Understanding the Cognitive Science of Cyber Security

Nancy J. Cooke

Arizona State University

LASER Workshop

5/26/2016

This work has been supported by the Army Research Office under MURI Grant W911NF-09-1-0525.

Overview

- Why is this so Hard?
- Definitions and Theoretical Drivers
- The Living Lab Approach
  - Cognitive Task Analysis
  - Testbed Development
  - Empirical Studies and Metrics
  - Modeling
- Conclusion and Next Steps

Why is this so Hard?

- Defining/scoping the system
  - Which humans? What roles?
  - What is the task?
  - What is the context?
  - How are they interconnected in the larger system?
- What are the Goals? Research Questions?
  - Measurement
  - Ground Truth
- Ubiquitous Internet

ASU Arizona State University

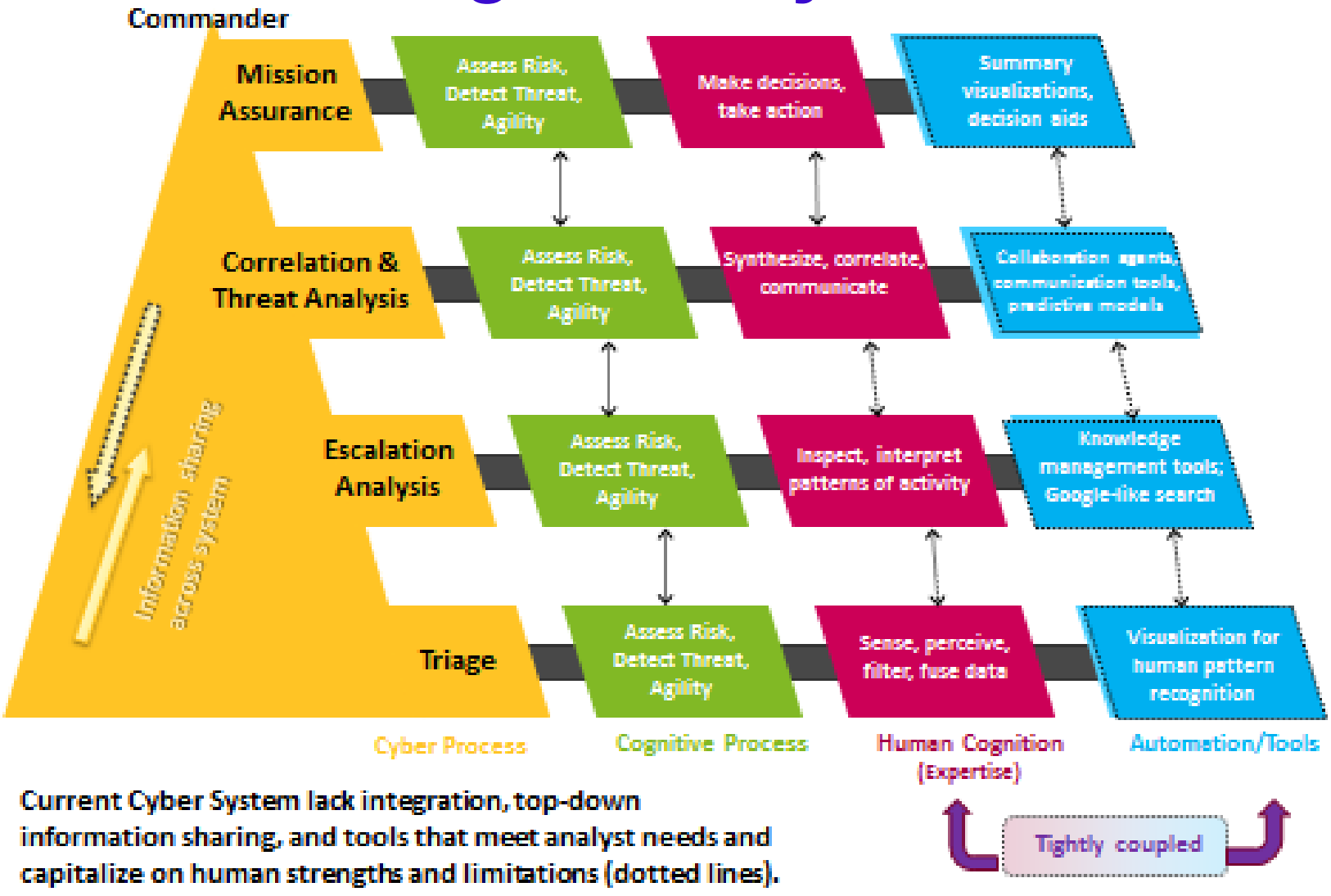
Definitions and Theoretical Drivers

- MURI (ARO) Cyber Situation Awareness
- Cyber Security as a Sociotechnical System
- Interactive Team Cognition
- Team Situation Awareness

Cyber Security as a Sociotechnical System

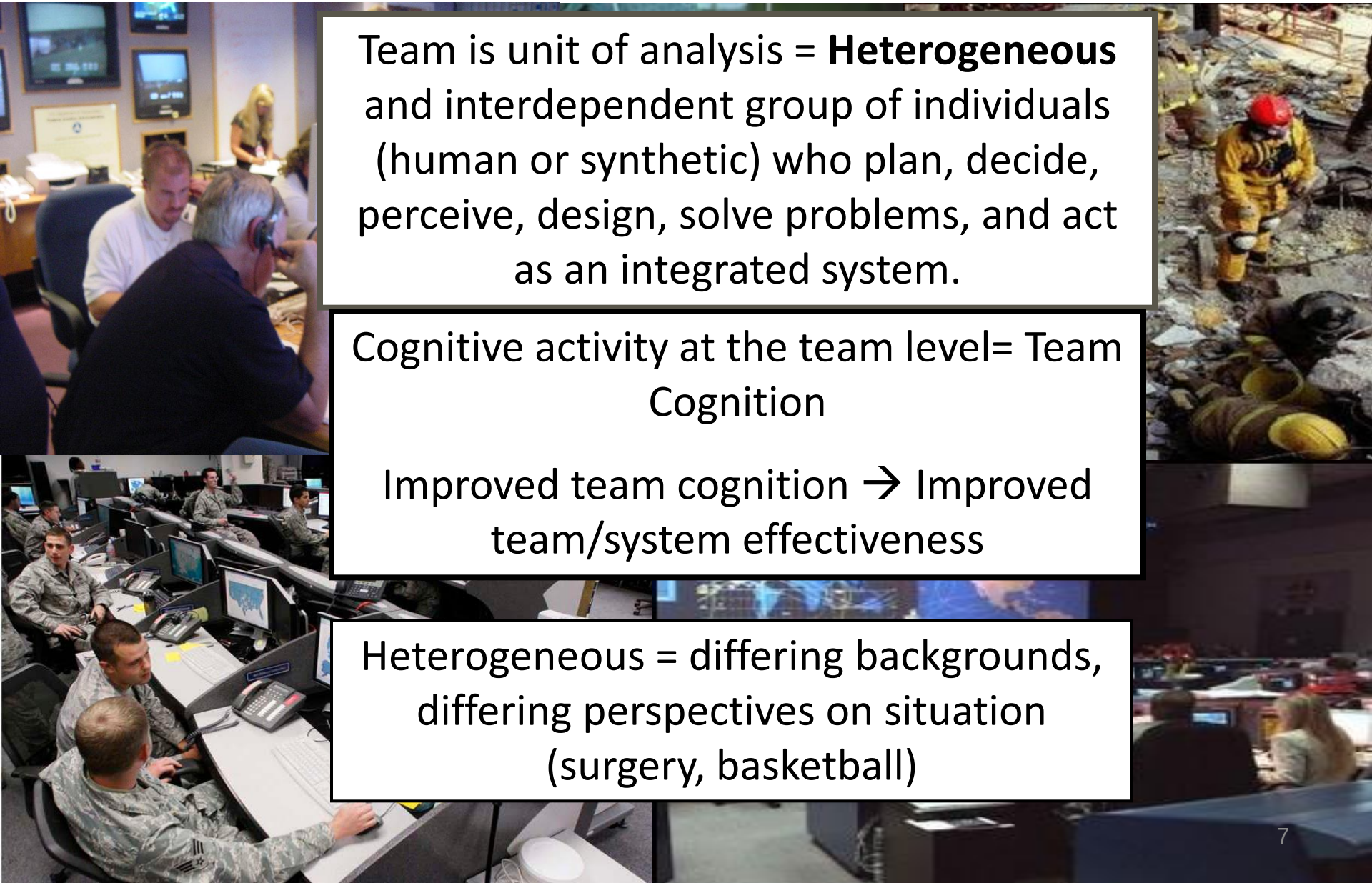
- **Cyber defense functions involve cognitive processes allocated to**
  - Human Operators of many kinds
  - Tools/Algorithms of many kinds
- **Human Operators**
  - Different roles and levels in hierarchy
  - Heterogeneity (Information, skills and knowledge)
- **Tools**
  - For different kinds of data analysis and visualization
  - For different levels of decision making
- **Together, human operators and tools are a sociotechnical system**
  - Human System Integration is required

Security Analysis: A Complex Cognitive System



Current Cyber System lack integration, top-down information sharing, and tools that meet analyst needs and capitalize on human strengths and limitations (dotted lines).

Interactive Team Cognition



Team is unit of analysis = **Heterogeneous** and interdependent group of individuals (human or synthetic) who plan, decide, perceive, design, solve problems, and act as an integrated system.

Cognitive activity at the team level= Team Cognition

Improved team cognition → Improved team/system effectiveness

Heterogeneous = differing backgrounds, differing perspectives on situation (surgery, basketball)

Interactive Team Cognition

Team interactions often in the form of explicit communications are the foundation of team cognition

ASSUMPTIONS

1) Team cognition is an activity; not a property or product
2) Team cognition is inextricably tied to context
3) Team cognition is best measured and studied when the team is the unit of analysis

ASU Arizona State University

Cooke, N. J., Gorman, J. C., Myers, C. W., & Duran, J.L. (2013). Interactive Team Cognition, *Cognitive Science, 37, 255-285,* DOI: 10.1111/cogs.12009.

Implications of Interactive Team Cognition

- Focus cognitive task analysis on team interactions
- Focus metrics on team interactions (team SA)
- Intervene to improve team interactions

Team Situation Awareness

A team's coordinated perception and action in response to a change in the environment

Contrary to view that all team members need to "be on the same page"

ASU Arizona State University

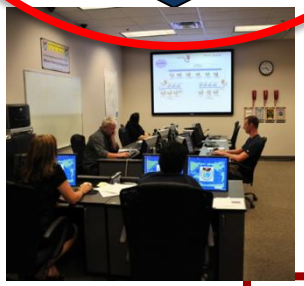
The Living Lab Procedure

BEGIN

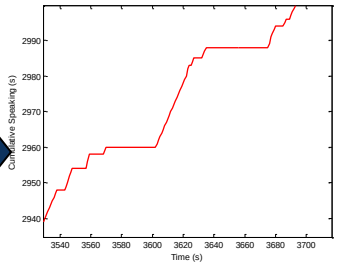
Field Data - CTA

END

Testbeds
1) CyberCog
2) DEXTAR/DETER

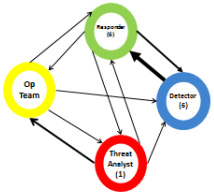


Empirical Studies in Testbeds

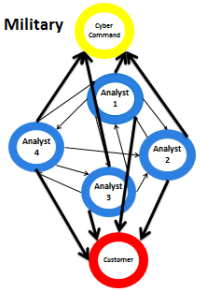


Social Network Diagrams of Incident Response/Network Defense Teams

Industry



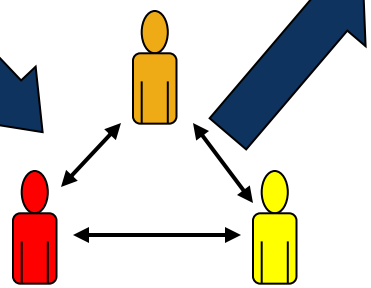
Military



ASU Arizona State University

EAST and Agent Based Modeling

Measures



Theory Development

Cognitive Task Analysis Activities

- Conducted literature review
- Cyber SA Workshop 2011
  - one hour breakout session with 3 cyber security analysts.

