Summary of Ongoing Cyber Analytic Landscape (CAL) Task

25th Annual Systems & Mission Engineering Conference

Sarah Standard
Cybersecurity/Interoperability Technical Director
OUSD R&E, ED,DTE&A
MC Suite 16F09-02

Washington, DC
2 November 2022

Outline

- Introduction
- Background
- Approach and Data Collection
- Observations and Findings
- Synthesizing from the Observations and Findings
- Looking Ahead

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Introduction

- **DoD is more dependent on cyber-enabled systems than ever**
  - Stakes are very high
- **DTE&A Area of Emphasis: Shift cyber testing earlier in program development**
  - Integrated throughout acquisition life cycle
  - Cyber Analytic Tools - Increase applicability, efficiency, effectiveness, accuracy, objectivity, and repeatability across the T&E continuum
- **Cyber Analytic Landscape (CAL) Initiative – 2 year effort**
  - Characterize the state of the "cyber analytic landscape"
    - Identify test-relevant analytic questions and related analytics
    - Determine analytic utility to questions, validation status, data needs, integrability
    - Identify gaps (e.g., missing questions, analytics)
    - Hold workshops along way to work through key issues
    - Catalog analytic techniques
  - **Out-of-Scope**: exhaustive coverage of analytics

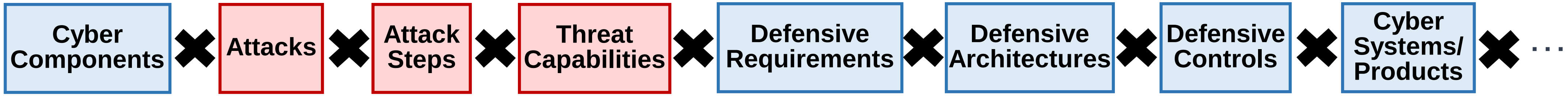
> ***"Nearly every warfighting and business capability is now software-defined. Simply put, the system – plane, ship, vehicle, radio, operations center, missile, satellite, health records management – doesn't work if the software doesn't work."***
>
> **DOT&E 2020 Annual Report**

Advocate for validated, repeatable analytics that answer test-relevant questions

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Humans Involvement with Cyber Analysis and Test

- **Cyber analysis and test is a complex space**



Cyber Components ✖ Attacks ✖ Attack Steps ✖ Threat Capabilities ✖ Defensive Requirements ✖ Defensive Architectures ✖ Defensive Controls ✖ Cyber Systems/ Products ✖ . . .

- **Historically systems-level cyber analysis/test has been manually intensive**

Problem: Humans are slow, expensive, and inconsistent

> *The [cyber risk] results indicate that the consensus of the raters is too low for the assessment results to provide a sound basis for decisions.*

Hallberg, et al., “The Significance of Information Security Risk Assessments,” 2017

> *[We] noted a diversity of practice in the [red team] test discipline, reinforcing a need to further study the reproducibility of test results...*

M. McNeil and T. Llansó, “An Analysis of Adversarial Cyber Testing Practice.” 2020

> *Whenever you use humans as a part of your measurement procedure, you have to worry about whether the results … are reliable or consistent.*

Trochim, “Research Method knowledge Base,” 2006

What Do We Mean by “Analytic” ?

