interception	TID-212: FW/SW Update Integrity Shared Secrets Extraction	TID-312: Credential Cr	
TID-115: Firmware/Data Extraction via Hardware Interface	TID-213: Faulty FW/SW Update Integrity Verification	TID-313: Unauthenti	
TID-116: Latent Privileged Access Port	TID-214: Secrets Extracted from Device Root of Trust	TID-314: Passwords Can	
TID-118: Weak Peripheral Port Electrical Damage Protection	TID-215: Unencrypted SW/FW Updates	TID-315: Password Ref	
TID-119: Latent Hardware Debug Port Allows Memory/Code Manipulation	TID-216: Firmware Update Rollbacks Allowed	TID-316: Incorrect Cert	
		TID-317: Predictab	

EMB3D™ Mitigations

- MID-001: Software Only Bootloader Authentication
- MID-002: Hardware-backed Bootloader Authentication
- MID-003: Periodic/Continuous Integrity Measurement and Remote Attestation
- MID-004: Memory Hardening Against Code Injection
- MID-005: Memory Safe Programming Languages
- MID-006: Driver Memory Isolation
- MID-007: Control Flow Manipulation Protections
- MID-008: Decidable Protocols and Parsers
- MID-009: Operating System-based Runtime Integrity Checks
- MID-010: No Runtime OS Driver Load
- MID-011: OS Driver/Peripheral Authentication
- MID-012: OS-based Access Control Mechanisms
- MID-013: Process and Thread Memory Segmentation
- MID-014: Sandboxing
- MID-015: Containerization
- MID-016: Least Functionality
- MID-017: Security-relevant Auditing and Logging
- MID-018: Require Authentication for Privileged Functions
- MID-019: ROP Gadget Minimization
- MID-020: Pointer Authentication
- MID-021: VM Hardening
- MID-022: Segmentation Through Hardware-assisted VMs

MID-010: No Runtime OS Driver Load

Mitigation Tier: Foundational

Description

The ability to load kernel modules and drivers during runtime is a vector for threat actors to exploit, either by loading an adversary-controlled module that is directly malicious or a vulnerable, but otherwise legitimate, module containing a privilege escalation vulnerability that can be later exploited. Therefore, if there is no need to support runtime loading and executing of drivers, removing that ability can eliminate this threat vector.

When there is a need for loadable drivers and kernel modules, MID-012 - OS Driver/Peripheral Authentication discusses how to do so safely.

IEC 62443 4-2 Mappings

- CR 7.7 - Least functionality

References

Mitigated Threats:

TID-203 - Malicious OS Kernel Driver/Module Installable

MITRE ATLAS™

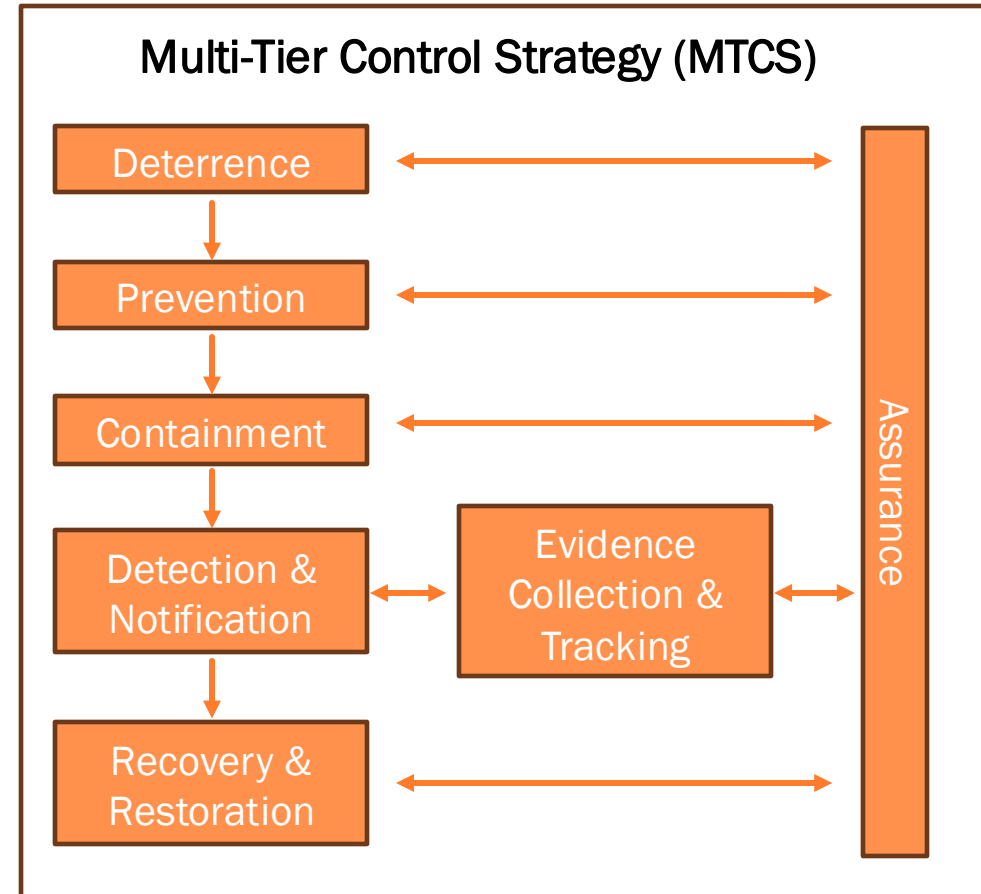
- The Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS) is a knowledge base to describe adversary Tactics, Techniques and Procedures when attacking AI Systems
- ATLAS also defines mitigations <https://atlas.mitre.org/mitigations/>

