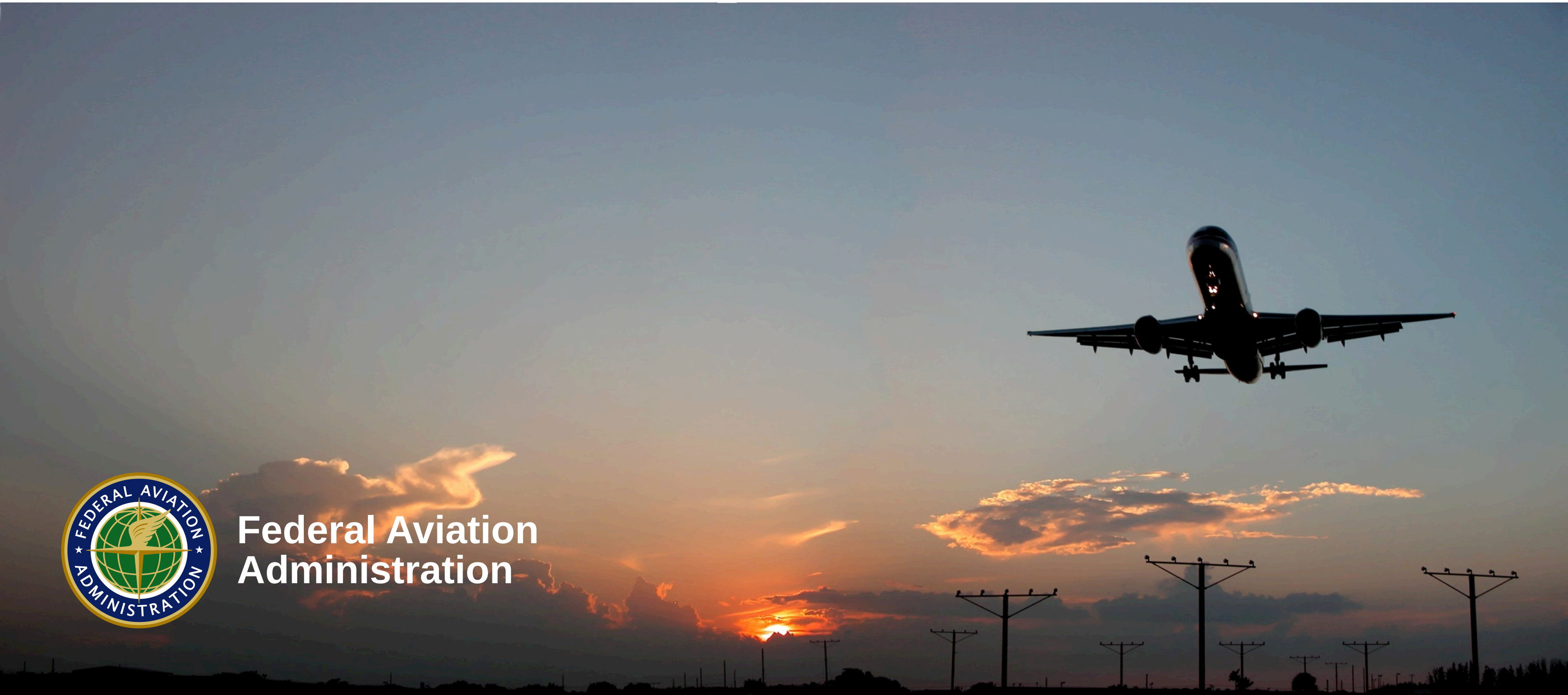
2020 FAA Cybersecurity Awareness Symposium

Securing the Aviation Ecosystem | “Cyber Hygiene”

Cybersecurity Risk Modelling (CyRM)

Date: October 20, 2020



Federal Aviation
Administration

Cybersecurity Risk Management (CyRM)

- **Mission Statement - CyRM is an Agency effort to define and create a capability to perform modelling of cyber-threats to the FAA so that mitigations can be identified and prioritized.**
- **CyRM Team Function 1 – Perform cyber risk assessments to establish the relationship between lower level systems and higher level services and business functions.**
- **CyRM Team Function 2 - Develops automation tools which show operations personnel how an emerging threat can affect FAA essential functions.**

CyRM Team Function #1 - CyRM Assessments

- Security at the FAA has traditionally been analyzed at a system level. The most recent NIST and OMB guidance calls for adding approaches which also measure the impact of security incidents on critical agency functions.
  - This permits better prioritization of remediation efforts.
- CyRM has developed new methods for analyzing risk from component and system events into higher level services and critical functions.
  - CyRM Assessments begin with an Agency service and analyze the connections between systems and agency functions.
  - Services are drawn from the FAA Services Hierarchy (FAASH).
- CyRM is a Cybersecurity Steering Committee (CSC) effort and ANG, AFN ASH and ATO are members.
- The CyRM processes and tools are intended to aid the Agency in increasing the timeliness of the response a cybersecurity risks and this aid in the overall FAA Cyber Hygiene effort.

