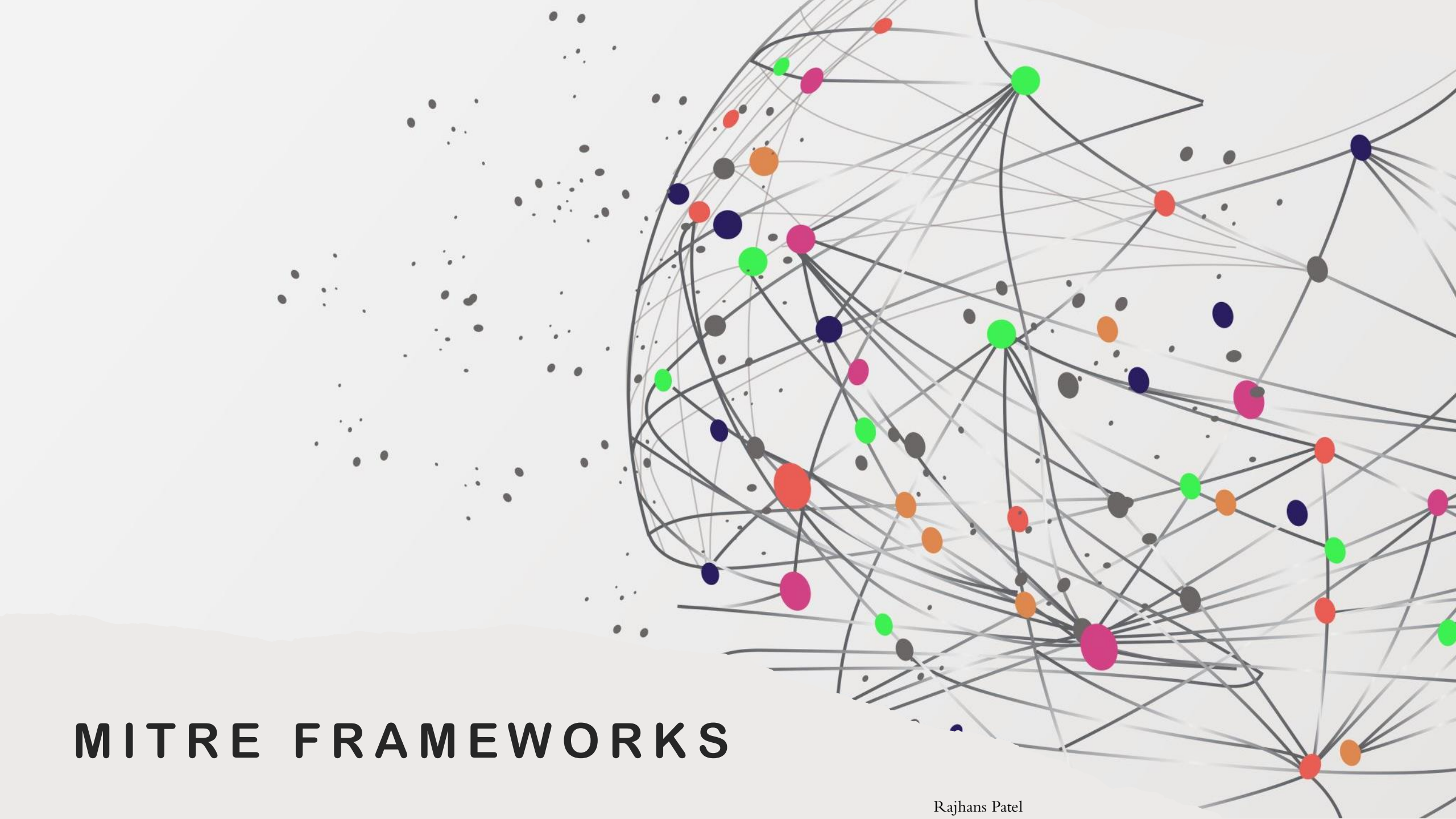
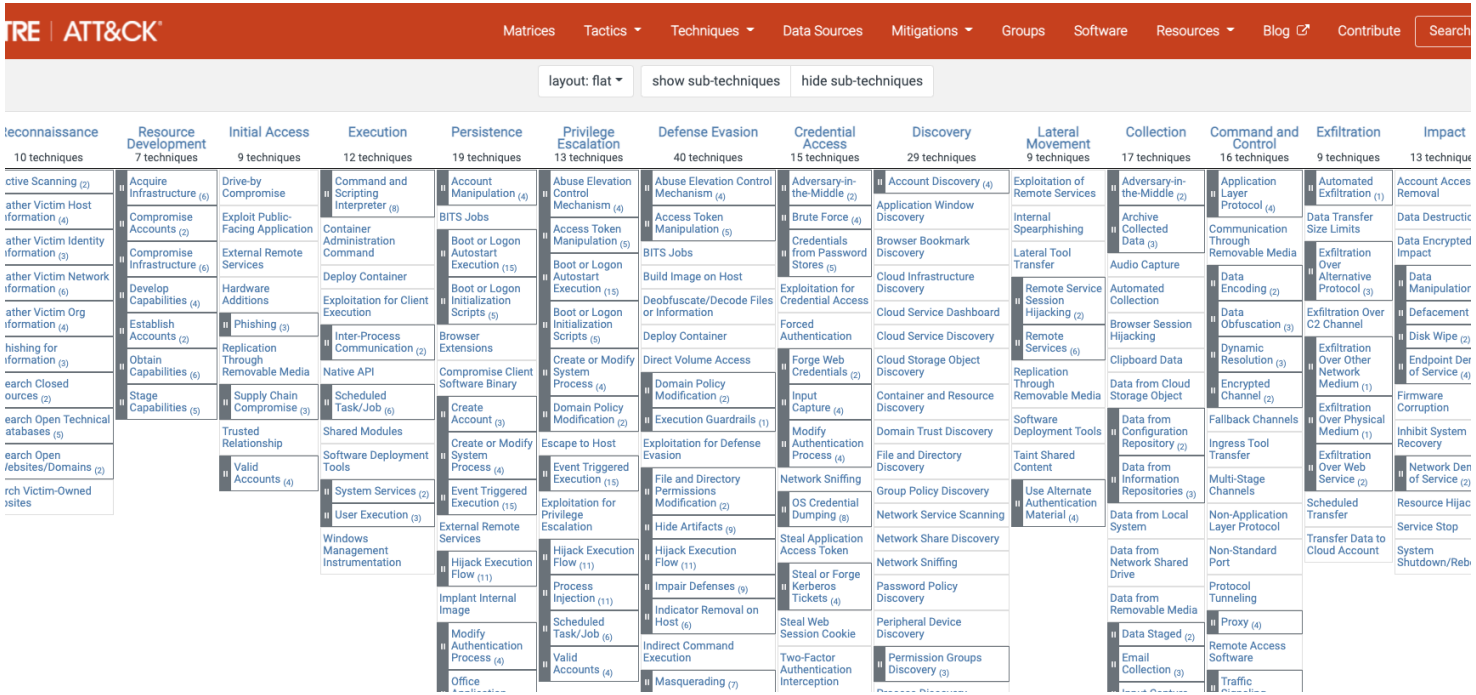


