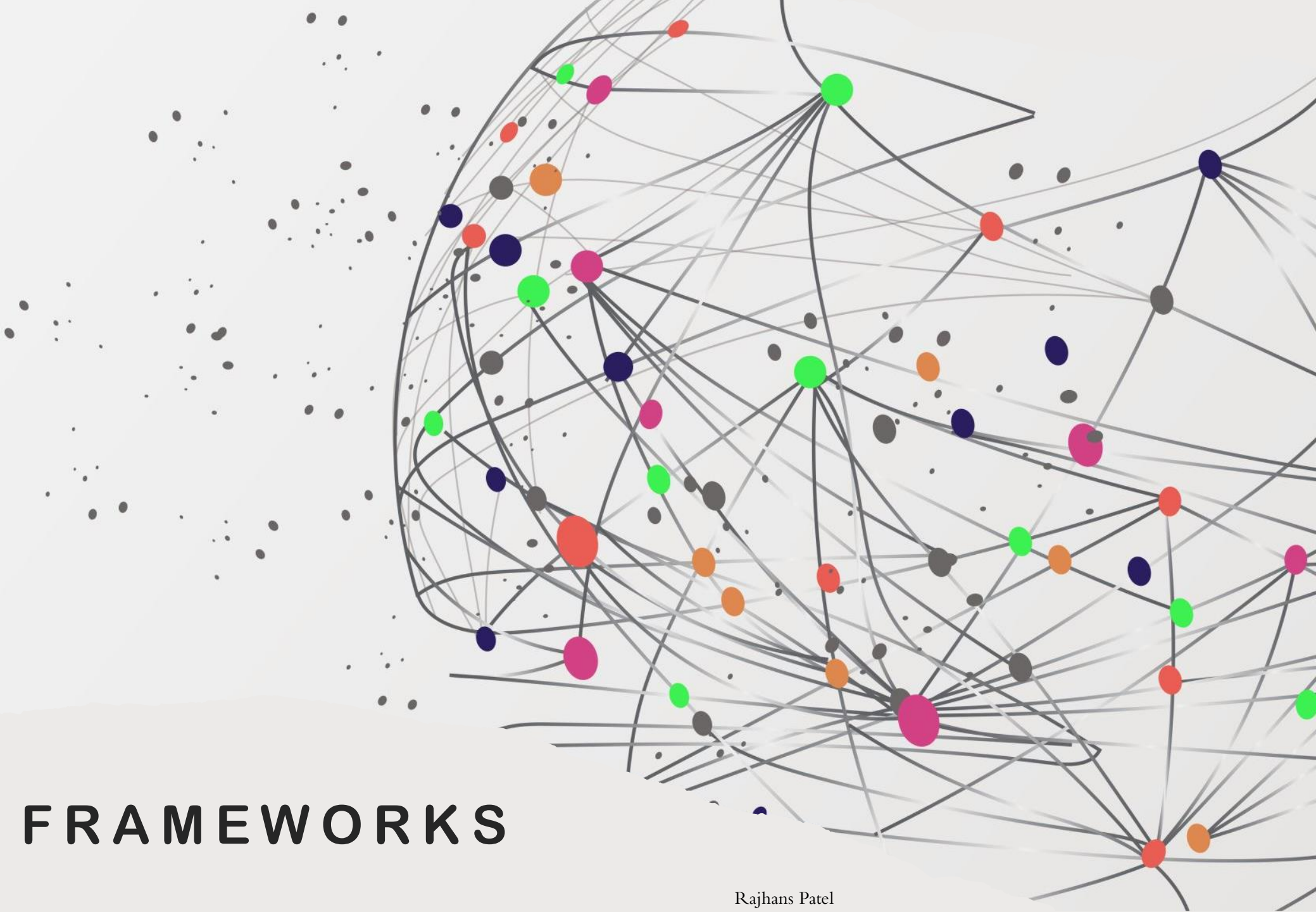


MITRE FRAMEWORKS



MITRE ATT&CK

MITRE ATT&CK													
Matrices Tactics Techniques Data Sources Mitigations Groups Software Resources Blog Contribute Search													
layout: flat show sub-techniques hide sub-techniques													
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Other Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Other Victim Identity Information (2)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture		Exfiltration Over Alternative Protocol (3)	Data Encrypted Impact
Other Victim Network Information (8)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Data Manipulation	
Other Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over C2 Channel	Defacement
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Direct Volume Access	Forge Web Credentials (2)	Cloud Storage Object Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (8)	Create or Modify System Process (4)	Domain Policy Modification (2)	Domain Policy Modification (2)	Input Capture (4)	Container and Resource Discovery	Data from Cloud Storage Object	Data from Configuration Repository (2)	Encrypted Channel (2)	Firmware Corruption	Endpoint Der of Service (4)
Search Open Technical Databases (9)		Trusted Relationship	Shared Modules	Event Triggered Execution (15)	Execution Guardrails (1)	Execution Guardrails (1)	Modify Authentication Process (4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (3)	Fallback Channels	Exfiltration Over Physical Medium (1)	Inhibit System Recovery
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Escape to Host	Exploitation for Defense Evasion	Network Sniffing	File and Directory Permissions Modification (2)	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Network Den of Service (2)
Search Victim-Owned Websites			System Services (2)	Exploitation for Privilege Escalation	Hide Artifacts (9)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Group Policy Discovery	Use Alternate Authentication Material (4)	Non-Application Layer Protocol	Multi-Stage Channels	Scheduled Transfer	Resource Hijack
			User Execution (3)	External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal Application Access Token	Network Service Scanning		Non-Standard Port	Transfer Data to Cloud Account	Service Stop	System Shutdown/Reb
			Windows Management Instrumentation	Hijack Execution Flow (11)	Process Injection (11)	Process Injection (11)	Steal or Forge Kerberos Tickets (4)	Network Share Discovery		Protocol Tunneling			
				Implant Internal Image	Scheduled Task/Job (8)	Indicator Removal on Host (6)	Steal Web Session Cookie	Peripheral Device Discovery		Proxy (4)			
				Modify Authentication Process (4)	Valid Accounts (4)	Indirect Command Execution	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Remote Access Software			
				Office Applications	Masquerading (7)	Masquerading (7)				Traffic Interception			

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

MITRE D3FEND

- Model				- Harden				- Detect							- Isolate		- Deceive		- Evict	
Asset Inventory	Network Mapping	Operational Activity Mapping	System Mapping	Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation	Decoy Environment	Decoy Object	Credential Eviction	File Eviction
