Product Manager
Cyber Analytics and Detection (CAD)
Operational Overview and the Big Data Platform

LTC Dakota Steedsman, Product Manager

November 8, 2022

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

Defensive Cyber Operations

Defensive Cyber Operations (DCO) rapidly delivers innovative and dominant cyberspace capabilities, as well as tailored information technology solutions for our national, joint and allied partners. We are the leader within the cyberspace domain, delivering innovative, integrated and cost-effective solutions.

Project Manager DCO
COL Mark Taylor

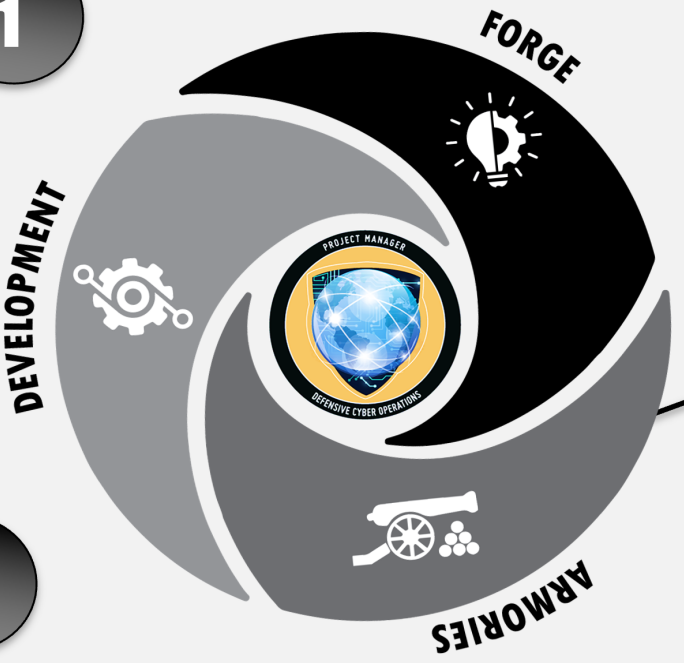
Defensive Cyber Operations (DCO)
High Level Stakeholders

WORKING TOGETHER TO DEFEND THE ARMY'S NETWORKS FROM CYBERSPACE ATTACKS

1 Industry Partners
Ideas and Integration

2 U.S. Army Contracting Command (ACC)
Contracts

3 Program Executive Office
Support



Cyber Protection Brigades (CPB)
Tactical Level

Army Information Warfare Operations Center IIWOC)
Strategic Level

Defensive Cyber Operations (DCO)
Acquire innovative cyberspace capabilities

Technical Warfare Center (TWC)
Accelerates innovation

Army Capabilities Manager (ACM)
Coordinates development and user activities

PROJECT MANAGER DEFENSIVE CYBER OPERATIONS

APPLIED CYBER TECHNOLOGIES

Cyber Analytics and Detection

Cyber Analytics and Detection (CAD) provides essential capabilities required to protect against, search and discover, mitigate and engage, and eradicate advanced cyberspace threats and vulnerabilities.

Product Manager
LTC Dakota Steedsman

MISSION

Deliver tailored, innovative, and dominant cyberspace capabilities to discover vulnerabilities and deter advanced cyber threats defending the Army's networks in support of joint all-domain operations

Cyber Analytics and Detection

Analyze | Identify | Mitigate

TOP GOALS & PRIORITIES

- To broaden cyberspace analytic capability to allow for the comprehensive collection, analysis, and visualization of data stemming from all tiers of the Army's network enterprise.
- Develop new cybersecurity capabilities through development and integration of defensive cybersecurity solutions
- Identify threat trends, behavior patterns, and tactics, techniques, and procedures associated with relevant portions of the designated network