MITRE FRAMEWORKS

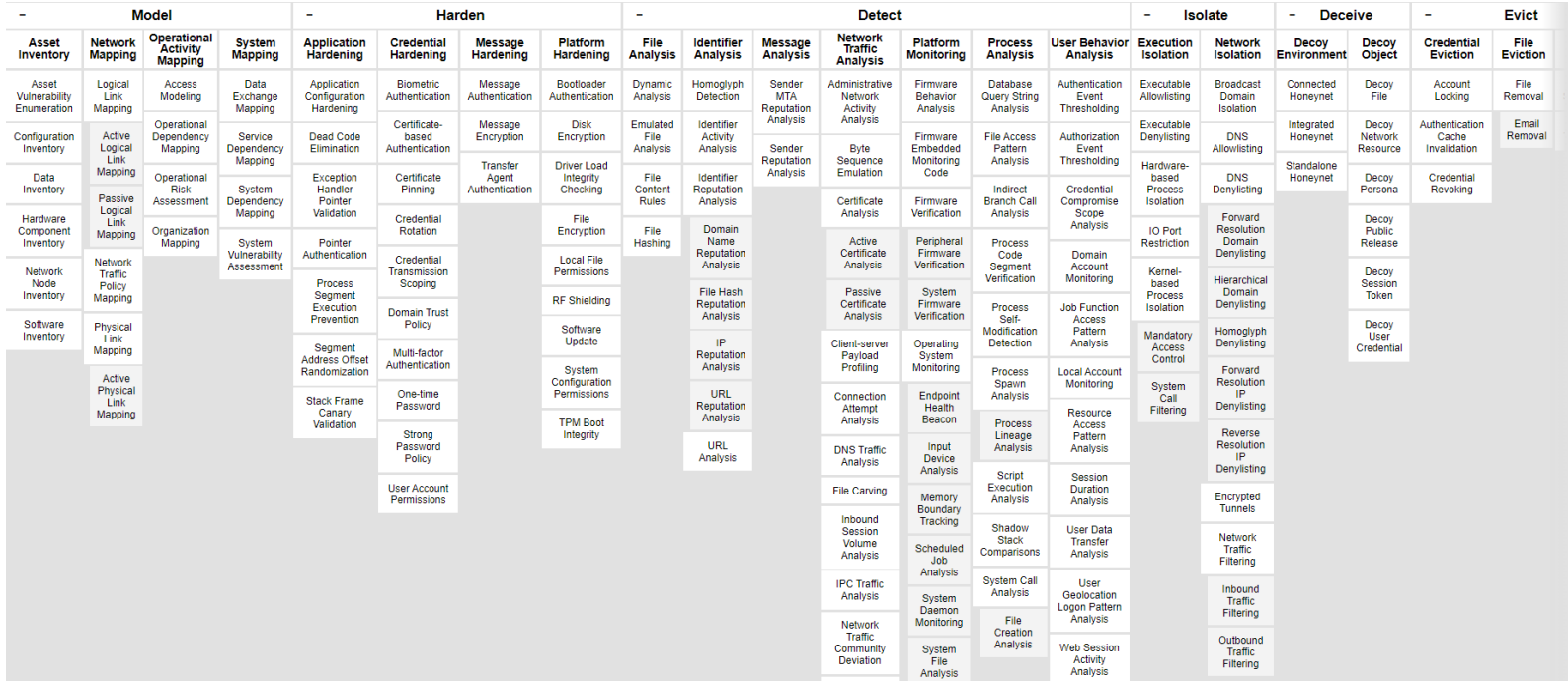
Rajhans Patel

MITRE ATT&CK



[MITRE ATT&CK](#) is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

MITRE D3FEND



MITRE D3FEND is a knowledge base, but more specifically a knowledge graph, of cybersecurity countermeasure techniques. In the simplest sense, it is a catalog