  Topics:
  - Structure of defense CERT departments work of the security analyst
  - Tasks performed by each analyst
  - Tools used by the analyst to perform the task
  - Team structure
  - Interaction among analysts within a team
  - Reporting hierarchy
- Cyber Defense Exercises
  - Air Force Academy, Colorado Springs, CO
  - CTA collaboration with PSU – WestPoint CDX logs
  - iCTF – International Capture the Flag at US Santa Barbara (Giovanni Vigna)
- Cyber Survey – web responses

Lessons Learned: Cyber Defense Analysts

- High stress
- High attrition rate
- High False Alarm Rate
- Low Situation Awareness

- Cyber analysis task does not make the best use of individual capabilities
- Expertise is challenging to identify

Lessons Learned: The Analyst Task

- Unstructured task; hierarchical within government, but within units it breaks down
- Variance across departments, agencies
- Ill-structured with no beginning or end
- Little to no standardized methodology in locating and response to an attack
- Massive amounts of data, information overload, high uncertainty
- No software standards
- Metrics of individual and team performance and process are lacking

ASU Arizona State University

Lessons Learned: Training Analysts

- No cohesive training programs for specific tasks or not standardized enough
- No feedback
- No way to benchmark or evaluate the efficacy of individuals in the real world. No ground truth
- No performance metrics

ASU Arizona State University

Lessons Learned: Teamwork Among Analysts

- Teamwork is minimal in cyber security
- Cyber analysts work as a group – Not as a team
- Possible Reasons
  - Cognitive overload
  - Organizational reward structures
  - “Knowledge is Power”
  - Lack of effective collaboration tools

- Little role differentiation among teammates
- Low interaction; a collective with each working independently
- Informal, *ad hoc* interactions, loosely coupled system, and lack of distribution of task

ASU Arizona State University

The Living Lab Procedure

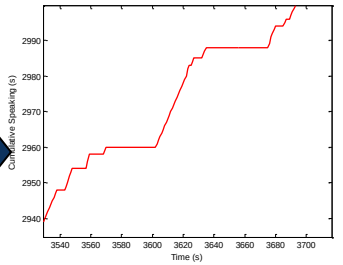
BEGIN

Field Data - CTA

END

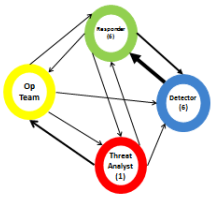
Testbeds
1) CyberCog
2) DEXTAR/DETER

Empirical Studies in Testbeds

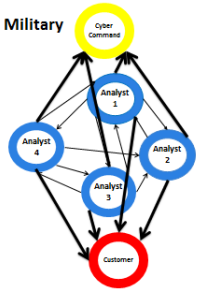


Social Network Diagrams
of Incident Response/Network Defense Teams

Industry



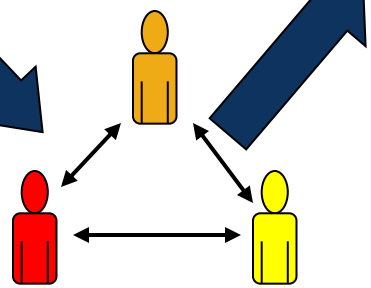
Military



ASU Arizona State University

EAST and Agent Based Modeling

Measures



Theory Development

CyberCog Synthetic Task Environment

- Simulation environment for team-based cyber defense analysis
- Emulating the work, interaction, and collaboration of Cyber Network Defense analyst teams
- A research testbed for:
  - Controlled experiments
  - Assessment of interventions, tools, aids

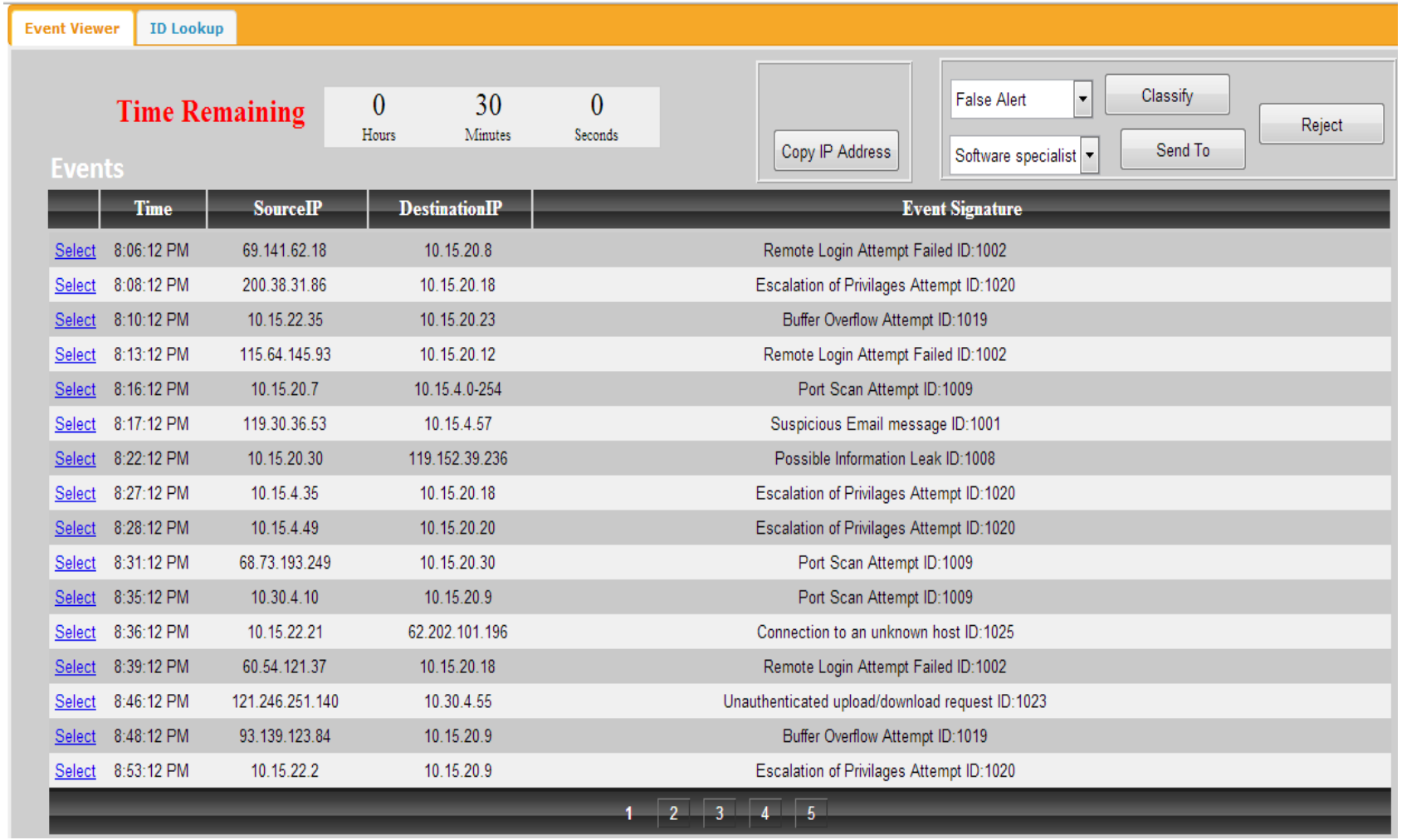
ASU Arizona State University

CyberCog Team Task

- Three team members monitor IDS alerts and network activity of 3 different sub-networks for a given scenario
- Find IDS alerts pertinent to the attack
- Find the systems affected and attack path
- On consensus, team submits their findings

ASU Arizona State University

CyberCog Display



ARIZONA STATE UNIVERSITY

CyberCog Measures

PERFORMANCE

- Alert classification accuracy

TEAM INTERACTION

- Communication – audio data
- Computer events
- Team situation awareness
  - » Attack path identified (systems, order)
  - » Attack information distributed across 2-3 team members
  - » Team coordination is required to identify and act on threat
  - » Roadblock can be introduced through equipment malfunctions (e.g., tool crash)

WORKLOAD

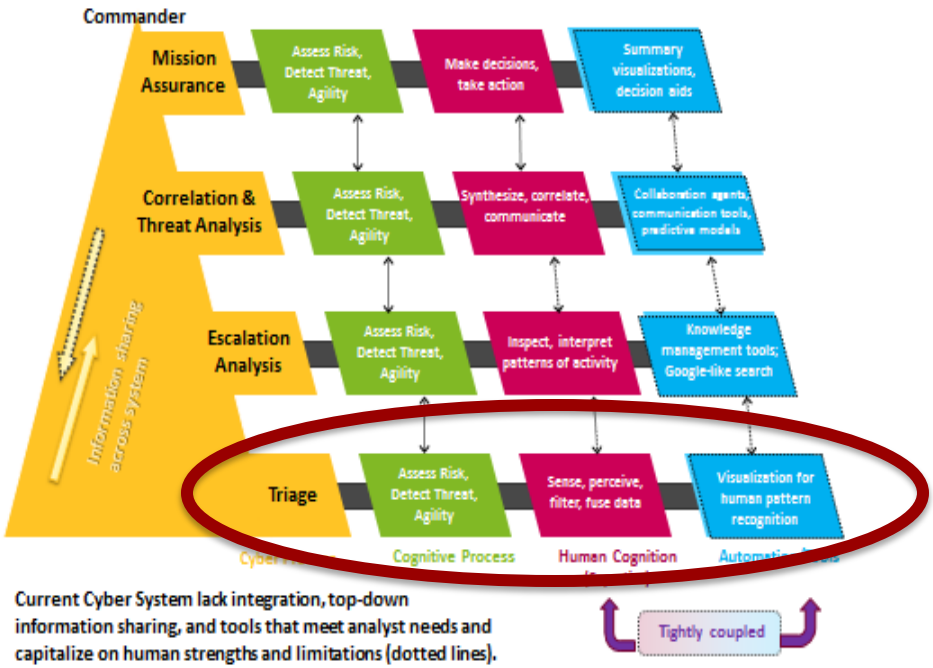
- NASA TLX – workload measure

CyberCog Modifications

- Task Distribution – Through task training emulate individual and specialized experience
  - Analyst 1 - database containing system vulnerabilities
  - Analyst 2 - wiki-styled website forum-information on possible attack scenarios
  - Analyst 3 - network map-illustrated systems and their physical layout
- Each analyst receives a distinct set of intrusion events to analyze and classify into a given set of categories.
- To effectively classify the events, the analyst
  - Must integrate and analyze information from multiple sources (network activity logs, vulnerability data etc.)
  - Must interact with other analysts
- Data Sets scripted based on 2009 WestPoint CDX logs
- Measures team performance and logs interaction

CyberCog Issues

- Low-level triage task
- Signal detection
- Not capturing richer problem solving tasks



Current Cyber System lack integration, top-down information sharing, and tools that meet analyst needs and capitalize on human strengths and limitations (dotted lines).

DEXTAR/DETER

Defense EXercises for Team Awareness Research/DEfense Technology Experimental Research

- Higher fidelity testbed for human-in-the loop cyber security research
- Marries CyberCog environment with DETER
- Analyze cyber-team performance with up to six members
- Collect user interaction and team performance data
- Screen capture and audio/video recording
- Large-scale virtual networks are fully customizable
- Supports Linux and Windows virtual machines and virtual servers
- Virtual network integration with real testbed machines
- Supports human, scripted, and agent cyberattacks
- Record temporal traffic and network performance data
- Requires skilled participants

ASU Arizona State University

The Living Lab Procedure

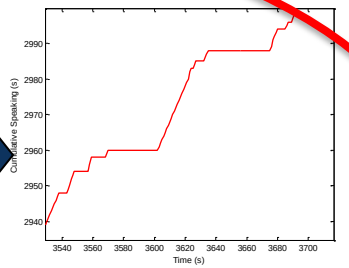
BEGIN

Field Data - CTA

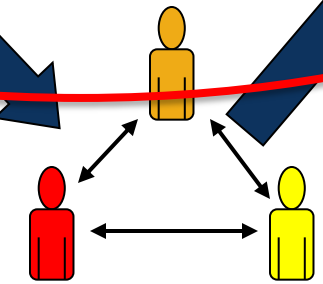
END

Testbeds
1) CyberCog
3) DEXTAR/DETER

Empirical Studies in Testbeds

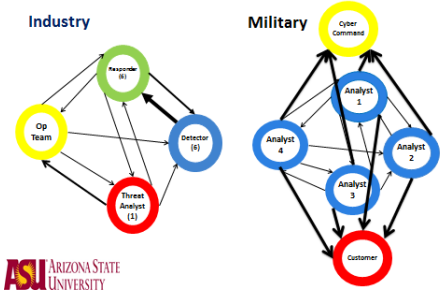


Measures



Theory Development

Social Network Diagrams of Incident Response/Network Defense Teams



ASU Arizona State University

EAST and Agent Based Modeling

Experiment 1: Cyber Groups vs. Teams

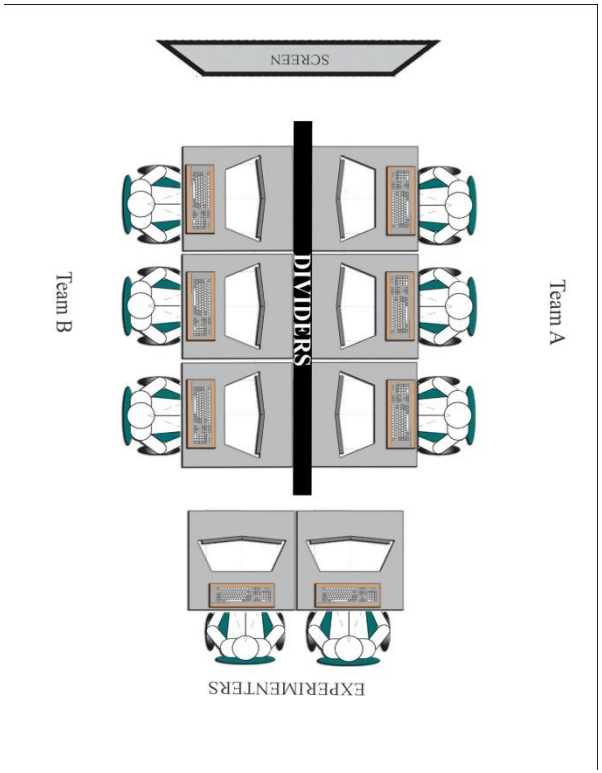
Hypotheses

- Reward structures conducive to team work in cyber defense analyst groups performing triage level analysis will lead to higher signal detection performance.
- Improving interactions between analysts can improve overall cyber defense performance