US ARMY PEO EIS
PEO Enterprise Information Systems

CAPABILITIES

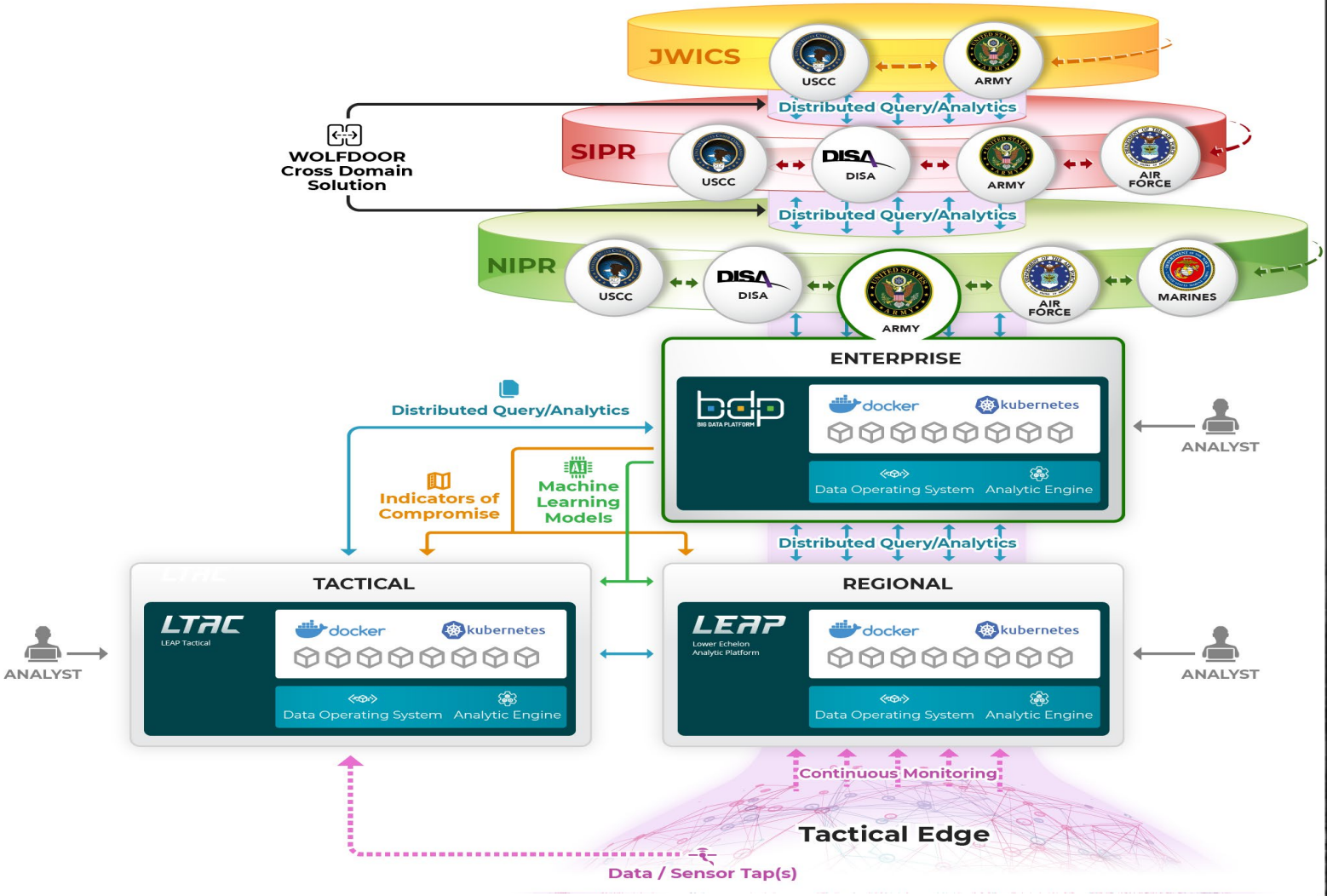
Cyber Analytics (CA)
Offers interfaces and visualizations accessible by cyberspace defenders at all levels to facilitate counter-reconnaissance activities meant to discover the presence of advanced or sophisticated cyber threats and vulnerabilities.

Defensive Cyber Operations Mission Planning (DCOMP)
Integrates cybersecurity requirements, intel, & vulnerability analyses with the outputs of mission analysis to determine probable attack vectors and produce a set of relevant internal defense measures, triggers, and decision points.

User Activity Monitoring (UAM)
A scalable solution that proactively identifies internal risks associated with the theft or misuse of critical and assists with the establishment of the Army's Insider Threat (InT) Program.

Threat Emulation (TE)
Allows the Cyber Community to conduct threat emulation in a garrison, deployed, or mission partner environment on information systems, net-enabled warfighting platforms, and critical infrastructure by closely resembling adversarial capabilities.