CyRM Team Function #2 - CyRM Automation Tools ARCAT

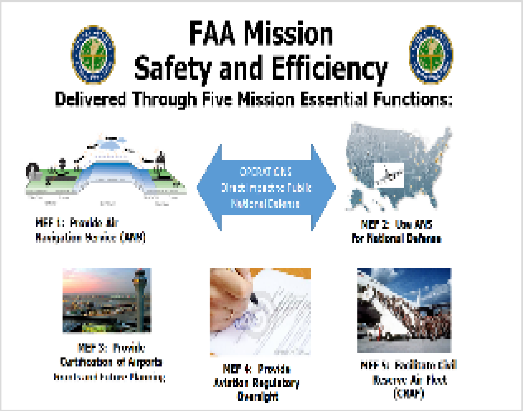
- Enterprise tool that provides the FAA Cybersecurity Steering Committee and Operating Domains users (NAS, MS, R&D) with strategic and tactical information necessary to make data-driven risk management decisions.

- Provides an enterprise capability to predict the risk exposures to cyber threats and enables efficient mitigation.

CyRM Team Function #2 - CyRM Automation Tools ARCAT

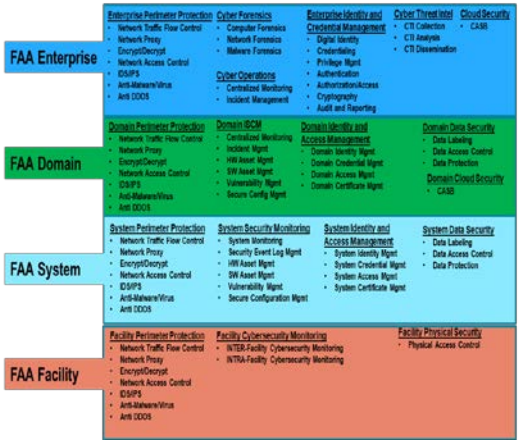
ARCAT Prototype Features

- Enterprise view of cyber threat and risk to FAA mission
- Automation of CyRM risk assessment process
- Cybersecurity Architecture Repository
- Enterprise cyber threat modeling capabilities
- Insight for planning acquisition improvements to FAA Cybersecurity



FAA Mission
Safety and Efficiency
Delivered Through Five Mission Essential Functions:

OPERATIONS
Direct Impact to Public
National Defense
MEF 1: Provide Air Navigation Service (ANS)
MEF 2: Use ANS for National Defense
MEF 3: Provide Certification of Airports
[illegible] Future Planning
MEF 4: Provide Aviation Regulatory Oversight
MEF 5: Facilitate Civil Reserve Air Fleet (CRAF)



FAA Enterprise

Enterprise Perimeter Protection
- Network Traffic Flow Control
- Network Proxy
- Encrypt/Decrypt
- Network Access Control
- IDS/IPS
- Anti-Malware/Virus
- Anti DDOS

Cyber Forensics
- Computer Forensics
- Network Forensics
- Malware Forensics

Cyber Operations
- Centralized Monitoring
- Incident Management

Enterprise Identity and Credential Management
- Digital Identity
- Credentialing
- Privilege Mgmt
- Authentication
- Authorization/Access
- Cryptography
- Audit and Reporting

Cyber Threat Intel
- CTI Collection
- CTI Analysis
- CTI Dissemination

Cloud Security
- CASB

FAA Domain

Domain Perimeter Protection
- Network Traffic Flow Control
- Network Proxy
- Encrypt/Decrypt
- Network Access Control
- IDS/IPS
- Anti-Malware/Virus
- Anti DDOS

Domain ISCM
- Centralized Monitoring
- Incident Mgmt
- HW Asset Mgmt
- SW Asset Mgmt
- Vulnerability Mgmt
- Secure Config Mgmt