The Experiment

- 3-person teams/groups in which each individual is trained to specialize in types of alerts
- 2 conditions:
  - Team Work (Primed & Rewarded for team work)
  - Group Work (Primed & Rewarded for group work)
- 6 individuals at a time
  - Team Work - Competition between the 2 teams
  - Group Work - Competition between the 6 individuals
- Experimental scenarios:
  - 225 alerts
  - Feedback on number of alerts correctly classified - constantly displayed on big screen along with other team or individual scores
- Simulates knowledge is power for group condition
- Measures

  Signal Detection Analysis of Alert Processing
  Amount of Communication
  Team situation awareness
  Transactive Memory
  NASA TLX – workload measure

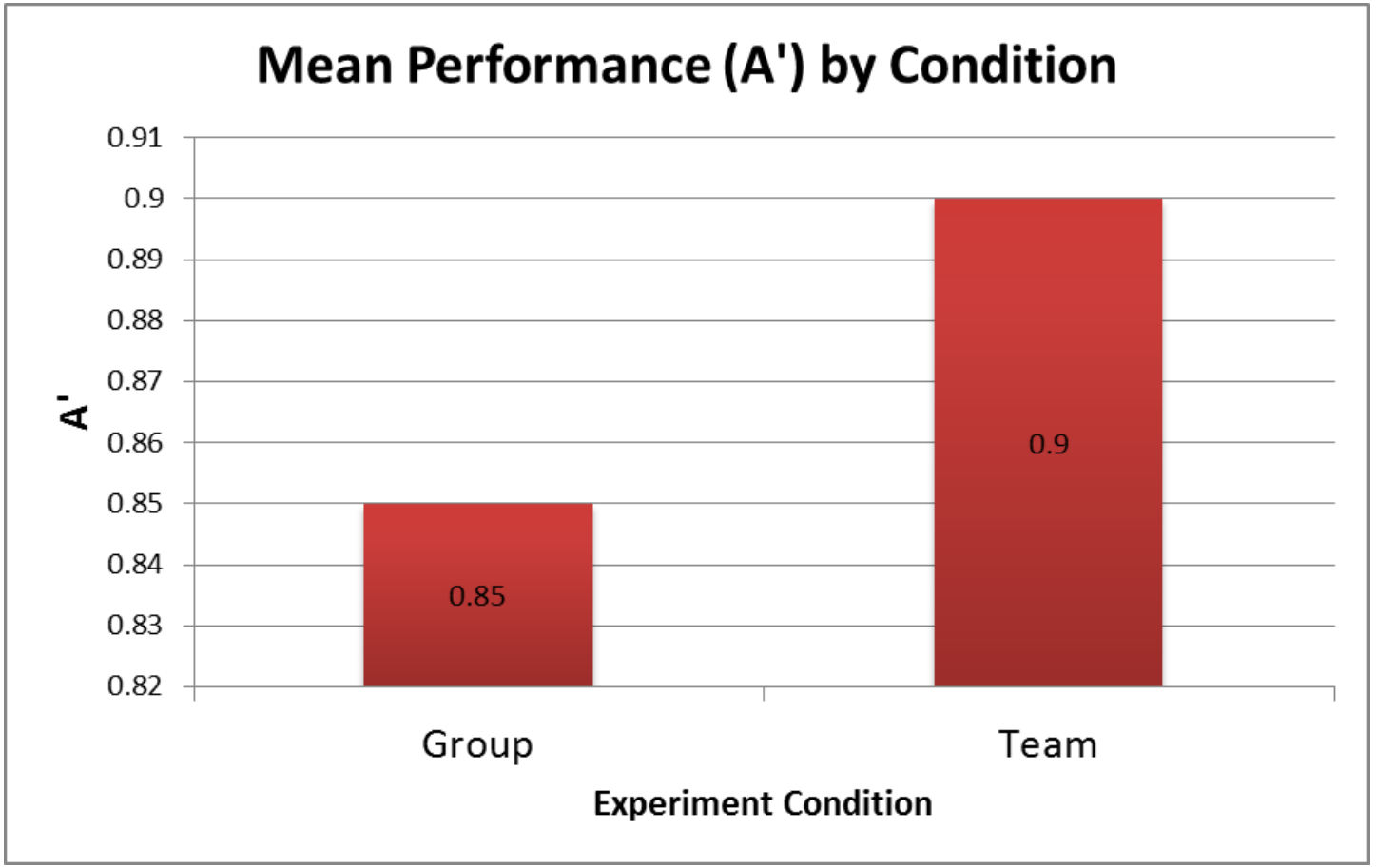


ARIZONA STATE UNIVERSITY

Cyber Teaming is Beneficial for Analyzing Novel and Difficult Alerts

- Working as team helps when alerts are novel and involves multi step analysis, not otherwise.
- Signal Detection Measure: A' as performance measure
- A' ranges from values 0.5 and 1 with 0.5 indicating lowest performance possible and 1 indicating highest performance possible.

Cyber Teaming Helps When the Going Gets Rough



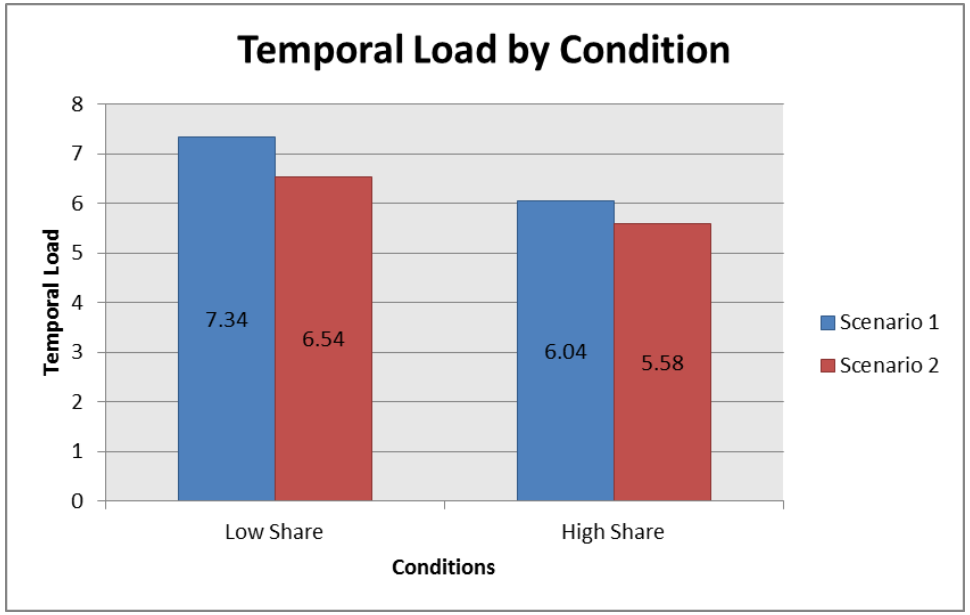
Sensitivity to true alerts

ARIZONA STATE UNIVERSITY

F(1,18) = 5.662, *p* = .029** (Significant effect of condition)

Groups that Share Less Information Perceive More Temporal Demands than High Sharers

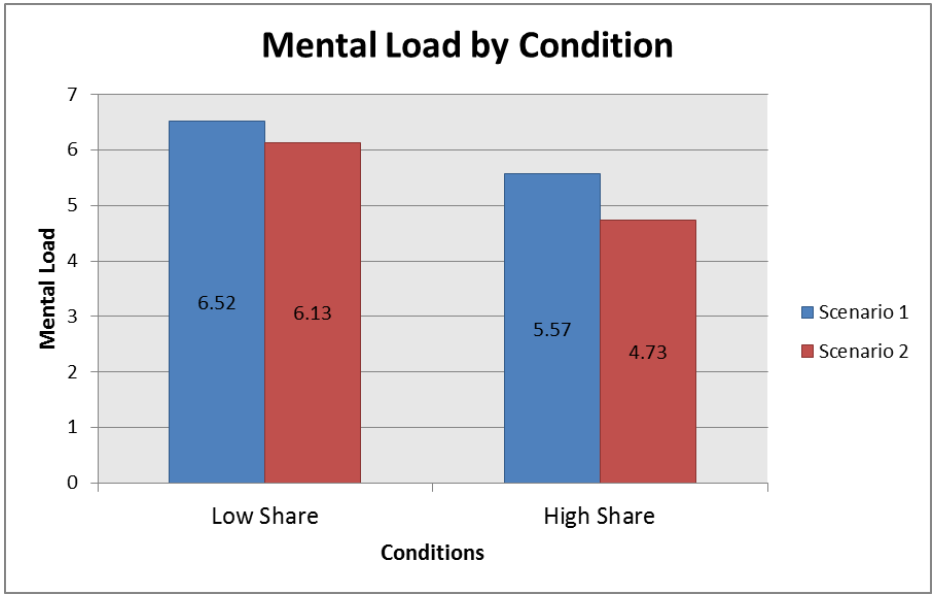
- NASA TLX Workload Measure: **Temporal Demand**
- Measures perception of time pressure
- Higher the value higher the task demand



Statistically significant across scenarios and conditions (p-value = 0.020)

Groups that Share Less Information Perceive Work to be More Difficult than High Sharers

- NASA TLX Workload Measure: **Mental Effort**
- Measures perception of mental effort
- Higher the value, more mental effort required



Statistically significant across scenarios and conditions (p-value = 0.013)

Conclusion

- Break the “Silos”
- Use the power of human teams to tackle information overload problems in cyber defense.
- Simply encouraging and training analysts to work as teams and providing team level rewards can lead to better triage performance
- Need collaboration tools and group decision making systems.

Experiment 2: Information Pooling Bias

The tendency for group members to spend more time and energy discussing information that all members are already familiar with (i.e., shared information), and less time and energy discussing information that only some members are aware of (i.e., unshared information)

- Poor decision-making can result
- It is impossible for every team member to know all the information (rely on others expertise)
- This may be an issue in the cyber domain

ASU Arizona State University

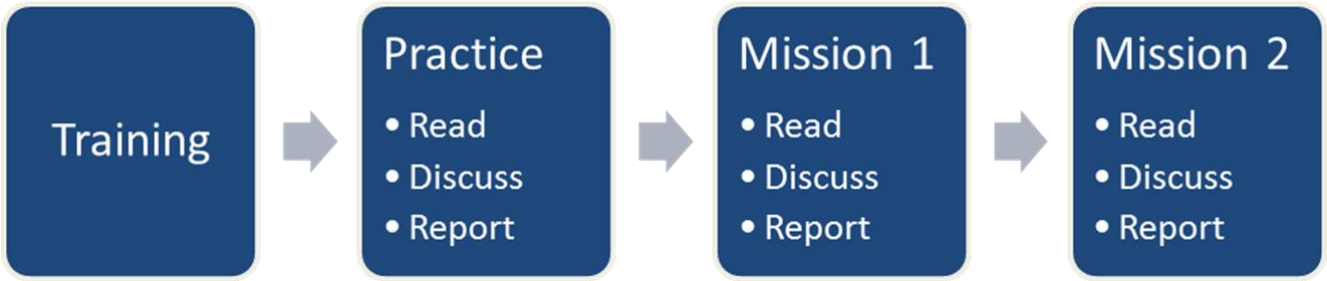
Rajivan, P. (2014). Information pooling bias in collaborative cyber forensics. PhD thesis, Simulation, Modeling, and Applied Cognitive Science, Arizona State University.

Research Questions

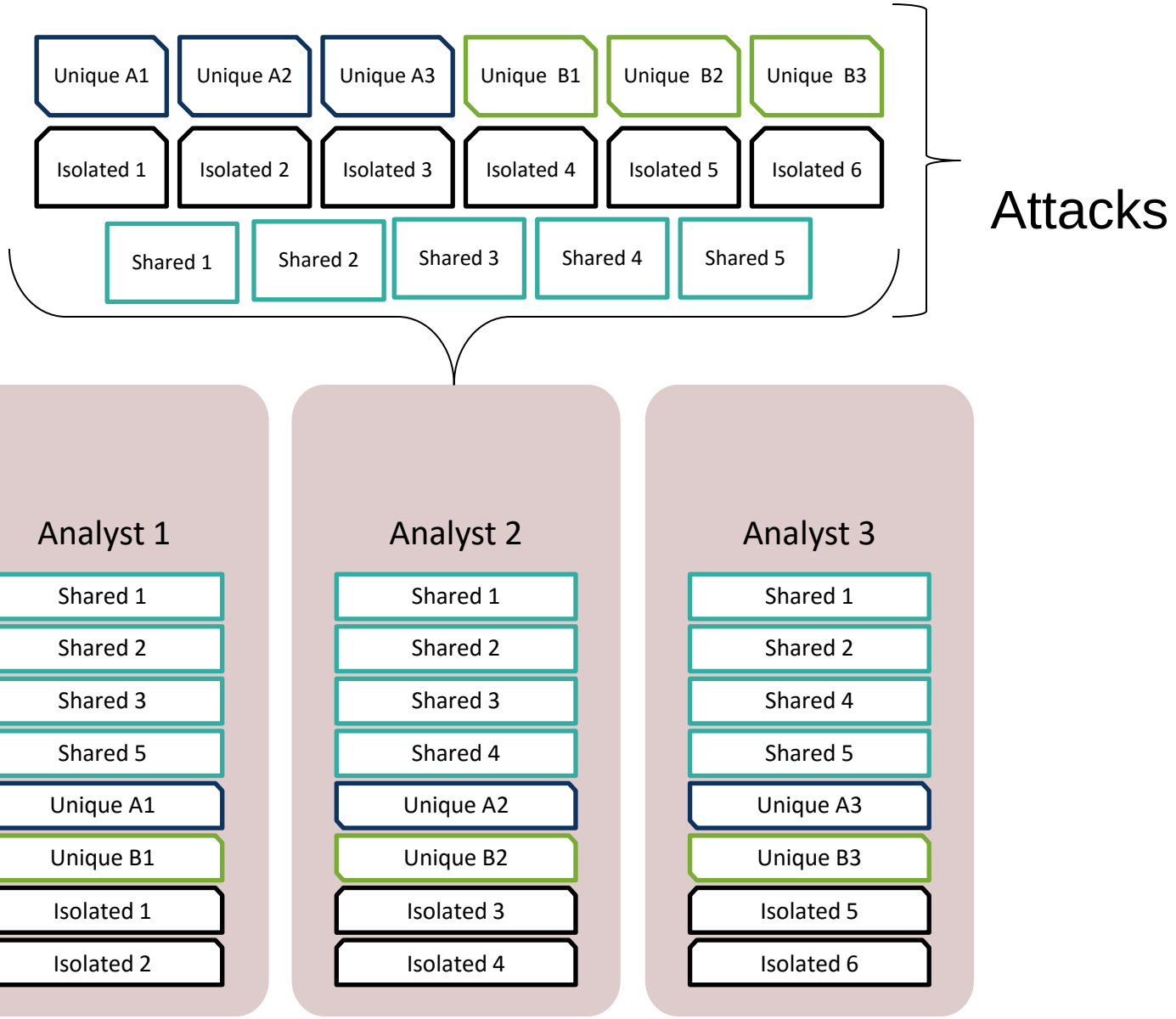
1. Does information pooling bias affect cyber forensic analyst team discussions and decisions?
2. Does a tailor made collaboration tool lead to superior analyst performance compared to using off-the-shelf collaboration tool such as wiki software?