Asset Vulnerability Enumeration	Logical Link Mapping	Access Modeling	Data Exchange Mapping	Application Configuration Hardening	Biometric Authentication	Message Authentication	Bootloader Authentication	Dynamic Analysis	Homoglyph Detection	Sender MTA Reputation Analysis	Administrative Network Activity Analysis	Firmware Behavior Analysis	Database Query String Analysis	Authentication Event Thresholding	Executable Allowlisting	Broadcast Domain Isolation	Connected Honeynet	Decoy File	Account Locking	File Removal
Configuration Inventory	Active Logical Link Mapping	Operational Dependency Mapping	Service Dependency Mapping	Dead Code Elimination	Certificate-based Authentication	Message Encryption	Disk Encryption	Emulated File Analysis	Identifier Activity Analysis	Sender Reputation Analysis	Byte Sequence Emulation	Firmware Embedded Monitoring Code	File Access Pattern Analysis	Authorization Event Thresholding	Executable Denylisting	DNS Allowlisting	Integrated Honeynet	Decoy Network Resource	Authentication Cache Invalidation	Email Removal
Data Inventory	Passive Logical Link Mapping	Operational Risk Assessment	System Dependency Mapping	Exception Handler Pointer Validation	Certificate Pinning	Transfer Agent Authentication	Driver Load Integrity Checking	File Content Rules	Identifier Reputation Analysis			Certificate Analysis	Firmware Verification	Indirect Branch Call Analysis	Credential Compromise Scope Analysis	Hardware-based Process Isolation	DNS Denylisting	Standalone Honeynet	Decoy Persona	Credential Revoking
Hardware Component Inventory		Organization Mapping	System Vulnerability Assessment	Pointer Authentication	Credential Rotation		File Encryption	File Hashing	Domain Name Reputation Analysis	Active Certificate Analysis	Peripheral Firmware Verification	Process Code Segment Verification	Domain Account Monitoring	IO Port Restriction	Forward Resolution Domain Denylisting		Decoy Public Release			
Network Node Inventory	Network Traffic Policy Mapping			Process Segment Execution Prevention	Credential Transmission Scoping		Local File Permissions		File Hash Reputation Analysis	Passive Certificate Analysis	System Firmware Verification		Process Self-Modification Detection	Job Function Access Pattern Analysis	Kernel-based Process Isolation	Hierarchical Domain Denylisting		Decoy Session Token		
Software Inventory	Physical Link Mapping			Segment Address Offset Randomization	Domain Trust Policy		Software Update		IP Reputation Analysis		Client-server Payload Profiling	Operating System Monitoring		Local Account Monitoring	Mandatory Access Control	Homoglyph Denylisting		Decoy User Credential		
	Active Physical Link Mapping			Stack Frame Canary Validation	Multi-factor Authentication		System Configuration Permissions		URL Reputation Analysis	Connection Attempt Analysis	Endpoint Health Beacon		Process Lineage Analysis	Resource Access Pattern Analysis	System Call Filtering	Forward Resolution IP Denylisting				
					One-time Password		TPM Boot Integrity		URL Analysis	DNS Traffic Analysis	Input Device Analysis		Script Execution Analysis	Session Duration Analysis		Reverse Resolution IP Denylisting				
					User Account Permissions					File Carving	Memory Boundary Tracking		Shadow Stack Comparisons	User Data Transfer Analysis		Encrypted Tunnels				
										Inbound Session Volume Analysis	Scheduled Job Analysis		System Call Analysis	User Geolocation Logon Pattern Analysis		Network Traffic Filtering				
										IPC Traffic Analysis	System Daemon Monitoring		File Creation Analysis	Web Session Activity Analysis		Inbound Traffic Filtering				
										Network Traffic Community Deviation	System File Analysis					Outbound Traffic Filtering				

