

Security Information Management for Enclave Networks (SIMEN)

Rosalie M. McQuaid

781-271-7676 • rmcquaid@mitre.org

Air Force MOIE

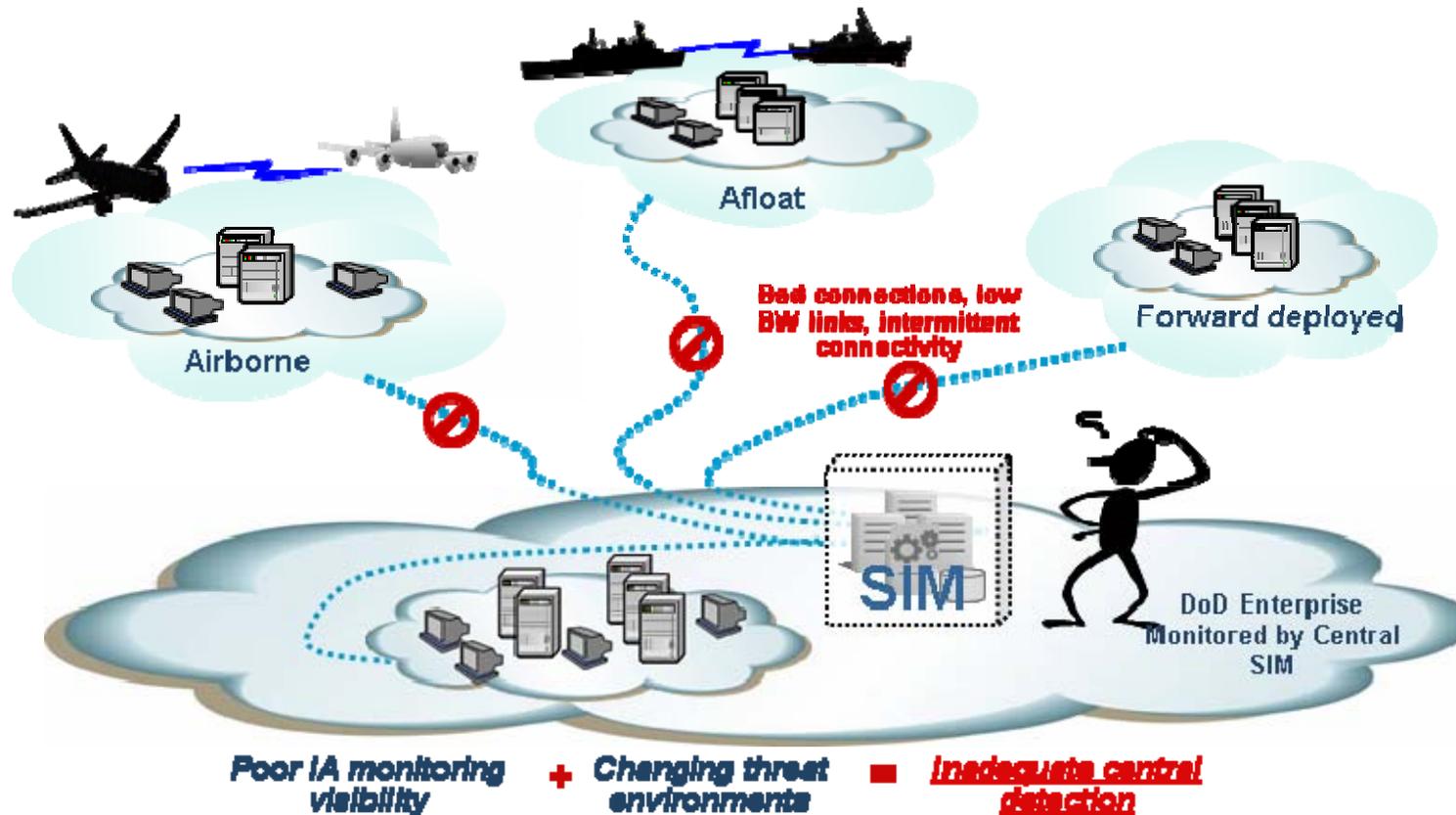
Approved for Public Release; Distribution Unlimited. Case Number: 07-0467