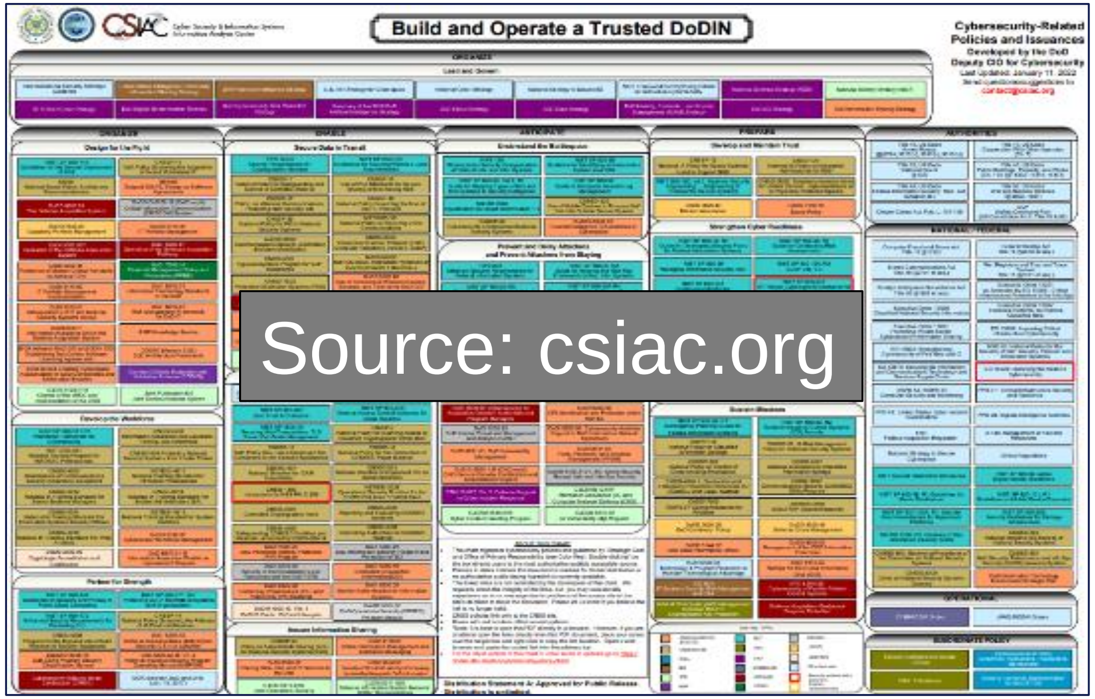
- **We mainly refer to executable analytics (but reusable data sets too)**
- **Computes some result (hopefully) of interest to security engineers and testers**
- **Examples – Compute / Identify**:
  - Cyber “Risk”
  - Cyber “Resilience” or “Survivability”
  - Attack paths
  - Vulnerabilities
  - Cyber component criticality
  - Mitigations

Ideally, Analytics Produce T&E Related ‘Objective Quality Evidence (OQE)’

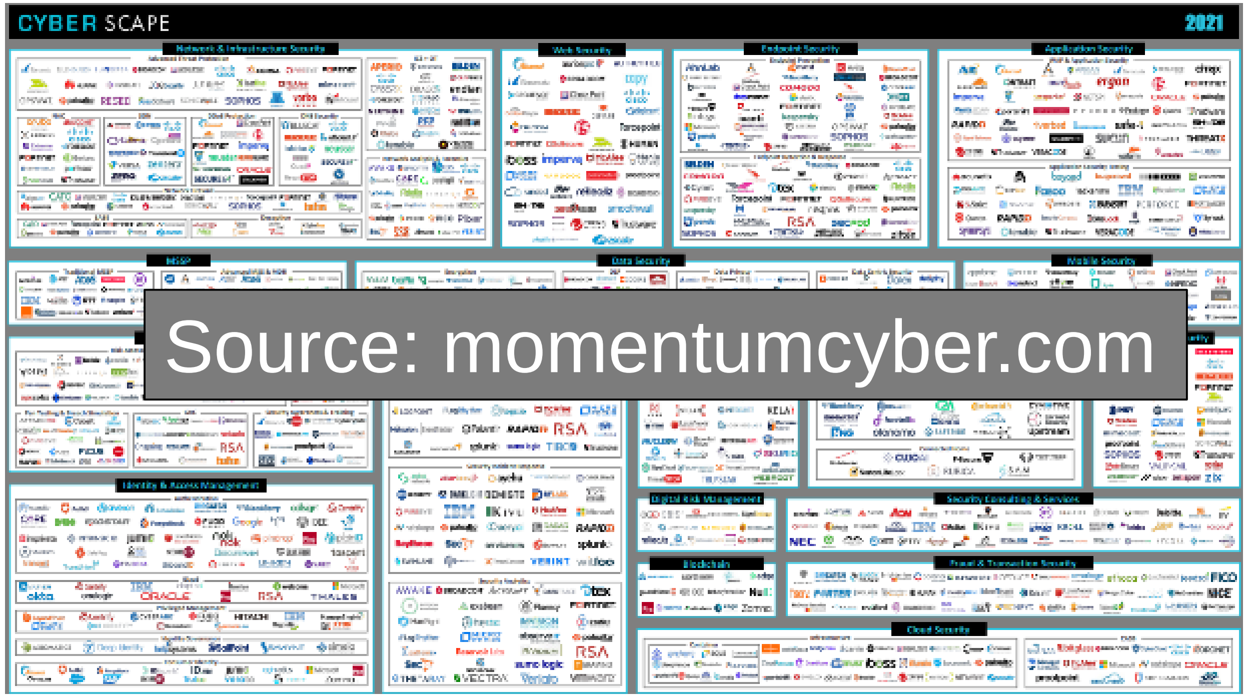
Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Community Response: Hundreds of Cyber Analytics

