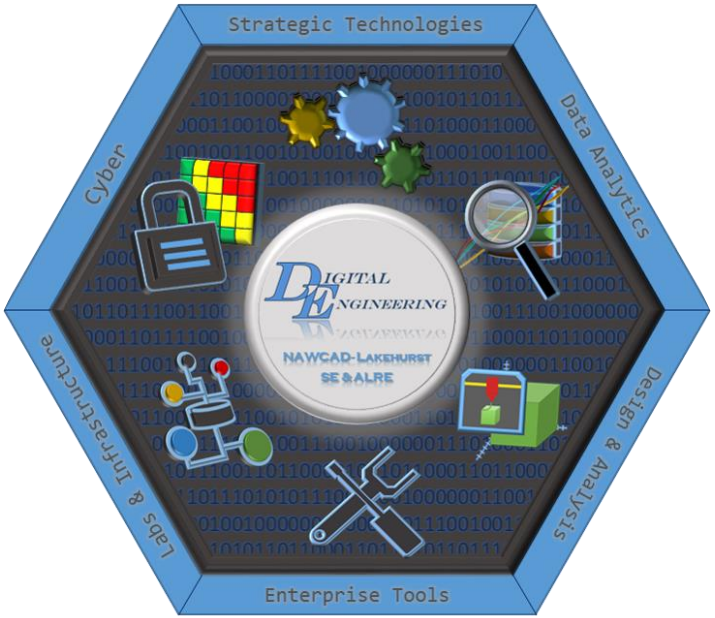


Data and Cyber Analytics

Introduction Brief

Presented by Matt Forrestal

V 0.1

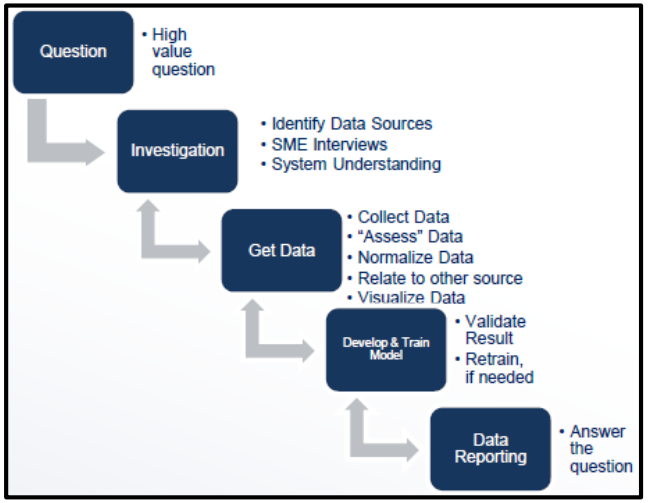
Data and Cyber Analytics Overview

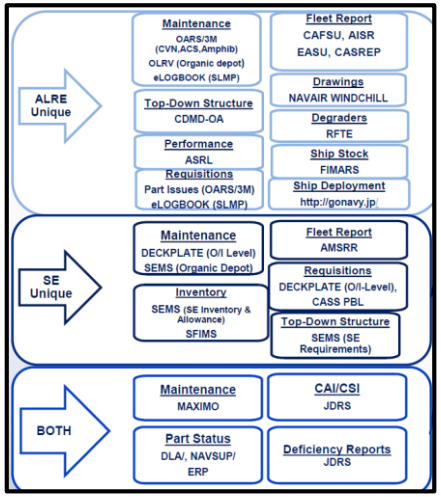
- Vision
  - Provide a unified solution for Data and Cyber Analytics, encompassing everything from Data Science to Visualization. Integrating Cyber Risk Assessments (CRAs), Cyber - Supply Chain Risk Management (C-SCRM) and continuous high level trend analysis. Providing incident response forensics and analytics.
- Mandate
  - Providing robust Data Analytics capabilities to customers. Allowing forecasting and trend analysis that help identify where resources are most effective. Broadening our scope with the intention of pairing SE and ALRE data with platform data.
  - Integration of Cyber Analytics, synthesizing the individual Cyber Analytics components we are responsible for into a robust Security Analytics capability.