Domain Identity and Access Management
- Domain Identity Mgmt
- Domain Credential Mgmt
- Domain Access Mgmt
- Domain Certificate Mgmt

Domain Data Security
- Data Labeling
- Data Access Control
- Data Protection

Domain Cloud Security
- CASB

FAA System

System Perimeter Protection
- Network Traffic Flow Control
- Network Proxy
- Encrypt/Decrypt
- Network Access Control
- IDS/IPS
- Anti-Malware/Virus
- Anti DDOS

System Security Monitoring
- System Monitoring
- Security Event Log Mgmt
- HW Asset Mgmt
- SW Asset Mgmt
- Vulnerability Mgmt
- Secure Configuration Mgmt

System Identity and Access Management
- System Identity Mgmt
- System Credential Mgmt
- System Access Mgmt
- System Certificate Mgmt

System Data Security
- Data Labeling
- Data Access Control
- Data Protection

FAA Facility

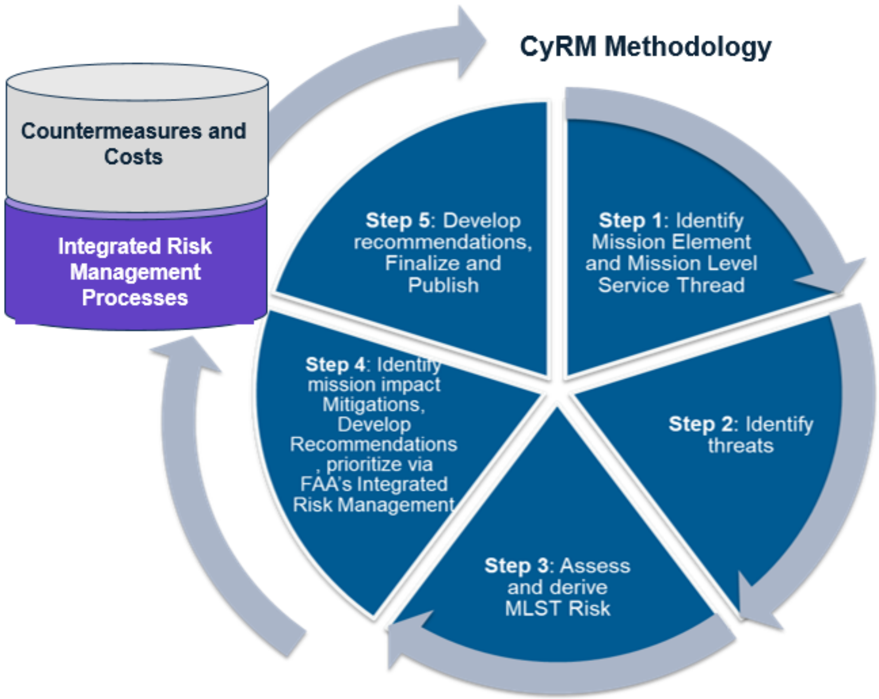
Facility Perimeter Protection
- Network Traffic Flow Control
- Network Proxy
- Encrypt/Decrypt
- Network Access Control
- IDS/IPS
- Anti-Malware/Virus
- Anti DDOS

Facility Cybersecurity Monitoring
- INTER-Facility Cybersecurity Monitoring
- INTRA-Facility Cybersecurity Monitoring

Facility Physical Security
- Physical Access Control

CyRM Team Function #2 - CyRM Automation Tools - CICAT

CICAT was adapted for use by the FAA and integrated into CyRM Methodology*


CyRM Methodology
Countermeasures and Costs
Integrated Risk Management Processes
Step 1: Identify Mission Element and Mission Level Service Thread
Step 2: Identify threats
Step 3: Assess and derive MLST Risk
Step 4: Identify mission impact Mitigations, Develop Recommendations , prioritize via FAA's Integrated Risk Management
Step 5: Develop recommendations, Finalize and Publish