An increasingly crowded and chaotic space: How do we make sense of this landscape?


CSIAC
Build and Operate a Trusted DoDIN
Cybersecurity-Related Policies and Issuances Developed by the DoD Deputy CIO for Cybersecurity

Source: csiac.org



Source: momentumcyber.com

Our focus is primarily on systems-level analytics and models with test relevance

Approach and Data Collection

- **Methodology**
  - Convenience sampling approach:

Top-down	Literature review – gov’t, academic, commercial
Middle-out	Two CAL workshops
Bottoms-up	Our own knowledge, referrals

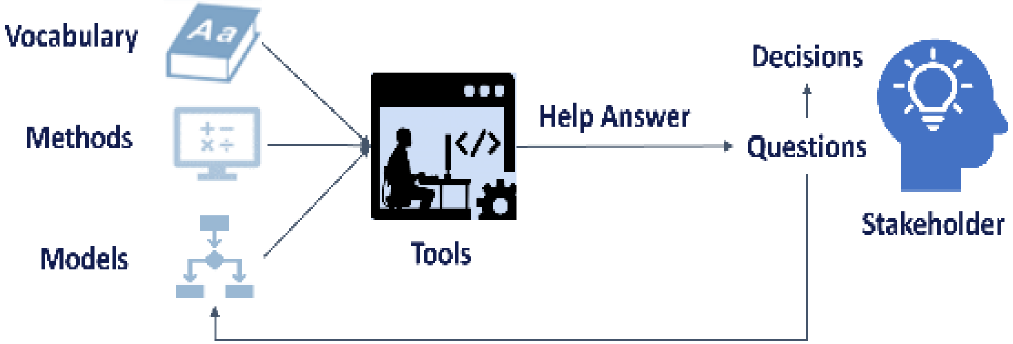
- **Data Collection**
  - Identify decision-support questions
  - For the analytics:
    - Mapping to questions above
    - Input / output data
    - Maturity / support
    - Validation status
  - Across analytics
    - Integration possibilities?
  - Model-Based Systems Engineering (MBSE)
    - Analytic data standardization for SysML models, etc.

