DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Big Data Platform (BDP) and Cyber Situational Awareness Analytic Capabilities (CSAAC)

Daniel V. Bart

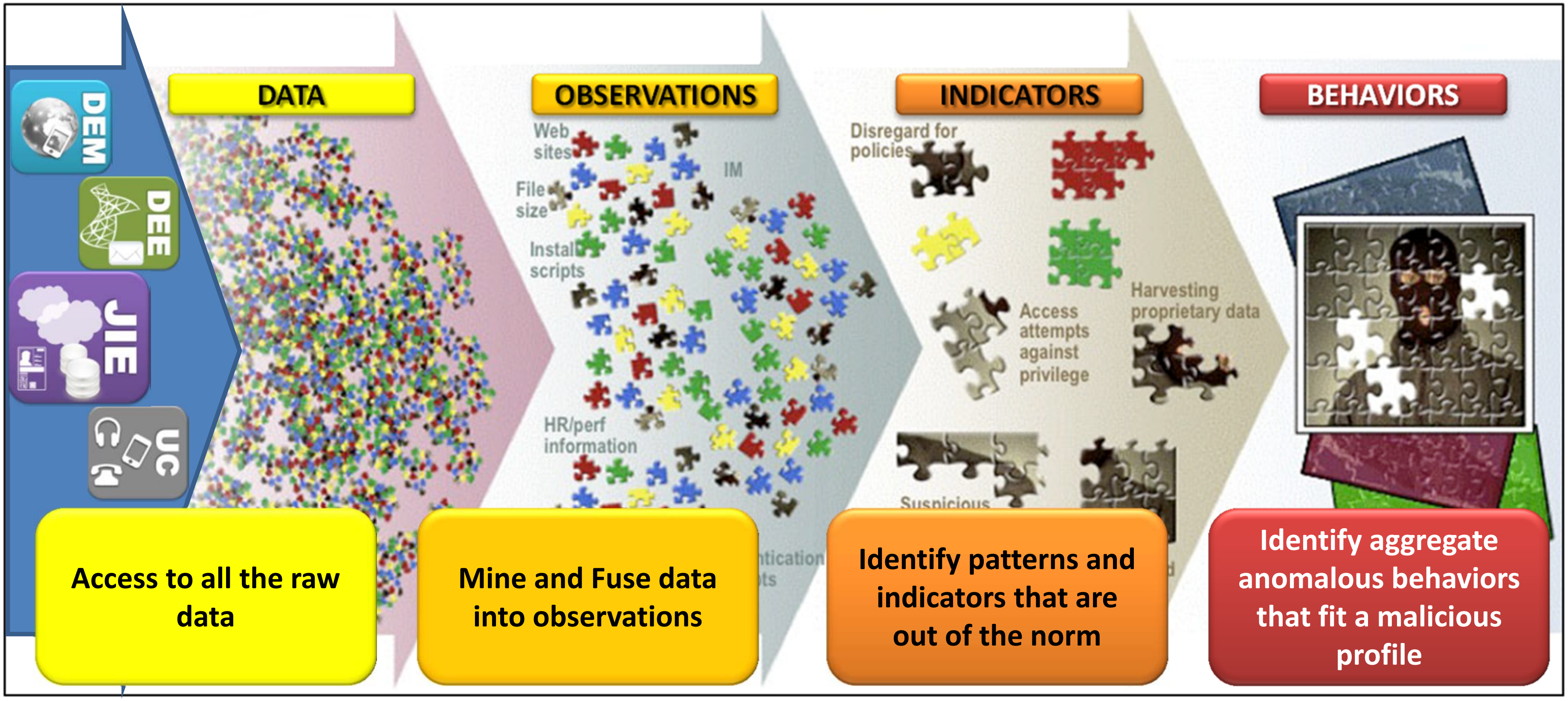
DISA Infrastructure Development
Cyber Situational Awareness and Analytics

22 April 2016

Presentation Disclaimer

“The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government. This brief may also contain references to United States Government future plans and projected system capabilities. Mention of these plans or capabilities in no way guarantees that the U.S. Government will follow these plans or that any of the associated system capabilities will be available or releasable to foreign governments.”