Procedure

- 30 teams of 3 participants
- Trained on cyber security concepts, types of attacks and tasks to be performed
- Pre-discussion reading and discussion
- Practice mission
- 2 main missions
- Goal – Detect large scale attacks



Attack Data Distribution in Missions

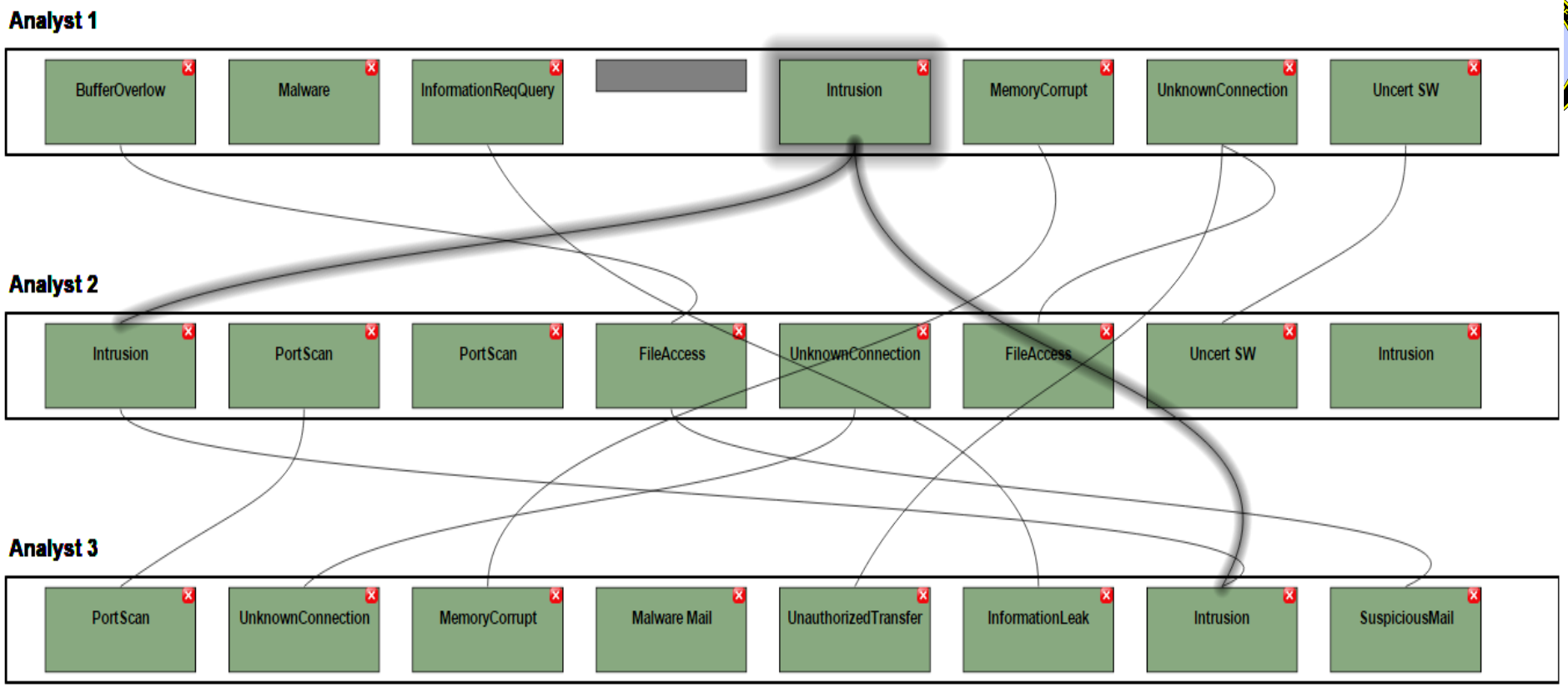


Experimental Design

	Trial 1 - Baseline	Trial 2
Tool Type	Slide Based	Slide Based
	Slide Based	Wiki
	Slide Based	Collaborative Visualization

Collaborative Visualization Tool

- Collaborative visualization tool designed from a cognitive engineering perspective
- To mitigate the information pooling bias in cyber defense analysts
- Improve information sharing and decision making performance



Observation Description

```
1001Title:Intrusion
---------
Analyst:1
---------
Time of Attack 11:30Am April 11 2014
Source IP 154.48.48.48
Destination IP 185.10.10.X
Type of Attack Intrusion
A brute force intrusion from a remote IP - 154.48.48.48 was detected on different machines on the sub-network1.
A unknown remote machine tried to gain access to employee machines through several brute force logins
Further investigation revealed that the remote system was successful in logging in to a router machine.
Used the login id - admin and password- arsenal123.
Using the login, the attacker tried to copy the address tables in the router  Possibly to gain access to other machines in the network.
```

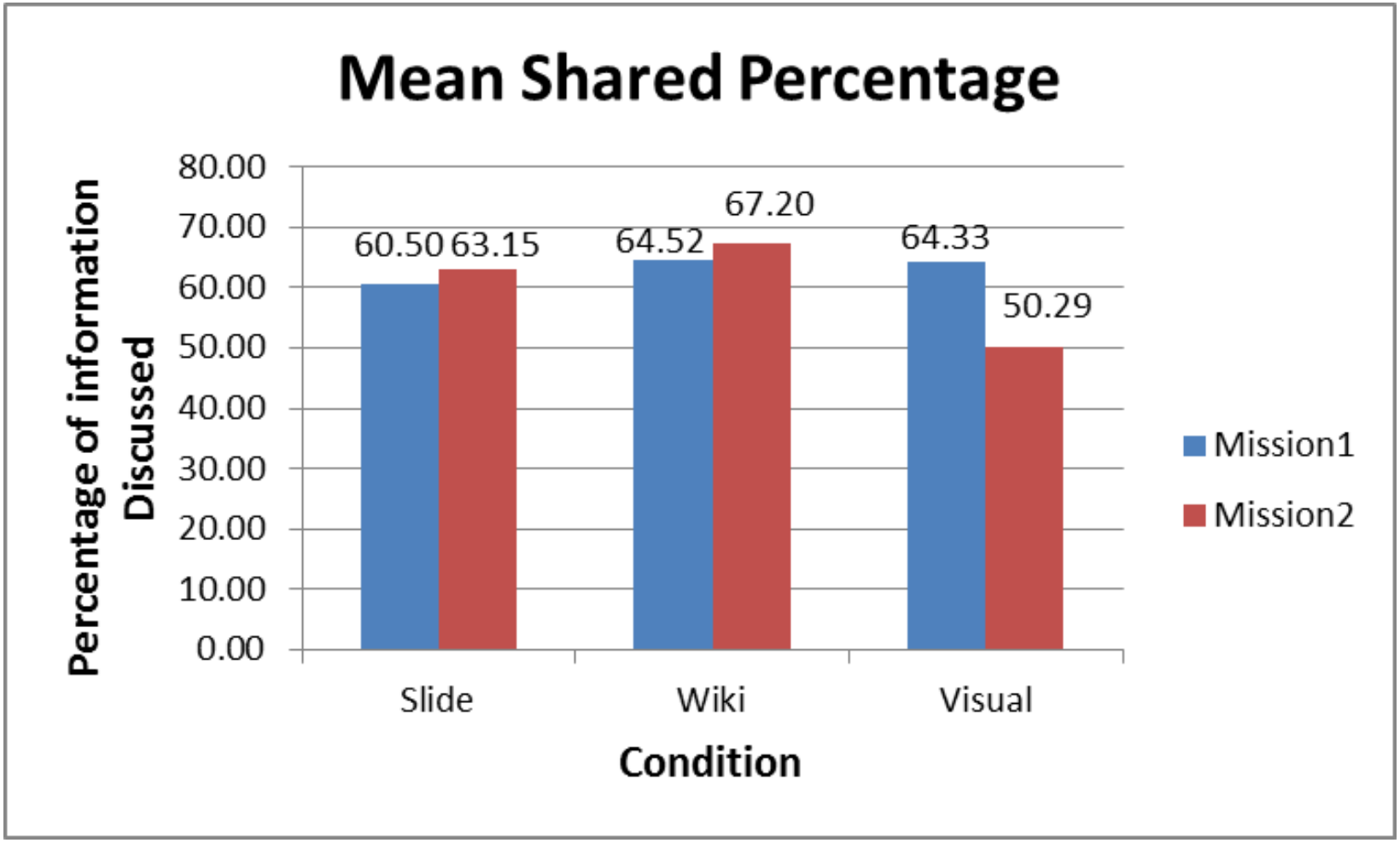
Measures

- Communication coding
  - Amount of time spent on discussing each attack
  - Number of mentions of each attack
- Decision quality
  - All attacks detected ?
- Workload & Demographics

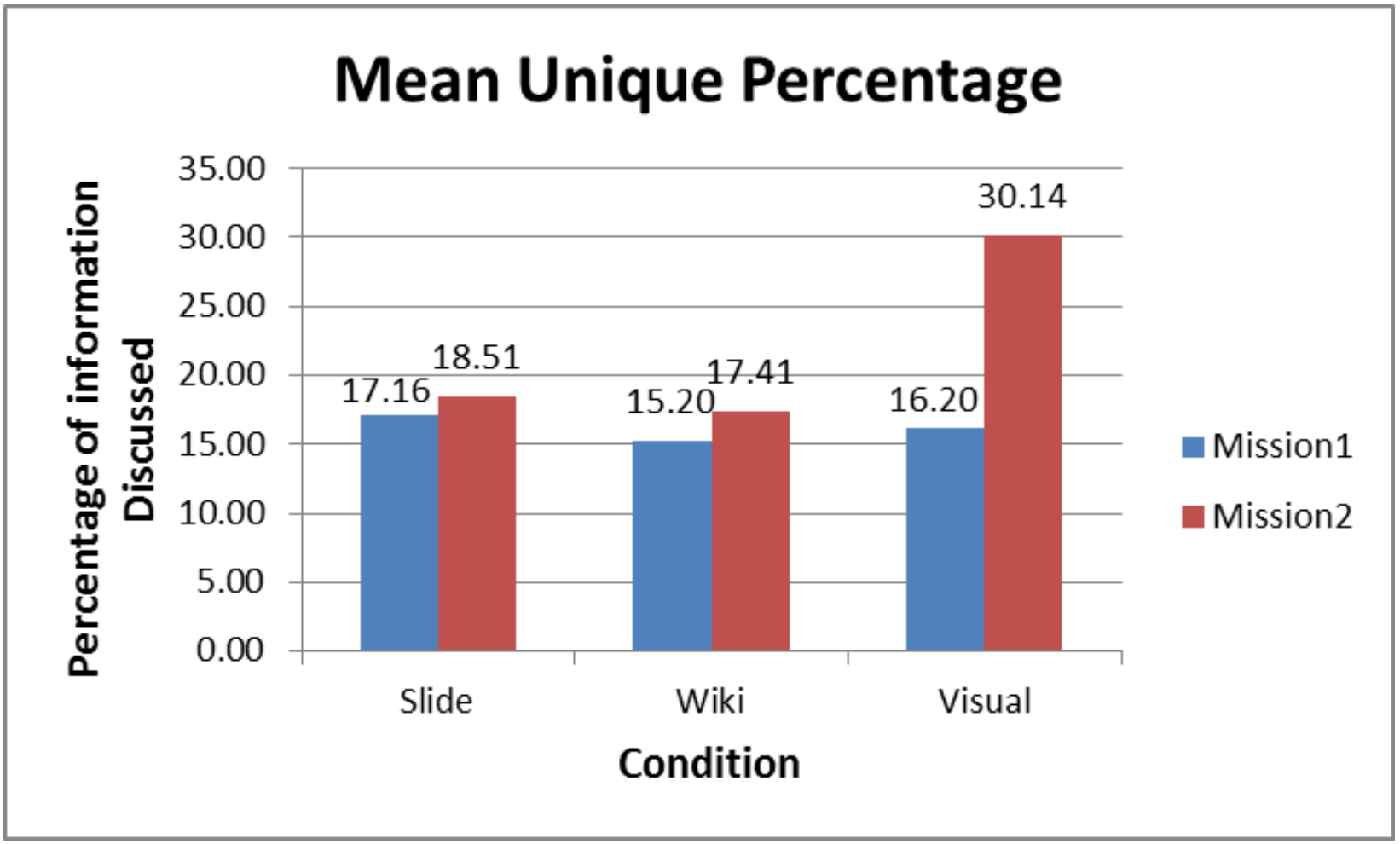
Team Level Measures

- Shared Discussion
  - Percentage of discussion spent on discussing attacks that are shared among members
- Unique Discussion
  - Percentage of discussion spent on discussing attacks are unique but are part of a large scale attack
- Detection Performance
  - Number of attacks detected (Both shared and unique)
  - Max possible = 18 (4*3 + 2*3)

