DAFMSS

May 9, 2023

Model-based Digital Engineering Data Fusion

Concepts, methodology, value

Mike Nash, P.E.
Solutions Director, Digital Engineering

GDIT

DoD Digital Engineering Strategy

The strategy promotes the use of digital representations of systems and components and the use of digital artifacts to design and sustain national defense systems.

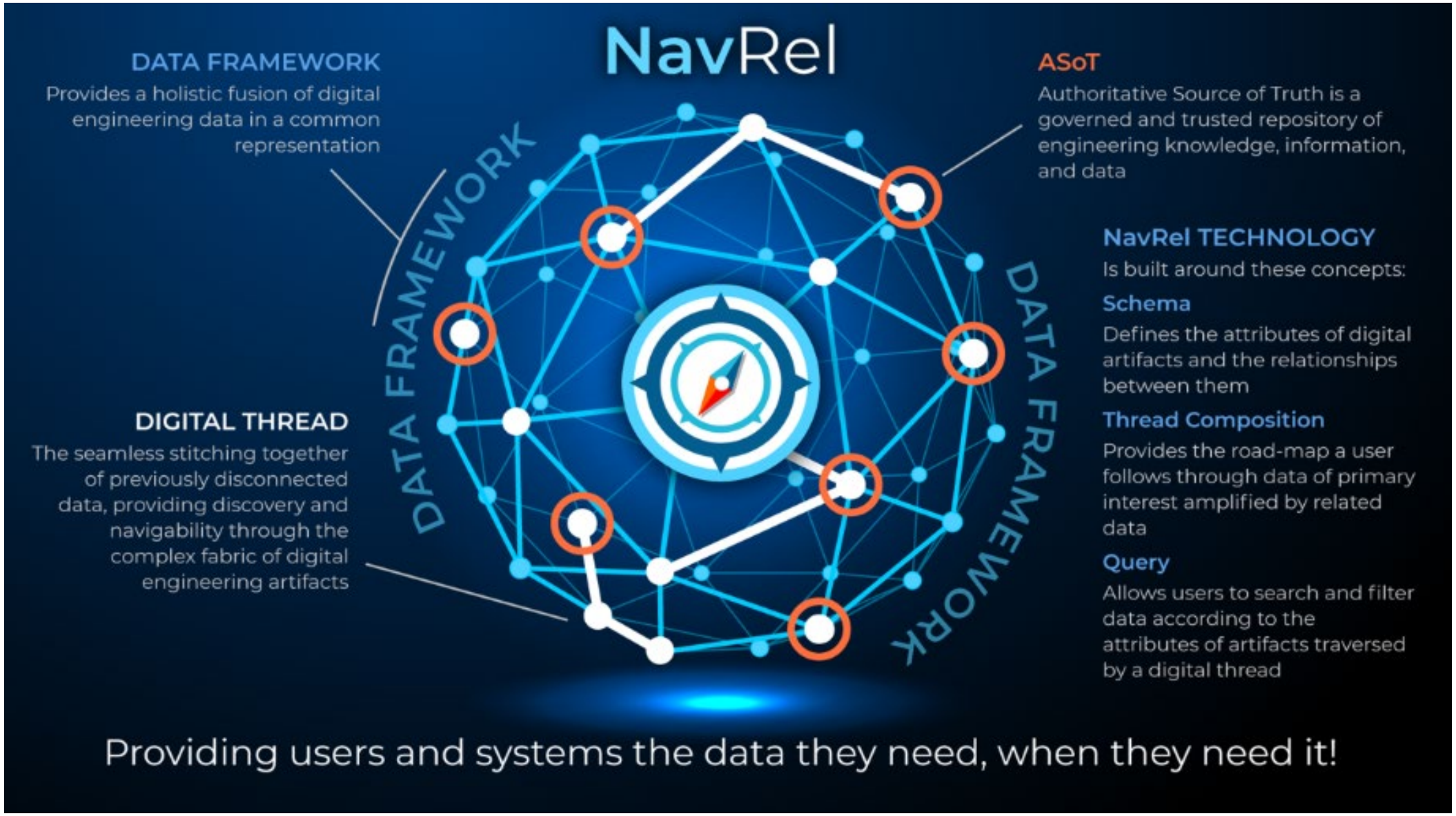
The department's five strategic goals for digital engineering are:

- Formalize the development, integration, and use of models to inform enterprise and program decision making
- Provide an enduring, authoritative source of truth
- Incorporate technological innovation to improve the engineering practice
- Establish a supporting infrastructure and environment to perform activities, collaborate and communicate across stakeholders
- Transform the culture and workforce to adopt and support digital engineering across the lifecycle

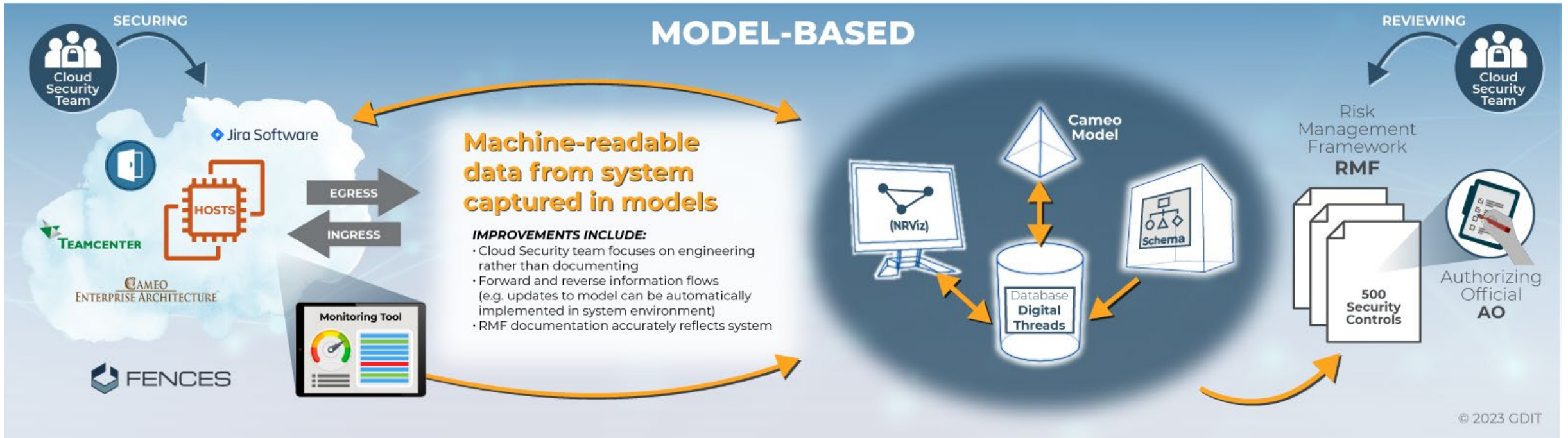
How many sources of truth exist in a single model of 1 national defense system?