Cyber Situational Awareness



Access to all the raw data

Mine and Fuse data into observations

Identify patterns and indicators that are out of the norm

Identify aggregate anomalous behaviors that fit a malicious profile

Key Definitions

Big Data Platform (BDP)

The BDP provides a common computing solution capable of ingesting, storing, processing, sharing, and visualizing multiple petabytes of data from DoD Information Network (DoDIN) sources

Cyber Situational Awareness Analytic Capabilities (CSAAC)

CSAAC is the set of widgets, analytics, ingest code, and data structures deployed on the BDP providing unified situational awareness across DODIN Operations and Defense Cyberspace Operations (DCO)

DODIN Ops / Situational Awareness
Enterprise Services Monitoring

DISA

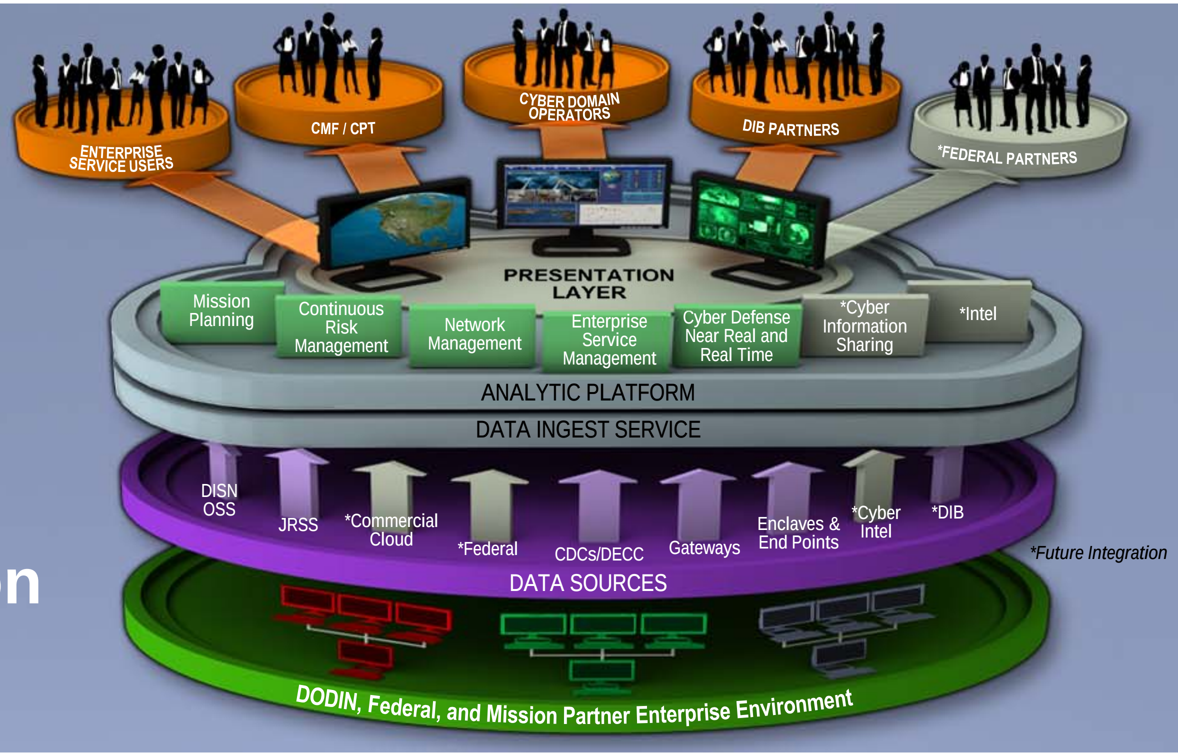
Cyber Situational Awareness Framework with Big Data