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		Affect			Elicit	
Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate
API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity
Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity
Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation
System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities
		Security Controls	Malware Detonation		Information Manipulation	Malware Detonation
			Network Manipulation		Network Diversity	Network Diversity
			Peripheral Management		Peripheral Management	Personas
			Security Controls		Pocket Litter	
			Software Manipulation			

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

Reconnaissance & 5 techniques	Resource Development & 7 techniques	Initial Access & 4 techniques	ML Model Access 4 techniques	Execution & 2 techniques	Persistence & 2 techniques	Defense Evasion & 1 technique	Discovery & 3 techniques	Collection & 3 techniques	ML Attack Staging 4 techniques	Exfiltration & 2 techniques	Impact & 7 techniques
Search for Victim's Publicly Available Research Materials	Acquire Public ML Artifacts	ML Supply Chain Compromise	ML Model Inference API Access	User Execution &	Poison Training Data	Evade ML Model	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		Discover ML Model Family	Data from Information Repositories &	Backdoor ML Model	Exfiltration via Cyber Means	Denial of ML Service
Search Victim-Owned Websites	Develop Adversarial ML Attack Capabilities	Evade ML Model	Physical Environment Access				Discover ML Artifacts	Data from Local System &	Verify Attack		Spamming ML System with Chaff Data
Search Application Repositories	Acquire Infrastructure	Exploit Public-Facing Application &	Full ML Model Access						Craft Adversarial Data		Erode ML Model Integrity
Active Scanning &	Publish Poisoned Datasets										Cost Harvesting
	Poison Training Data										ML Intellectual Property Theft
	Establish Accounts &										System Misuse for External Effect

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

Navigator ?

Goals

Anticipate	Withstand	Recover	Adapt
------------	-----------	---------	-------

Objectives

Prevent or Avoid	Prepare	Continue	Constrain	Reconstitute	Understand	Transform	Re-Architect
------------------	---------	----------	-----------	--------------	------------	-----------	--------------