of defensive cybersecurity techniques and their relationships to offensive/adversary techniques

MITRE ENGAGE

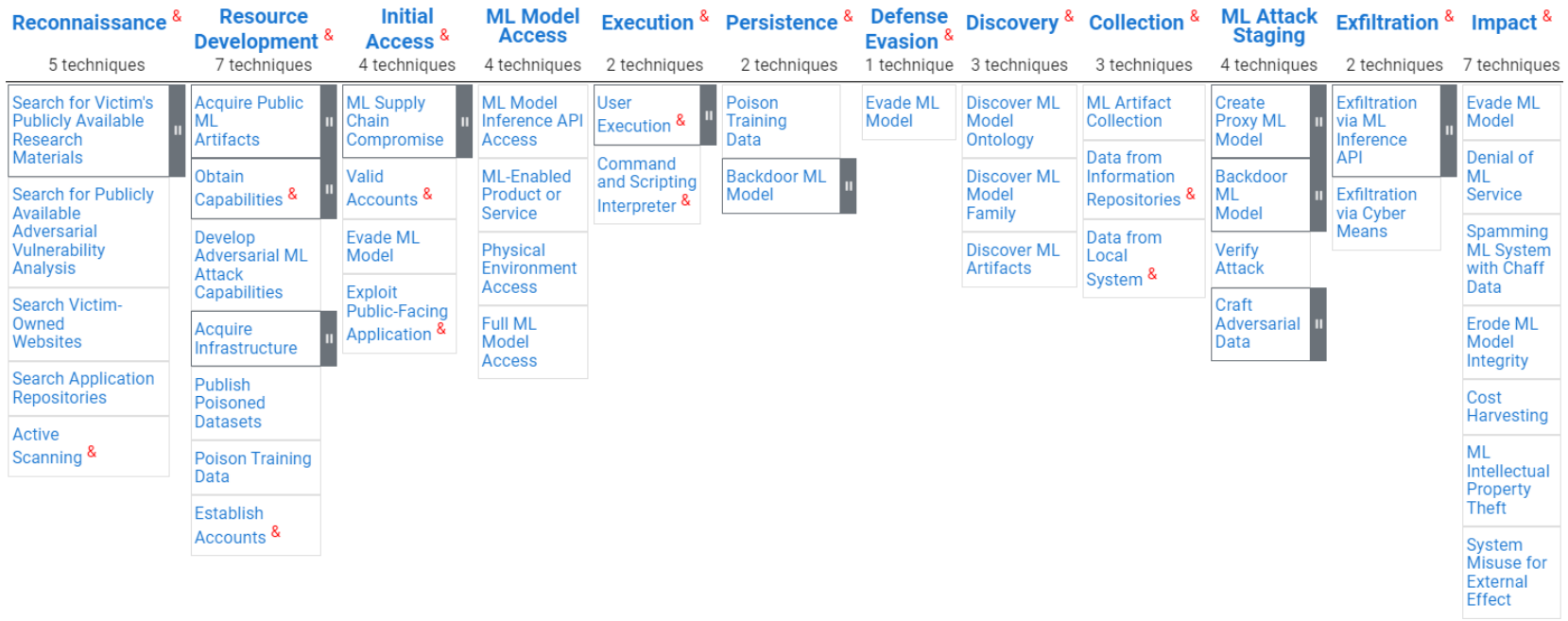
Expose	
Collect	**Detect**
API Monitoring	Introduced Vulnerabilities
Network Monitoring	Lures
Software Manipulation	Malware Detonation
System Activity Monitoring	Network Analysis

