DODIN Defense in a Dynamic Cyber Environment

Beyond Static Defenses

Mr. Darrell Fountain

Chief, CSSP Programs Office
DISA J34
13 February 2024

Adapting to a Dynamic Cyber Environment

- Driving to the Endpoint
- Collaboratively Defending “the Cloud”
- Synchronizing Defensive Operations

<u>Strategy</u>:

- Improve the Common Analytic Environment
- Leverage DoD defensive advantages; Know our Cyber Terrain
- Partner with Cloud Service Providers for Security Relevant Data

Background

DISA's Cyber forward edge of the battle area: 450+ distinct CSSP mission partners defended

15K personnel in 21 states, 7 countries and 1 US Territory

- 4M DoD computers
- 3M DODIN users
- 142K mobility devices
- Over 1,500 tickets & 151 changes daily

10 Internet Access Points and 2 Cloud Access Points

- 1.3B events per day
- 790M blocks per day
- 1.3 GB/s of scans blocked per day
- 453K phishing & spam emails blocked per day
- 27 TIPPERS per day

Continual Enterprise Hunt Operations

Driving to the Endpoint

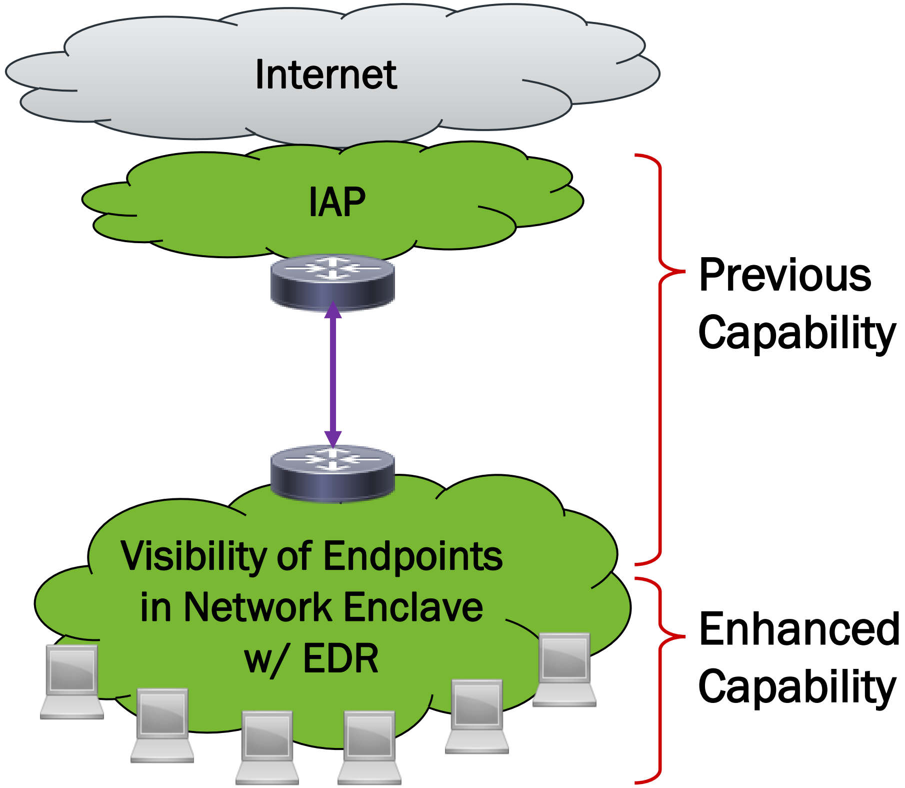
What DISA Is Doing

- Implementing Endpoint Detection Response (EDR)
  - Reduced workload
  - Enhanced visualizations
  - Implemented live response
- Piloting EDR for servers