Techniques

Adaptive Response	Realignment	Redundancy	Segmentation	Substantiated Integrity	Unpredictability	Analytic Monitoring
Dynamic Reconfiguration	Purposing	Protected Backup and Restore	Predefined Segmentation	Integrity Checks	Temporal Unpredictability	Monitoring and Damage Assessment
Dynamic Resource Allocation	Restriction	Surplus Capacity	Dynamic Segmentation and Isolation	Provenance Tracking	Contextual Unpredictability	Sensor Fusion and Analysis
Adaptive Management	Specialization	Replication		Behavior Validation		Forensic and Behavioral Analysis
Coordinated Protection	Deception	Diversity	Dynamic Positioning	Contextual Awareness	Non-Persistence	Privilege Restriction
Self-Challenge	Obfuscation	Architectural Diversity	Functional Relocation of Sensors	Dynamic Resource Awareness	Non-Persistent Information	Trust-Based Privilege Management
Calibrated Defense-in-Depth	Disinformation	Design Diversity	Functional Relocation of Cyber Resources	Dynamic Threat Awareness	Non-Persistent Services	Attribute-Based Usage Restriction

[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

The 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.

[help](#) [changelog](#) [theme ▾](#)

Create New Layer	Create a new empty layer	▾
Open Existing Layer	Load a layer from your computer or a URL	▾
Create Layer from other layers	Choose layers to inherit properties from	▾
Create Customized Navigator	Create a hyperlink to a customized 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	<ul style="list-style-type: none">• Create or Modify System Process• Scheduled Task/Job		Windows
CAR-2013-01-003	SMB Events Monitoring	January 25 2013	<ul style="list-style-type: none">• Data from Network Shared Drive• Remote Services	Pseudocode	N/A
CAR-2013-02-003	Processes Spawning cmd.exe	February 05 2013	<ul style="list-style-type: none">• Command and Scripting Interpreter	Dnif, Logpoint, Pseudocode	Windows
CAR-2013-02-008	Simultaneous Logins on a Host	February 18 2013	<ul style="list-style-type: none">• Valid Accounts	Pseudocode	Windows, Linux, macOS
CAR-2013-02-012	User Logged in to Multiple Hosts	February 27 2013	<ul style="list-style-type: none">• Valid Accounts		Windows, Linux, macOS
CAR-2013-03-001	Reg.exe called from Command Shell	March 28 2013	<ul style="list-style-type: none">• Query Registry• Modify Registry	Dnif, Pseudocode	Windows
CAR-2013-04-002	Quick execution of a series of suspicious commands	April 11 2013	<ul style="list-style-type: none">• 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

M A E C

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.

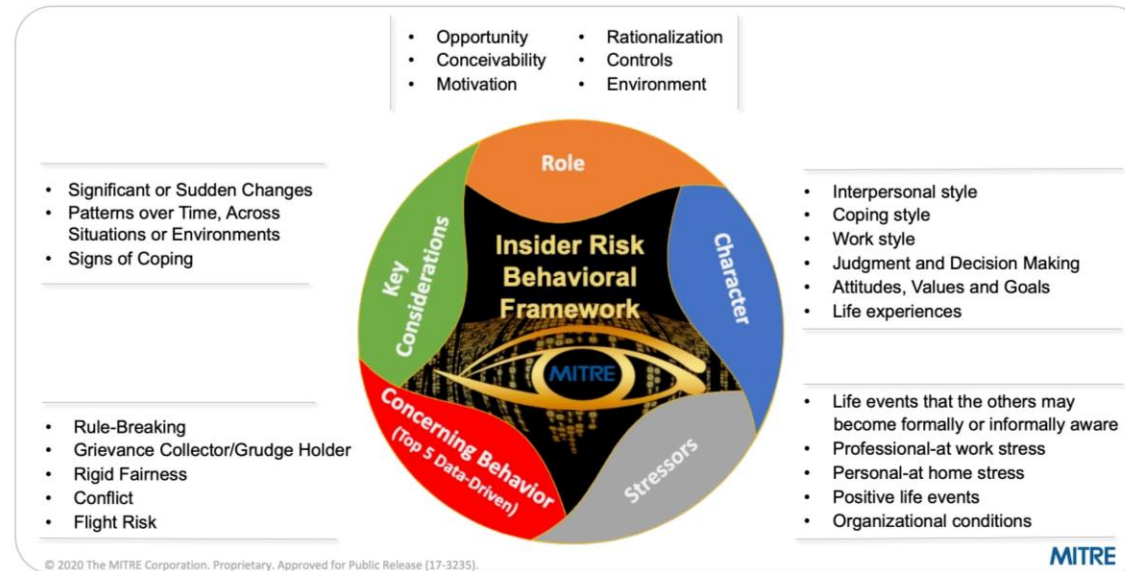
MITRE CAPEC



[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.