(a) 1 (b) 100 (c) 1,000 (d) 1,000,000

Navigable Relationships: NavRel



Continuous Monitoring of RMF Controls



Requirements Verification

DOCUMENT BASED

Requirements Model

CAMEO ENTERPRISE ARCHITECTURE

Manually Updating a Spreadsheet

Lacks Traceability!

OTHER CHALLENGES INCLUDED:
- Lacks version control
- Inefficiency in meetings
- Disparate data types and fields
- No digital navigability to source
- Unreliable Quality of information

Agile Lifecycle Management Tool

Jira Software

NAVREL ENABLED

Requirements Model

CAMEO ENTERPRISE ARCHITECTURE

Navigable Relationships Visualization Tool (NRViz)

Req'ts | Tasks

FILTER

UPDATE

Schema

Database Digital Threads

AUTOMATED TRACEABILITY!

IMPROVEMENTS INCLUDED:
- Includes version control
- Efficiency in meetings
- Like data types and fields
- Digital navigability to source
- Reliable Quality of information

Agile Lifecycle Management Tool

Jira Software

A USG User performs their work by simply drawing an arrow to the Requirements within the tool, thereby *automating its traceability*.

Model-Driven Testing

MANUAL INSPECTION

Manual Inspection of Pass/Fail Result

Lacks Traceability!

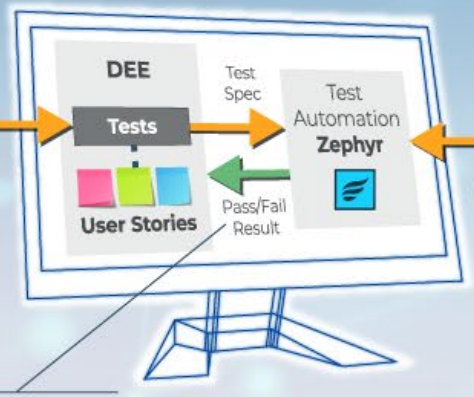
OTHER CHALLENGES INCLUDED:
- Version control
- No digital navigability to source
- Quality of information: not reliable
- Relies on human subjectivity

AUTOMATED MODEL-DRIVEN TESTING

AUTOMATED TRACEABILITY!

IMPROVEMENTS INCLUDED:
- Includes version control
- Digital navigability to source
- Reliable Quality of information
- No human subjectivity

TEST SPECS



TESTS USApp

This is an *automated pass / fail result* generated from the USApp that was previously done via manual inspection.

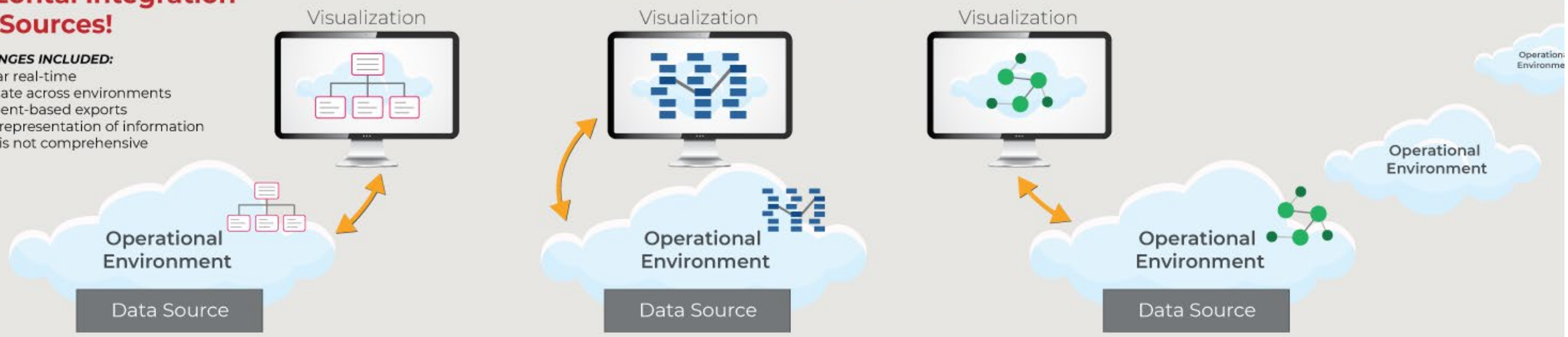
Jira Software

Common Visualization

DOCUMENT-BASED

No Horizontal Integration of Data Sources!

OTHER CHALLENGES INCLUDED:
- Often not near real-time
- Cannot simulate across environments
- Often document-based exports
- No common representation of information
- Visualization is not comprehensive