ATLAS MATRIX

Reconnaissance ^{&} 5 techniques	Resource Development ^{&} 9 techniques	Initial Access ^{&} 6 techniques	ML Model Access 4 techniques	Execution ^{&} 3 techniques	Persistence ^{&} 4 techniques	Privilege Escalation ^{&} 3 techniques	Defense Evasion ^{&} 3 techniques	Credential Access ^{&} 1 technique	Discovery ^{&} 6 techniques	Collection ^{&} 3 techniques	ML Attack Staging 4 techniques	Exfiltration ^{&} 4 techniques	Impact ^{&} 7 techniques
Search for Victim's Publicly Available Research Materials	Acquire Public ML Artifacts	ML Supply Chain Compromise	AI Model Inference API Access	User Execution ^{&}	Poison Training Data	LLM Prompt Injection	Evade ML Model	Unsecured Credentials ^{&}	Discover ML Model Ontology	ML Artifact Collection	Create Proxy ML Model	Exfiltration via ML Inference API	Evade ML Model
Search for Publicly Available Adversarial Vulnerability Analysis	Obtain Capabilities ^{&}	Valid Accounts ^{&}	ML-Enabled Product or Service	Command and Scripting Interpreter ^{&}	Backdoor ML Model	LLM Plugin Compromise	LLM Prompt Injection	LLM Prompt Injection	Discover ML Model Family	Data from Information Repositories ^{&}	Backdoor ML Model	Exfiltration via Cyber Means	Denial of ML Service
Search Victim-Owned Websites	Develop Capabilities ^{&}	Evade ML Model	Physical Environment Access	LLM Plugin Compromise	LLM Prompt Injection	LLM Jailbreak	LLM Jailbreak		Discover ML Artifacts	Data from Local System ^{&}	Verify Attack	LLM Meta Prompt Extraction	Spamming ML System with Chaff Data
Search Application Repositories	Acquire Infrastructure	Exploit Public-Facing Application ^{&}	Full ML Model Access		LLM Prompt Self-Replication				LLM Meta Prompt Extraction		Craft Adversarial Data	LLM Data Leakage	Erode ML Model Integrity
Active Scanning ^{&}	Publish Poisoned Datasets	LLM Prompt Injection							Discover LLM Hallucinations				Cost Harvesting
	Poison Training Data	Phishing ^{&}							Discover AI Model Outputs				External Harms
	Establish Accounts ^{&}												Erode Dataset Integrity
	Publish Poisoned Models												
	Publish Hallucinated Entities												

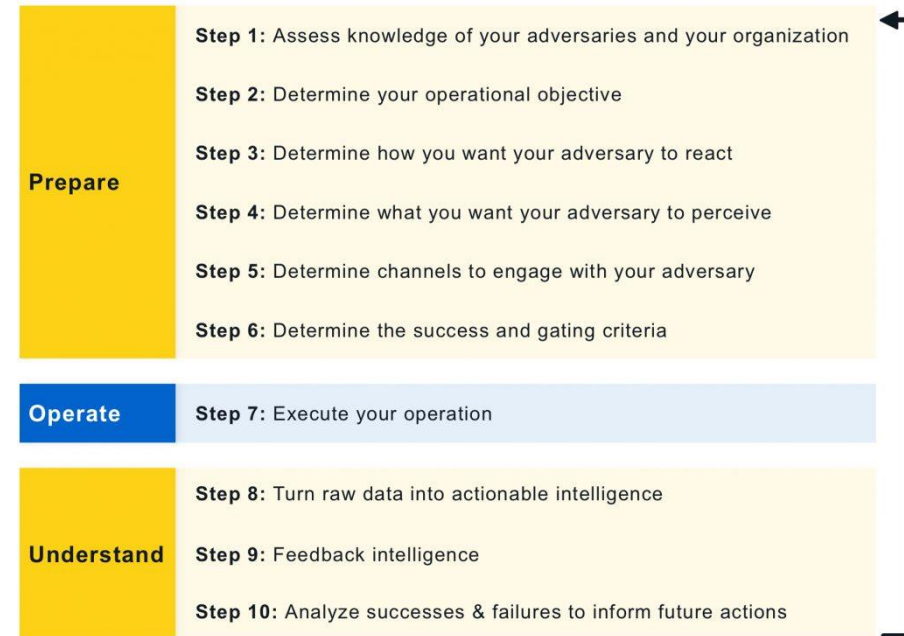
HOW D3FEND™, EMB3D™ AND ATLAS™ CAN INTEGRATE WITH SABSA

- 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



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				

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