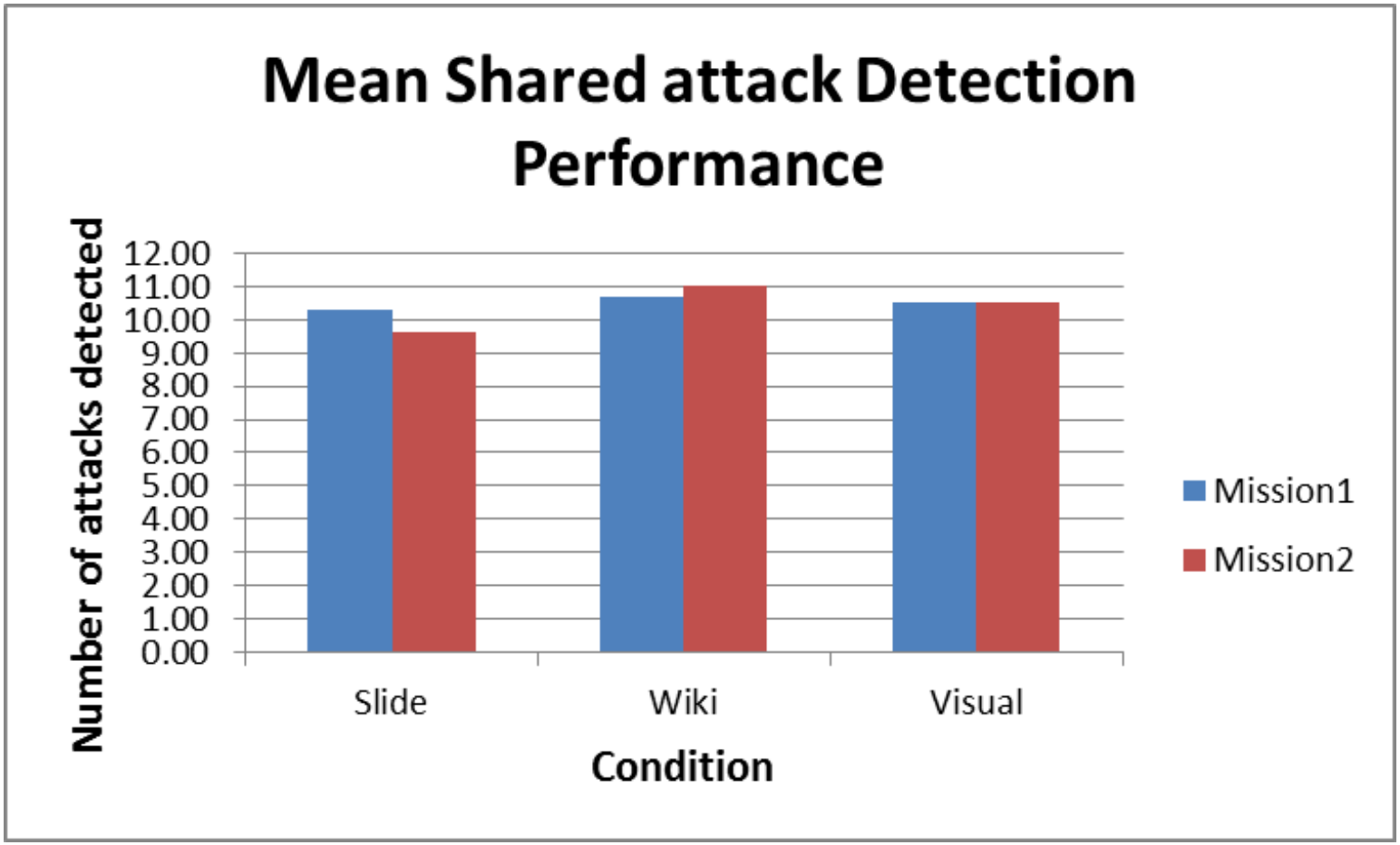
Percentage of shared information discussed compared between Missions



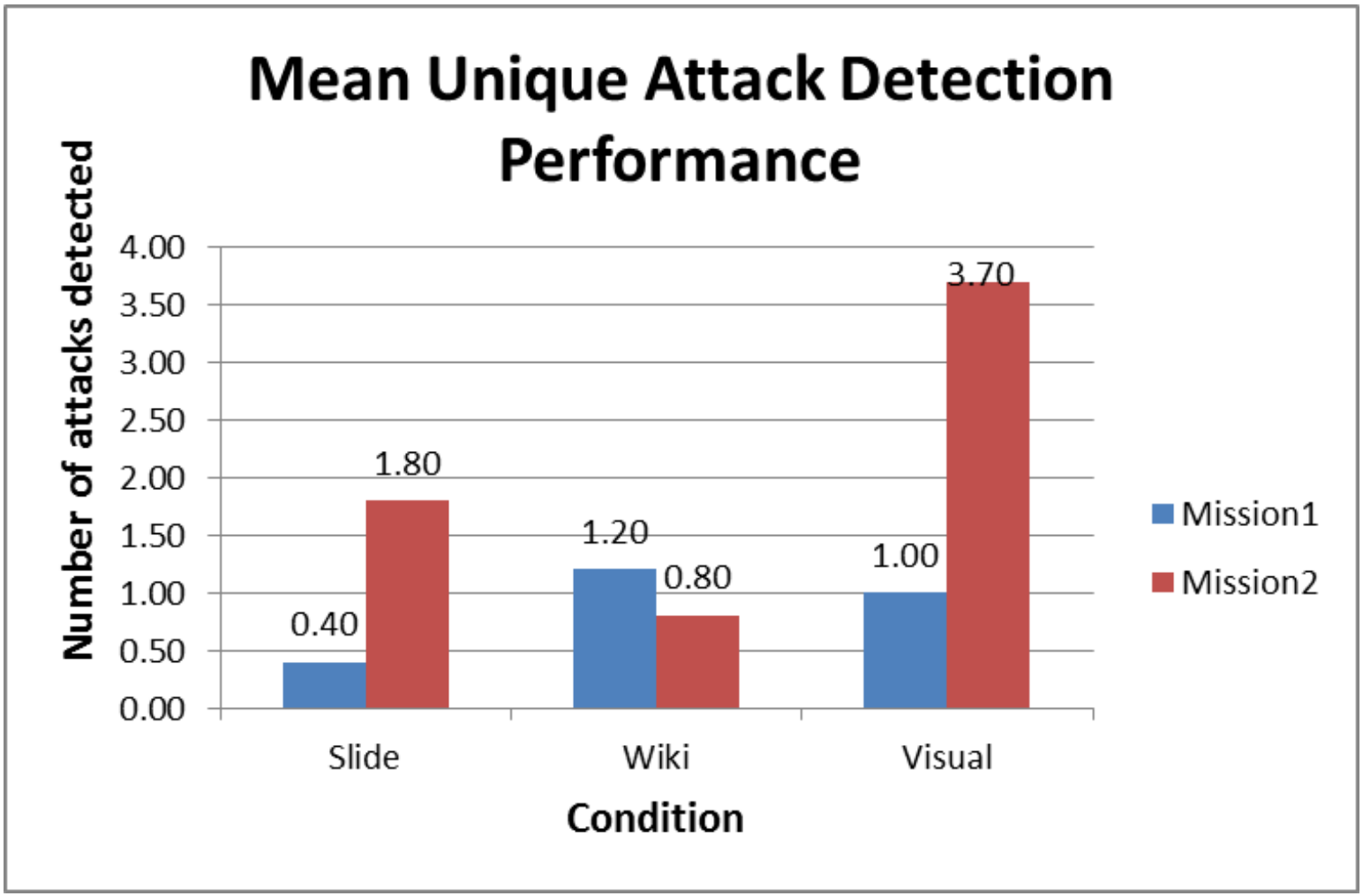
Percentage of unique information discussed compared between Missions



Number of shared attacks detected (Performance) compared between Missions



Number of unique attacks detected (Performance) compared between Missions



Summary of Results

- Significantly more shared attack information discussed
  - Cyber Defense analysts undergo information pooling bias
  - Prevents detecting APT kinds of attacks
- Use of cognitive friendly visualization reduces the bias, improves performance
- Off the shelf collaboration tools don't help

ASU Arizona State University

The Living Lab Procedure

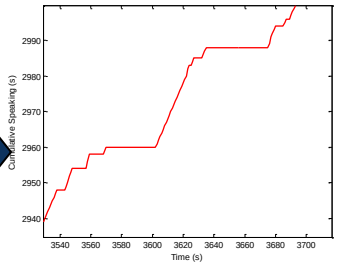
BEGIN

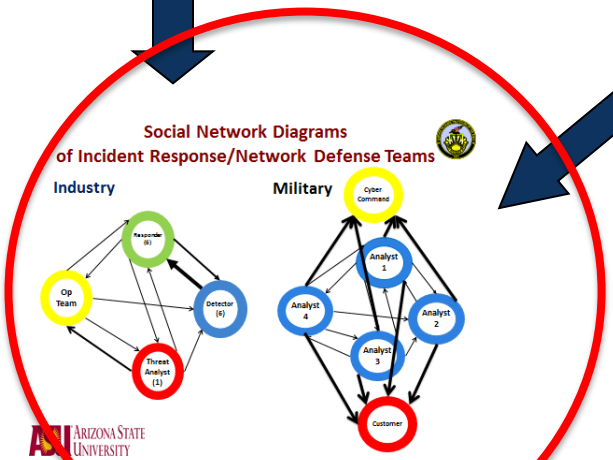
Field Data - CTA

END

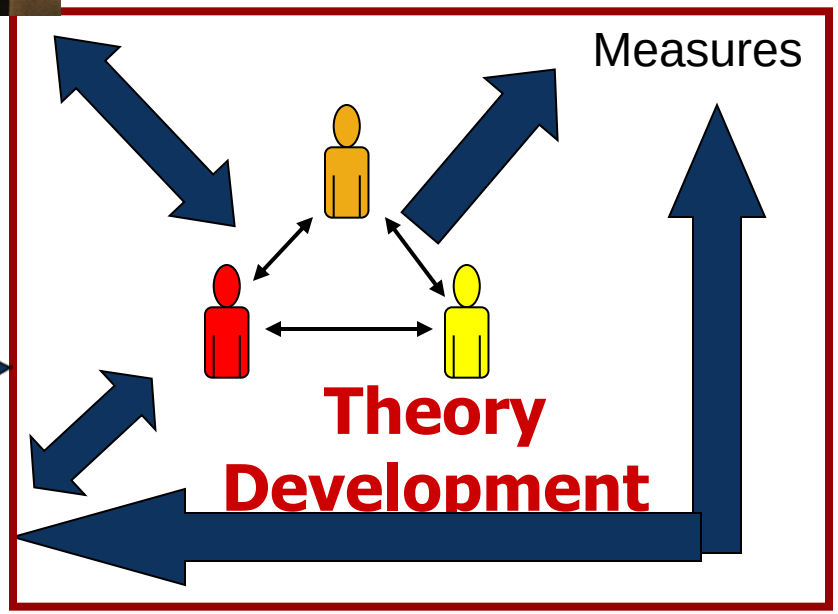
Testbeds
1) CyberCog
2) DEXTAR/DETER

Empirical Studies in Testbeds





EAST and Agent Based Modeling



Agent-Based Modeling

- Human-in-loop experiment
  - Traditional method to study team cognition
- Agent based model
  - A complimentary approach
- Modeling computational agents with
  - Individual behavioral characteristics
  - Team interaction patterns
- Extend Lab Based Experiments