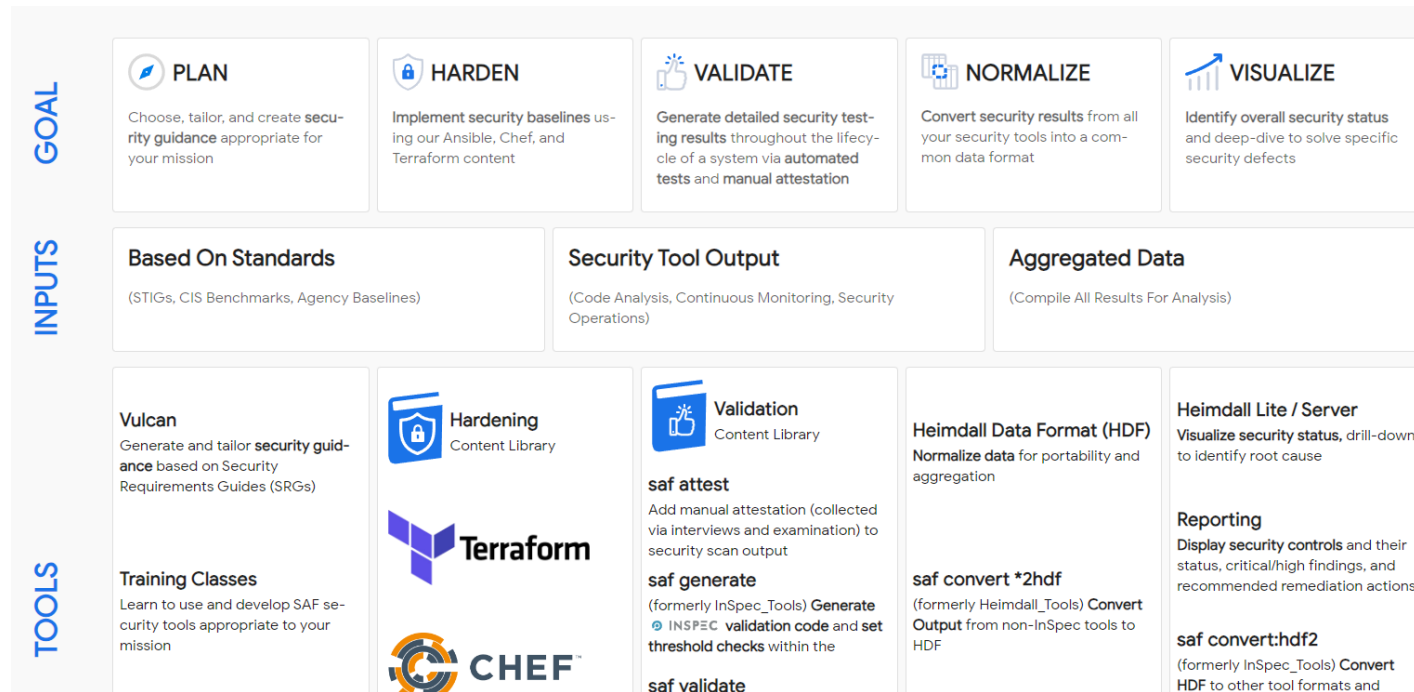
MITRE INSIDER THREAT FRAMEWORK

MITRE Insider Risk Behavioral Framework



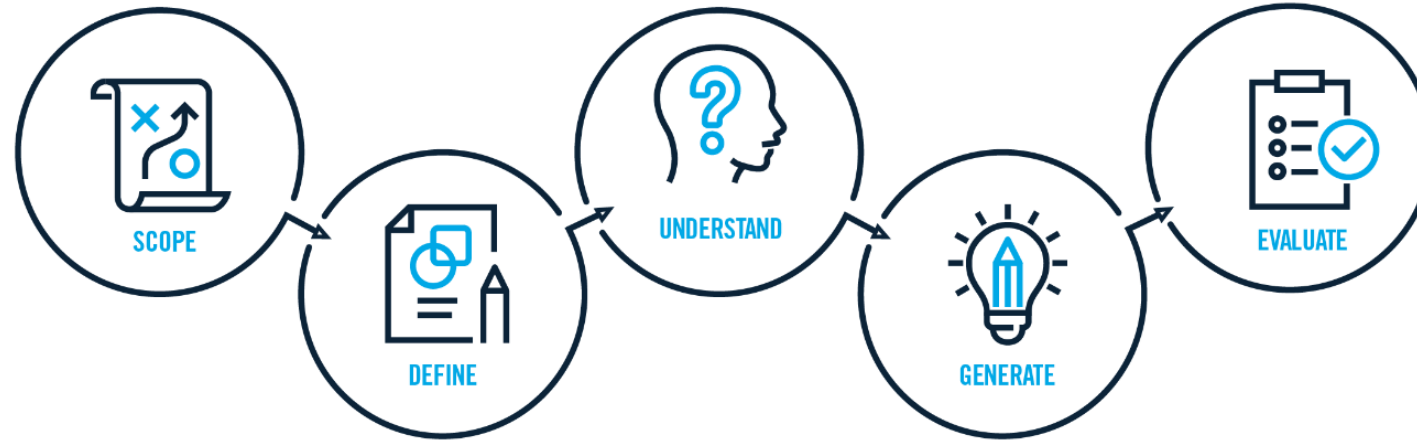
[MITRE INSIDER THREAT](#) is an Insider Risk Behavioral Framework to help practitioners think about the whole-person and triage risk based on a person's Role, Character, Stressors, Concerning Behaviors, and other Key Considerations.

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

Space Attack Research & Tactic Analysis (SPARTA)								
show sub-techniques hide sub-techniques								
Reconnaissance 9 techniques	Resource Development 4 techniques	Initial Access 12 techniques	Execution 15 techniques	Persistence 4 techniques	Defense Evasion 6 techniques	Lateral Movement 4 techniques	Exfiltration 9 techniques	Impact 6 techniques
Gather Spacecraft Design Information (1)	Acquire Infrastructure (2)	Compromise Supply Chain (2)	Replay (2)	Memory Compromise (1)	Disable Fault Management (1)	Hosted Payload (1)	Replay (1)	Deception (or Misdirection) (1)
Gather Spacecraft Descriptors (2)	Compromise Infrastructure (2)	Compromise Software Defined Radio (2)	Position, Navigation, and Timing (PNT) Geofencing (1)	Backdoor (2)	Prevent Downlink (1)	Exploit Lack of Bus Segregation (1)	Side-Channel Attack (1)	Disruption (1)
Gather Spacecraft Communications Information (2)	Obtain Capabilities (2)	Crosslink via Compromised Neighbor (1)	Modify Authentication Process (1)	Ground System Presence (1)	Modify On-Board Values (12)	Constellation Hopping via Crosslink (1)	Eavesdropping (2)	Denial (1)