** CyRM Methodology was defined collaboratively by the FAA and MITRE in FY17.*

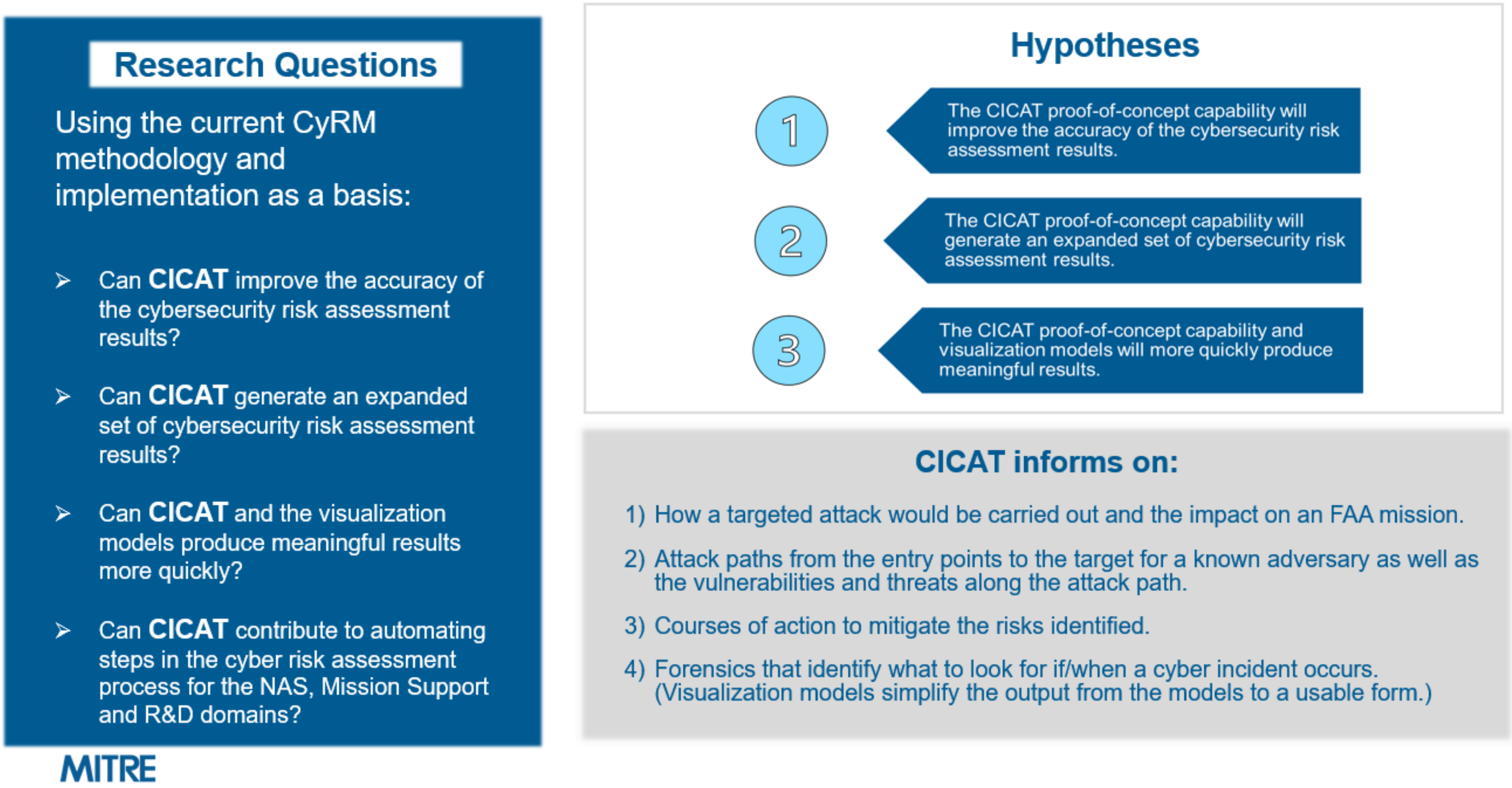
CICAT was adapted for use by FAA CyRM, simulating an attack against the FAA's network based on the FAA enterprise environment, vulnerabilities identified by CVEs and threat information encoded in ATT&CK.

CICAT business logic, reporting, and interactive visualizations are data-driven capabilities. Other CyRM capabilities, such as the architecture repository, could provide the necessary data, such as mission, service, and FAA enterprise data and vulnerabilities to CICAT for use by the underlying models.

CICAT was adapted with ARCAT proof-of-concept models in mind to ease integration of the capabilities.

