Secure Cyber Incident Information Sharing

UTSA Team Leads

Dr. Ram Krishnan, Assistant Professor, ECE

Dr. Ravi Sandhu, Executive Director, ICS

April 30, 2014

UTSA Engineering

I·C·S
The Institute for Cyber Security

LMI Research Institute (LRI): Academic Partnership Program

- Through formal working relationships with universities across the country, LMI bridges the gap between academia and industry to create innovative solutions and explore new research topics
- The partnership program exposes students to real-world challenges faced by the federal government through structured, funded research projects

VirginiaTech
Invent the Future®

PENNSTATE
1855

HOWARD UNIVERSITY
School of Business

R·I·T

UTSA
The University of Texas at San Antonio™

SAINT LOUIS UNIVERSITY

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON DC

UNIVERSITY of VIRGINIA

GEORGE MASON UNIVERSITY

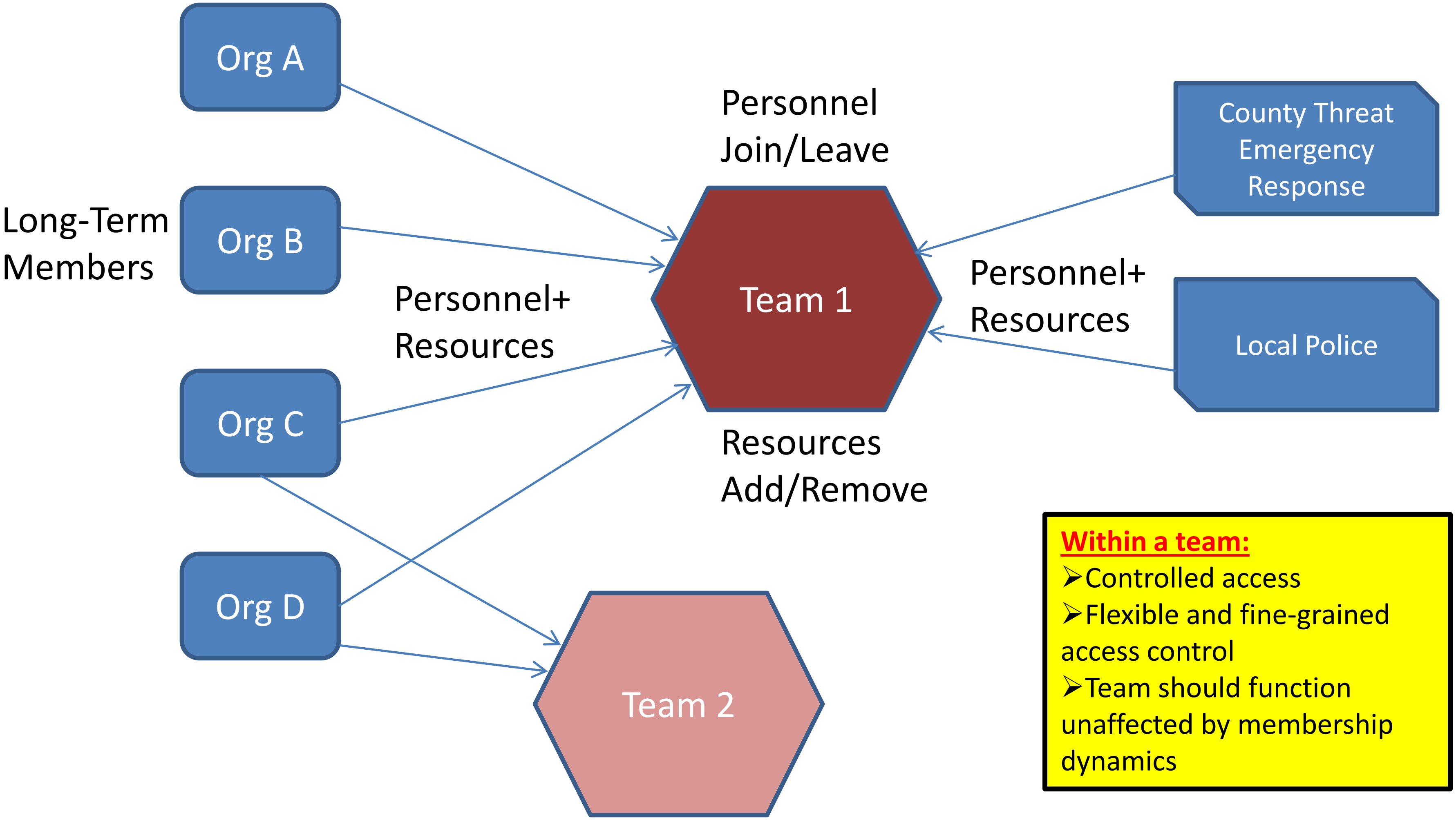
UTSA Engineering

I·C·S
The Institute for Cyber Security

Cyber Incident Response

- Secure information sharing amongst a set of entities/organizations
  - Often ad hoc
- What are the effective ways to facilitate information sharing in such circumstances?
  - Information sharing models
  - Infrastructure, technologies, platforms