Gather Launch Information (2)	Stage Capabilities (2)	Secondary/Backup Communication Channel (1)	Compromise Boot Memory (1)	Replace Cryptographic Keys (1)	Masquerading (1)	Visiting Vehicle Interface(s) (1)	Out-of-Band Communications Link (1)	Degradation (1)
Eavesdropping (1)		Rendezvous & Proximity Operations (1)	Exploit Hardware/Firmware Corruption (2)		Exploit Reduced Protections During Safe-Mode (1)		Proximity Operations (1)	Destruction (1)
Gather FSW Development Information (2)		Compromise Hosted Payload (1)	Disable/Bypass Encryption (1)		Modify Whitelist (1)		Modify Software Defined Radio (1)	Theft (1)
Monitor for Safe-Mode Indicators (1)		Compromise Ground Station (2)	Trigger Single Event Upset (1)				Compromised Ground Station (1)	
Gather Supply Chain Information (1)		Rogue External Entity (2)	Time Synchronized Execution (2)				Compromised Developer Site (1)	
Gather Mission Information (1)		Trusted Relationship (1)	Exploit Code Flaws (1)				Compromised Partner Site (1)	
		Exploit Reduced Protections During Safe-Mode (1)	Inject Malicious Code (1)					
		Auxiliary Device Compromise (1)	Exploit Reduced Protections During Safe-Mode (1)					
		Assembly, Test, and Launch Operation Compromise (1)	Modify On-Board Values (13)					
			Flooding (2)					
			Spoofing (1)					
			Side-Channel Attack (1)					

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.