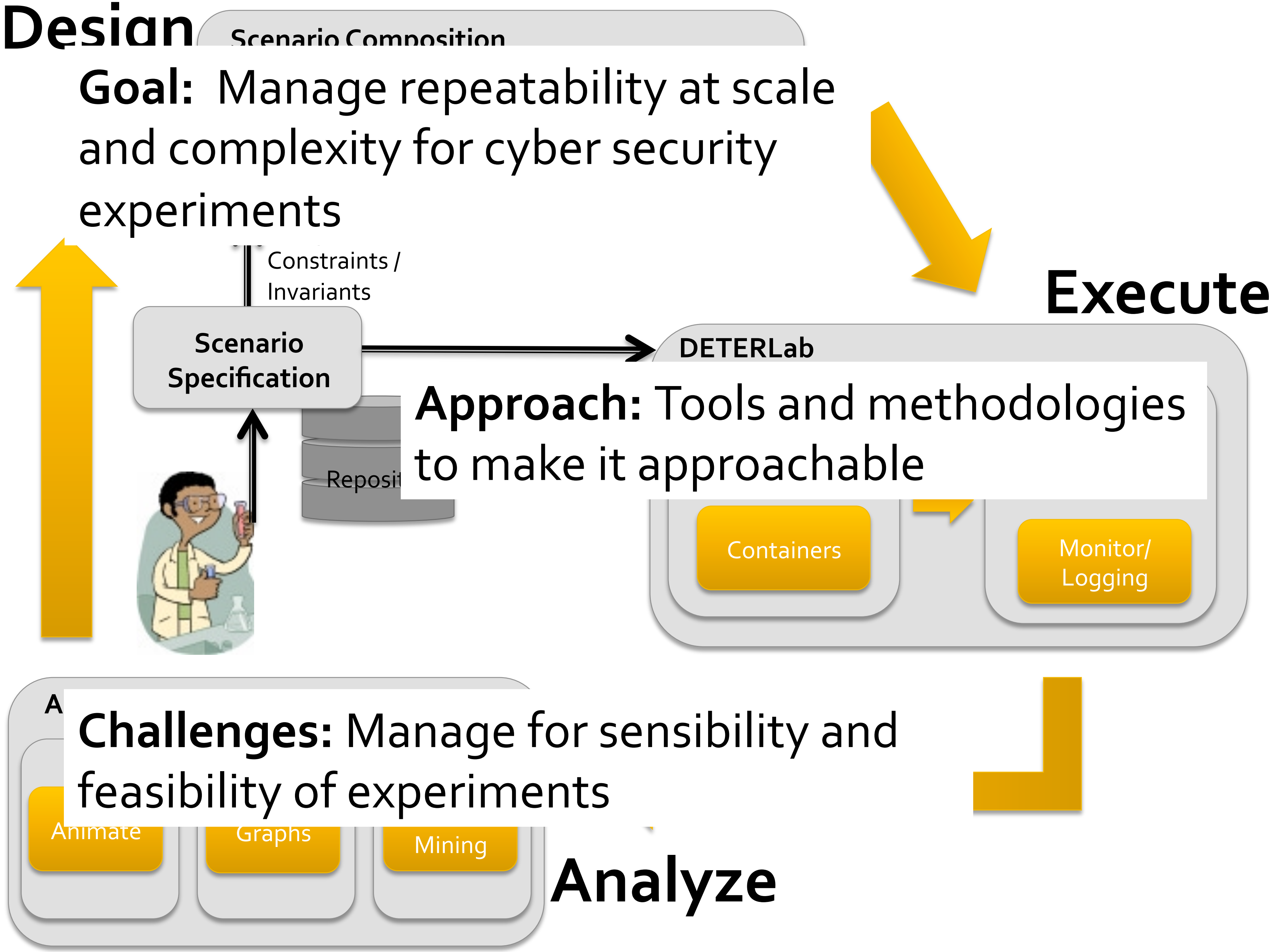
The DETER Project

Montage: Experiment Lifecycle Management Tools

Alefiya Hussain, Prateek Jaipuria, Geoff Lawler
Terry Benzel, John Wroclawski



Goal: Manage repeatability at scale and complexity for cyber security experiments