Agile Incident Response



Within a team:

- ➢Controlled access
- ➢Flexible and fine-grained access control
- ➢Team should function unaffected by membership dynamics

Cyber Incident Information Sharing Scenarios

- Community
  - Cyber incidents across critical infrastructure providers in a community
    - Emergency response, healthcare, banks, utility
- Electric grid
  - Cyber incidents in electric power provider orgs
    - Local utilities, ISOs, ERCOT, NERC

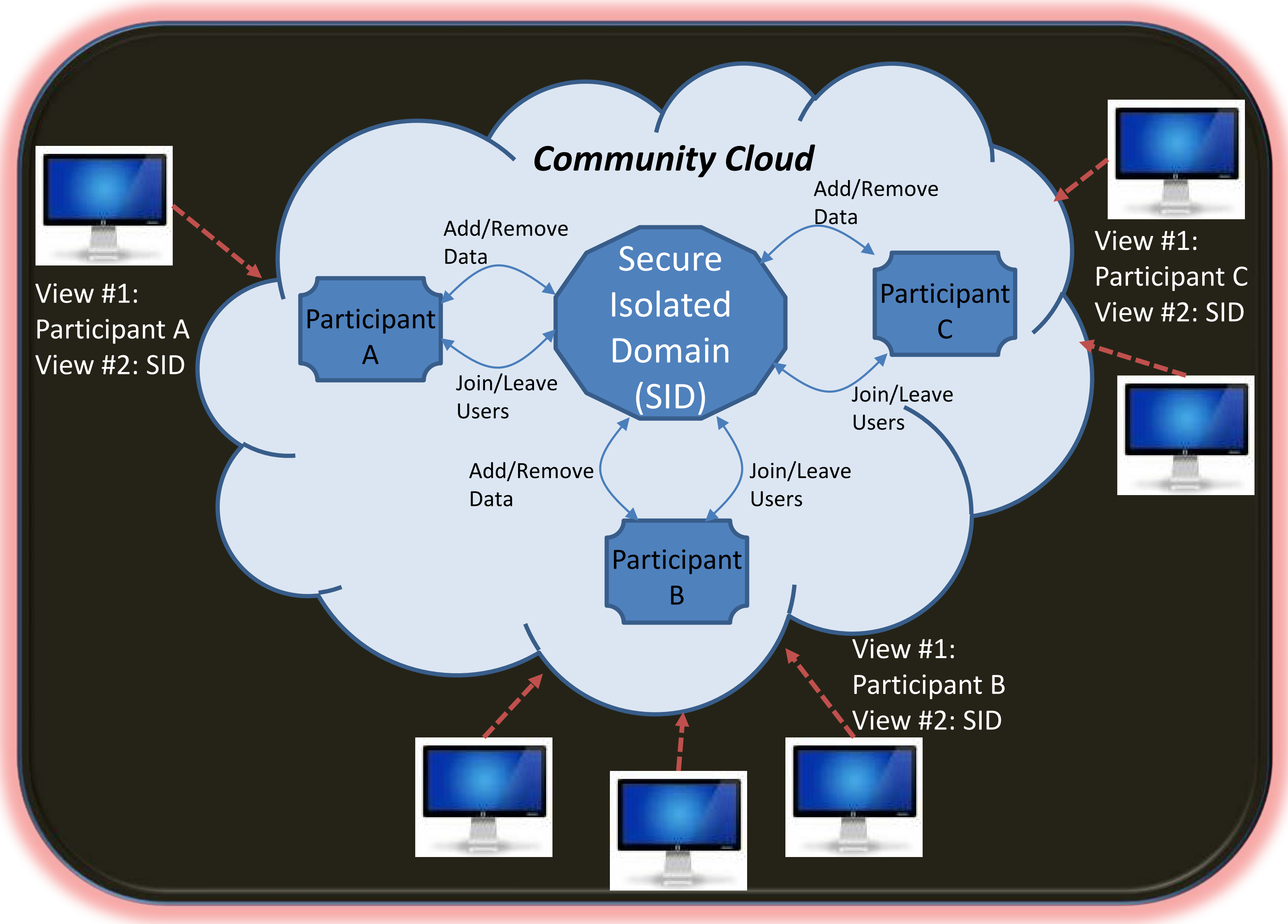
Key Requirements

- Cyber infrastructure sharing to support data and compute
  - Need a community information sharing platform
    - Controlled access
- Light-weight and agile
- Rapid deployment and configuration
- Secure environment