Data Collection Stats as of September 2022

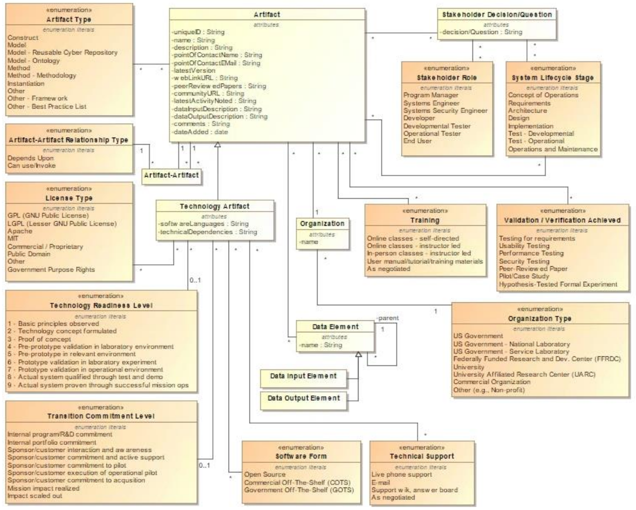
- **CAL team cataloged**:
  - 94 analytic questions in 13 categories
  - 72 representative analytics from 38 organizations
  - 119 mappings of analytics to questions
  - 59 data types tied to the analytics

FY22 Performers

JOHNS HOPKINS APPLIED PHYSICS LABORATORY   MITRE



Team developed an information capture model; data held in a relational database



«enumeration» Artifact Type
Construct
Model
Model - Reusable Cyber Repository
Model - Ontology
Method
Method - Methodology
Instantiation
Other
Other - Framework
Other - Best Practice List
Artifact
-uniqueID : String
-name : String
-description : String
-pointOfContactName : String
-pointOfContactEMail : String
-latestVersion
-webLinkURL : String
-peerReviewedPapers : String
-communityURL : String
-latestActivityNoted : String
-dataInputDescription : String
-dataOutputDescription : String
-comments : String
-dateAdded : date
Stakeholder Decision/Question
-decision/Question : String
«enumeration» Stakeholder Role
Program Manager
Systems Engineer
Systems Security Engineer
Developer
Developmental Tester
Operational Tester
End User
«enumeration» System Lifecycle Stage
Concept of Operations
Requirements
Architecture
Design
Implementation
Test - Developmental
Test - Operational
Operations and Maintenance
«enumeration» Artifact-Artifact Relationship Type
Depends Upon
Can use/Invoke
Artifact-Artifact
«enumeration» License Type
GPL (GNU Public License)
LGPL (Lesser GNU Public License)
Apache
MIT
Commercial / Proprietary
Public Domain
Other
Government Purpose Rights
Technology Artifact
-softwareLanguages : String
-technicalDependencies : String
Organization
-name
«enumeration» Training
Online classes - self-directed
Online classes - instructor led
In-person classes - instructor led
User manual/tutorial/training materials
As negotiated
«enumeration» Validation / Verification Achieved
Testing for requirements
Usability Testing
Performance Testing
Security Testing
Peer-Reviewed Paper
Pilot/Case Study
Hypothesis-Tested Formal Experiment
«enumeration» Technology Readiness Level
1 - Basic principles observed
2 - Technology concept formulated
3 - Proof of concept
4 - Pre-prototype validation in laboratory environment
5 - Pre-prototype in relevant environment
6 - Prototype validation in laboratory experiment
7 - Prototype validation in operational environment
8 - Actual system qualified through test and demo
9 - Actual system proven through successful mission ops
Data Element
-name : String
-parent
Data Input Element
Data Output Element
«enumeration» Organization Type
US Government
US Government - National Laboratory
US Government - Service Laboratory
Federally Funded Research and Dev. Center (FFRDC)
University
University Affiliated Research Center (UARC)
Commercial Organization
Other (e.g., Non-profit)
«enumeration» Transition Commitment Level
Internal program/R&D commitment
Internal portfolio commitment
Sponsor/customer interaction and awareness
Sponsor/customer commitment and active support
Sponsor/customer commitment to pilot
Sponsor/customer execution of operational pilot
Sponsor/customer commitment to acqusition
Mission impact realized
Impact scaled out
«enumeration» Software Form
Open Source
Commercial Off-The-Shelf (COTS)
Government Off-The-Shelf (GOTS)
«enumeration» Technical Support
Live phone support
E-mail
Support wik, answer board
As negotiated