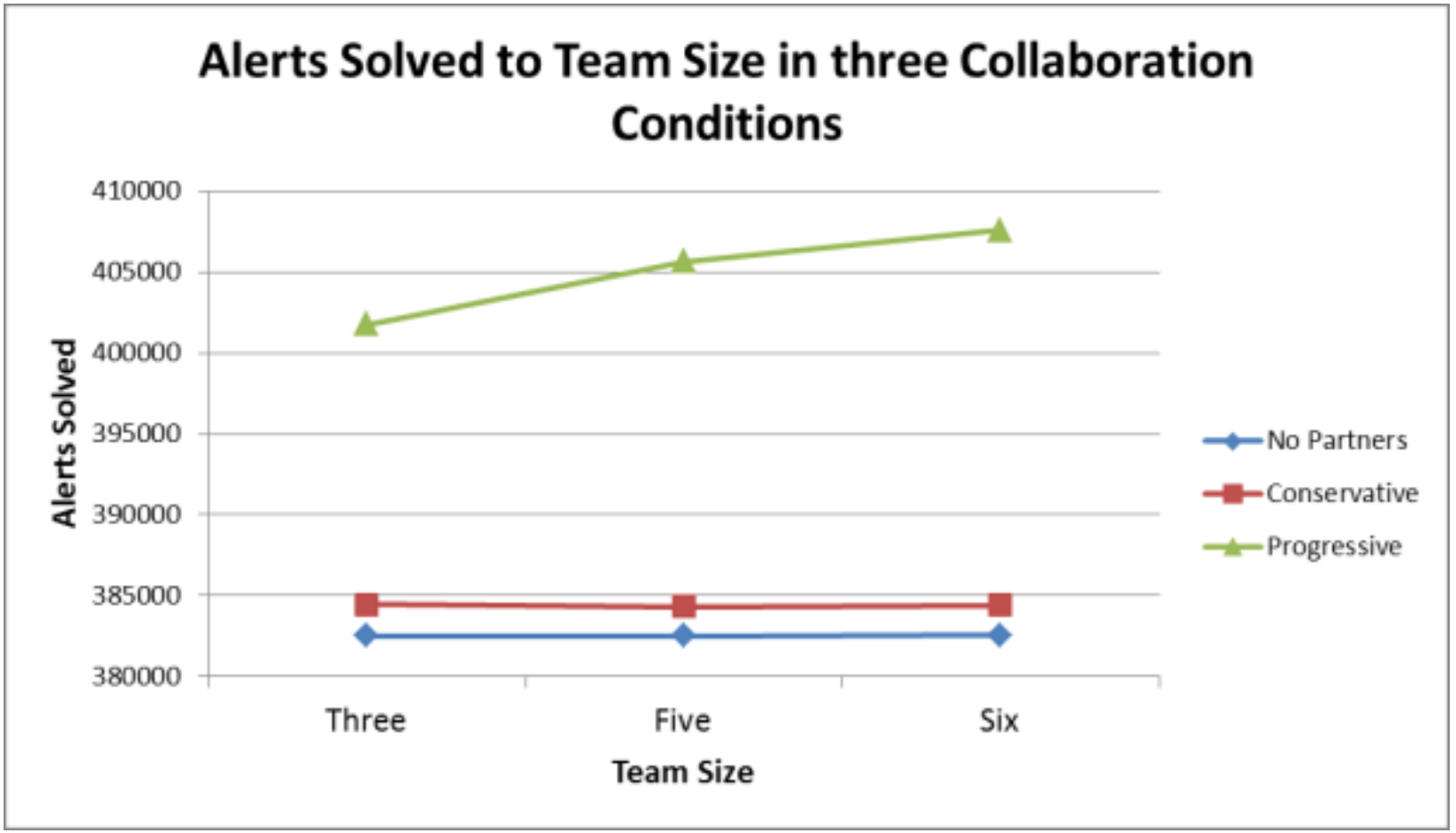
Model Description

- Agents: Triage analysts
- Task: Classify alerts
- Rewards for classification
- Cognitive characteristics:
  - Knowledge and Expertise
  - Working memory limit
  - Memory Decay

Model Description

- **Learning Process**: Simplified – Probability based – 75% chance to learn
  - Cost: 200 points
  - Payoff: 100 points
- **Collaboration**: Two strategies to identify partners
  - Conservative (homogeneous partners) or Progressive (heterogeneous partners)
  - Cost: 100 points for each
  - Payoff: 50 points for each
- **Attrition**

Irrespective of Team Size Agents in Progressive Condition Classified More Alerts



Conservative – select homogeneous partners;
Progressive – select heterogeneous partners

Conclusions

- Small heterogeneous teams of triage analysts could be beneficial.
- Agent based modeling
  - Can extend lab based experiments
  - Can be used to ask more questions quickly
  - Can raise new questions and identify gaps

Two Case Studies and EAST Models

EAST

Event Analysis of Systemic Teamwork) framework (Stanton, Baber, & Harris, 2012)

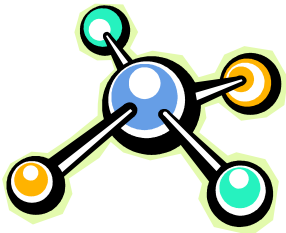
- **Integrated suite of methods allowing the effects of one set of constructs on other sets of constructs to be considered**
  - Make the complexity of socio-technical systems more explicit
  - Interactions between sub-system boundaries may be examined
  - Reduce the complexity to a manageable level
- **Social Network**
  - Organization of the social system (i.e., communications structure)
  - Communications taking place between the actors working in the team.
- **Task Network**
  - Relationships between tasks
  - Sequence and interdependences of tasks
- **Information Network**
  - Information that the different actors use and communicate during task performance

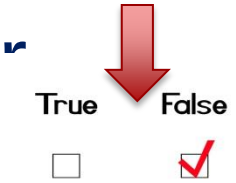
ASU Arizona State University

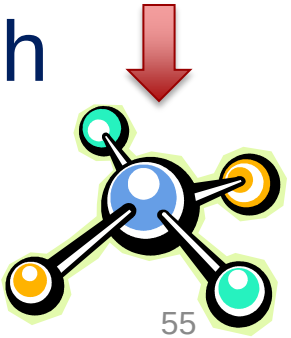
With Neville Stanton, University of Southampton, UK

Approach

- Interviews with cyber network defense leads from two organizations on social structure, task structure, and information needs
- Hypothetical EAST models created
- Surveys specific to organization for cyber defense analysts developed
- Surveys administered to analysts in each organization to refine models