Share

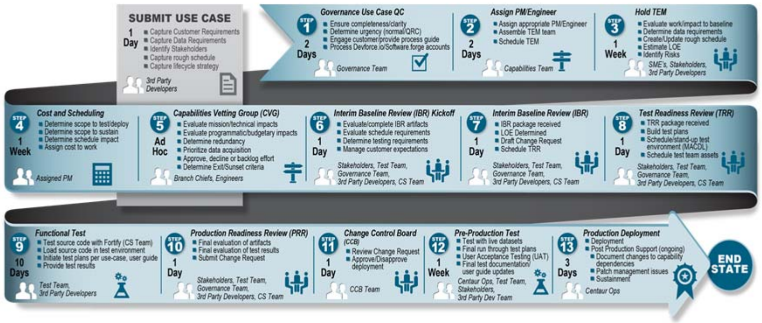
Visualize

Analyze

Collect Information



Infrastructure, Data, Analytic Integration Management (IDAIM)



SUBMIT USE CASE
1 Day
- Capture Customer Requirements
- Capture Data Requirements
- Identify Stakeholders
- Capture rough schedule
- Capture lifecycle strategy

3rd Party Developers

STEP 1 – *Governance Use Case QC* – 2 Days
- Ensure completeness/clarity
- Determine urgency (normal/QRC)
- Engage customer/provide process guide
- Process Devforce.io/Software.forge accounts

Governance Team

STEP 2 – *Assign PM/Engineer* – 2 Days
- Assign appropriate PM/Engineer
- Assemble TEM team
- Schedule TEM

Capabilities Team

STEP 3 – *Hold TEM* – 1 Week
- Evaluate work/impact to baseline
- Determine data requirements
- Create/Update rough schedule
- Estimate LOE
- Identify Risks

SME's, Stakeholders, 3rd Party Developers

STEP 4 – *Cost and Scheduling* – 1 Week
- Determine scope to test/deploy
- Determine scope to sustain
- Determine schedule impact
- Assign cost to work

Assigned PM

STEP 5 – *Capabilities Vetting Group (CVG)* – Ad Hoc
- Evaluate mission/technical impacts
- Evaluate programmatic/budgetary impacts
- Determine redundancy
- Prioritize data acquisition
- Approve, decline or backlog effort
- Determine Exit/Sunset criteria

Branch Chiefs, Engineers

STEP 6 – *Interim Baseline Review (IBR) Kickoff* – 1 Day
- Evaluate/complete IBR artifacts
- Evaluate schedule requirements
- Determine testing requirements
- Manage customer expectations

Stakeholders, Test Team, Governance Team, 3rd Party Developers, CS Team

STEP 7 – *Interim Baseline Review (IBR)* – 1 Day
- IBR package received
- LOE Determined
- Draft Change Request
- Schedule TRR

Stakeholders, Test Team, Governance Team, 3rd Party Developers, CS Team

STEP 8 – *Test Readiness Review (TRR)* – 1 Day
- TRR package received
- Build test plans
- Schedule/stand-up test environment (MACDL)
- Schedule test team assets

Stakeholders, Test Team, Governance Team, 3rd Party Developers, CS Team

STEP 9 – *Functional Test* – 10 Days
- Test source code with Fortify (CS Team)
- Load source code in test environment
- Initiate test plans per use-case, user guide
- Provide test results

Test Team, 3rd Party Developers

STEP 10 – *Production Readiness Review (PRR)* – 1 Day
- Final evaluation of artifacts
- Final evaluation of test results
- Submit Change Request

Stakeholders, Test Team, Governance Team, 3rd Party Developers, CS Team

STEP 11 – *Change Control Board (CCB)* – 1 Day
- Review Change Request
- Approve/Disapprove deployment

CCB Team

STEP 12 – *Pre-Production Test* – 1 Week
- Test with live datasets
- Final run through test plans
- User Acceptance Testing (UAT)
- Final test documentation/ user guide updates

Centaur Ops, Test Team, Stakeholders, 3rd Party Dev Team

STEP 13 – *Production Deployment* – 3 Days
- Deployment
- Post Production Support (ongoing)
  - Document changes to capability dependencies
  - Patch management issues
  - Sustainment

Centaur Ops

END STATE

Data acquisition – **Data acquisition methodology and operations based upon user/community use case requirements**

Analytic Development Management – **Governance policies and processes for internal/external tool development and cloud integration**

Big Data Platform (BDP) Baseline Change Management – **BDP baseline tool integration based upon community use cases/requirements**

Requirements Management – **Requirements gathering, dissemination, scoring and integration for BDP/CSAAC enhancements**