Affect		
Prevent	**Direct**	**Disrupt**
Baseline	Attack Vector Migration	Isolation
Hardware Manipulation	Email Manipulation	Lures
Isolation	Introduced Vulnerabilities	Network Manipulation
Network Manipulation	Lures	Software Manipulation
Security Controls	Malware Detonation	
	Network Manipulation	
	Peripheral Management	
	Security Controls	
	Software Manipulation	

Elicit	
Reassure	**Motivate**
Application Diversity	Application Diversity
Artifact Diversity	Artifact Diversity
Burn-In	Information Manipulation
Email Manipulation	Introduced Vulnerabilities
Information Manipulation	Malware Detonation
Network Diversity	Network Diversity
Peripheral Management	Personas
Pocket Litter	

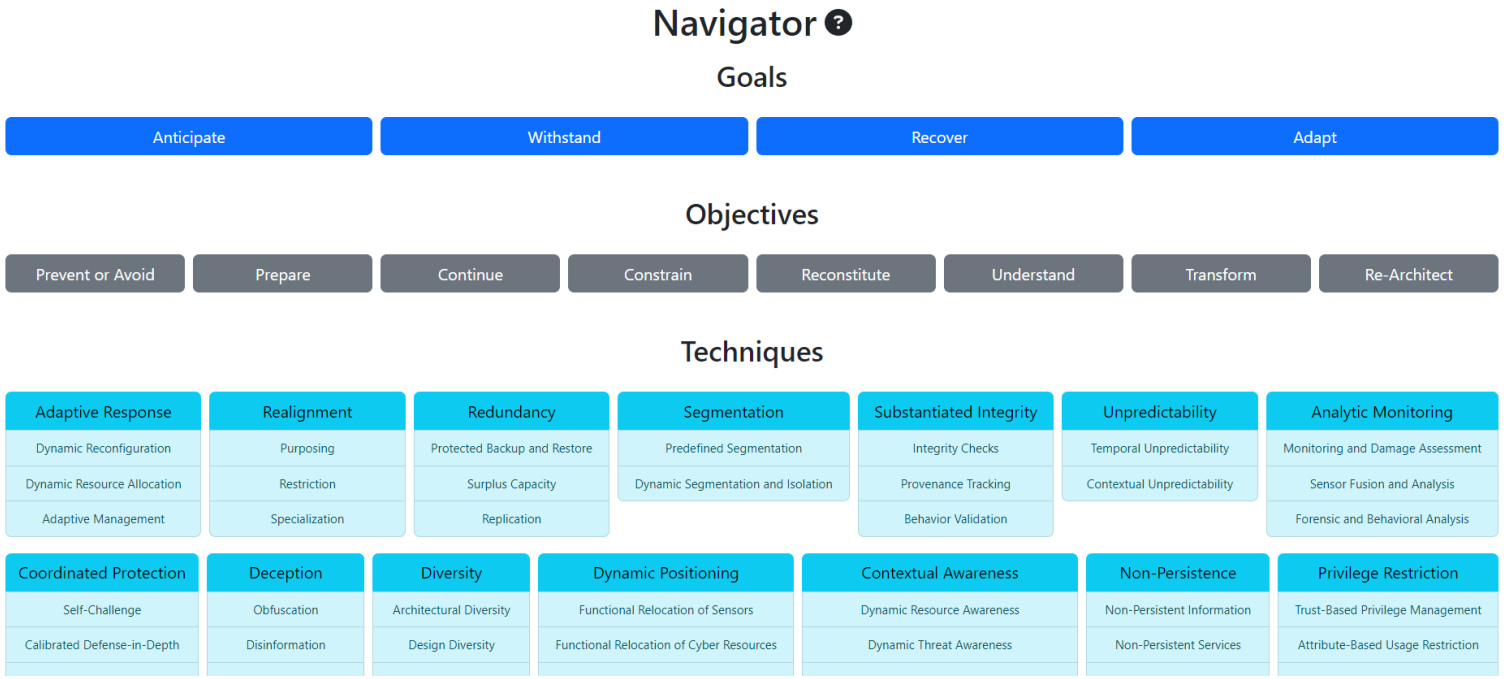
MITRE ENGAGE is a framework
for planning and discussing adversary engagement operations
that empowers you to engage your adversaries
and achieve your cybersecurity goals.