Cyber Analytics and Detection (CAD)
Big Data Platform (BDP) Operational Concept

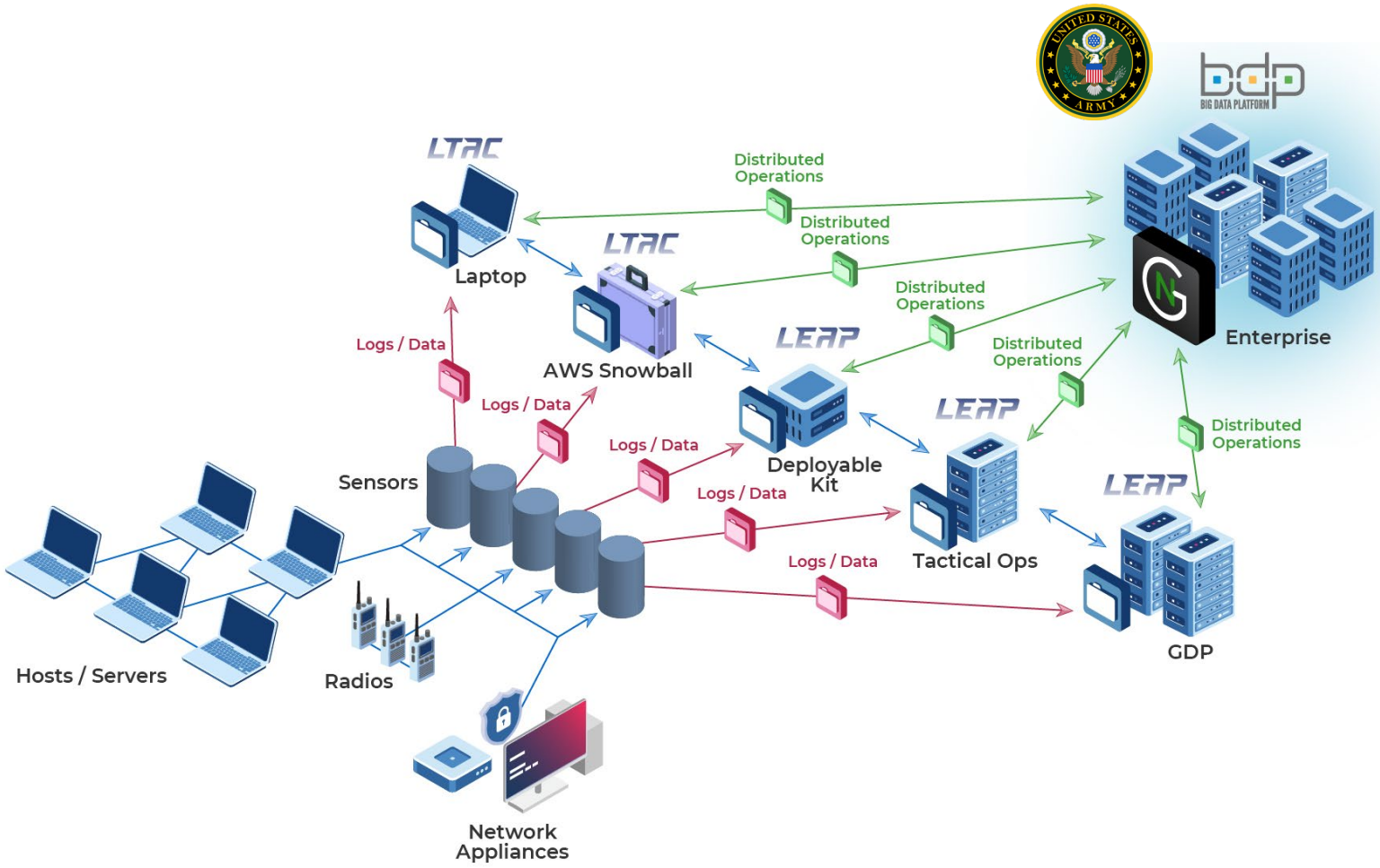


THE BIG DATA PLATFORM (BDP) AND THE ARMY

supports data centric operations in a variety of deployment environments allowing data to be presented to decision makers at all levels and Services.