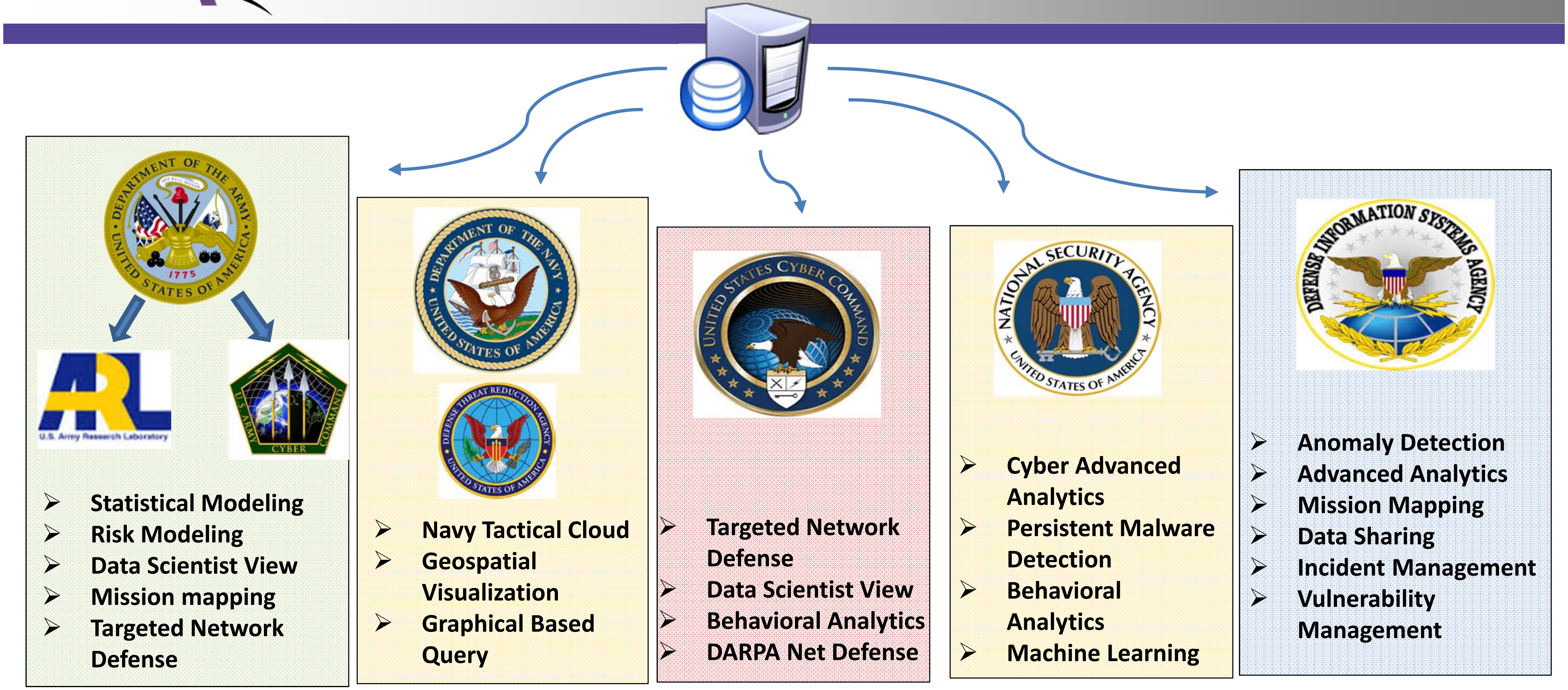
Knowledge Base / Collaboration – **Environment for developers to access what other analysts / data scientists are working on across the DoD**

Governance Portal - https://disa.deps.mil/ext/cop/mae/netops/Governance/SitePages/Home.aspx

Data Portal - https://disa.deps.mil/org/ID6/CSAACDataAcquisition/SiteAssets/DataPortal%20html%20redesign.html

DISA

Big Data Platform Community efforts



- Statistical Modeling
- Risk Modeling
- Data Scientist View
- Mission mapping
- Targeted Network Defense