MITRE ATLAS



MITRE ATLAS is a knowledge base of adversary tactics, techniques, and case studies for machine learning (ML) systems based on real-world observations, demonstrations from ML red teams and security groups, and the state of the possible from academic research.

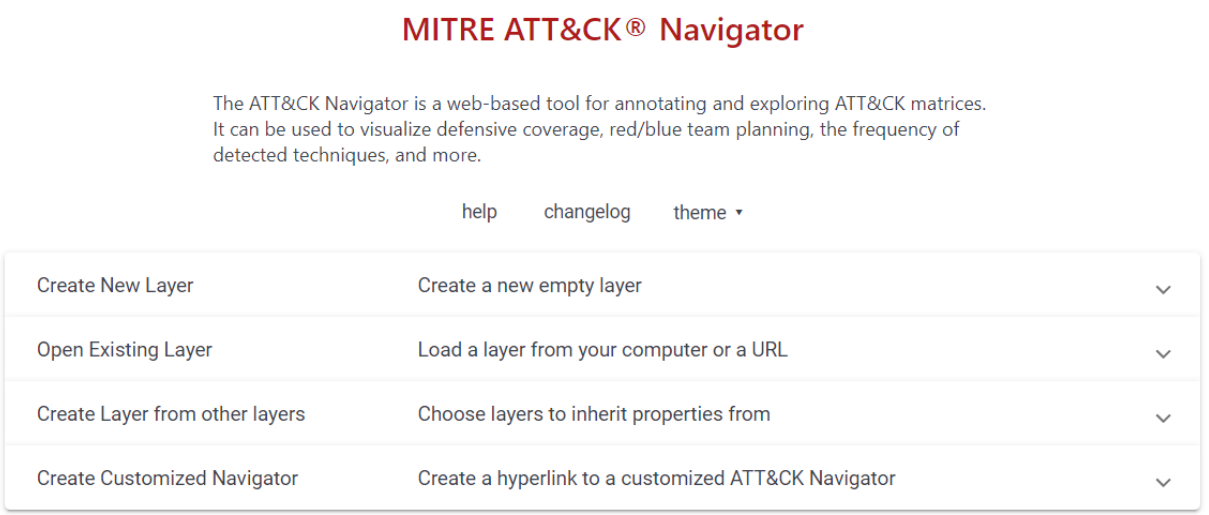
MITRE CREF NAVIGATOR



MITRE CREF Navigator is designed to be a simple, easy to use tool for Cyber Engineers and Architects and can be used for:

- Review relationships between Goals, Objectives, and Techniques
- Include as a data example in PowerPoints and presentations