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Key Observations in FY22

- **Lexicon** – as a community, we struggle to agree on commonly-used terms
- **Large Number of Questions** – we’re not always sure what to ask or how to use the answers
- **Large Number of Analytics** – low barrier to entry; everyone has their own approach
- **Hypotheses** – many competing hypotheses for how systems cyber analysis/test should work
- **Human Footprint** – remains large even with analytic use
- ➡ **Analytic Validation** – almost non-existent – used mostly “on faith”
- ➡ **Key Analytic Gap** – probability cyber-enabled system will perform as required despite cyber effects
- ➡ **Analytic Techniques** – analytic “black-boxes” – method and techniques often unknown

➡**Proposed Key Areas of Focus for FY23**

Key Findings in FY22

- **Data** – obtaining detailed, accurate, repeatable data on target cyber systems for analysis is still too hard
- **Integration** – analytics tend to be stovepiped; difficult to integrate together (not designed to be integrated)
- **Human Dimension** – analytics tend to be technically focused; human side has less attention – is less mature
- **Resilience** – today’s focus on resilience is almost always technical – also need mission-impact focus

Bottom Line:

Current state of system cyber analysis/test is a reflection of the immaturity of the field (engineering has outrun the underlying science)

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Synthesizing from the Observations and Findings

We should start here - It is all ultimately about the mission

Mission

What mission planners want to know:

(1) **Probability** I'll achieve my mission? (P_m)

(2) How to improve the **probability** above?

Supporting Cyber Systems

What cyber stakeholders want to know about each contributing cyber-enabled system:

(1) **Probability** system will perform adequately given cyber threat? (P_s)

(2) How to improve the **probability** above?

Today's Chasm

Even with (unvalidated) analytic artifacts, we still have a heavy reliance on subjective human judgment

- Slow
- Expensive
- Not reproducible

Cyber Artifacts Today

We analyze what we can, but don't validate the approaches

Threat actors?

Threat capabilities?

Risk?

Attack paths?

Criticality?

Dependency?

Vulnerabilities?

Resilience?

Mitigations?

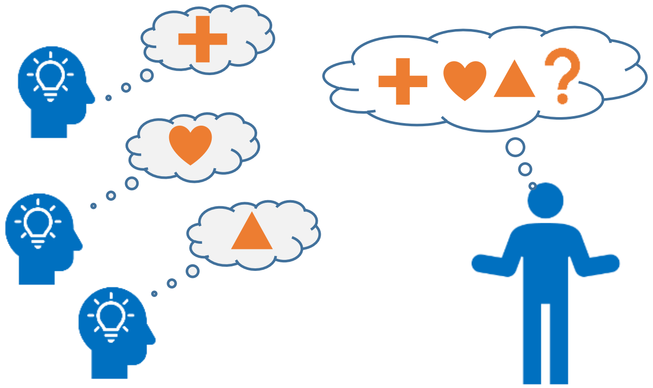
We want to be here

Today we are here

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

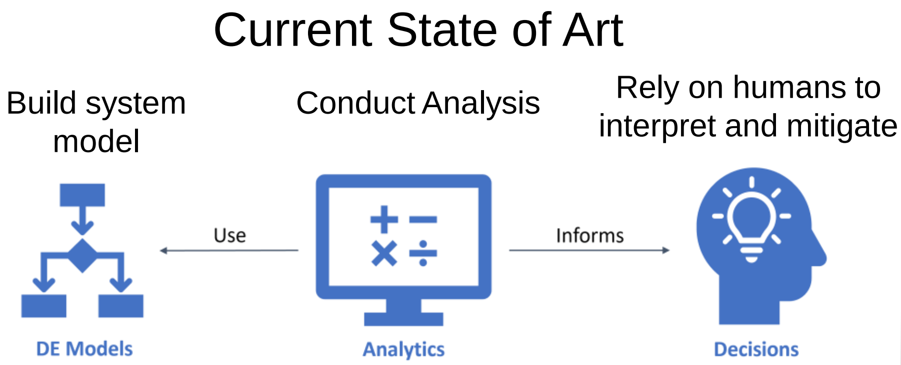
Summary of Current State of Systems Cyber Analysis and Related Challenges