 MITRE
Technology
Program

Problem

- **Security Information Management (SIM) technology has IA monitoring and threat assessment limitations for enclaves when centrally deployed in the Air Force Enterprise**
- **Enclaves have changing threat environments – event importance is situational**
- **Security events descriptions are unique to devices**

Background



Centralized SIM Deployment is Problematic for Enclave Networks

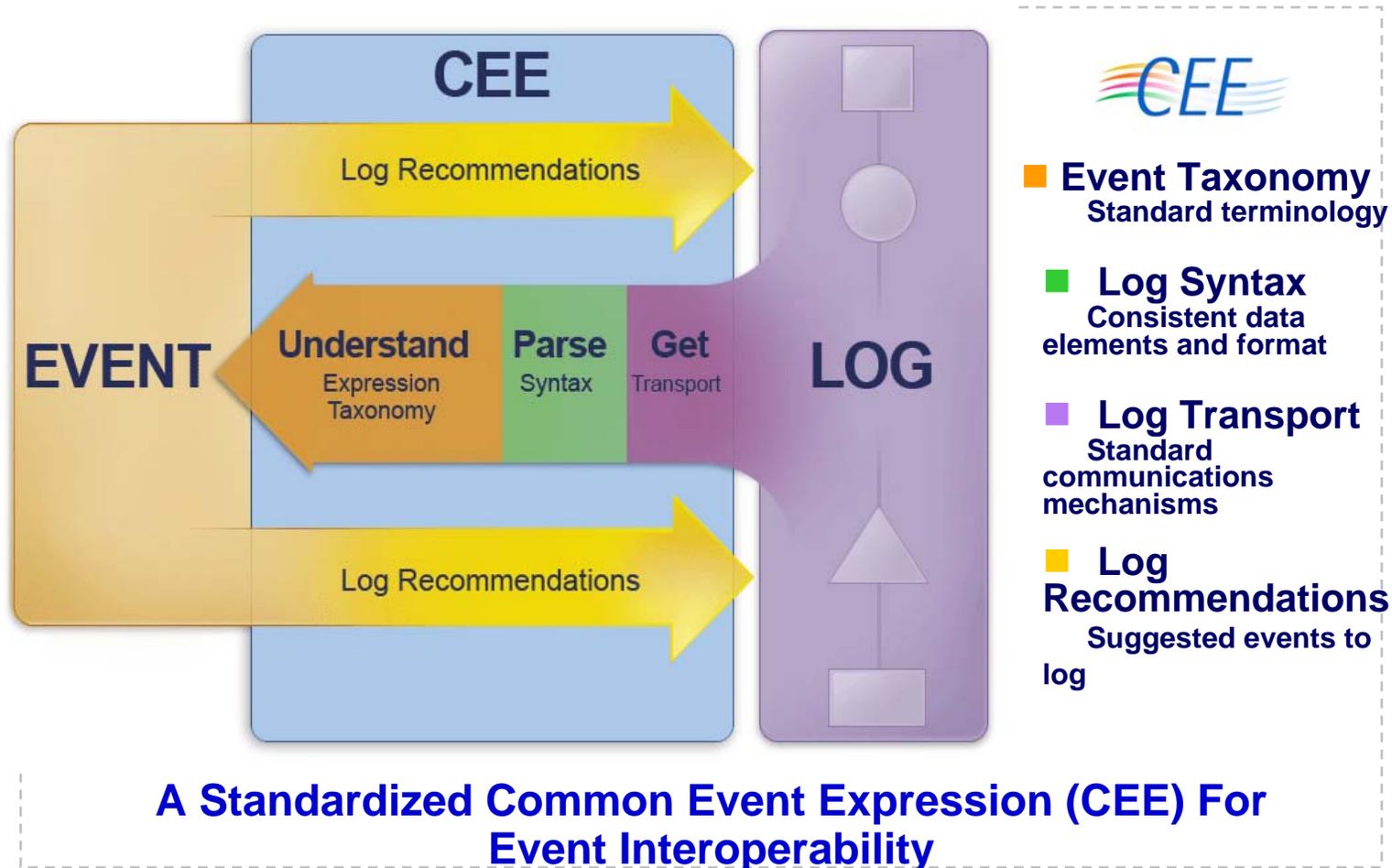
Objective

- Create IA monitoring solution that provides responsive and adaptive SIM visibility into constrained networks
- Achieve standardization of security event data
- Validate interoperability with COTS SIM technology and other research prototypes
- Transition to Air Force and industry partners