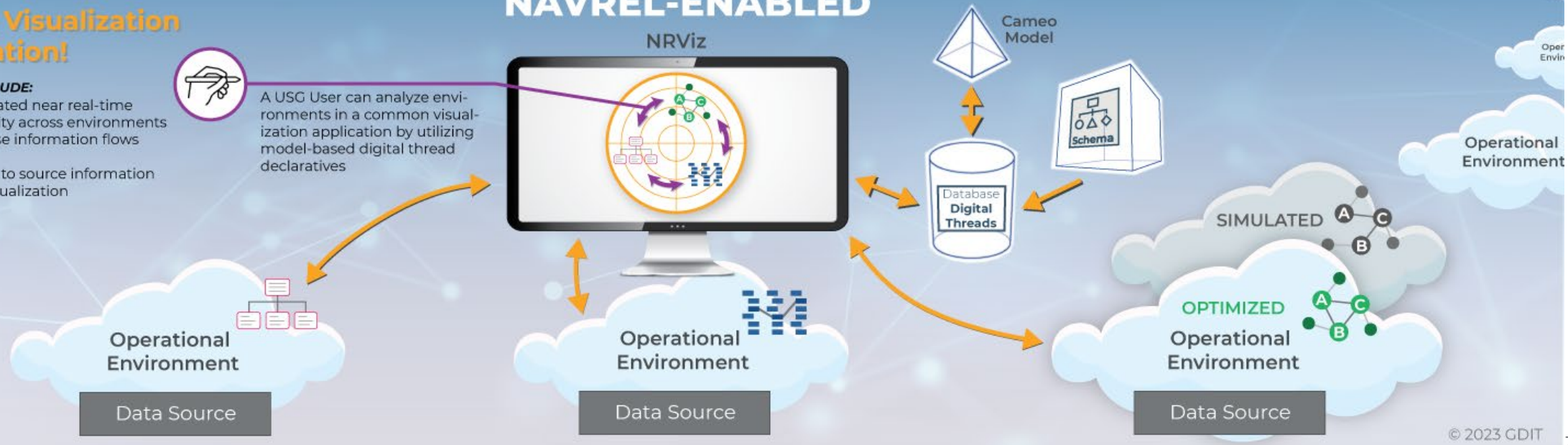


NAVREL-ENABLED

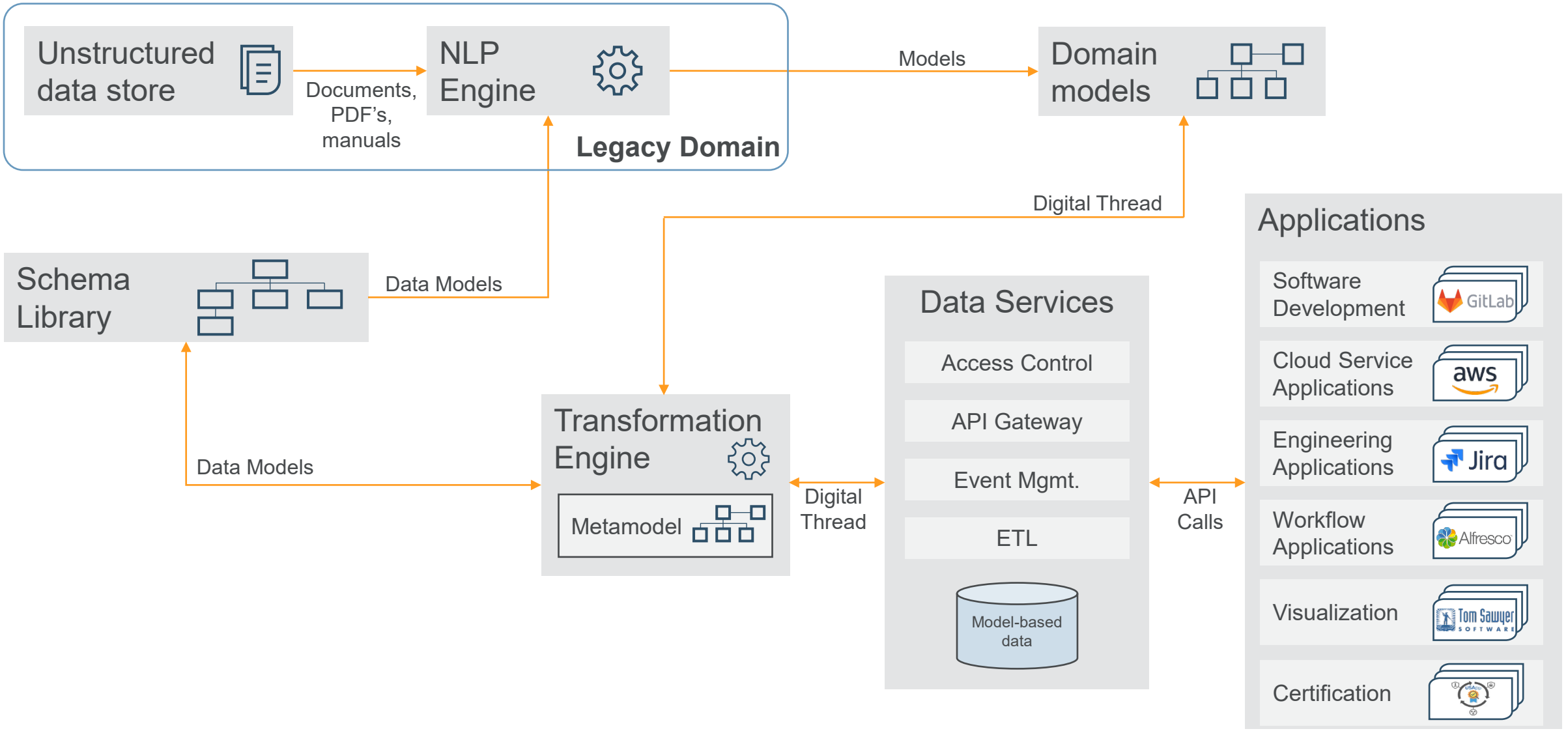
Integrated Visualization and Simulation!

IMPROVEMENTS INCLUDE:
- Data changes updated near real-time
- Simulation capability across environments
- Forward and reverse information flows
- Version control
- Digital navigability to source information
- Comprehensive visualization

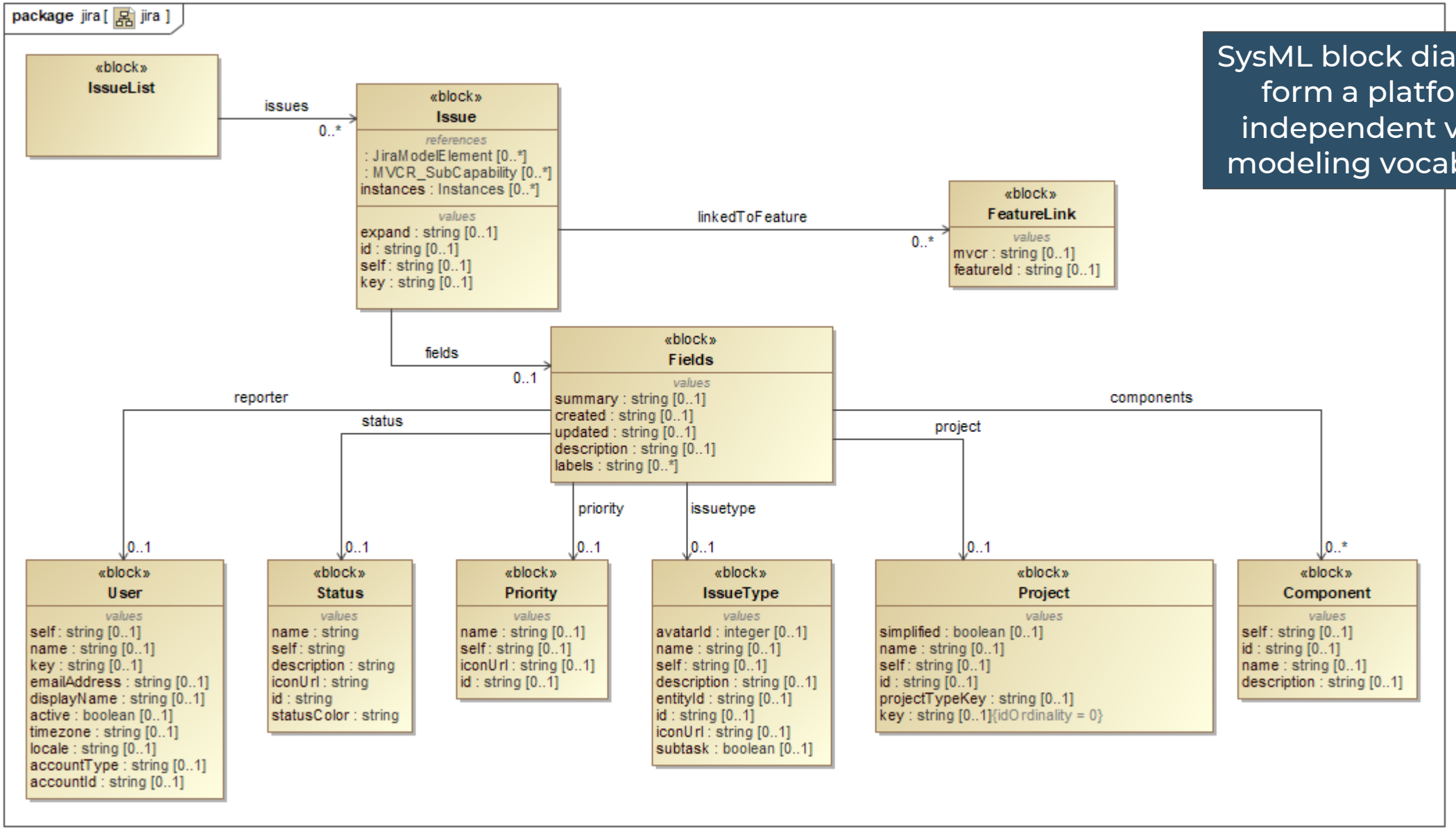
A USG User can analyze environments in a common visualization application by utilizing model-based digital thread declaratives