CyRM Team Function #2 - CyRM Automation Tools - CICAT

Critical Infrastructure Cyberspace Analysis Tool (CICAT)



Research Questions

Using the current CyRM methodology and implementation as a basis:

- Can **CICAT** improve the accuracy of the cybersecurity risk assessment results?
- Can **CICAT** generate an expanded set of cybersecurity risk assessment results?
- Can **CICAT** and the visualization models produce meaningful results more quickly?
- Can **CICAT** contribute to automating steps in the cyber risk assessment process for the NAS, Mission Support and R&D domains?

MITRE

Hypotheses

1 The CICAT proof-of-concept capability will improve the accuracy of the cybersecurity risk assessment results.

2 The CICAT proof-of-concept capability will generate an expanded set of cybersecurity risk assessment results.

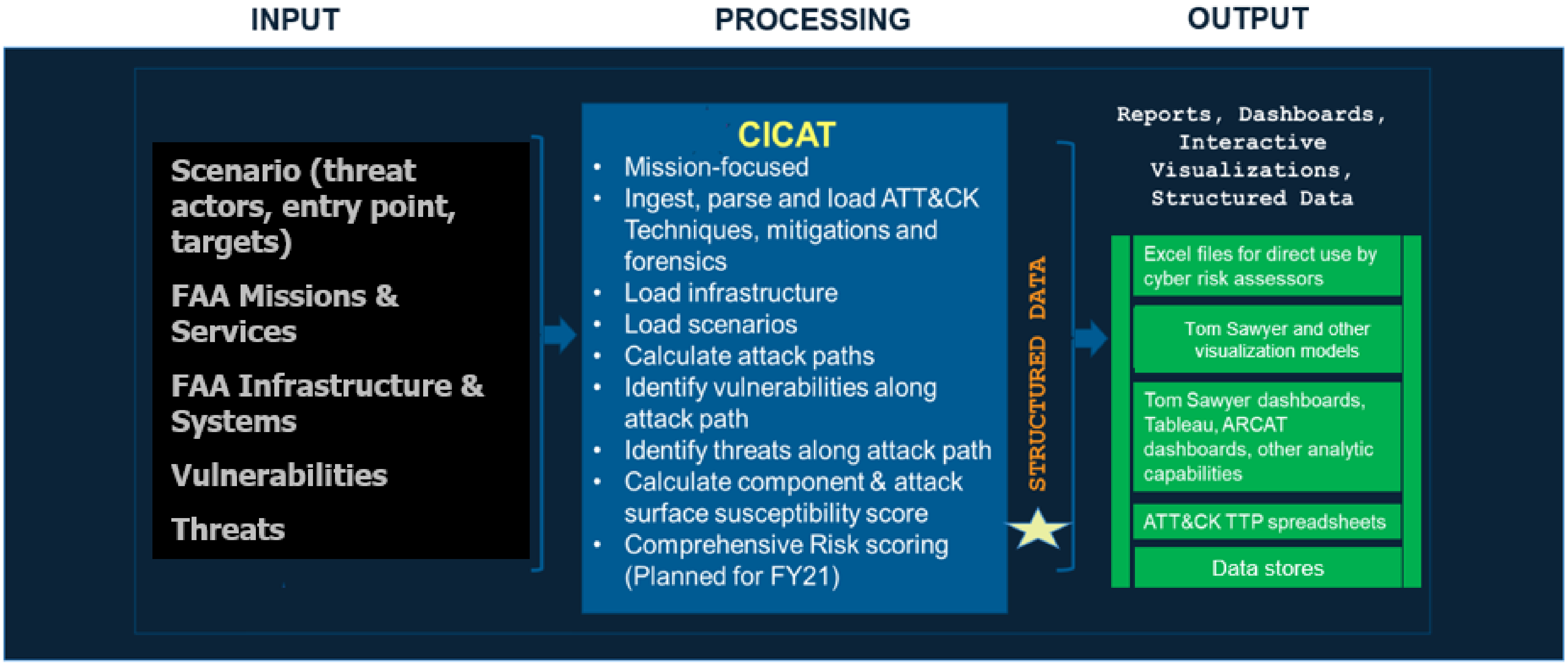
3 The CICAT proof-of-concept capability and visualization models will more quickly produce meaningful results.

CICAT informs on:

1) How a targeted attack would be carried out and the impact on an FAA mission.
2) Attack paths from the entry points to the target for a known adversary as well as the vulnerabilities and threats along the attack path.
3) Courses of action to mitigate the risks identified.
4) Forensics that identify what to look for if/when a cyber incident occurs. (Visualization models simplify the output from the models to a usable form.)