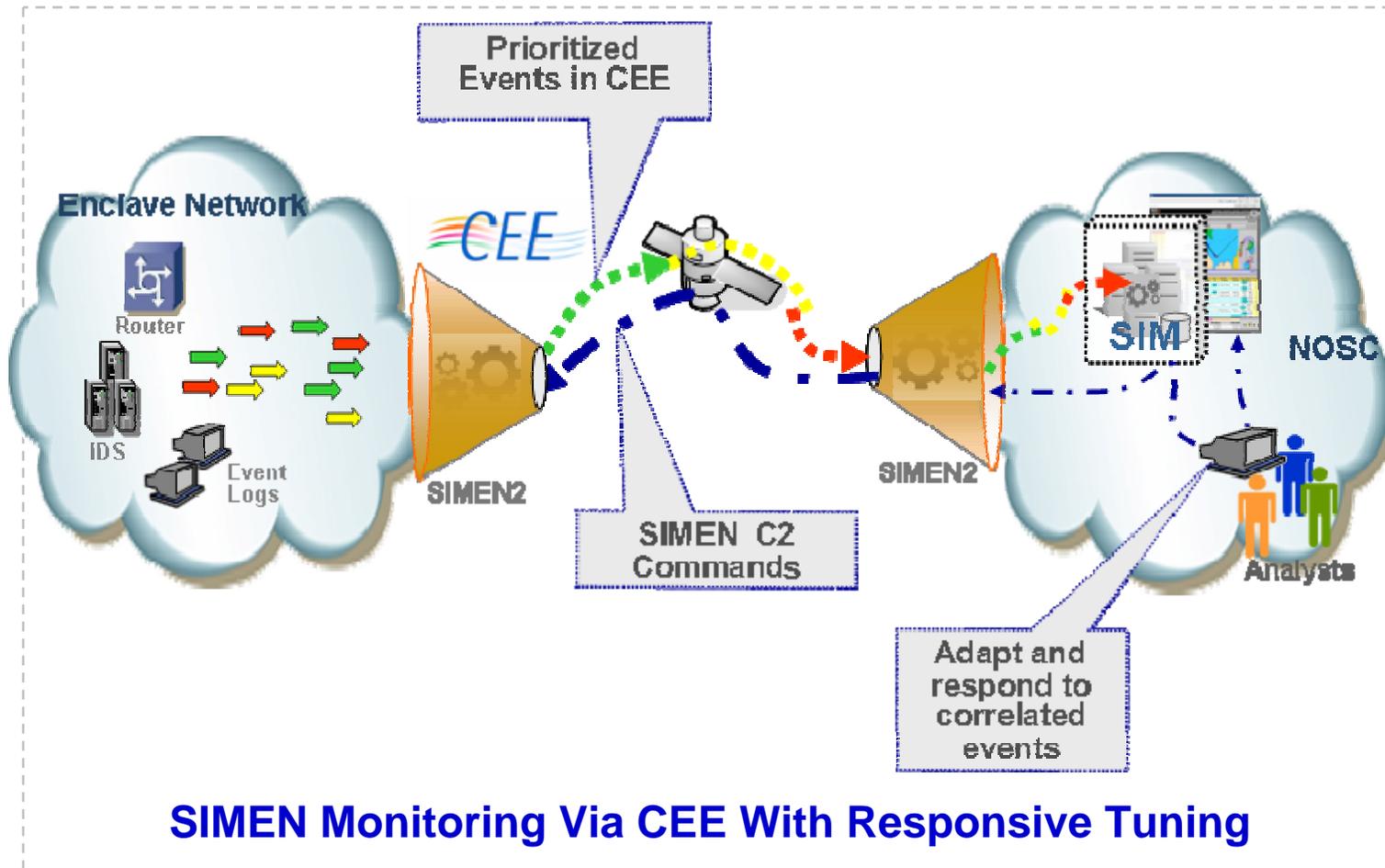
Activities

- **Research, develop and implement the SIMEN 2 prototype for adaptable and responsive enclave monitoring**
- **Validate bandwidth efficient prototype in fielded user experiments via CWID and NATO CWID**
- **Collaborate with industry partners to develop a Common Event Expression**
- **Collaborate with Airborne Network IA interest groups**