Challenges

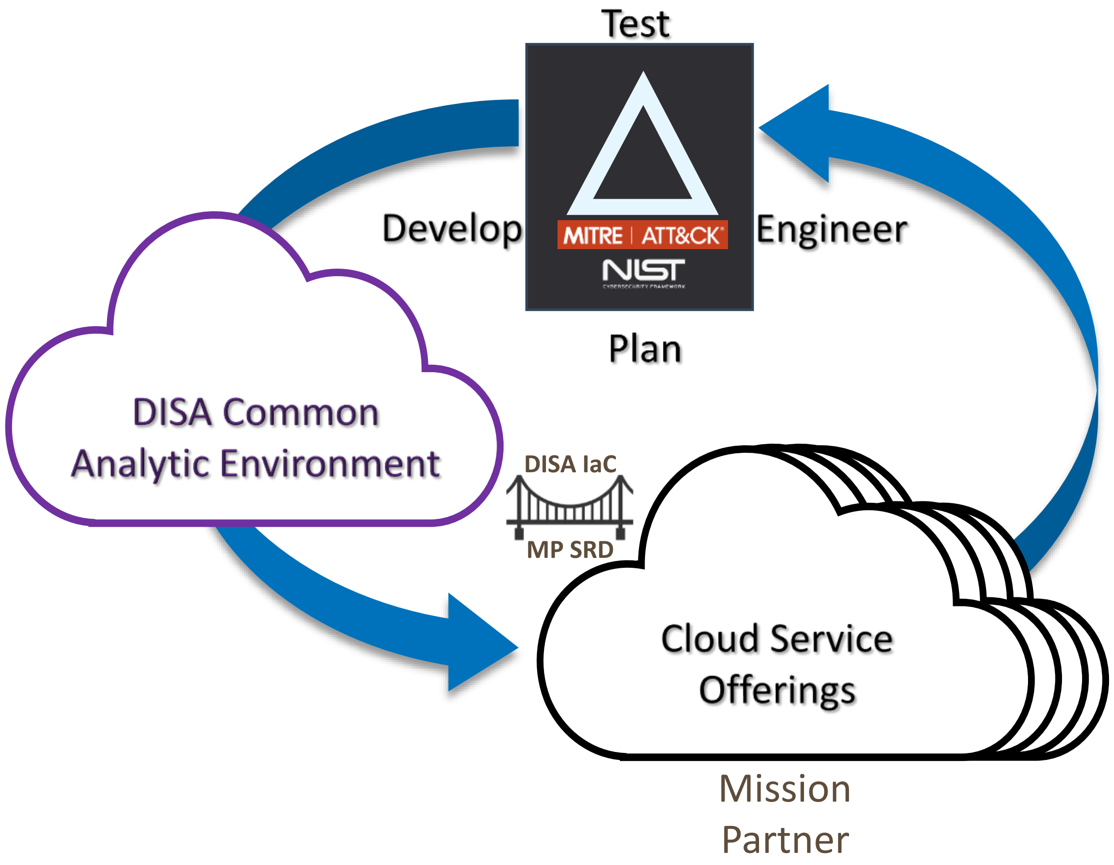
- Integration of different EDRs into the common analytic environment
- Analytic transparency needed for AI/ML implementations
- EDR limitations for:
  - Appliances (printers, routers, firewalls, etc.)
  - Serverless compute
  - Internet of Things (IoT)

DISA CSSP Service Delivery w/ EDR



Leverage DoD Defensive Advantages; Know our Cyber Terrain

Collaboratively Defending "the Cloud"