MITRE ATT&CK NAVIGATOR



MITRE ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

MITRE CAR

ID	Name	Submission Date	ATT&CK Techniques	Implementations	Applicable Platforms
CAR-2013-01-002	Autorun Differences	January 25 2013	• Create or Modify System Process • Scheduled Task/Job		Windows
CAR-2013-01-003	SMB Events Monitoring	January 25 2013	• Data from Network Shared Drive • Remote Services	Pseudocode	N/A
CAR-2013-02-003	Processes Spawning cmd.exe	February 05 2013	• Command and Scripting Interpreter	Dnif, Logpoint, Pseudocode	Windows
CAR-2013-02-008	Simultaneous Logins on a Host	February 18 2013	• Valid Accounts	Pseudocode	Windows, Linux, macOS
CAR-2013-02-012	User Logged in to Multiple Hosts	February 27 2013	• Valid Accounts		Windows, Linux, macOS
CAR-2013-03-001	Reg.exe called from Command Shell	March 28 2013	• Query Registry • Modify Registry	Dnif, Pseudocode	Windows
CAR-2013-04-002	Quick execution of a series of suspicious commands	April 11 2013	• Account Discovery • OS Credential Dumping	Dnif, Logpoint, Pseudocode, Sigma	Windows, Linux, macOS

MITRE CAR analytics were developed to detect the adversary behaviors in ATT&CK. Identifying and prioritizing adversary behaviors from the ATT&CK adversary model

MAEC

Malware Attribute Enumeration and Characterization (MAEC™)

New! MAEC 5.0 now available!

Start here if you're new to MAEC

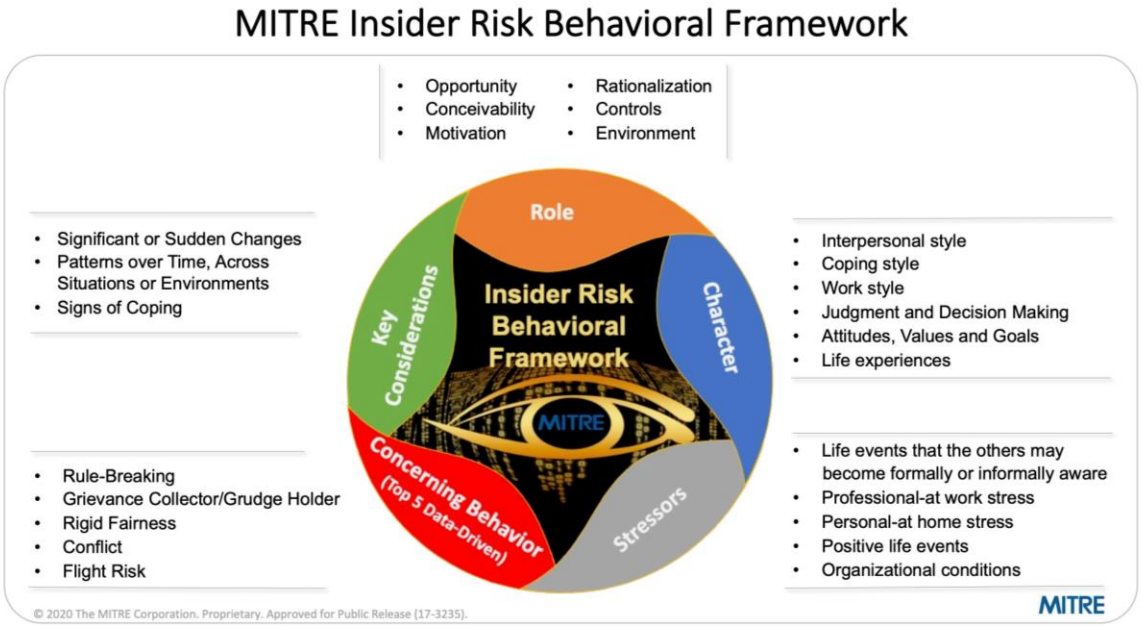
About MAEC » Get Started »

MAEC is a community-developed structured language for encoding and sharing high-fidelity information about malware based upon attributes such as behaviors, artifacts, and relationships between malware samples.