Approach: Tools and methodologies to make it approachable

Challenges: Manage for sensibility and feasibility of experiments

Research Programs

- Advanced Testbed Technologies

  O(500) → O(100,000)

  http://containers.deterlab.net

- Experiment Control and Monitoring

  nodes → agents

  http://montage.deterlab.net

- Large scale Data Analysis

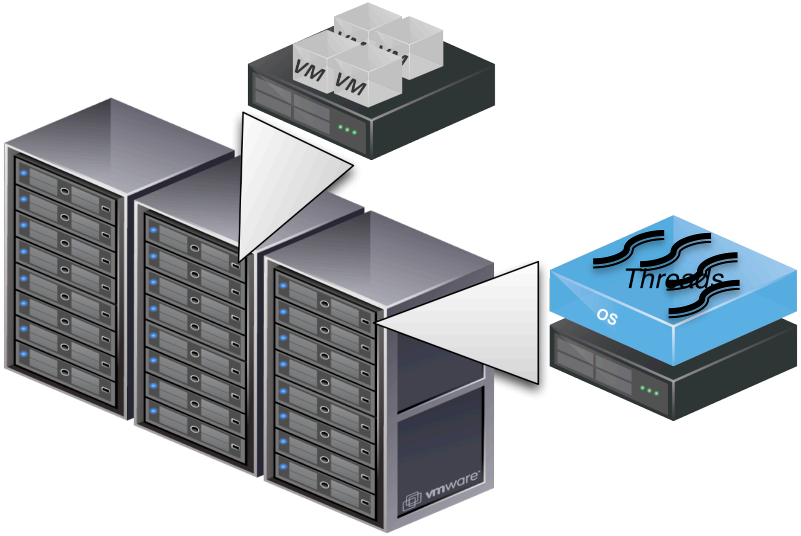
  data → understanding

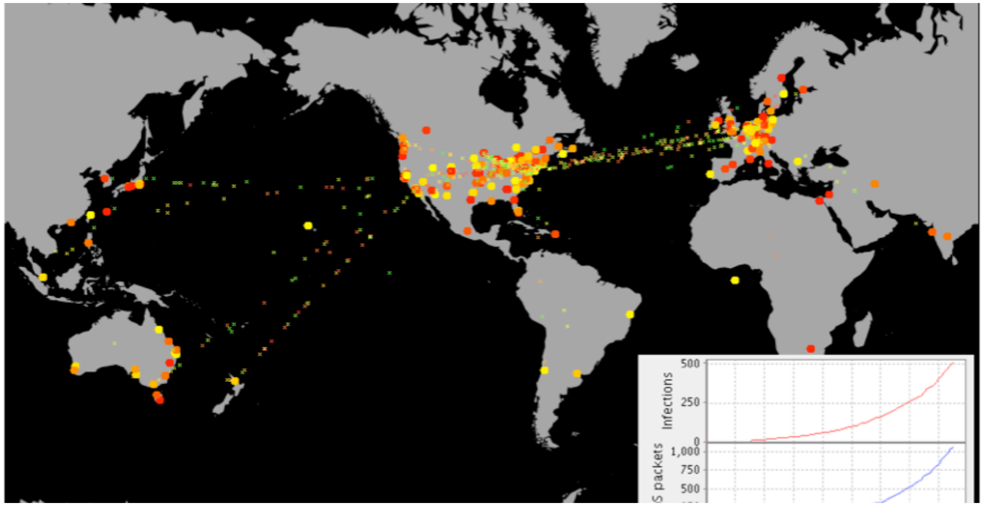
  http://thirdeye.deterlab.net

Testbed Technologies

O(500) → O(100,000)