What DISA Is Doing

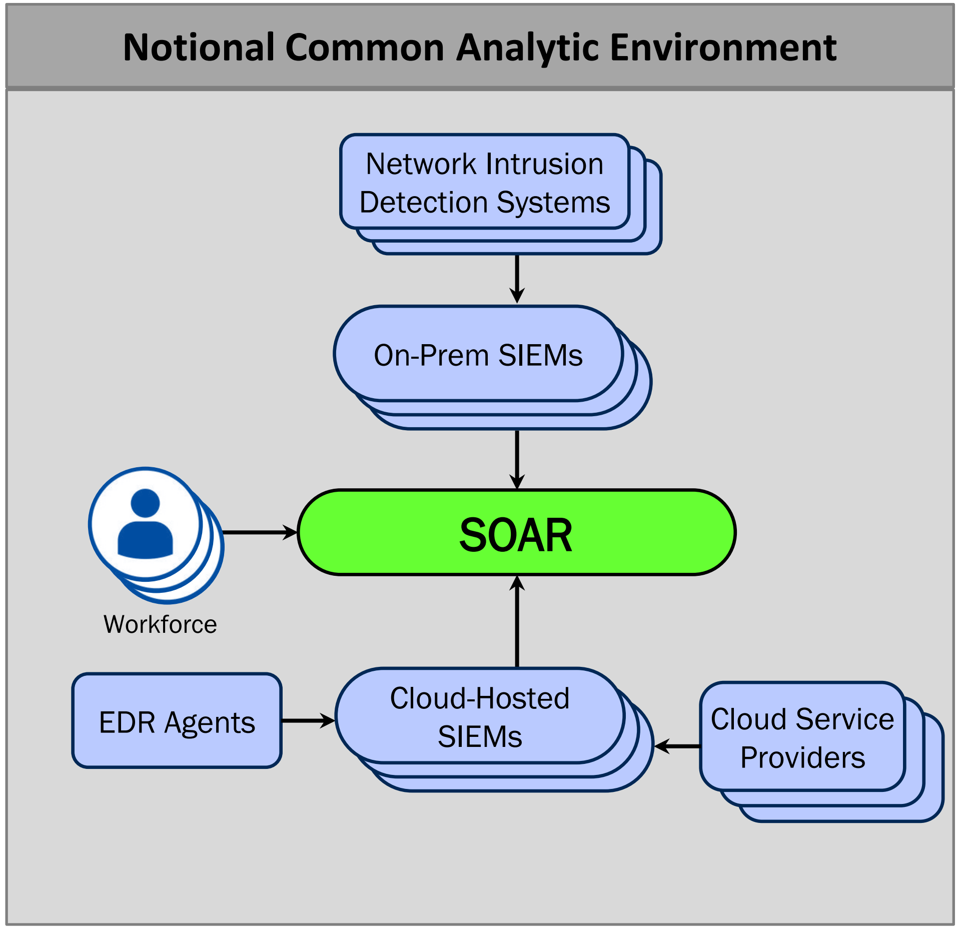
- Defend the cloud, in the cloud, with the cloud
  - Security Relevant Data (SRD) IAW NIST 800.53 and MITRE ATT&CK
  - Baseline cloud native Security Relevant Tools (SRT) enables consumption of SRD
  - Infrastructure as Code (IaC) automates and significantly reduces time to execution
  - Continuous Improvement achieved through Threat Detection Testing, analytic development, and optimization of MP CSSP configurations

Challenges

- Security tool and data parity across vendors and Impact Levels increases difficulty in standardizing common DCO framework
- Lack of vendor service mapping to DoD Cybersecurity Activities Performed for Cloud Service Offerings significantly impacts CSSP service delivery
- Analysts must leverage multiple cloud instances instead of a single cloud environment

Partner with Cloud Service Providers for Security Relevant Data

Synchronizing Defensive Operations: SOAR



What DISA Is Doing

- Piloting the integration of SIEMs through a SOAR
- Automating data standardization and enrichment
- Investigating the use of robotic process automation

Challenges

- Managing Security Relevant Data
- Integrating multiple SIEMs into a single SOAR
- Automating triage and data correlation across analytic environments