MITRE CAPEC

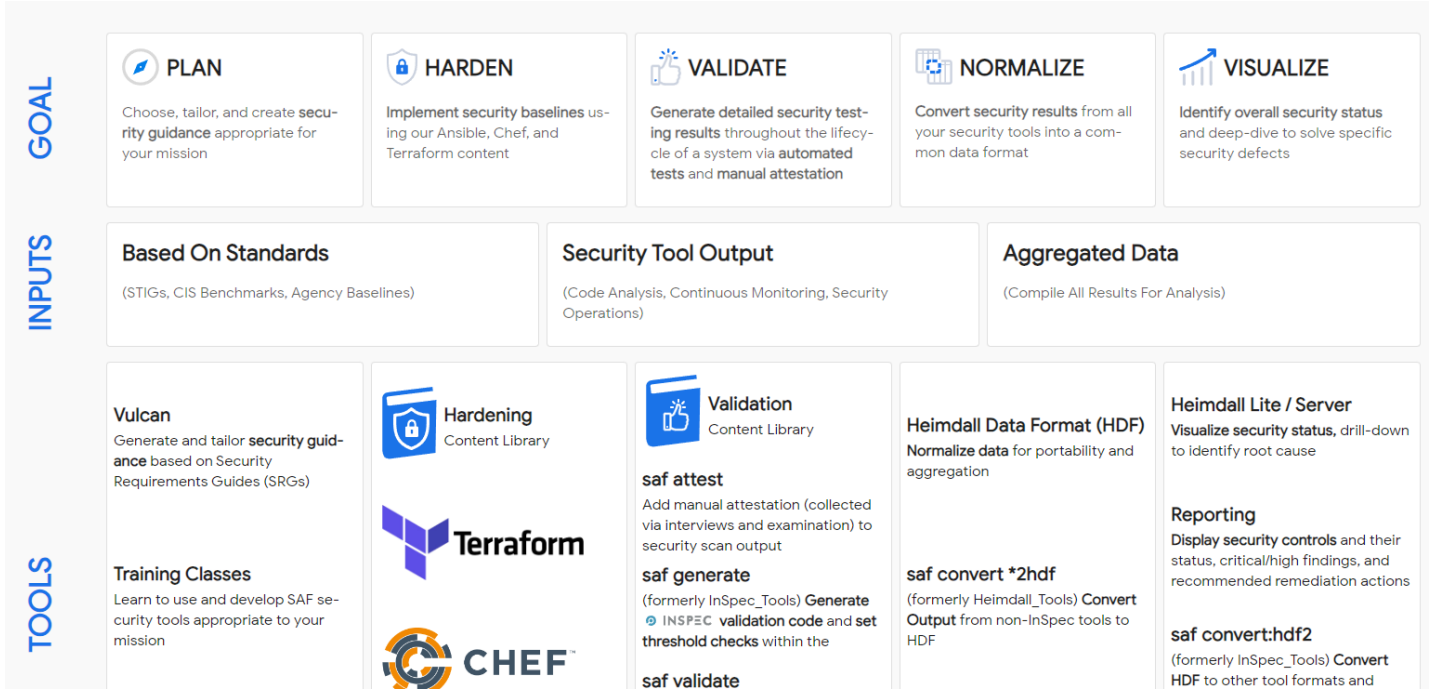
MITRE CAPEC Common Attack Pattern Enumerations and Classifications can offer a publicly available catalog of common attack patterns that helps users understand how adversaries exploit weaknesses in applications and other cyber-enabled capabilities.