PRODUCT MANAGER
CYBER ANALYTICS AND DETECTION

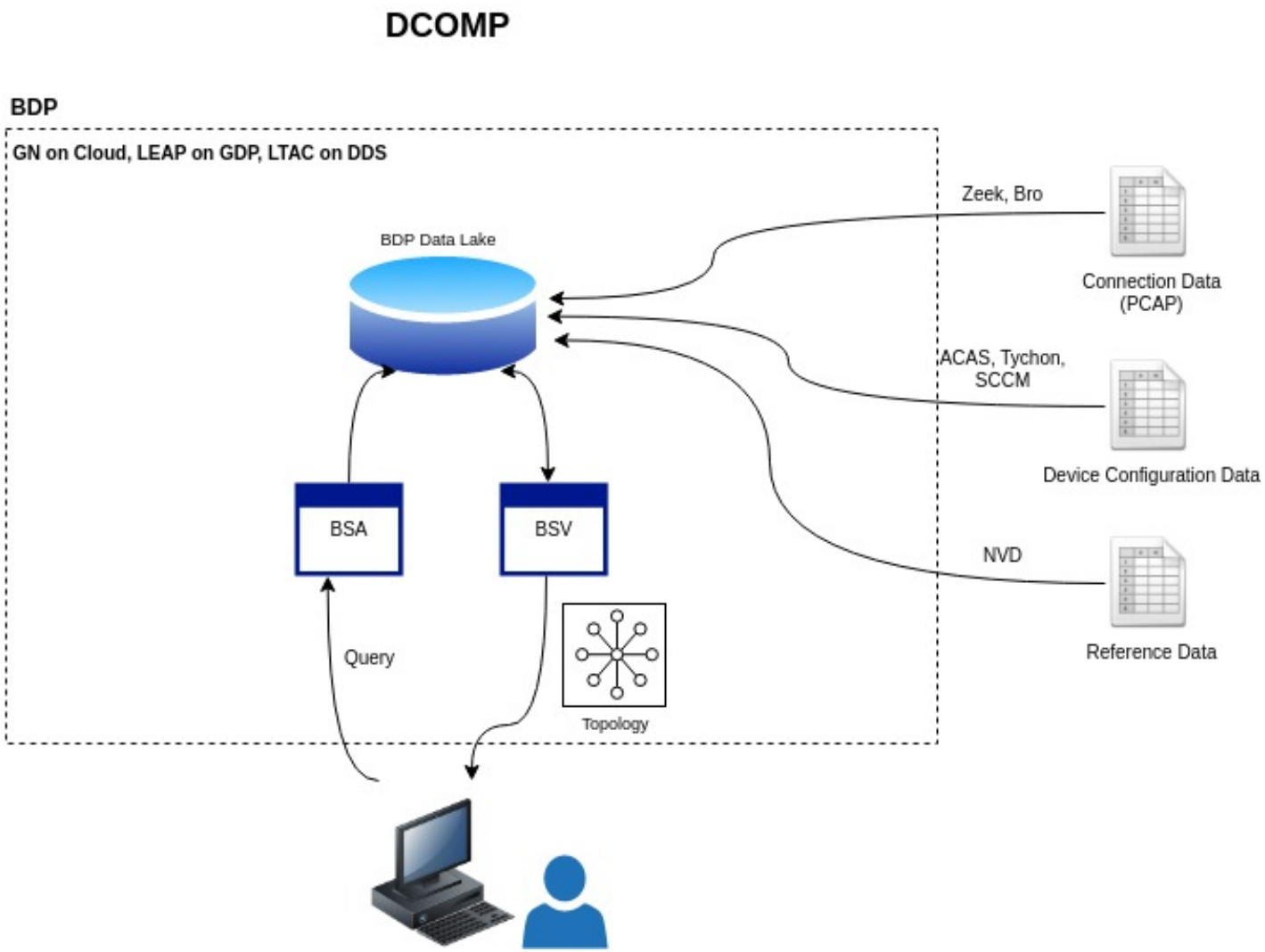
Cyber Analytics and Detection (CAD)
Cyber Analytics - Gabriel Nimbus (GN) Operational Concept



CYBER ANALYTICS (CA)

Offers interfaces and visualizations accessible by cyberspace defenders at all levels to facilitate counter-reconnaissance activities meant to discover the presence of advanced or sophisticated cyber threats and vulnerabilities.