Navigable Relationships OV-2



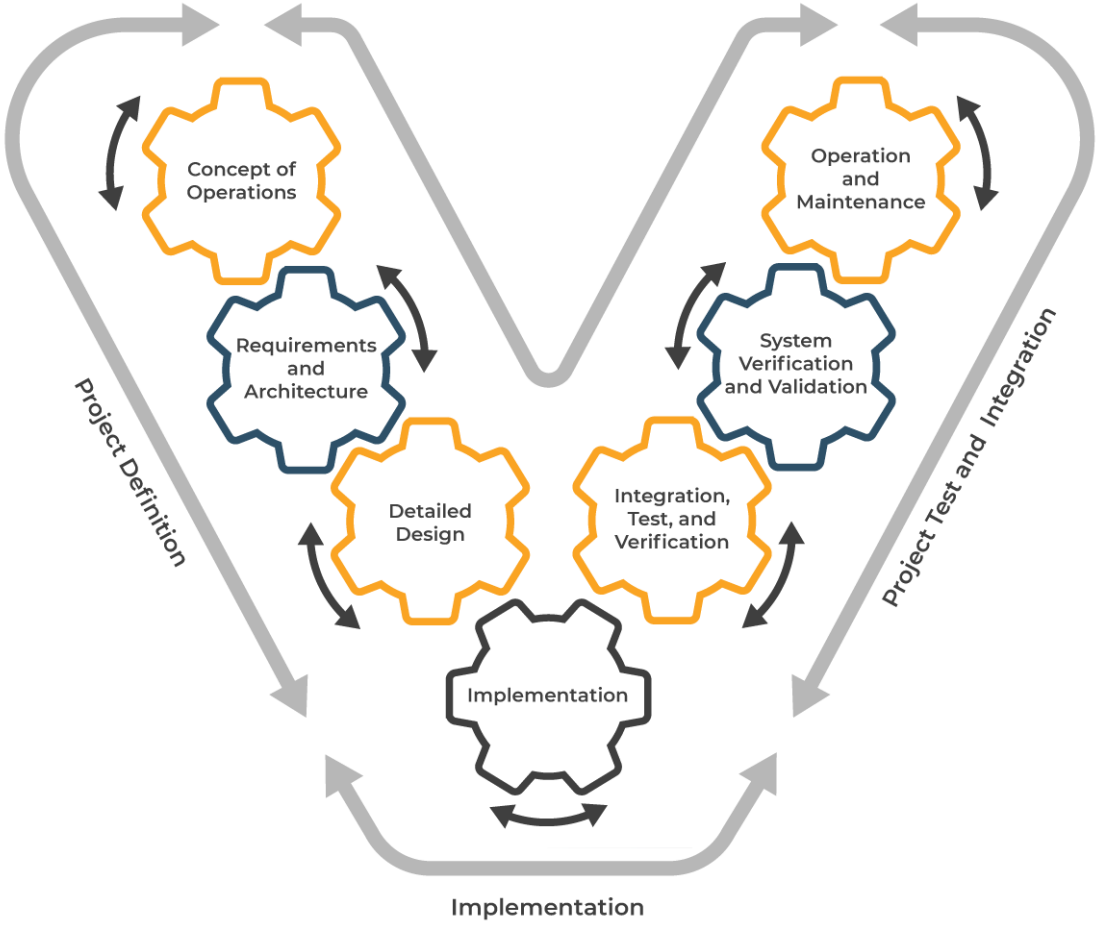
Schema Declarative : Jira example



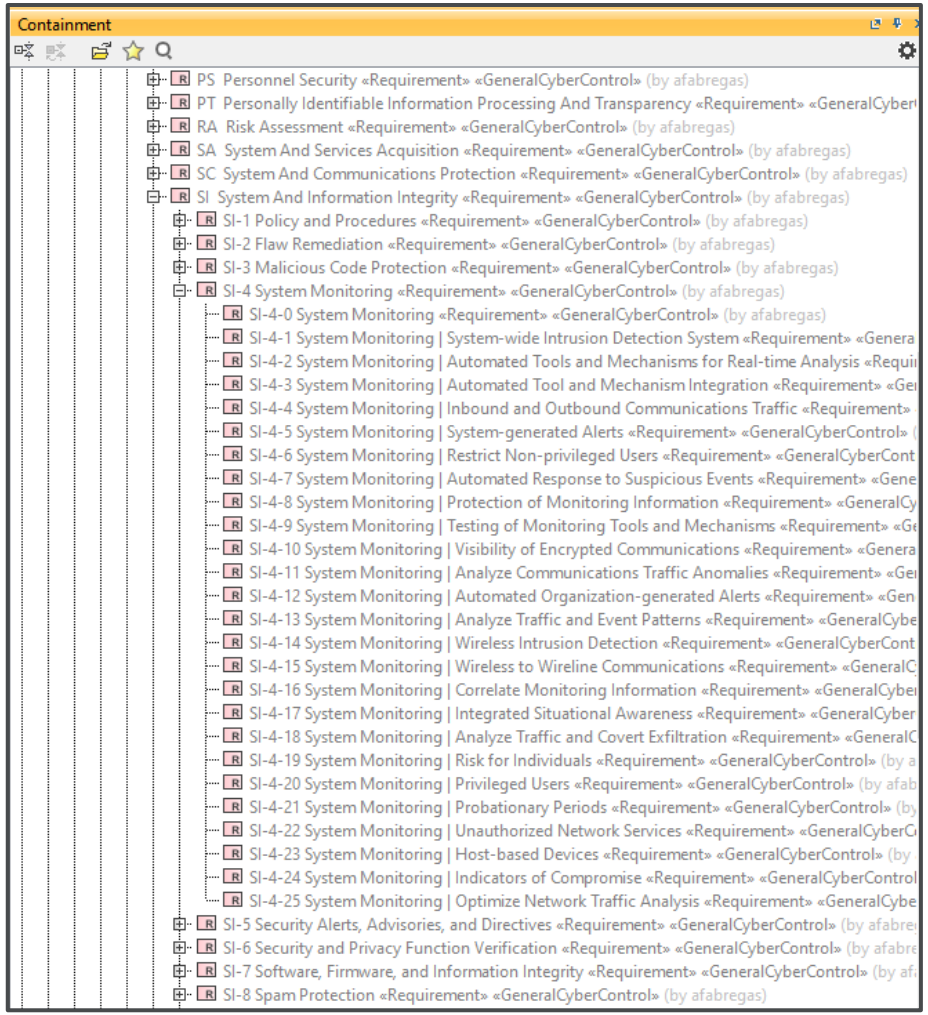
SysML block diagrams form a platform-independent visual modeling vocabulary