MITRE INSIDER THREAT FRAMEWORK



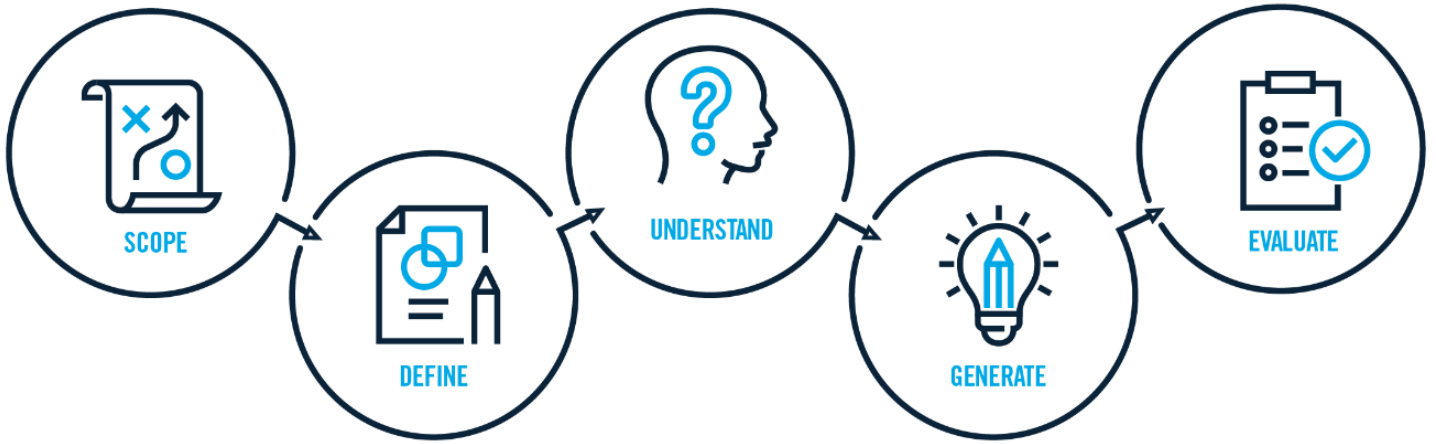
MITRE INSIDER THREAT is an Insider Risk Behavioral Framework to help practitioners think about the whole-person and triage risk based on a person's Role, Character, Stressors, Concerning Behaviors, and other Key Considerations.

MITRE SAF



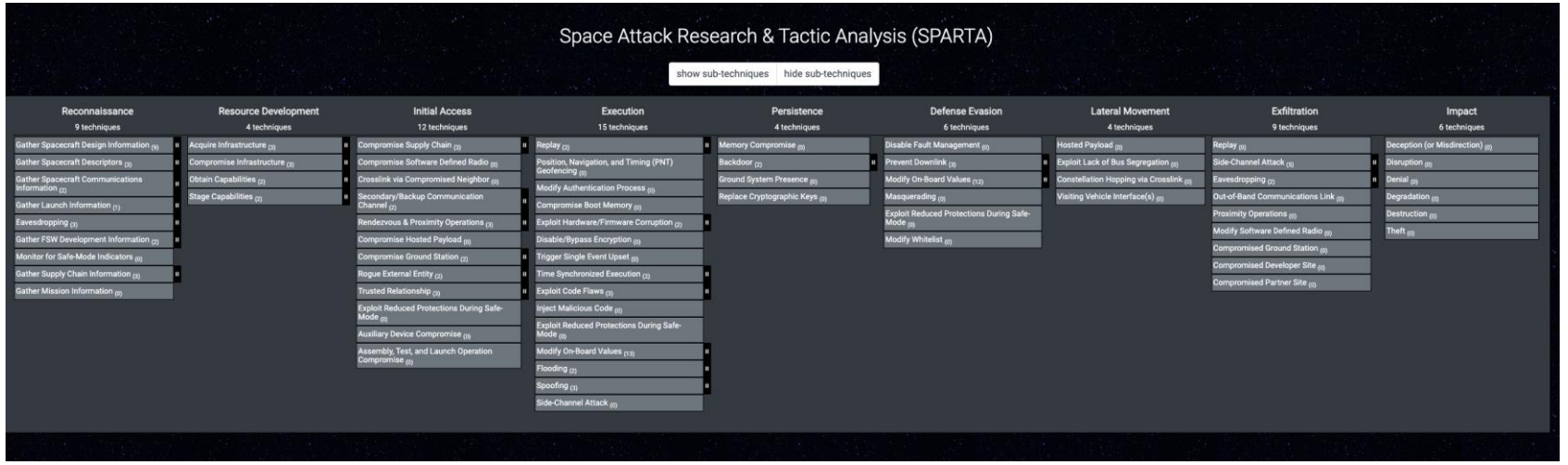
MITRE SAF brings together applications, techniques, libraries, and tools developed by MITRE and the security community to streamline security automation for systems and DevOps pipelines.

MITRE INNOVATION TOOLKIT



MITRE's Innovation Toolkit (ITK) is a freely available collection of field-tested approaches and methods to help your team work together more effectively and deliver innovative solutions to hard problems.

SPARTA



SPARTA matrix serves to ensure the space-cyber community is empowered to continually educate engineers and system defenders so they can overcome the unique cyber-threats they face in the domain.