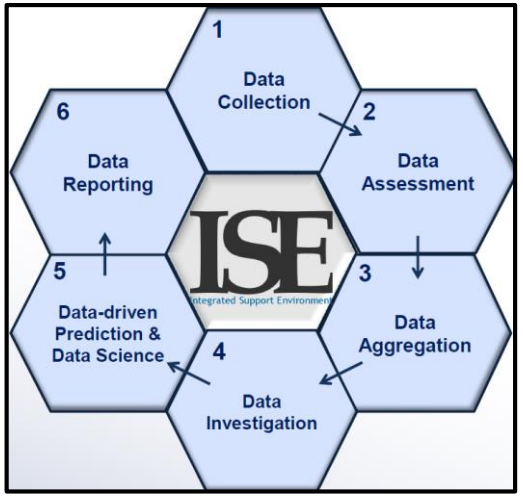
Data and Cyber Analytics Overview

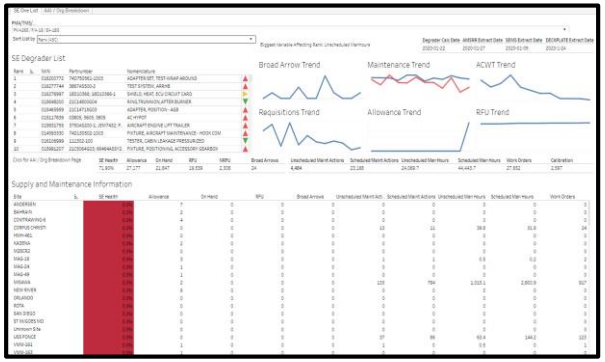
- Focus Areas
  - Data Analytics
    - Integrated Support Environment (ISE): The primary Data Analytics system used for Support Equipment (SE) and Aircraft Launch and Recovery Equipment (ALRE)
    - Digital transformation through Enterprise metrics: Supporting process re-engineering with robust metrics and analytics capabilities.
  - Cybersecurity
    - Cyber Supply Chain Risk Management (C-SCRM): Ensure that the supply chain for items identified as cyber is secure. Protect the cyber components of the supply chain.
    - Incident Response: Using cybersecurity and forensic skills to provide a robust response to cyber incidents.
    - Cyber Analytics: Planning tools to help evaluate, understand, and remediate cyber risk.

ISE









ISE
Integrated Support Environment

Projects:

1. **Dashboards/Metrics**
   - **One List**
   - **Customized dashboards**
2. **Data Science Research (NISE & S&T Funded)**
   - **Data Driven Obsolescence Discovery**
   - **Value of SE for A/C Readiness**

ISE

Products:

1. **Dashboards/Metrics**
   - One List
     - Support Equipment (in Production)
     - ALRE (March 2020)
   - Customized dashboards (Example dashboards only)
     - ALRE
       - CPC (Cockpit Chart)
       - Quad Chart providing information about cost degraders
       - Biggest Increase (compare current quarter against 3 previous month average)
       - Line Of Balance (DLA)
     - SE
       - CPC (PMA260)
       - CASS (PMA260D) Quad Chart
       - Automated Deep Dive Report (PMA260)
       - CPC (PSE)
2. **Data Science Research (NISE & S&T Funded)**
   - Data Driven Obsolescence Discovery (FY20)
   - Value of SE for A/C Readiness (FY20)
   - Text Mining of MAFs (PMA251 – Production)
   - One List Ranking (SE – Production)

ISE
Integrated Support Environment

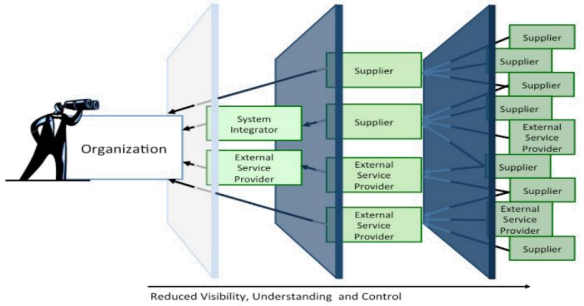
Cybersecurity

- C-SCRM
  - Assist ALRE/SE programs in understanding, mitigating and managing their supply chain risk.
  - SCRM Lab – Utilize existing capabilities such as X-Ray, Circuit Card testing, Penetration Testing, CT Scan and EMI to perform testing on products.
- Incident Response
  - Development of Incident Response Plans for ALRE/SE systems.
  - Assist in Incident Response activities.
  - Expand integrated capabilities across the NAVAIR Enterprise.
- Cyber Analytics
  - Performing Cyber Risk Assessments (CRA) and Tabletops (CTT) on ALRE/SE systems.
  - Aggregation of ALRE/SE SCRM, IR, and CRA/CTT data for data analysis.