Cybersecurity / c-ATO demonstration

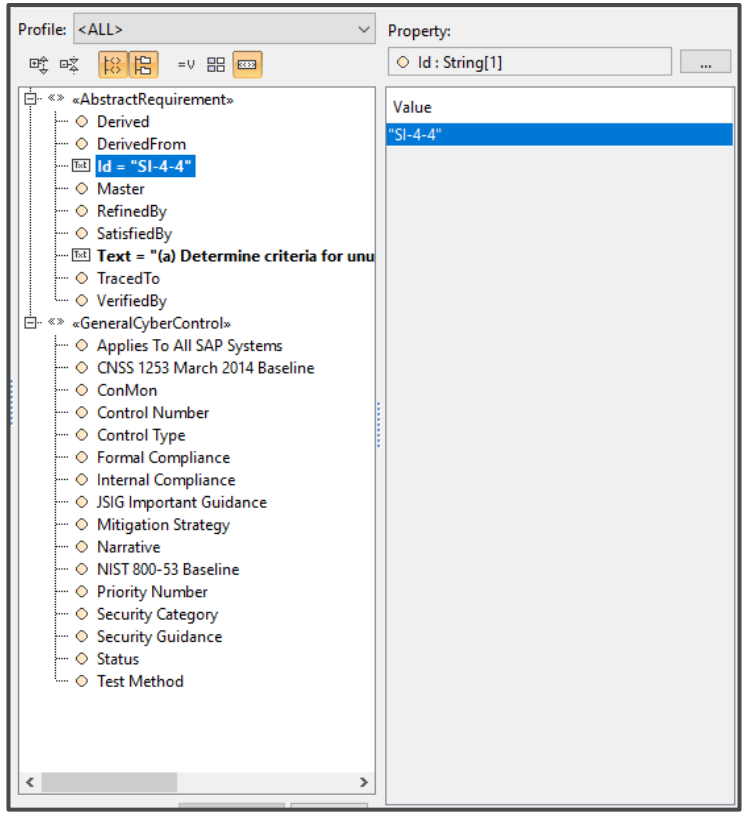
- Model-based cyber control family library
- Logical modeling of cyber controls
- System requirements
- Logical Architecture
- Automated model creation from solution environment
  - Host information from cloud environment (AWS)
  - Project management information from ALM tool (Jira)
- Satisfaction of requirements with dashboard
- Platform-independent visualization



Cybersecurity / c-ATO demonstration



- Imported from NIST 800-53 standard

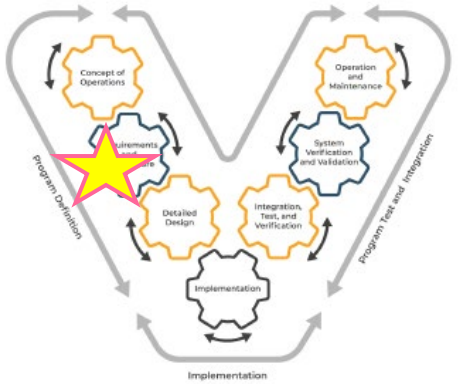


- Applied a cyber control profile to detail additional properties during system design