Lack of an established foundation



- Varying Jargons
- Many Competing Hypotheses
- Incompatible Methods
- Unvalidated Data Sets
- Segregated Technologies

Immature cyberspace analytic processes



Current State of Art

Build system model

Conduct Analysis

Rely on humans to interpret and mitigate

- Heavy Dependence on Human Input
- Nonrepeatable Processes
- Unknown Results Accuracy
- Slow Analysis

Creation of tools looking for problems

NO MATTER HOW MUCH EFFORT YOU PUT IN
IF YOU USE THE WRONG TOOLS, YOU WON'T MAKE IT

- Lack of Rigorous Validation
- Potential False Sense of Security
- Wasted Cost/Schedule/Resources
- Frustrated Stakeholders

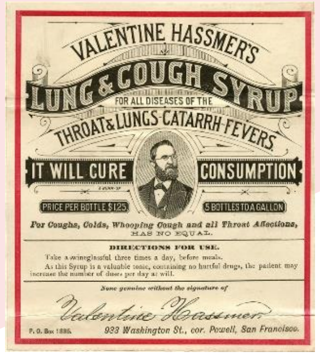
Long Term CAL Vision

Starting Place

- Varying Jargons
- Many Competing Hypotheses
- Incompatible Methods
- Unvalidated Data Sets
- Segregated Technologies

- Heavy Dependence on Human Input
- Nonrepeatable Processes
- Unknown Results Accuracy
- Slow Analysis

- Lack of Rigorous Validation
- Potential False Sense of Security
- Wasted Cost/Schedule/Resources
- Frustrated Stakeholders



VALENTINE HASSMER'S
LUNG & COUGH SYRUP
FOR ALL DISEASES OF THE
THROAT & LUNGS-CATARRH-FEVERS
IT WILL CURE CONSUMPTION
PRICE PER BOTTLE $1.25
5 BOTTLES TO A GALLON

For Coughs, Colds, Whooping Cough and all Throat Affections,
HAS NO EQUAL.

DIRECTIONS FOR USE.

Take a wineglassful three times a day, before meals.

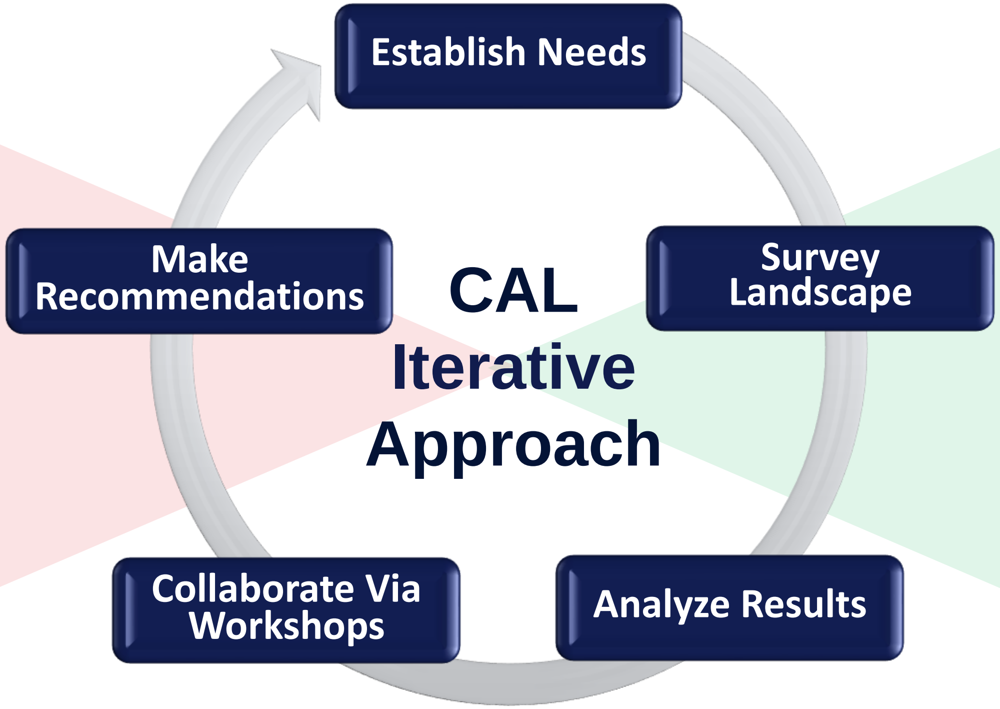
As this Syrup is a valuable tonic, containing no hurtful drugs, the patient may increase the number of doses per day at will.