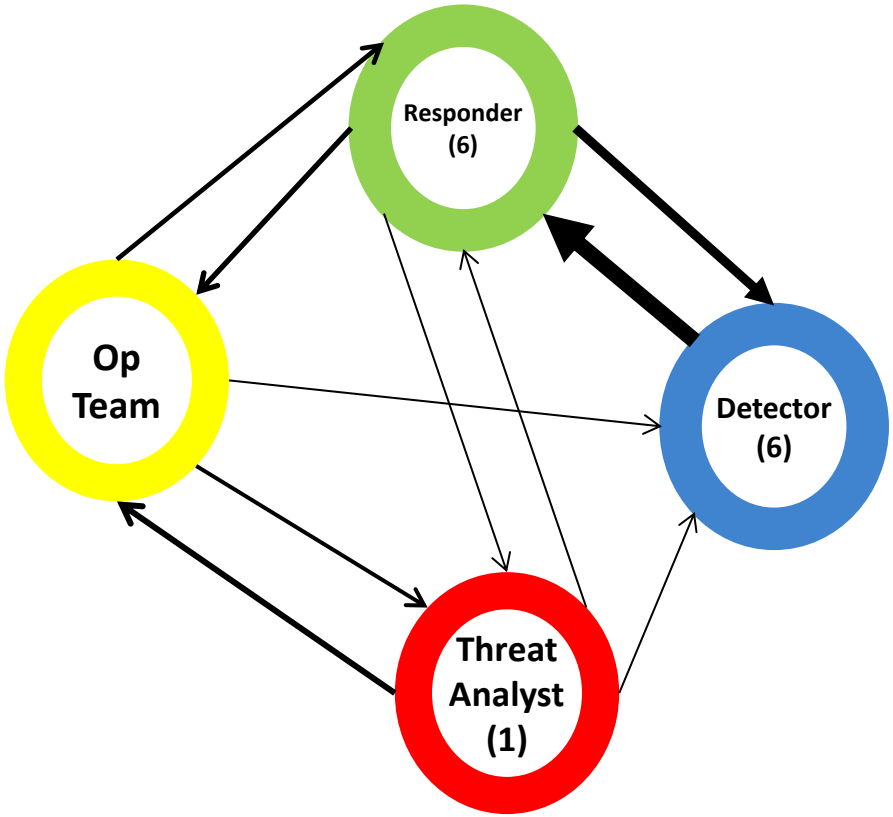




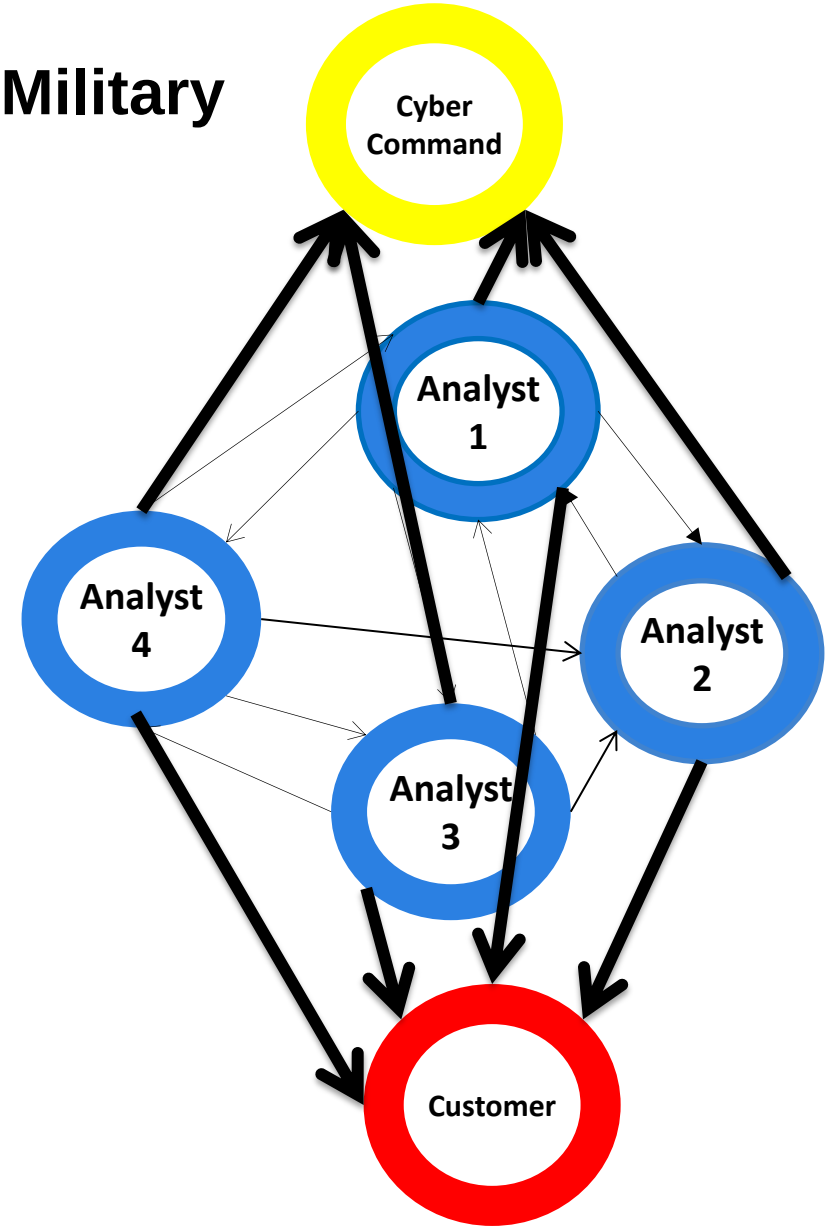


Social Network Diagrams of Incident Response/Network Defense Teams

Industry

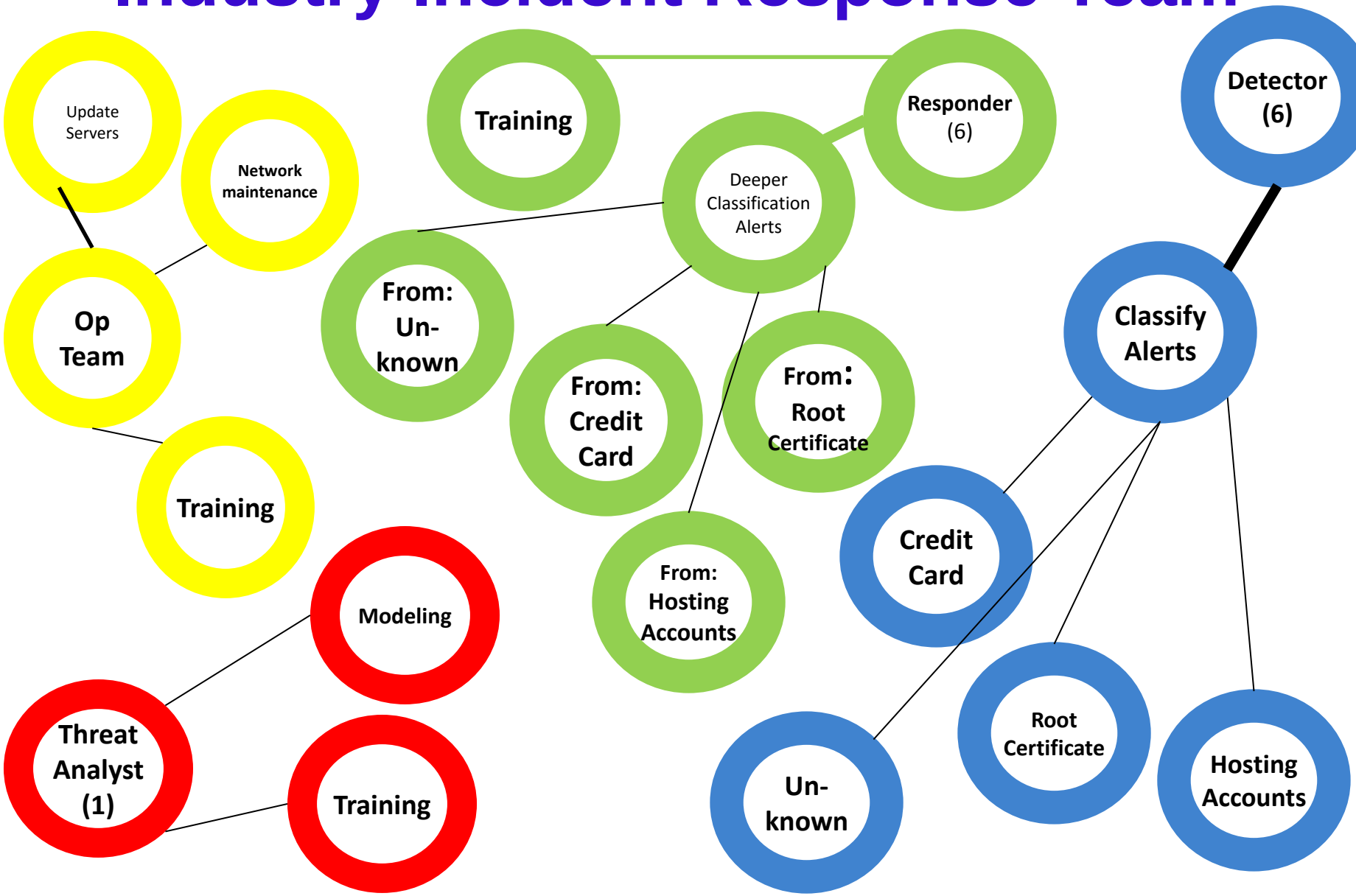


Military

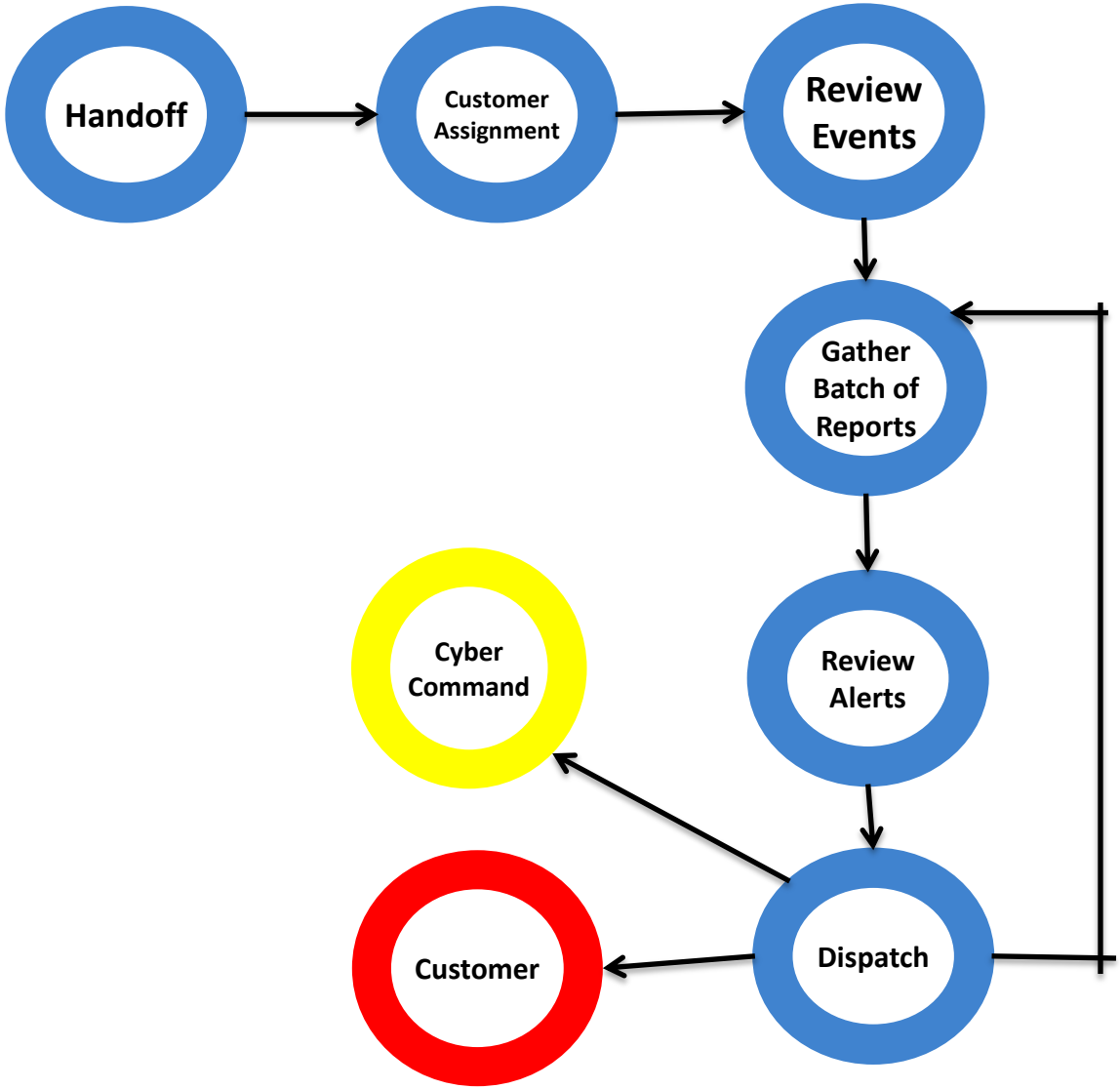


ASU Arizona State University

Sequential Task Network Diagram
Industry Incident Response Team



Sequential Task Network Diagram Military Network Defense Team



ARIZONA STATE UNIVERSITY

EAST Conclusions

- A descriptive form of modeling that facilitates understanding of sociotechnical system
- Can apply social network analysis parameters to each of these networks and combinations
- Can better understand system bottlenecks, inefficiencies, overload
- Can better compare systems
- Combined with empirical studies and agent-based modeling can allow us to scale up to very complex systems

Conclusion

- Analysts tend to work alone
- Teamwork improves performance
- Work is heavily bottom up
- Much technology is not suited to analyst task
- Human-Centered approach can improve SA

Next Steps

- **Use DEXTAR-DETER to explore more complex tasks of cyber analyst**
- **Use DEXTAR-DETER to compare analyst tools, models, and visualizations**
- **Examine other human roles and tasks**

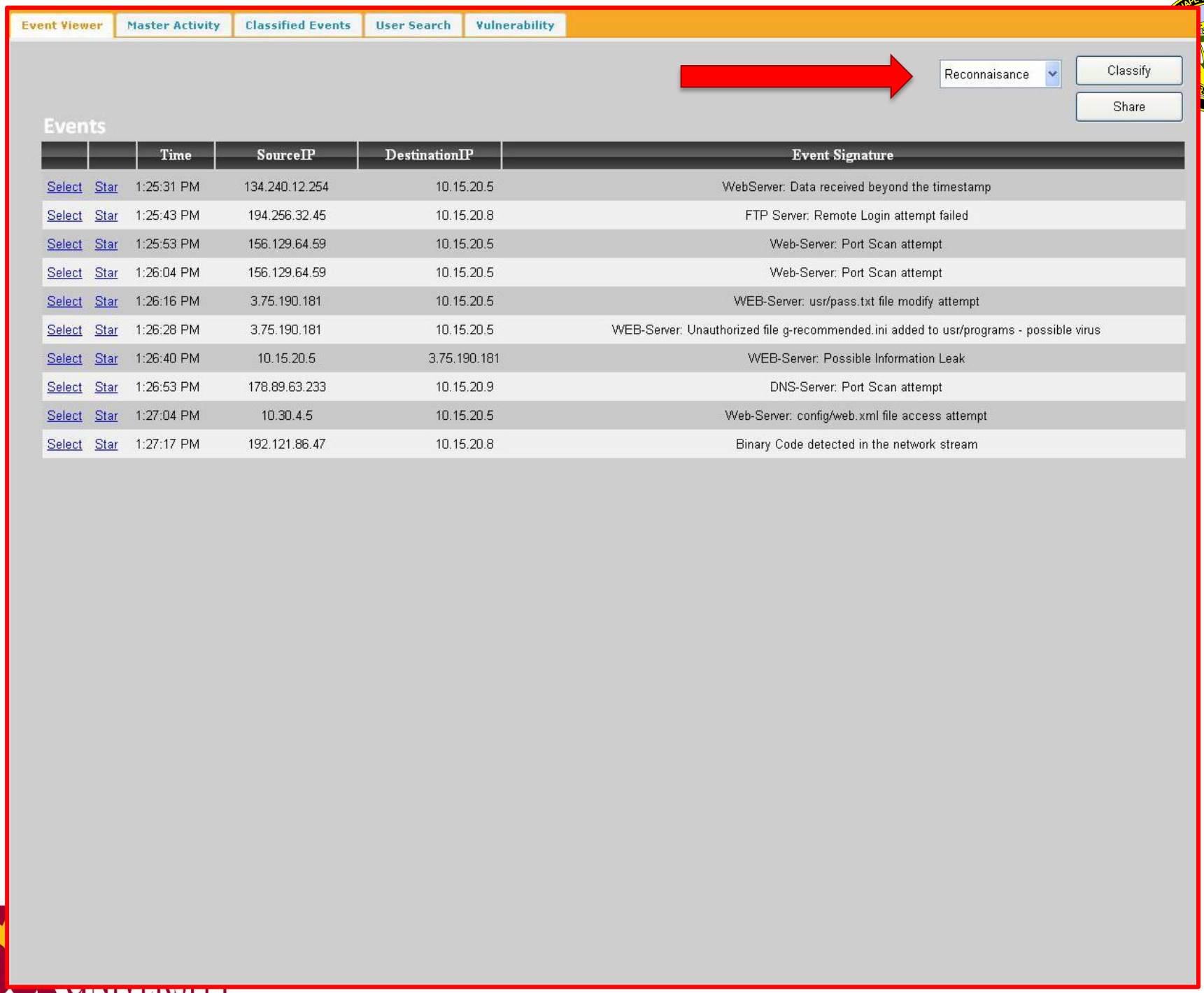
Thanks & Questions

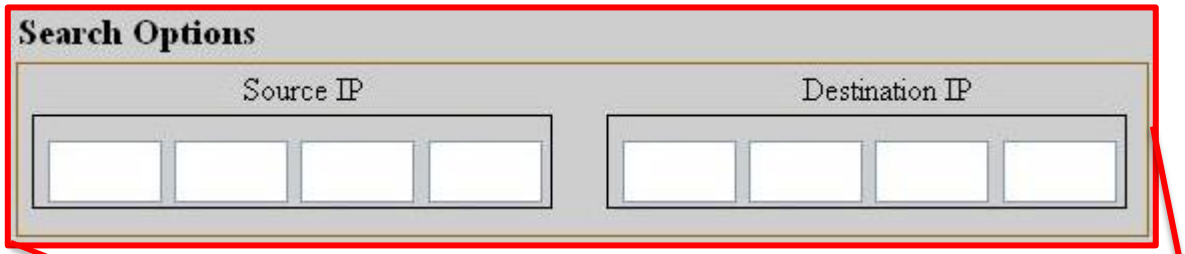
Army Research Office (Cliff Wang)
Sandia Research (DEXTAR)
USC DeterLab

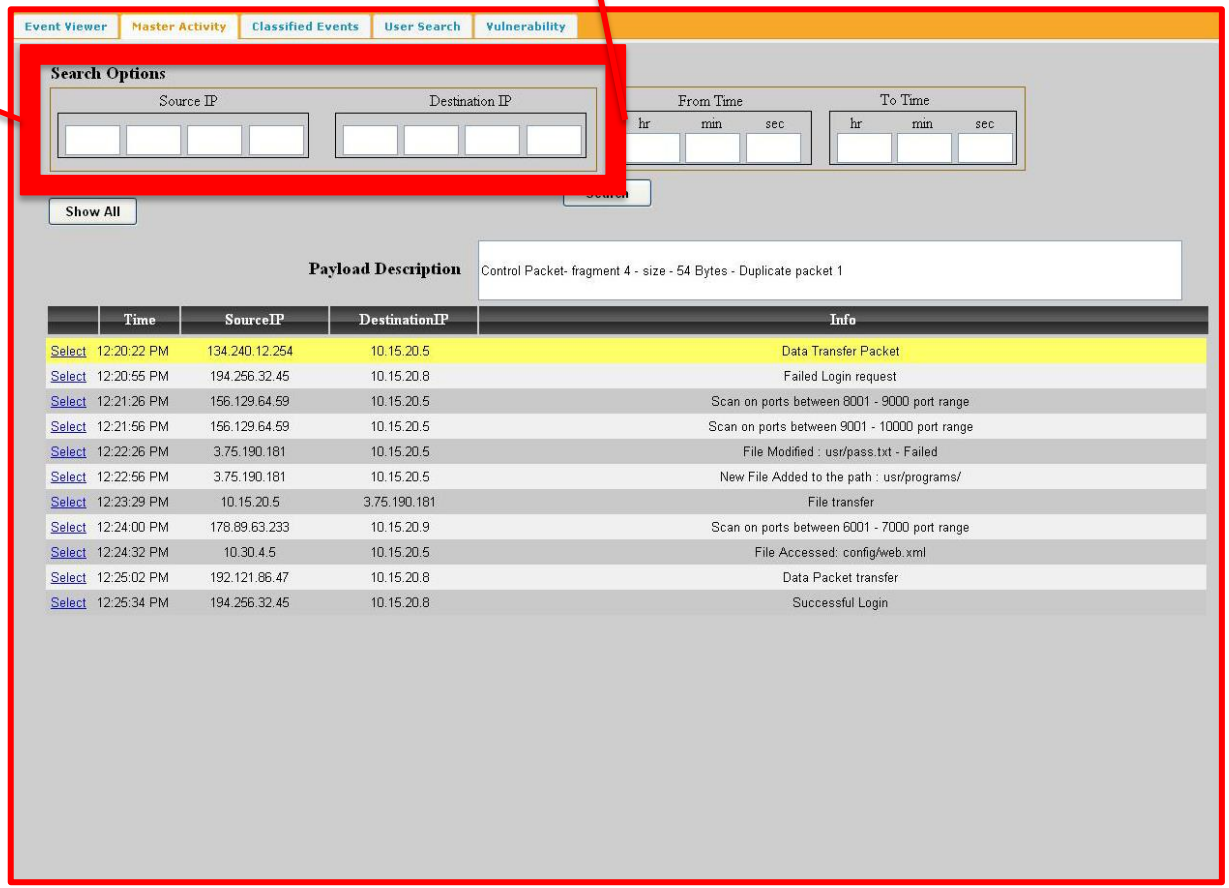
Jim Blythe, PhD
Aaron Bradbury
Rachel Howes
Sarah Kusumastuti
Prashanth Rajivan, PhD
Steve Shope, PhD
Jessica Twyford