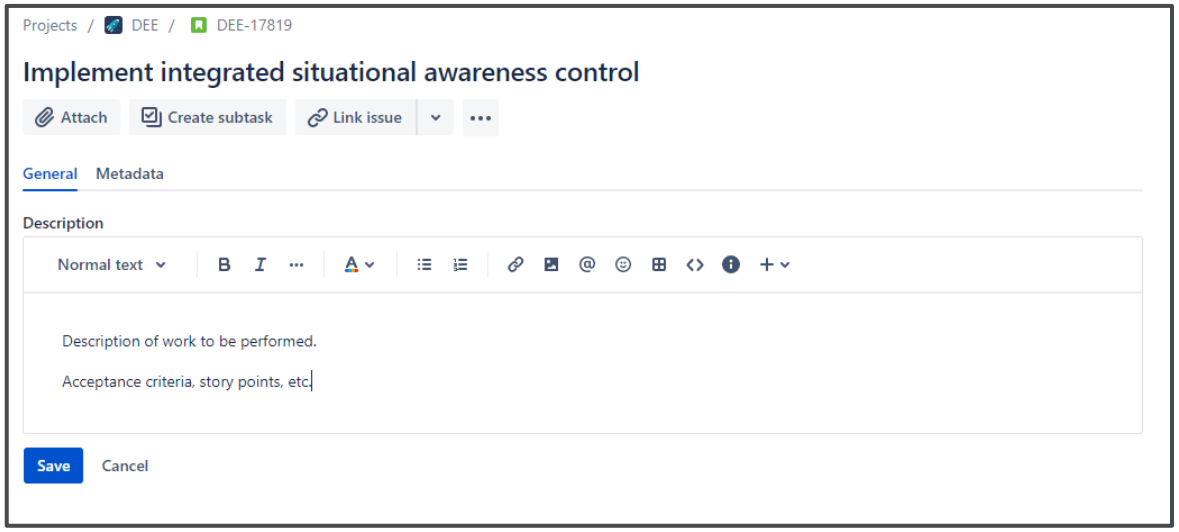
Cybersecurity / c-ATO demonstration

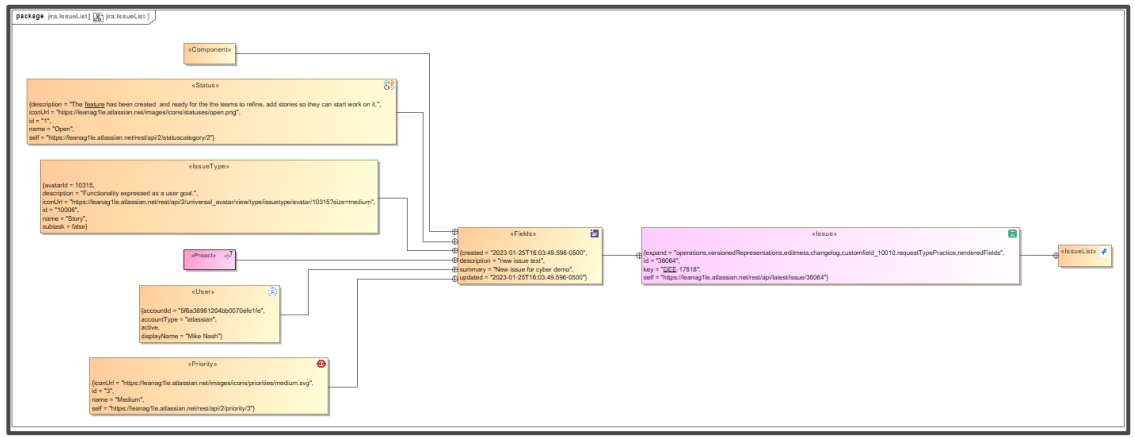
#	Id	Name	Text	Status	Control Type	Priority Number
1	18.1	System Monitoring | Probationary Periods	Implement the following additional monitoring of individuals during [Assignment: organization-defined probationary period]: [Assignment: organization-defined additional monitoring].	Planned	Process	P1
2	18.2	System Monitoring | Wireless to Wireline Communications	Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	Tailored-Out	Technology	P1
3	18.3	System Monitoring | Automated Organization-generated Alerts	Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].	Planned	Technology	P2
4	18.4	System Monitoring | Restrict Non-privileged Users	Withdrawn: incorporated into AC-6(10).	Tailored-Out	Technology	P3
5	18.5	System Monitoring | System-Generated Alerts	Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].	Planned	Technology	P1
6	18.6	System Monitoring | Integrated Situational Awareness	Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.	Planned	Technology	P1

- System design-time considerations applied to the cyber controls model
  - System categorization
  - Control applicability
  - Implementation type
  - Prioritization



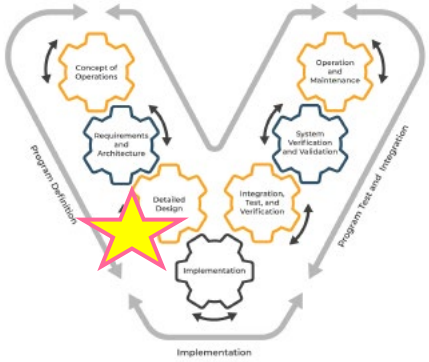
Cybersecurity / c-ATO demonstration



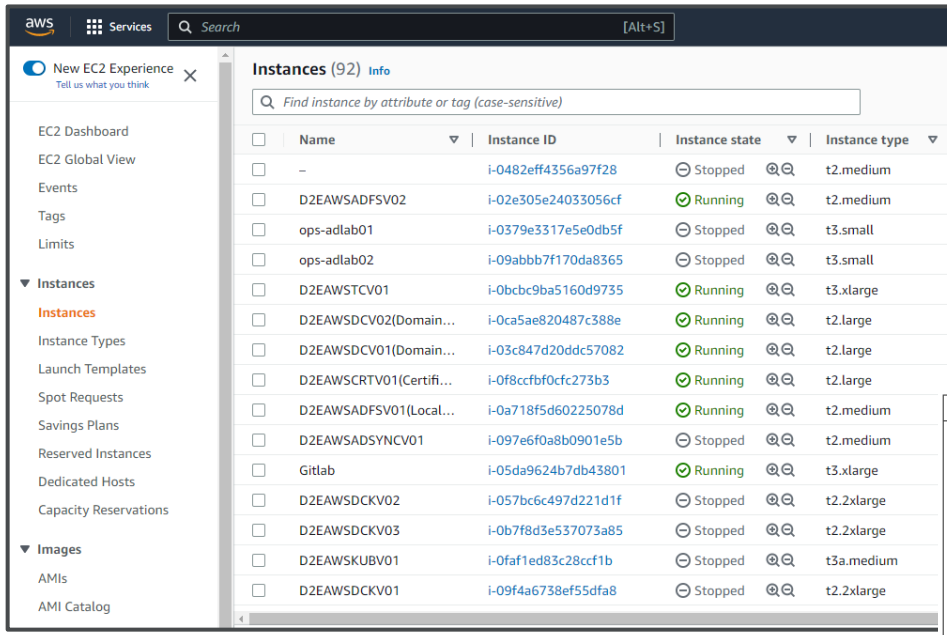


- Automated model-based representation of design

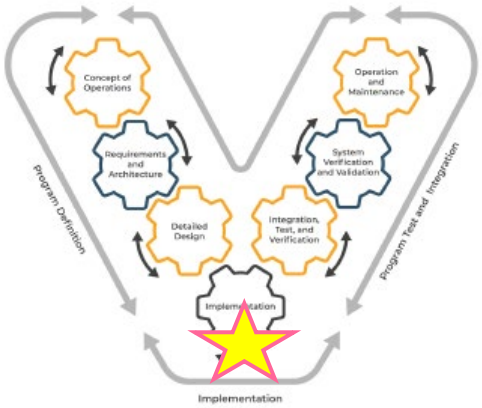
- Begin implementation of system to address control(s)
  - Who will perform the work?
  - Description of work to be performed
  - When will it be performed?
  - Status of work to be performed