Cloud Infrastructure as a Service

- Virtualized IT infrastructure (servers, storage, networks, OS, etc.)
  - Delivered as a service over a network, on demand, dynamic scaling, etc.
- Prominent examples
  - Amazon AWS
  - OpenStack

Enforcement in Cloud IaaS



Next Steps

- UTSA to incorporate INL input
- Develop prototype in OpenStack
- Share research results with INL
  - August/September

Thanks

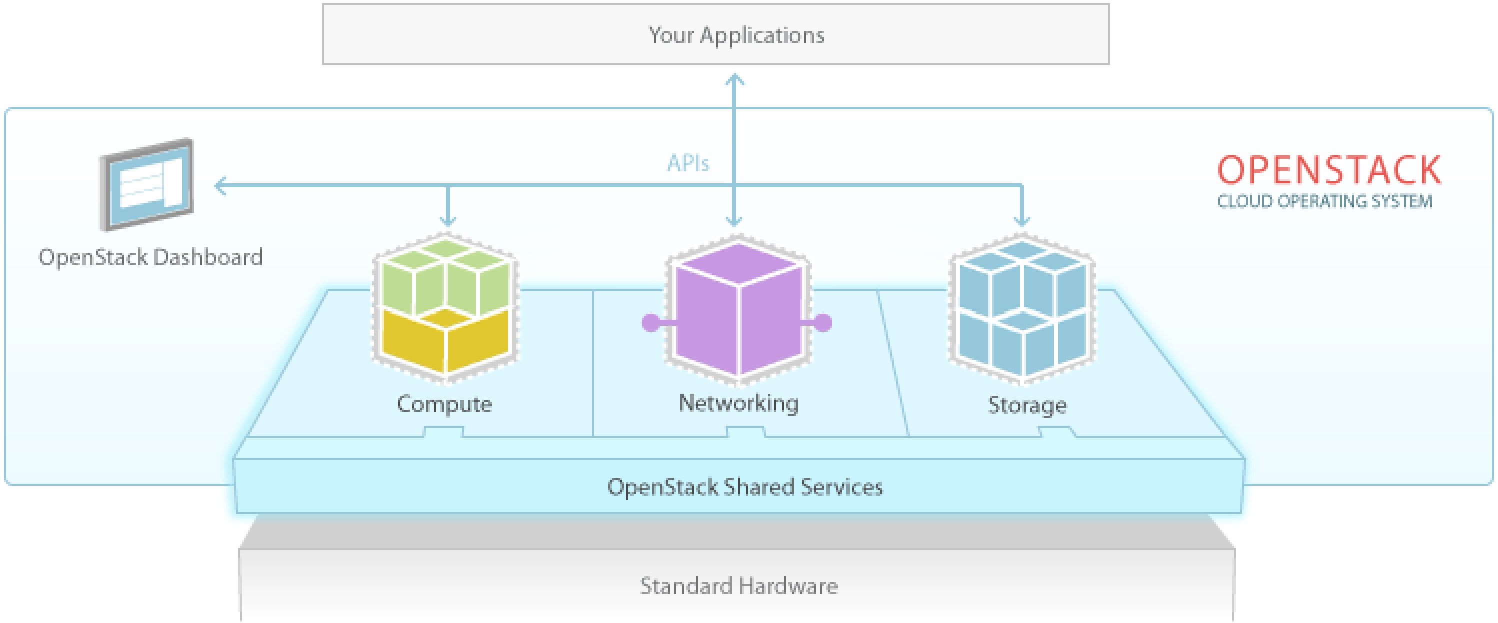
- Comments, Q&A

Backup

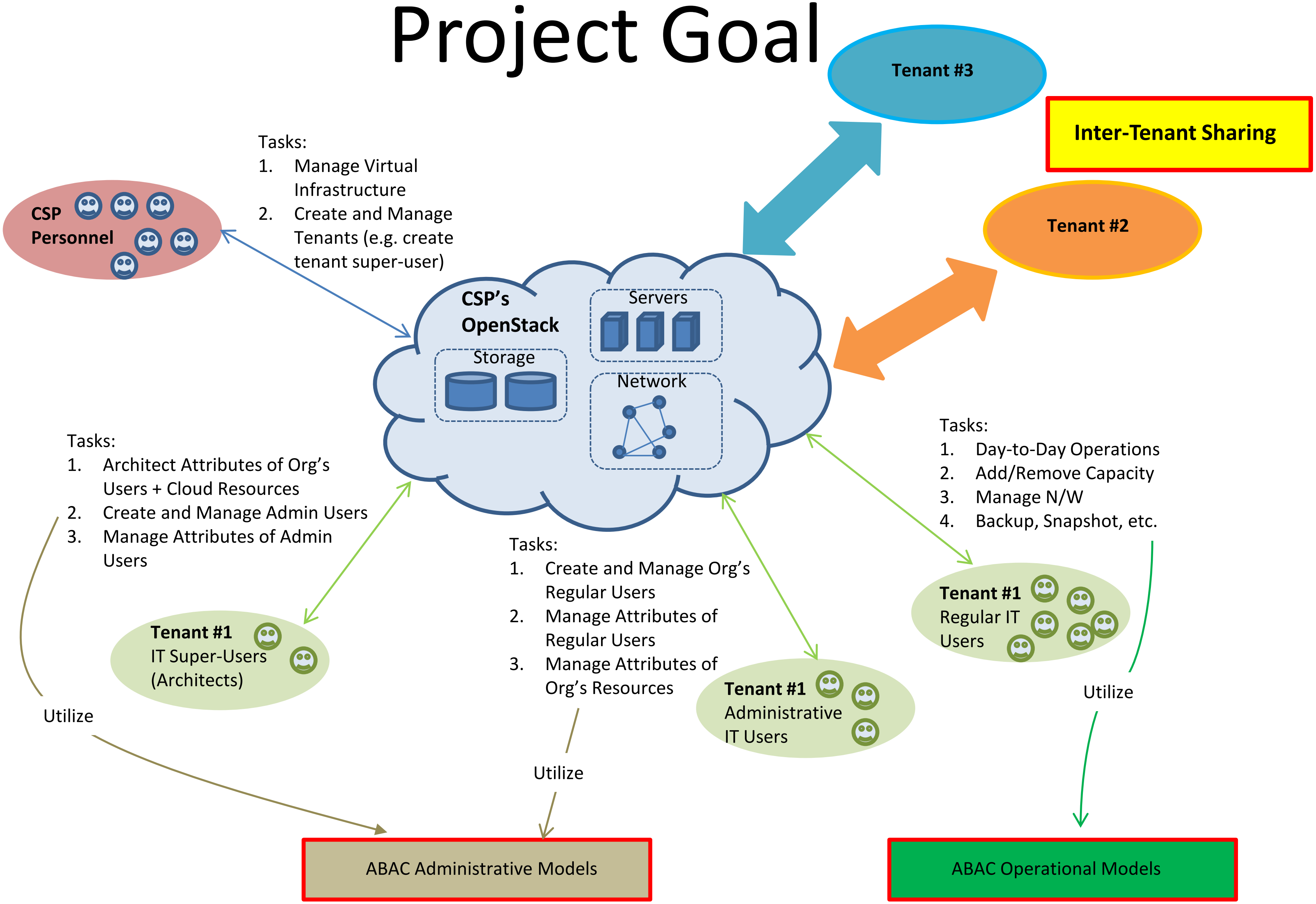
OpenStack

- OpenStack
  - Dominant open source cloud IaaS platform

- ➢ > 200 companies
- ➢ ~14000 developers
- ➢ >130 countries



Project Goal



Tenant #3

Inter-Tenant Sharing

Tenant #2

CSP Personnel

Tasks:

1. Manage Virtual Infrastructure
2. Create and Manage Tenants (e.g. create tenant super-user)

CSP's OpenStack

Servers

Storage

Network

Tasks:

1. Architect Attributes of Org's Users + Cloud Resources
2. Create and Manage Admin Users
3. Manage Attributes of Admin Users

Tenant #1 IT Super-Users (Architects)

Tasks:

1. Create and Manage Org's Regular Users
2. Manage Attributes of Regular Users
3. Manage Attributes of Org's Resources

Tenant #1 Administrative IT Users

Tasks:

1. Day-to-Day Operations
2. Add/Remove Capacity
3. Manage N/W
4. Backup, Snapshot, etc.

Tenant #1 Regular IT Users

Utilize

Utilize

Utilize

ABAC Administrative Models

ABAC Operational Models

Closed Network Scenario

- Unusual activity in Air Force, Navy & Army networks
- A physically secure and air-gapped meeting room with members from AFCYBER, ARCYBER and FLTCYBER
- Members bring data for analysis and collaboration
  - Maps, a VM configured with software tools, a VM image with a virus/worm, log files, etc.
- Strict control on data import/export

Data Exfiltration Scenario

- Unusual file transfers from IP addresses within an org to an external IP address
- Similar activities observed in partner orgs
- Need to find if these events are connected
  – Any correlation between those files?
- Members bring data for analysis+collaboration