Improve the Common Analytic Environment

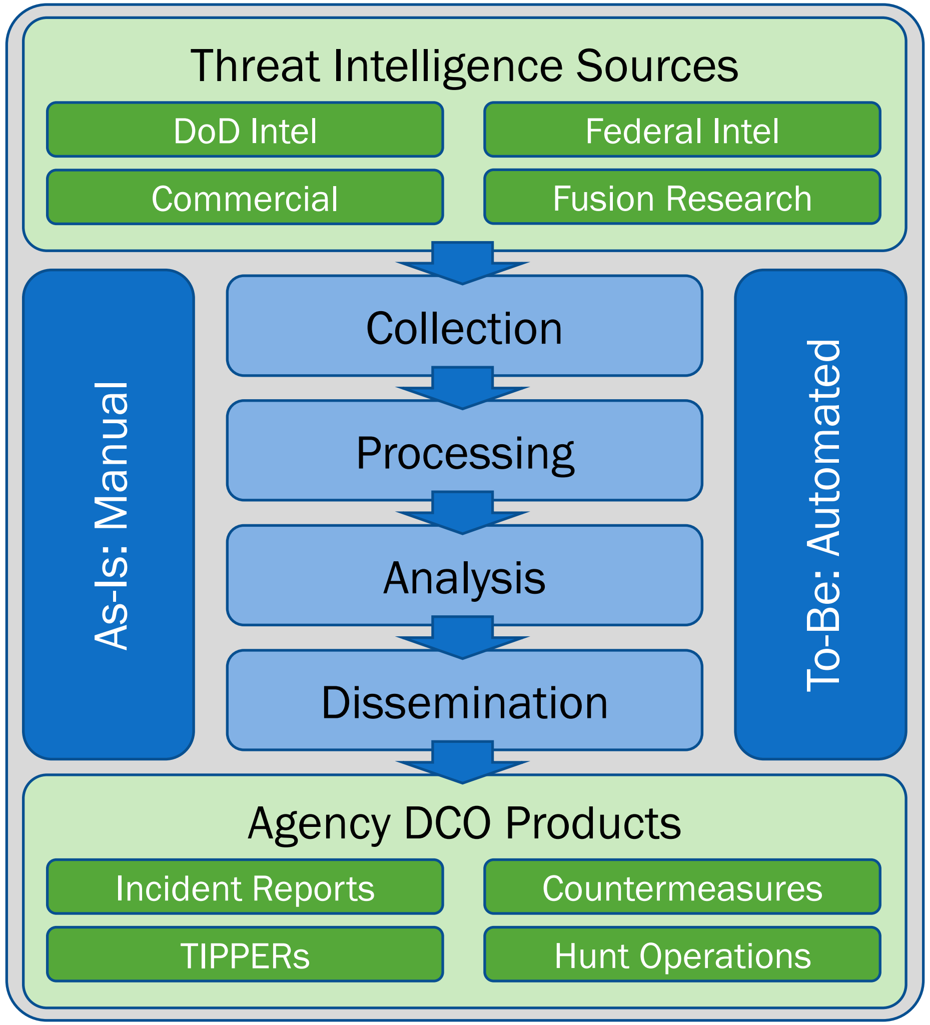
Synchronizing Defensive Operations: Threat Intelligence

What DISA Is Doing

- Processing Threat Intelligence received from multiple sources manually
- Prioritizing threats based on MITRE ATT&CK framework manually
- Developing threat-based Enterprise Hunt Operations
- Utilizing Intelligence focused on AOR threat

Challenges

- Automating Threat Intelligence processes
- Disseminating Threat Intelligence to DISA SIEMs



Threat Intelligence Sources

DoD Intel

Federal Intel

Commercial

Fusion Research

As-Is: Manual

Collection

Processing

Analysis

Dissemination

To-Be: Automated

Agency DCO Products

Incident Reports

Countermeasures

TIPPERs

Hunt Operations

Leverage All Sources of Threat Intelligence

Adapting to a Dynamic Cyber Environment

- DISA evolving with the environment
  - Committed to continuous improvement
  - Open to new ideas
- Transparent AI/ML to synchronize defensive operations
- We need your help solving priority challenges

DEFENSE INFORMATION SYSTEMS AGENCY

DISA: The premier IT and telecommunications provider for the US military

in /DISA   X @USDISA   f /USDISA   DISA.mil