CyRM Team Function #2 - CyRM Automation Tools - CICAT

CICAT Input, Output and Processing



INPUT

PROCESSING

OUTPUT

Scenario (threat actors, entry point, targets)

FAA Missions & Services

FAA Infrastructure & Systems

Vulnerabilities

Threats

CICAT

- Mission-focused
- Ingest, parse and load ATT&CK Techniques, mitigations and forensics
- Load infrastructure
- Load scenarios
- Calculate attack paths
- Identify vulnerabilities along attack path
- Identify threats along attack path
- Calculate component & attack surface susceptibility score
- Comprehensive Risk scoring (Planned for FY21)

STRUCTURED DATA

Reports, Dashboards, Interactive Visualizations, Structured Data

Excel files for direct use by cyber risk assessors

Tom Sawyer and other visualization models

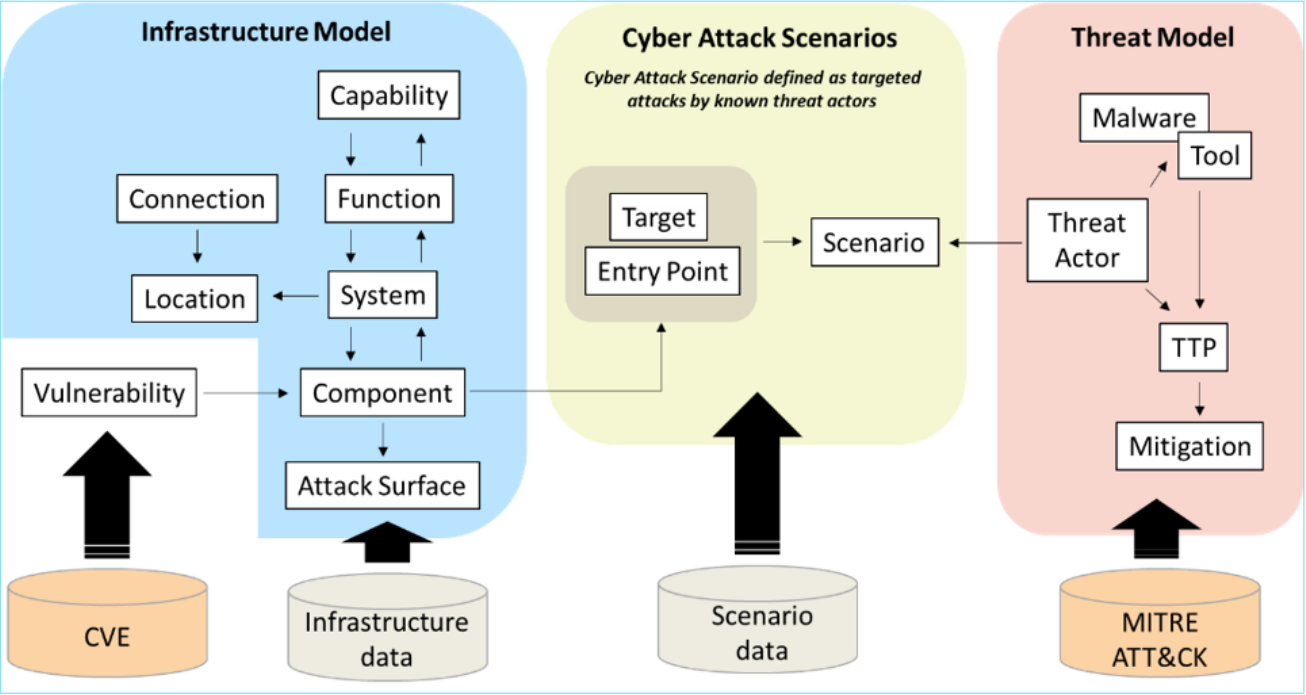
Tom Sawyer dashboards, Tableau, ARCAT dashboards, other analytic capabilities

ATT&CK TTP spreadsheets

Data stores

CyRM Team Function #2 - CyRM Automation Tools - CICAT

CICAT Data Model



Imported as XML data

Imported from STIX/TAXII service

The CICAT data model includes data imported as XML files (CVE and ATT&CK for Industrial Control Systems (ICS)), as JSON files (Enterprise ATT&CK), and as Excel spreadsheets (Infrastructure and scenario data).