Highlight



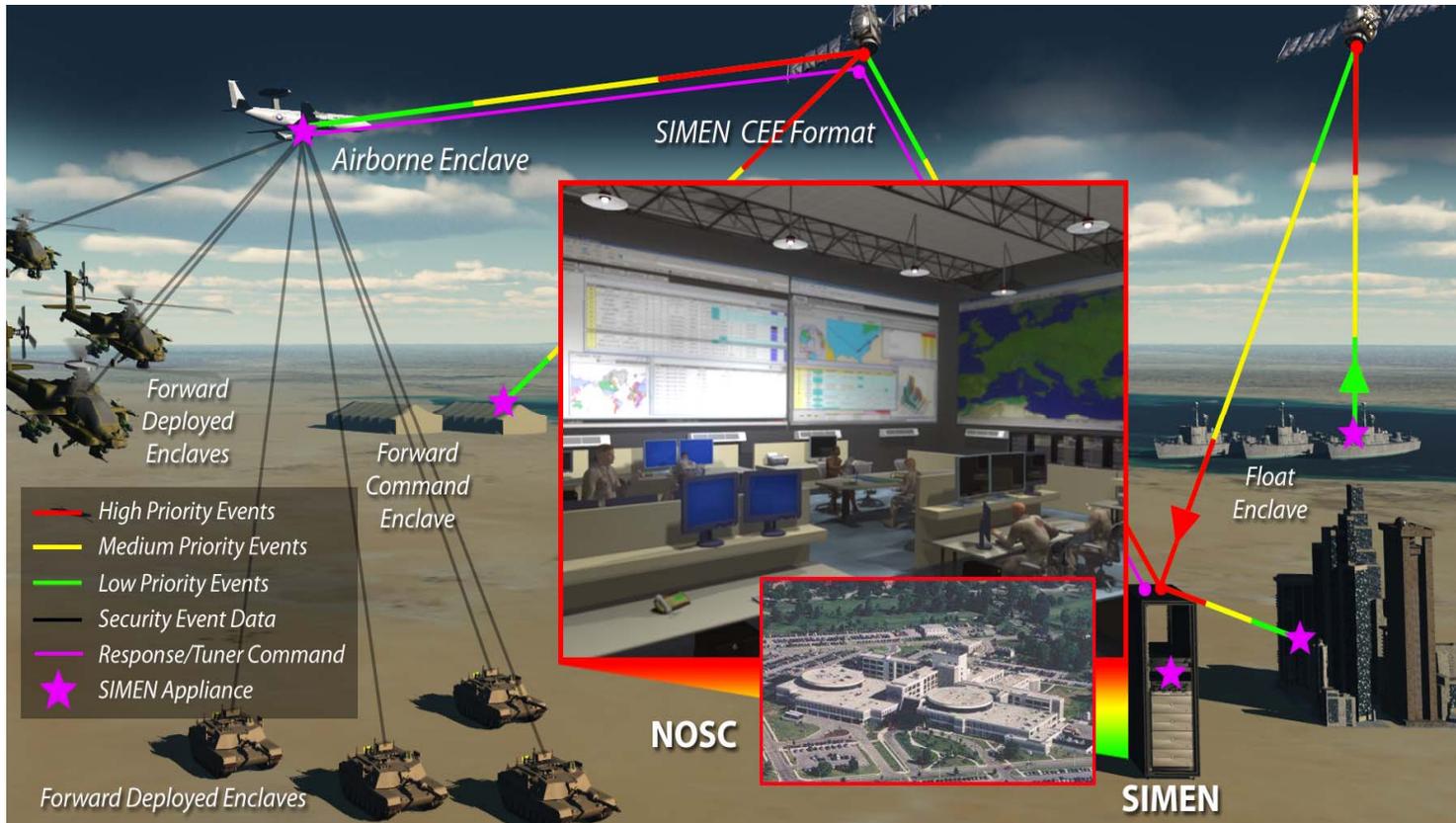
Demonstration



Impacts

- Provides a viable option for enclave IA monitoring and threat assessment
- Increases CND impact for DoD SIM deployments
- Influences COTS SIM vendor development
- Influences IA event standards development (CEE)
- Provides feedback to Airborne Network IA community

Future Plans



Community Adoption of SIMEN Technology and Common Event Expression