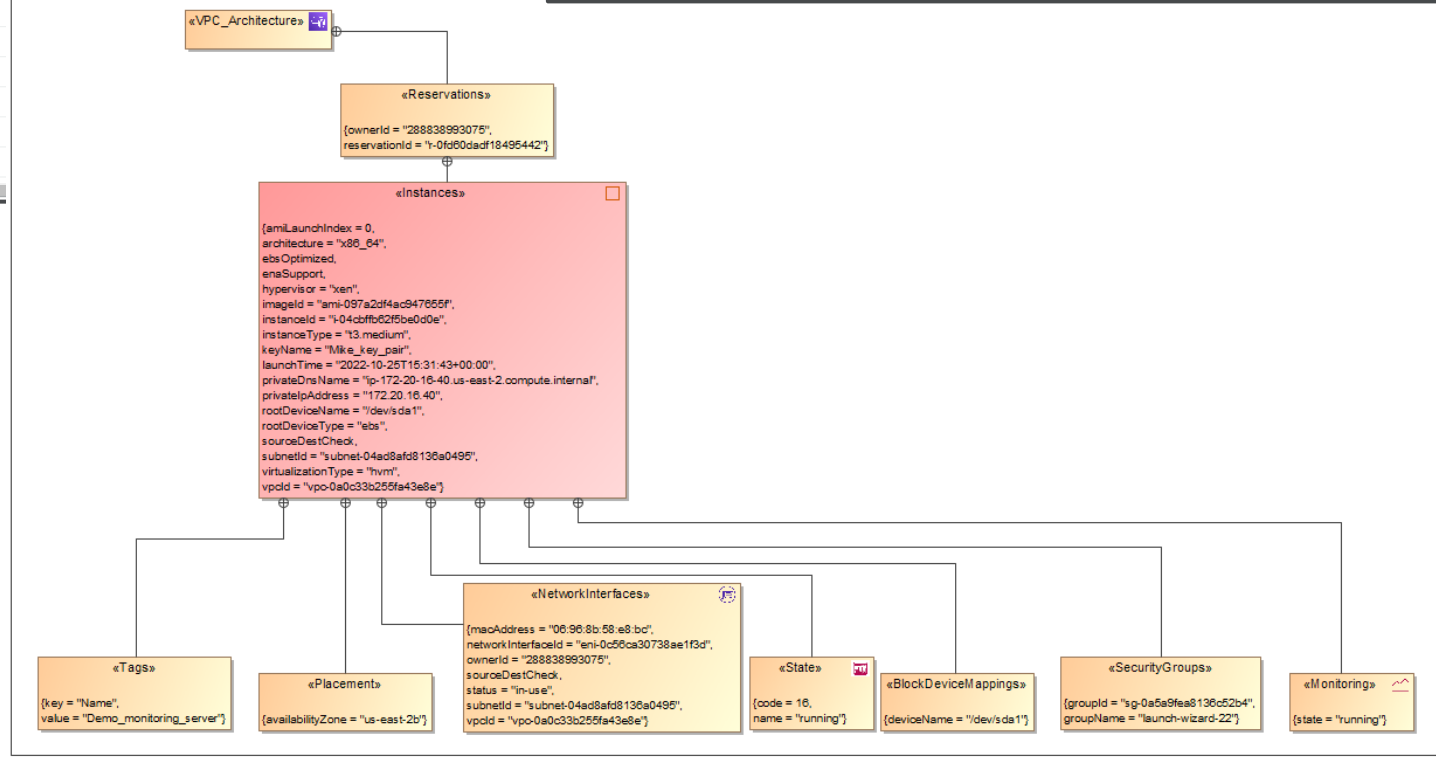


Cybersecurity / c-ATO demonstration

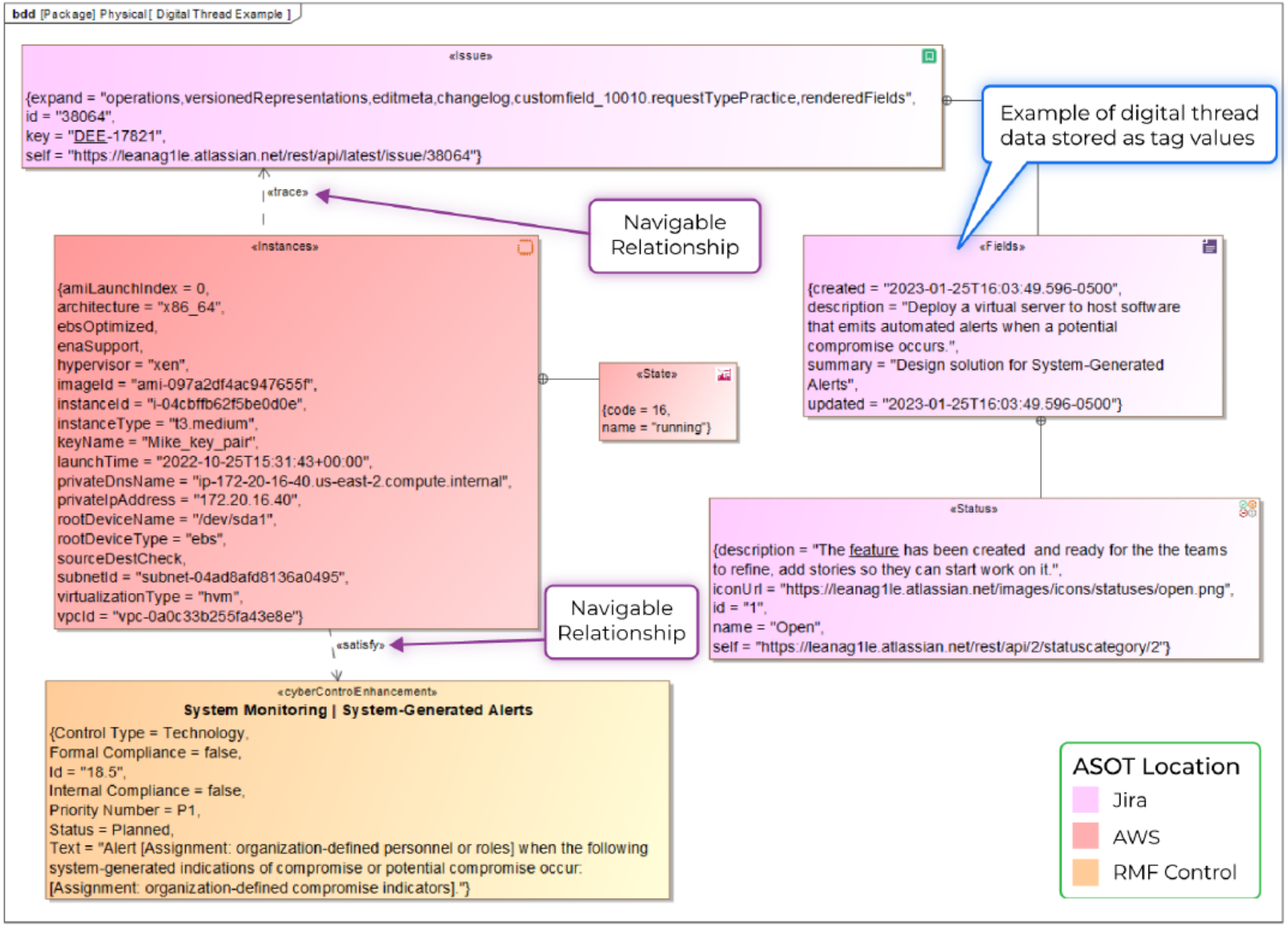


- Solution implementation
  - EC2 instance deployed to address specific control
  - Automated model-based representation of solution