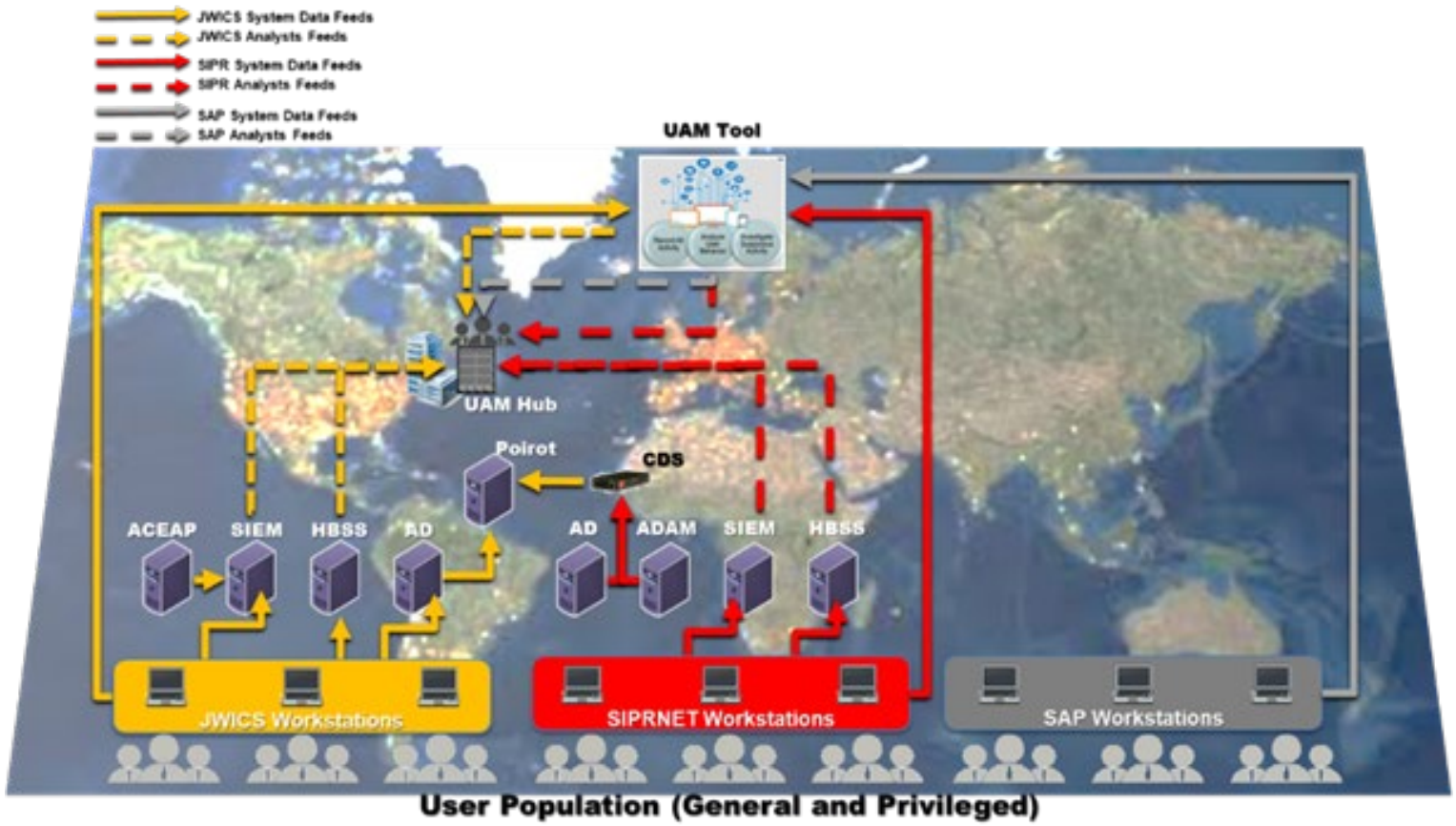
Cyber Analytics and Detection (CAD)
Defensive Cyberspace Operations Mission Planning (DCOMP)



DCO MISSION PLANNING (DCOMP)

Integrates cybersecurity requirements, intel, & vulnerability analyses with the outputs of mission analysis to determine probable attack vectors and produce a set of relevant internal defense measures, triggers, and decision points.