None genuine without the signature of

Valentine Hassmer

P. O. Box 1886. *933 Washington St., cor. Powell, San Francisco.*

Might be Good,
No Way to Know



Establish Needs

Survey Landscape

Analyze Results

Collaborate Via Workshops

Make Recommendations

CAL Iterative Approach

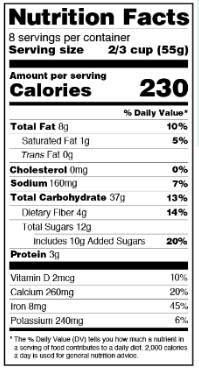
Moving the landscape towards

Strategic Vision

- Consistent Vocabulary
- Well-supported Theories
- Compatible Methods
- Validated Data Sets
- Integrated Lifecycle Tools

- Reduced Human Dependence
- Repeatable Processes
- Validated Results
- Efficient Analysis

- Validated Analytics
- Increased Confidence in Security
- Reduced Cost/Schedule/Resources
- Satisfied Stakeholders



Nutrition Facts

8 servings per container

Serving size	**2/3 cup (55g)**
Amount per serving **Calories**	**230**
	% Daily Value*
Total Fat 8g	**10%**
Saturated Fat 1g	**5%**
Trans Fat 0g	
Cholesterol 0mg	**0%**
Sodium 160mg	**7%**
Total Carbohydrate 37g	**13%**
Dietary Fiber 4g	**14%**
Total Sugars 12g	
Includes 10g Added Sugars	**20%**
Protein 3g	
Vitamin D 2mcg	10%
Calcium 260mg	20%
Iron 8mg	45%
Potassium 240mg	6%

* The % Daily Value (DV) tells you how much a nutrient in a serving of food contributes to a daily diet. 2,000 calories a day is used for general nutrition advice.

Label is
Trustworthy

Looking Ahead – Year 2

- **Analytics Methods/Techniques**
  - Document analytic methods and techniques; capture in an “Analytic Characterization Framework” (ACF)
  - Create an ACF ontology and knowledge graph to enable consistent test and evaluation
- **Analytic Validation**
  - Develop validation approaches and describe the quality of evidence they produce
  - Look at validation piloting opportunities
  - Think through the longer term policy/resourcing implications
- **Analytic Gap for Key Questions**
  - Gap: What is the probability that a cyber-enabled system will perform as required despite cyber effects?
  - Gap: What are options for raising the probability above if deemed too low?
  - Develop an analytic approach to answer the questions above
  - Consider integration opportunities and validation

Workshops in Support of Above

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Questions

sarah.m.standard.civ@mail.mil

Distribution A: Cleared for Public Release by the DoD Office of Prepublication Security Review, 29 October 2022, Case 22-S-2998