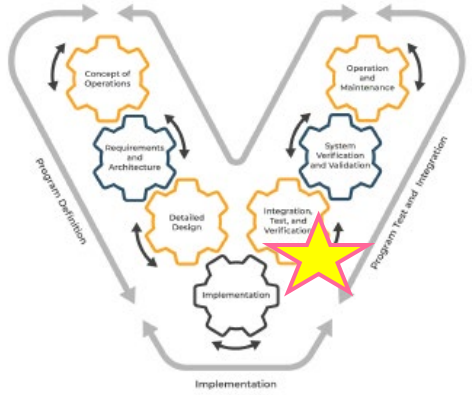


Cybersecurity / c-ATO demonstration



Composed digital thread

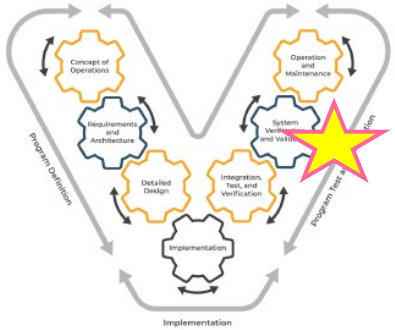
- Requirements
- Design
- Solution



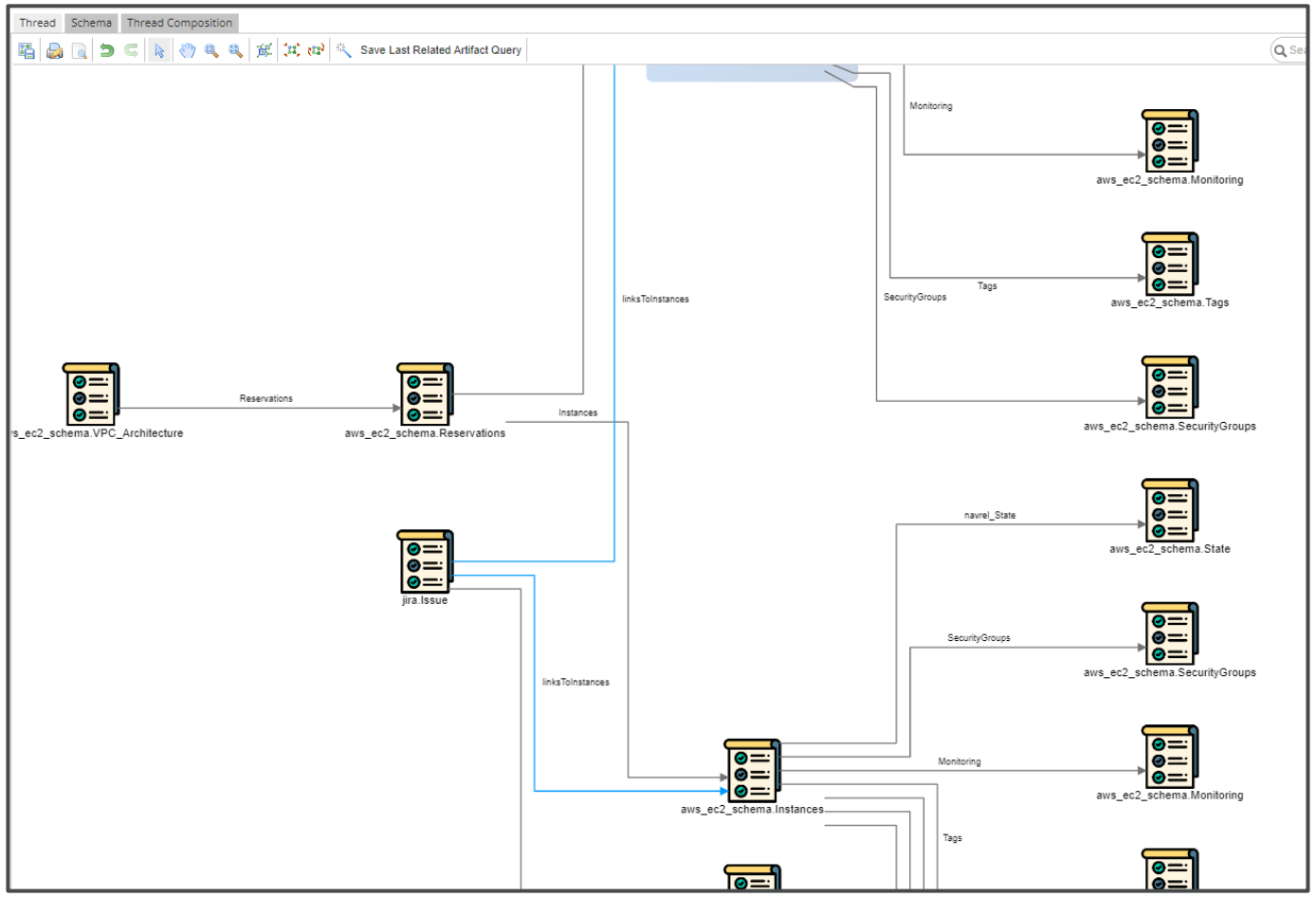
Cybersecurity / c-ATO demonstration

#	Id	Name	Text	Status	Control Type	Priority Number	Control Satisfied	Host State	Jira Link	AWS EC2 Link
1	18.5	System Monitoring | System-Generated Alerts	Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].	Planned	Technology	P1	☑ true	running	https://leanag1le.atlassian.net/browse/DEE-17818	https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#Instances:
2	18.1	System Monitoring | Probationary Periods	Implement the following additional monitoring of individuals during [Assignment: organization-defined probationary period]: [Assignment: organization-defined additional monitoring].	Planned	Process	P1	☐ false			
3	18.2	System Monitoring | Wireless to Wireline Communications	Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	Tailored-Out	Technology	P1	☐ false			
4	18.3	System Monitoring | Automated Organization-generated Alerts	Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].	Planned	Technology	P2	☐ false			
5	18.4	System Monitoring | Restrict Non-privileged Users	Withdrawn: incorporated into AC-6(10).	Tailored-Out	Technology	P3	☐ false			
6	18.6	System Monitoring | Integrated Situational Awareness	Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.	Planned	Technology	P1	☐ false			

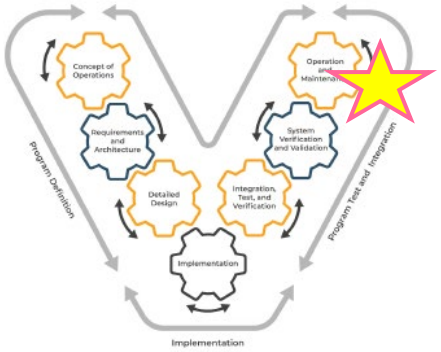
- Cyber control dashboard with navigable relationships to design and solution
  - Dynamic satisfaction of controls according to state of solution (“running”)
  - Hyperlinks to sources of truth for related artifacts



Cybersecurity/c-ATO demonstration



- Visualization of cyber thread outside of modeling tool for stakeholder analysis, monitoring



GENERAL DYNAMICS
Information Technology

Mike Nash
Solutions Director, Digital Engineering
mike.nash@gdit.com