ncooke@asu.edu

ASU Arizona State University


Event Viewer
Master Activity
Classified Events
User Search
Vulnerability
Reconnaisance
Classify
Share
Events
Time
SourceIP
DestinationIP
Event Signature
Select Star 1:25:31 PM 134.240.12.254 10.15.20.5 WebServer: Data received beyond the timestamp
Select Star 1:25:43 PM 194.256.32.45 10.15.20.8 FTP Server: Remote Login attempt failed
Select Star 1:25:53 PM 156.129.64.59 10.15.20.5 Web-Server: Port Scan attempt
Select Star 1:26:04 PM 156.129.64.59 10.15.20.5 Web-Server: Port Scan attempt
Select Star 1:26:16 PM 3.75.190.181 10.15.20.5 WEB-Server: usr/pass.txt file modify attempt
Select Star 1:26:28 PM 3.75.190.181 10.15.20.5 WEB-Server: Unauthorized file g-recommended.ini added to usr/programs - possible virus
Select Star 1:26:40 PM 10.15.20.5 3.75.190.181 WEB-Server: Possible Information Leak
Select Star 1:26:53 PM 178.89.63.233 10.15.20.9 DNS-Server: Port Scan attempt
Select Star 1:27:04 PM 10.30.4.5 10.15.20.5 Web-Server: config/web.xml file access attempt
Select Star 1:27:17 PM 192.121.86.47 10.15.20.8 Binary Code detected in the network stream





	Time	SourceIP	DestinationIP	Info
Select	12:20:22 PM	134.240.12.254	10.15.20.5	Data Transfer Packet
Select	12:20:55 PM	194.256.32.45	10.15.20.8	Failed Login request
Select	12:21:26 PM	156.129.64.59	10.15.20.5	Scan on ports between 8001 - 9000 port range
Select	12:21:56 PM	156.129.64.59	10.15.20.5	Scan on ports between 9001 - 10000 port range
Select	12:22:26 PM	3.75.190.181	10.15.20.5	File Modified : usr/pass.txt - Failed
Select	12:22:56 PM	3.75.190.181	10.15.20.5	New File Added to the path : usr/programs/
Select	12:23:29 PM	10.15.20.5	3.75.190.181	File transfer
Select	12:24:00 PM	178.89.63.233	10.15.20.9	Scan on ports between 6001 - 7000 port range
Select	12:24:32 PM	10.30.4.5	10.15.20.5	File Accessed: config/web.xml
Select	12:25:02 PM	192.121.86.47	10.15.20.8	Data Packet transfer
Select	12:25:34 PM	194.256.32.45	10.15.20.8	Successful Login

ASU ARIZONA STATE UNIVERSITY

Event Viewer | Master Activity | Classified Events | User Search | Vulnerability

Search Options

Source IP: 194 . 256 . 32 . 45

Destination IP:

From Time: hr min sec

To Time: hr min sec

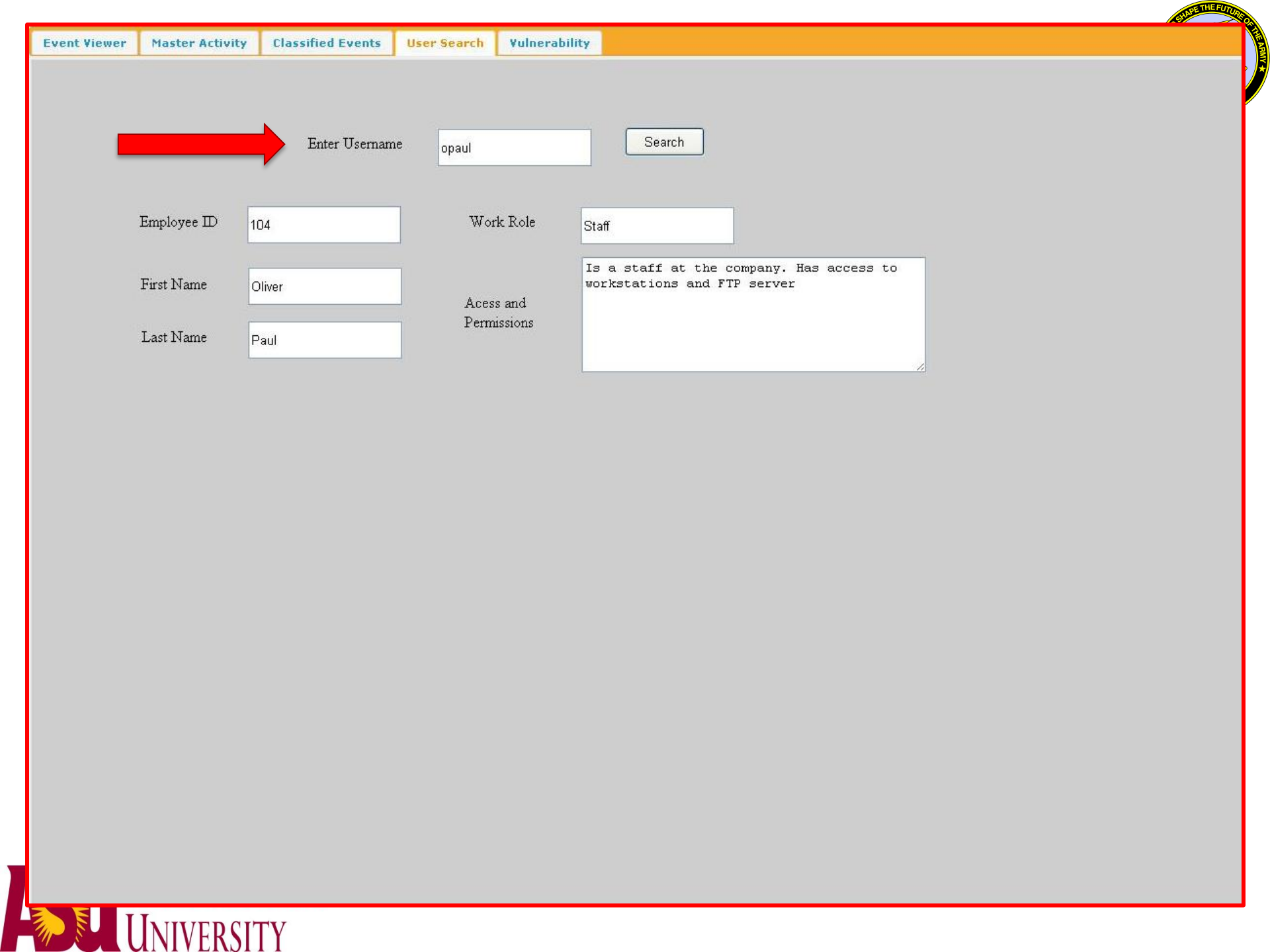
Search

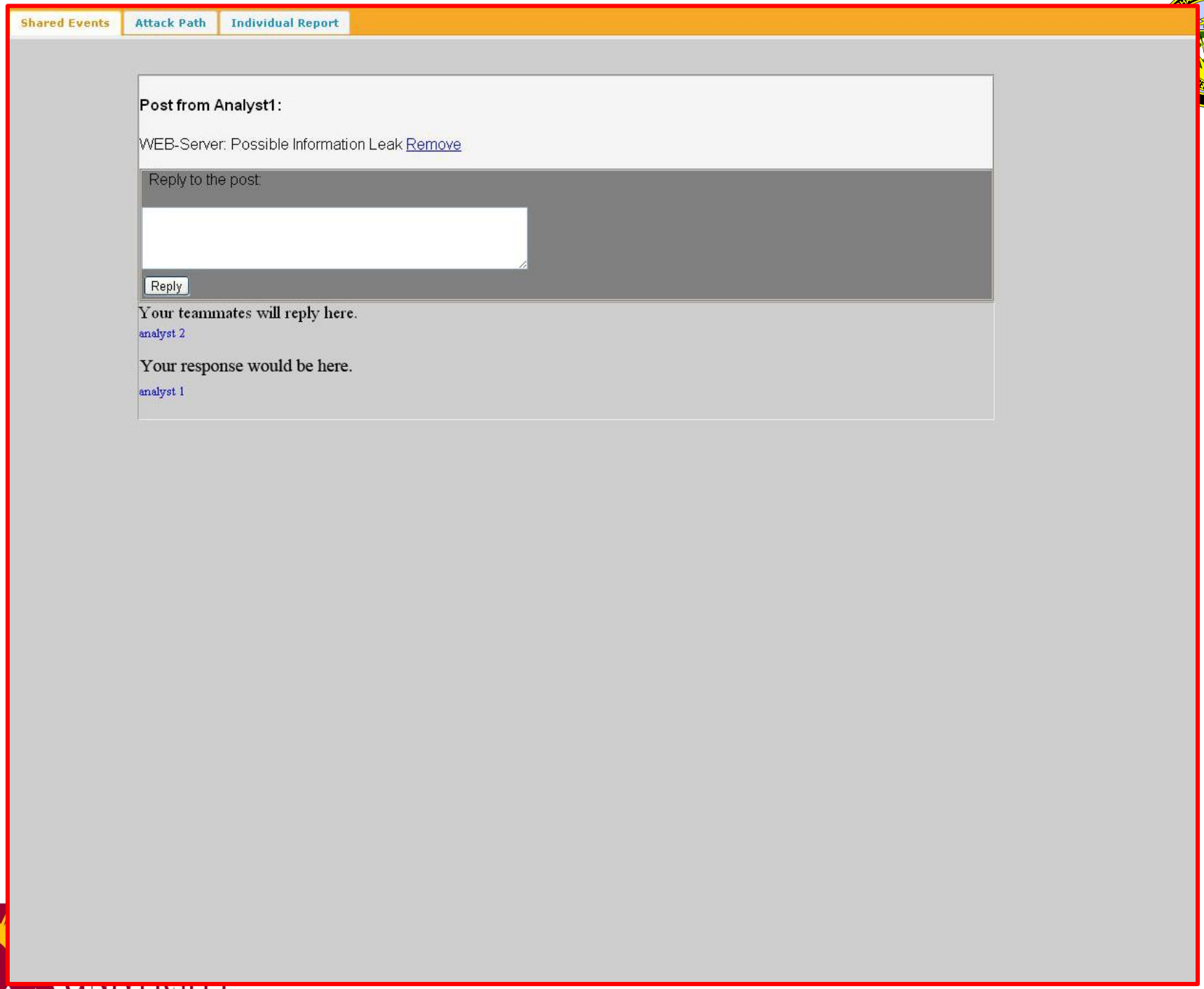
Show All

Payload Description Control Packet- fragment 4 - size - 54 Bytes - Duplicate packet 1

	Time	SourceIP	DestinationIP	Info
Select	12:20:55 PM	194.256.32.45	10.15.20.8	Failed Login request
Select	12:25:34 PM	194.256.32.45	10.15.20.8	Successful Login

ASU UNIVERSITY


Event Viewer
Master Activity
Classified Events
User Search
Vulnerability
Enter Username
opaul
Search
Employee ID
104
Work Role
Staff
First Name
Oliver
Last Name
Paul
Acess and Permissions
Is a staff at the company. Has access to workstations and FTP server


Shared Events
Attack Path
Individual Report
Post from Analyst1:
WEB-Server: Possible Information Leak Remove
Reply to the post:
Reply
Your teammates will reply here.
analyst 2
Your response would be here.
analyst 1

Shared Events | Attack Path

Systems

	Name	IP Address	Subnet
Select	App Server	10.30.4.3	10.30.4.0/20
Select	NIDS(Network Intrusion Detection System)	10.15.20.4	10.15.20.0/24
Select	PC	10.19.59.6	10.19.59.0/21
Select	PC	10.19.59.7	10.19.59.0/21
Select	PC	10.19.59.8	10.19.59.0/21
Select	PC	10.19.59.9	10.19.59.0/21
Select	PC	10.30.4.5	10.30.4.0/20
Select	PC	10.30.4.6	10.30.4.0/20
Select	PC	10.30.4.7	10.30.4.0/20
Select	PC	10.30.4.8	10.30.4.0/20

1 2 3

>>

Systems Affected

	Name	IP Address	Subnet
Select	Web Server	10.15.20.5	10.15.20.0/24
Select	App Server	10.30.4.3	10.30.4.0/20
Select	PC	10.30.4.5	10.30.4.0/20
Select	PC	10.30.4.6	10.30.4.0/20
Select	PC	10.30.4.7	10.30.4.0/20
Select	PC	10.30.4.8	10.30.4.0/20

Submit Plan

ASU Arizona State University