Backup

Examples of Analytic Questions

Mission	What systems support a given mission-essential task list (METL)?
	What systems are intended as backups to a given cyber-enabled system in case the cyber system fails or becomes distrusted?
Mission Probabilities	What is the probability, Pm, that my mission will succeed despite adverse cyber events in supporting cyber-enabled systems during the mission timeline?
	How do changes (e.g., systems used, dependencies) affect the probability, Pm? (see MP-1 for Pm definition)
Threat and Mitigation	What cyber threat capabilities by kill chain stage are possessed by a given type of adversary?
	Which mitigation capabilities can help defend against a given cyber threat capability?
	Which threat capabilities apply to a given cyber asset type?
System	What are the mission essential functions (MEFs) of the system under analysis?
	What are the performance metrics tied to a given MEF?
	What is the allowable range of values for each MEF performance metric?
	What are the cyber assets (components) in my system and what are their corresponding asset types?
	What cyber assets have network connectivity with other cyber assets?
	What is the impact on MEF performance of a cyber effect on a supporting cyber asset's data?
	What cyber mitigations are currently designed into the system?
	Which cyber assets benefit from which cyber mitigations?
	What is the rolled-up criticality of a cyber asset based on its support for supported MEFs?
	What is the worst-case adversary type expected for the system in a given mission context?
Adverse Cyber Events	What is the probability that a malicious attack involving a given cyber asset will occur at a given time during the mission timeline?
	What is the probability that a hardware cyber asset will physically fail at a given time during the mission timeline?
	What is the probability that an operator error will occur for a given cyber asset at a given time during the mission timeline?
	What is the probability that an undetected flaw/bug will manifest for a given cyber asset at a given time during the mission timeline?
	What is the probability that an act of God will occur for a given cyber asset at a given time during the mission timeline?
MEF Probability	What is the probability, Ps, that the performance of the mission-essential functions (MEFs) of a given cyber-enabled system will remain at or above their corresponding minimum threshold values despite adverse cyber events during a given mission timeline?
	How do changes (e.g., risk tolerance, mitigations, criticalities, budget) affect the probability, Ps? (see MEF-1 for Ps definition)
Risk and Mitigations	Which applicable adversary threat capabilities remain unmitigated for a cyber asset in my system?
	What is the risk to the system's MEFs from adverse cyber effects?
	What mitigations to cyber threat capabilities should I consider based on a set of tradespace constraints? (e.g., risk tolerance, budget)
	What is the priority of possible cyber mitigations based on a set of tradespace constraints?

Examples of Analytics/Models Reviewed

- ArcReACTOR
- Automated Vulnerability and Risk Assessment
- BluGen
- Common Attack Pattern Enumeration Classification
- Compromise Probability (stochastic model-based/attack graph-based/Bayesian attack graph-based)
- Critical Infrastructure Cyberspace Analysis Tool
- CSA Tool
- Cyber Assassin
- Cyber Operational Risk Tool
- Cyber Operations Rapid Assessment
- Cyber Security Game
- Cyber Security Modeling Language
- Cyber Vulnerability Assessment Tool
- CyberReason XDR
- Cybersecurity Figure of Merit
- CyberSpaceSuite
- D3FEND
- Dagger
- HAMLET
- Integrated Resilience Analysis Tool
- Mean Time to Failure/Compromise (MTTF & MTTC) Metric
- Meta Attack Language
- Mission Focused Cyber Hardening: Mitigation Prioritization Framework
- Mission-Based Risk Assessment Process for Cyber
- NSA Technical Cyber Threat Framework
- Ontology for Attacks in Cyber Risk Assessment
- Path length (shortest path, mean path length, number of paths)
- PRUNE
- Resilience Index Simulator
- Security, Agility, Resilience and Risk (SARR) Framework
- SOFIA, RMF/Cyber Automation
- Tabletop Mission Cyber Risk Assessment (TMCRA) Overview
- Unified Risk Assessment and Measurement System