Lakehurst SCRM Capability Overview

Supply Chain Risk Assessment (SCRA)

- Illumination – identify vendors, packaging/testing/shipping details, revenues, program use, etc.
- Threat Analysis – identify vendor incidents, foreign ties, regional stability, etc.
- Component Inspection – verify component via X-ray, integrated circuit, and/or pentest inspection



Supply Chain Risk Management Plan

- Baseline - assess how NIST SA-12 controls are used, document controls listed as N/A
- Application - review requirements to implement to satisfy missing controls
- Reassessment - set periodicity of control re-evaluation on annual basis, per ECP, as needed, etc.

Supply Chain Risk Management Reporting Tool

- Capture results of all SCRAs and SCRM Plans
- Feed data from external sources
- Aggregate and analyze isolated datasets for unknown cyber issues

Cyber Analytics

Cyber Tabletop

- Low technology, low cost, intellectually intensive exercise to introduce and explore the effects of cyber offensive operations on the capability of a System

Cyber Risk Assessment

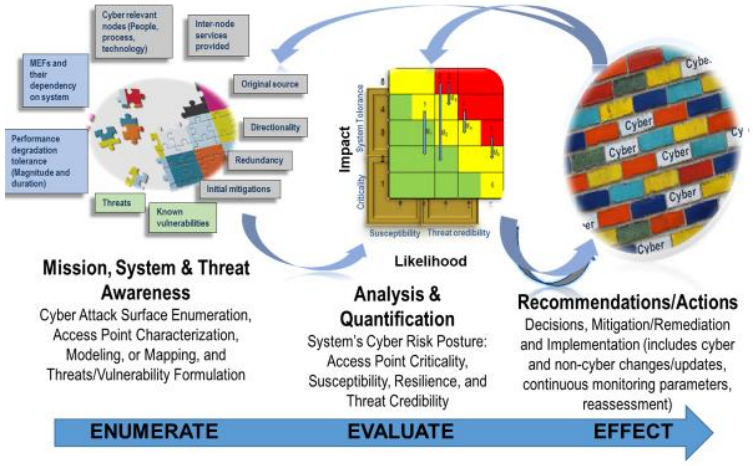
- In depth approach to evaluate the susceptibilities and attacks that could result in impacts and quantify probability of occurrence

Model Based

- Utilize mission, system, and threat modeling software tools to support risk assessments and engineering analysis

Cyber Analytics

- Use CTT/CRA aggregated data to establish cyber risk trends in acquisition and development
  - Model software to augment manual CRA process
  - Highlight potential improvement areas during acquisition cycle; concept development, design maturation, production deployment, and sustainment



Support Needs

- People
  - Data scientists have strong backgrounds in mathematics and usually some programming abilities. They evaluate data and use techniques such as various forms of regression analysis and tools such as Python and R to develop models to transform data into useful, actionable information.
  - Computer scientists who work in Data Science have some understanding of the objectives of Data Science. They are able to help develop programing solutions to mathematical models developed by Data Scientists. They are strong programmers and also have good mathematics and statistics capabilities. Machine Learning is particularly of interest here, as we are incorporating it into our model development.
  - Information Technology experts in incident response. Strong cybersecurity skills, understanding of forensics and incident response procedures. Programming a strong plus.

Support Needs

- Products
  - Machine Learning Tools
  - Data Integration and Amalgamation Tools
  - Supply Chain Analysis Tools
  - Caveats
    - Black box solutions do not work here. We must understand how the data is being used and transformed. Proprietary systems/models are not useful to us if we cannot see the underlying logic and how the data is being processed.
    - Is there an OEM for this tool? What is the value added you bring? Why shouldn't I just go to the OEM? Keep in mind the GSA likely has an Enterprise level agreement with the OEM, so be prepared to explain what else you bring to the table.

- Solutions
  - Problems can be solved in many different ways. We are open to hearing new and different methods to approach the challenges we face.