- Navy Tactical Cloud
- Geospatial Visualization
- Graphical Based Query

- Targeted Network Defense
- Data Scientist View
- Behavioral Analytics
- DARPA Net Defense

- Cyber Advanced Analytics
- Persistent Malware Detection
- Behavioral Analytics
- Machine Learning

- Anomaly Detection
- Advanced Analytics
- Mission Mapping
- Data Sharing
- Incident Management
- Vulnerability Management

Network Operations Capability

- Focused on situational awareness of enterprise services
- Gives visual indications for health and status of DoD Enterprise Email
- Allows for quick problem overview
- Allows understanding of customers affected if system issues are occurring
    - How many customers?
    - Where are they located?
    - What Service do they work for?
- Utilized by DISA Operations and DoD Enterprise Email customers

DODIN Ops / Situational Awareness

Enterprise Services Monitoring

Computer Network Defense Capability

- Focused on Cyber Threat Analysis
- Ability to automatically ingest, analyze, and update cyber threat information from reports
- Answers the following questions based on data already ingested
  - Have we seen this threat before ?
  - Where have we seen this threat across the DoDIN ?
  - Who else has reported this threat ?
  - Do we have an existing counter measure in place / where ?
- Allows a automated workflow to create new counter measures
- Utilized by DISA DCC and Cyber Operations teams across DoD

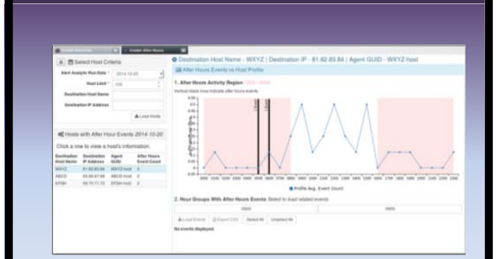
Defensive Cyber Ops

Fight by Indicator (FbI)

Anomaly Detection Suite Capability

- Focused on Internal Threat Analysis
- Brings together data from NIPR and SIPR to identify anomalies
- Provides visibility into DoD users' network activity to assist with inquiry and investigation procedures
- Uses Big Data to perform complex analytics which result in focused results
- Utilized by DISA Risk management, Missile Defense, Army ARCYBER

Audit Management



Alert Analytic Run Date * 2014-10-20

Host Limit * 100

Destination Host Name

Destination IP Address

Click a row to view a host's information.

Destination Host Name	Destination IP Address	Agent GUID	After Hours Event Count
WXYZ	81.82.83.84	WXYZ-host	2
ABCD	65.66.67.68	ABCD-host	2
EFGH	69.70.71.72	EFGH-host	2

Destination Host Name - WXYZ | Destination IP - 81.82.83.84 | Agent GUID - WXYZ-host

1. After Hours Activity Region

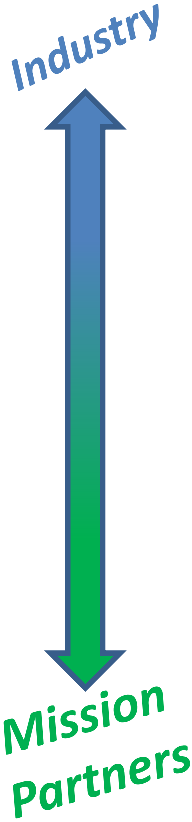
Vertical black lines indicate after hours events.

2. Hour Groups With After Hours Events *Select to load related events*

No events displayed.

Insider Threat Detection Service

Opportunities to Assist



Industry

Mission Partners

- Commitment to Open Architecture / Open Standards
  - Can’t tear out and replace large parts of a capability with each good idea
- Enterprise Architecture
  - How to best support the DoD level at scale, federation, and hierarchy
- Data Standards, Catalogs, and Tagging
  - Foundational for analytics reuse and common Situational Awareness
- Data Scientists
  - Need more subject matter expertise for problem determination/solving
- Collaboration Environment
  - How to facilitate information sharing to minimize redundant efforts
- DEVOPS / Agile Environment
  - Need automated capability(s) to enable secure continuous integration into operations
- Leverage Data Repositories
  - Strengthen authoritative lineage and reduce excessive storage instances

DISA

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

UNITED IN SERVICE TO OUR NATION