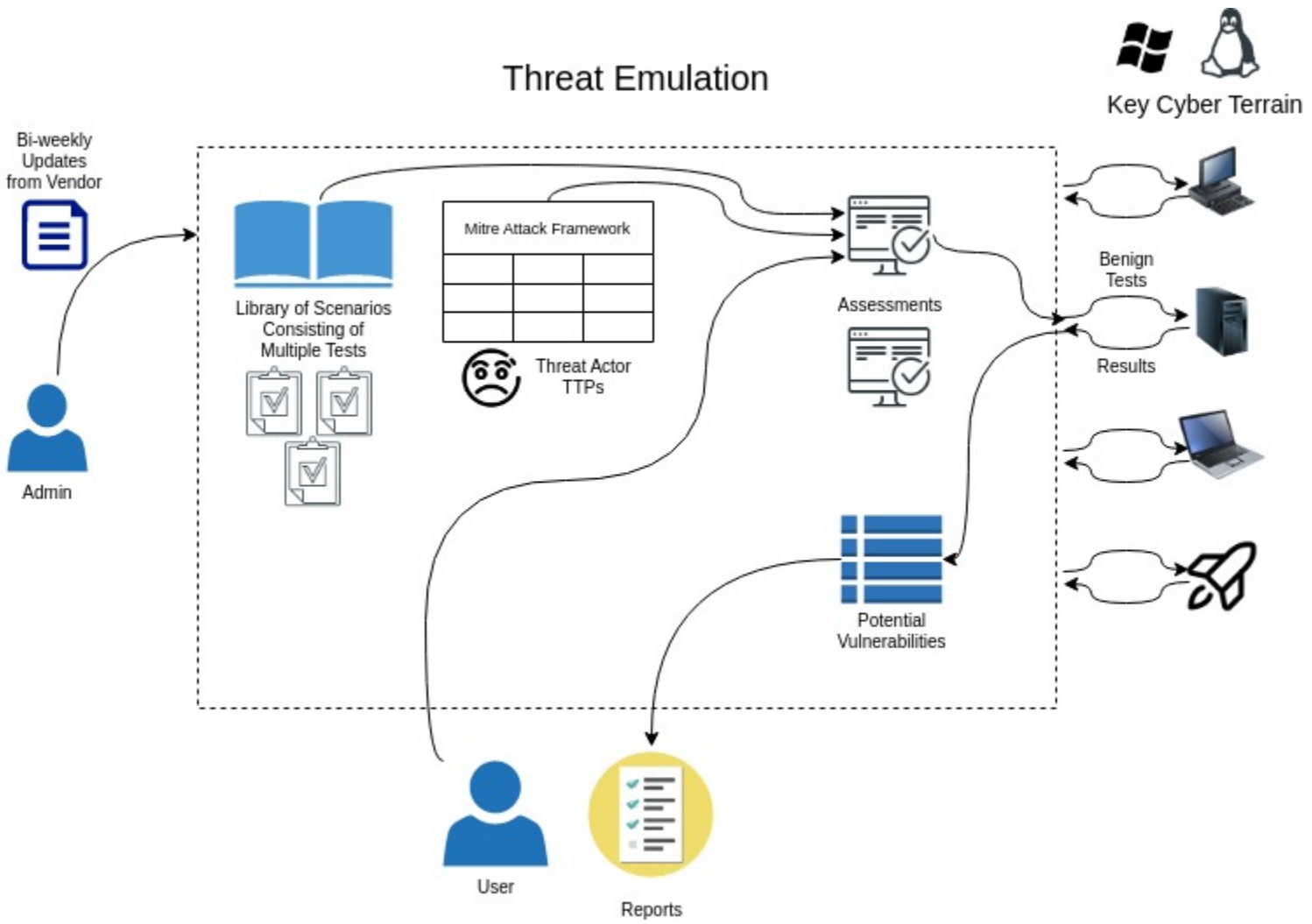
Cyber Analytics and Detection (CAD)
Defensive Cyberspace Operations Mission Planning (DCOMP)



USER ACTIVITY MONITORING (UAM)

A scalable solution that proactively identifies internal risks associated with the theft or misuse of critical and assists with the establishment of the Army's Insider Threat (InT) Program.

Cyber Analytics and Detection (CAD)
Threat Emulation (TE)



THREAT EMULATION (TE)

Allows the Cyber Community to conduct threat emulation in a garrison, deployed, or mission partner environment on information systems, net-enabled warfighting platforms, and critical infrastructure by closely resembling adversarial capabilities.

