Enterprise Business Intelligence in Support of Cyber Operations

Bob Landreth
Acting Chief, Cyber Analytics Branch
Cyber Directorate

Andrea Gonzalez
Requirements Analyst
Requirements & Analysis Office

14 June 2017
Outline

• Evolution of Service Provider – JIE

• DoD Cyber Challenge

• Business Intelligence for Cyber Awareness

• Purpose/Objective for Providing Situational Awareness

• Cyber Situational Awareness (SA) and Big Data (Current Efforts)

• Data Analysis Lifecycle

• Data Presentation Evolution Timeline

• What’s next?
As a combat support agency, DISA is a Joint Information Environment (JIE) Service Provider operating, managing, and securing DODIN enterprise services. As such, DISA has responsibility to provide service intelligence and Situational Awareness (SA) to its mission partners.

- Expose enterprise service data
- Share enterprise service data
- Enhance situational awareness and mission decision support
- We must transform data into information, then further refine that information into intelligence
- Better automation is critical

Network and threat data (Four Vs)
- **Volume** (Data at rest): Hundreds of terabytes daily
- **Velocity** (Data in motion): Data is constantly flowing
- **Variety** (Data in different forms): No single format
- **Veracity** (Data in doubt): False positives and ambiguity

Limited number of analysts

Missed Data
Limited storage can cause data to be dropped, how much should we store and what is the cost?
Business Intelligence for Cyber Awareness

Data Scientists/Cyber Analysts

Big Data Platform

End Users/End Points

Business Continuity for other Combat Support Agencies

Business Intelligence

Machine Learning

Correlation with Mission Dependency

Combatant Command Situational Awareness

Data Visibility

structured
unstructured
DATA
Purpose/Objective for Providing Situational Awareness

**Situational Awareness**

**Purpose:**
- Make operational information actionable
- Provide awareness to Warfighter and Mission Partners

**Objective:**
- View situational awareness dashboards in support of business/mission

**Insider Threat/Counterintelligence**

**Purpose:**
- Support Mission Partner insider threat defense

**Objective:**
- Access to system logs and other data in support of insider threat detection

Mission Partners will have different cyber situational awareness needs depending on their cyber terrain that their missions utilize.
Cyber Situational Awareness (SA) and Big Data

Situational Awareness

- Collect/Data/Observed
- Analyze/Information/Orient
- Visualize/Knowledge/Decide
- Share/Understanding/Act

Mission Planning
Continuous Risk Management
Network Management
Enterprise Service Management
Cyber Defense Near Real and Real Time
Cyber Information Sharing
* intel

Data Ingest Service

Data Sources

DODIN, Federal, and Mission Partner Enterprise Environment

*Commercial Cloud
*Federal
CCDC/DEC
Enclaves & Endpoints
*Cyber intel
*DIB

Enterprise Service Users
CMF/CPT
Cyber Domain Operators
DIB Partners
*Federal Partners
Using big data processing to identify events that raise alarms and threats through indicators which can increase awareness of critical changes in the operational environment.
Data Presentation Evolution

Business Intelligence / Federated Query
- Self service visualizations

DEVOPS / Ad-hoc Analytics
- Meets operational tempo but limited management

Agile Development
- Timeframes for capability delivery not meeting operational pace
Business Intelligence tools for Cyber Situational Awareness

- Provide data visibility to Mission Partners for various operational and mission needs
- Provide visualizations in support of executive dashboards
- Provide cyber analysts ability to discover/explore sensor output without development
- Provide machine learning toolsets
- Support joint data strategy

Mission Partners rely on the information environment to help them understand the operational status which influences the service of critical capabilities.
rate us
visit us
follow us
take the 3-question survey available on the AFCEA 365 app

DISA Booth # 443

Facebook/USDISA
Twitter/USDISA