U.S.ARMY

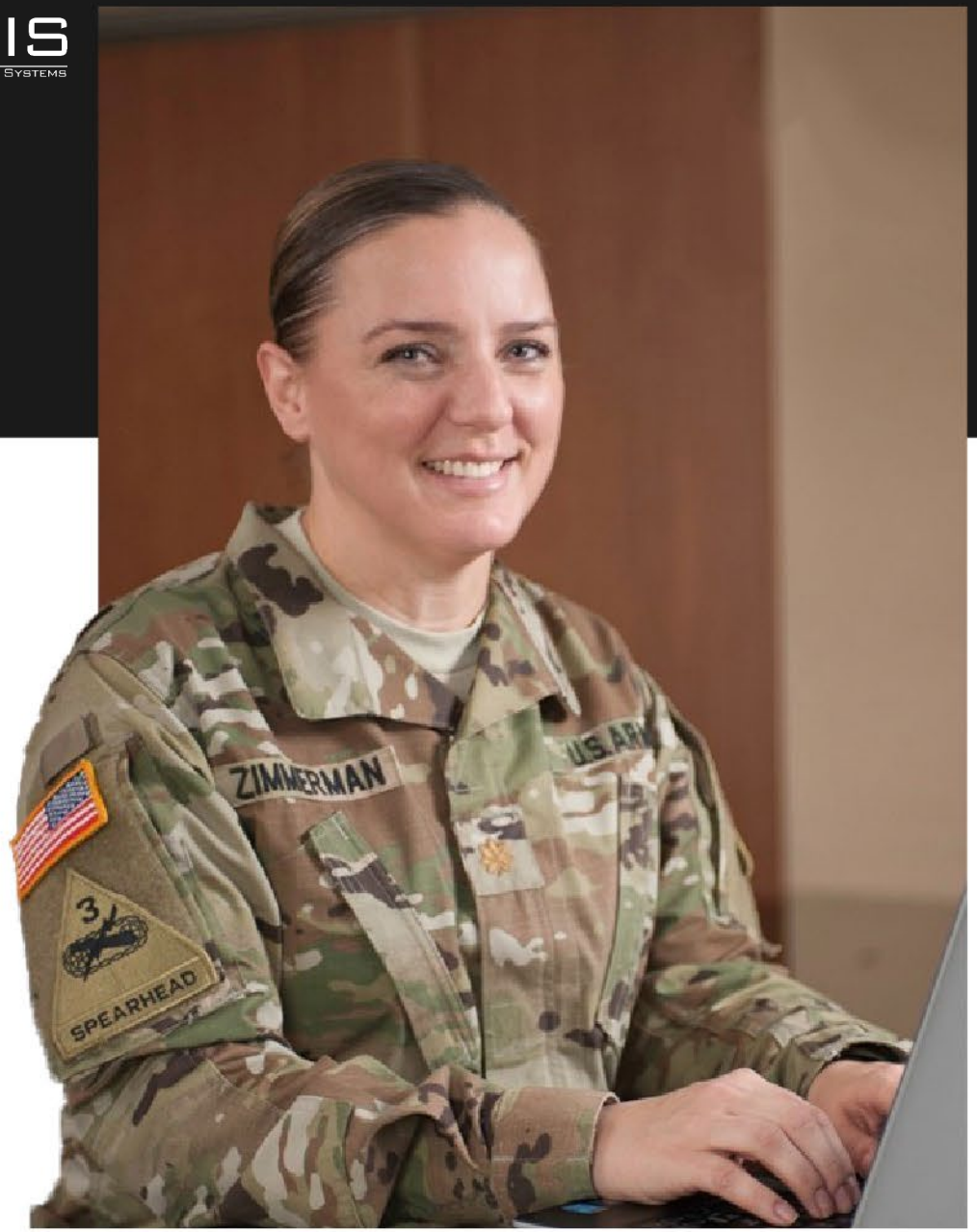
US ARMY PEO EIS
PEO Enterprise Information Systems

For procurement opportunities:

https://www.eis.army.mil/opportunities

These Slides

https://www.eis.army.mil/newsroom/publications



PROJECT MANAGER DEFENSIVE CYBER OPERATIONS

MEET WITH US

theforge.force.com/peoeis/s/

CONNECT WITH US

eis.army.mil/mission-areas/cad

Company/ArmyDCO

DCO-CAD@army.mil