http://containers.isi.deterlab.net

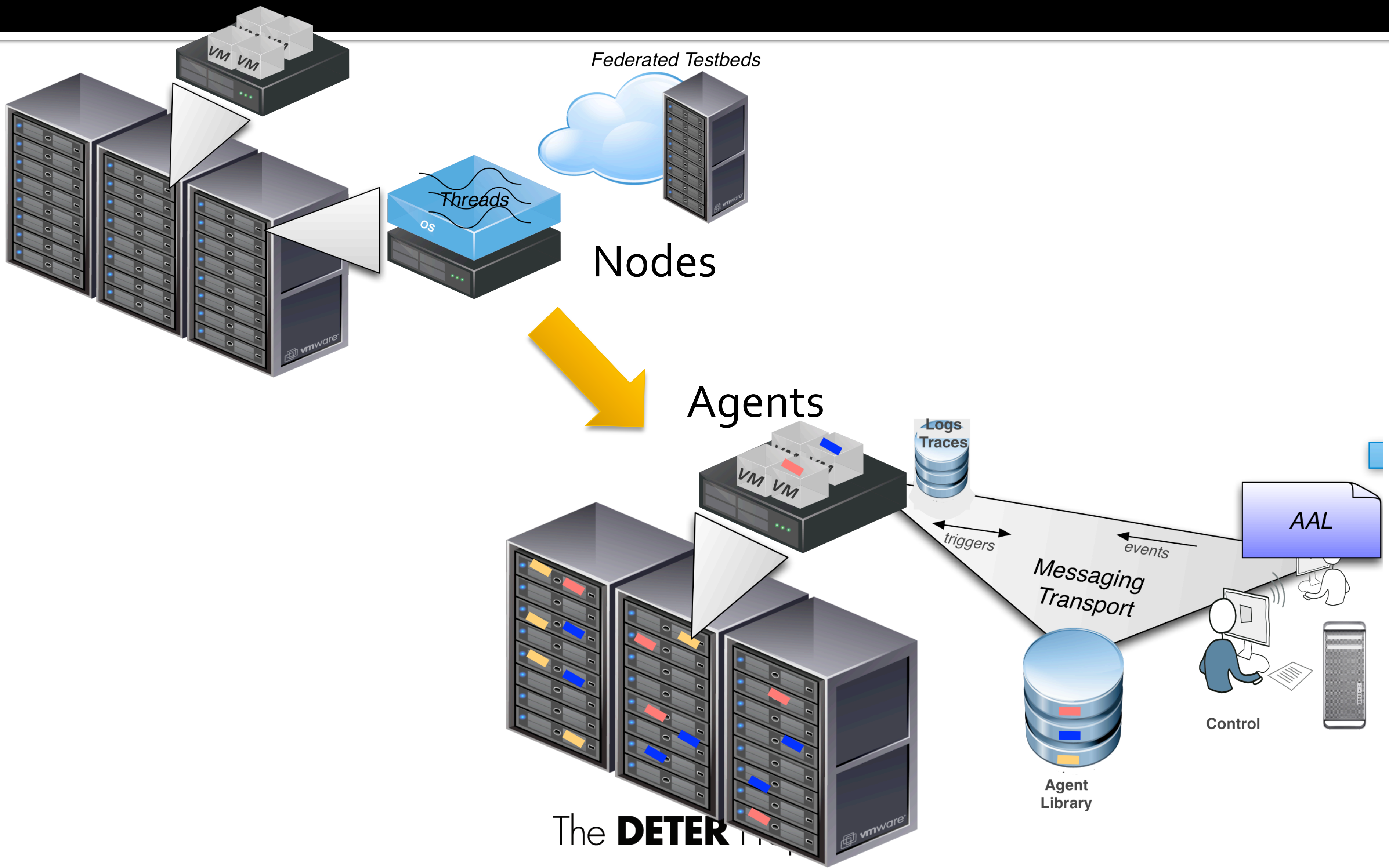




100K host, worm,botnet, ddos attack

http://www.deter-project.net

Experiment Control & Monitoring



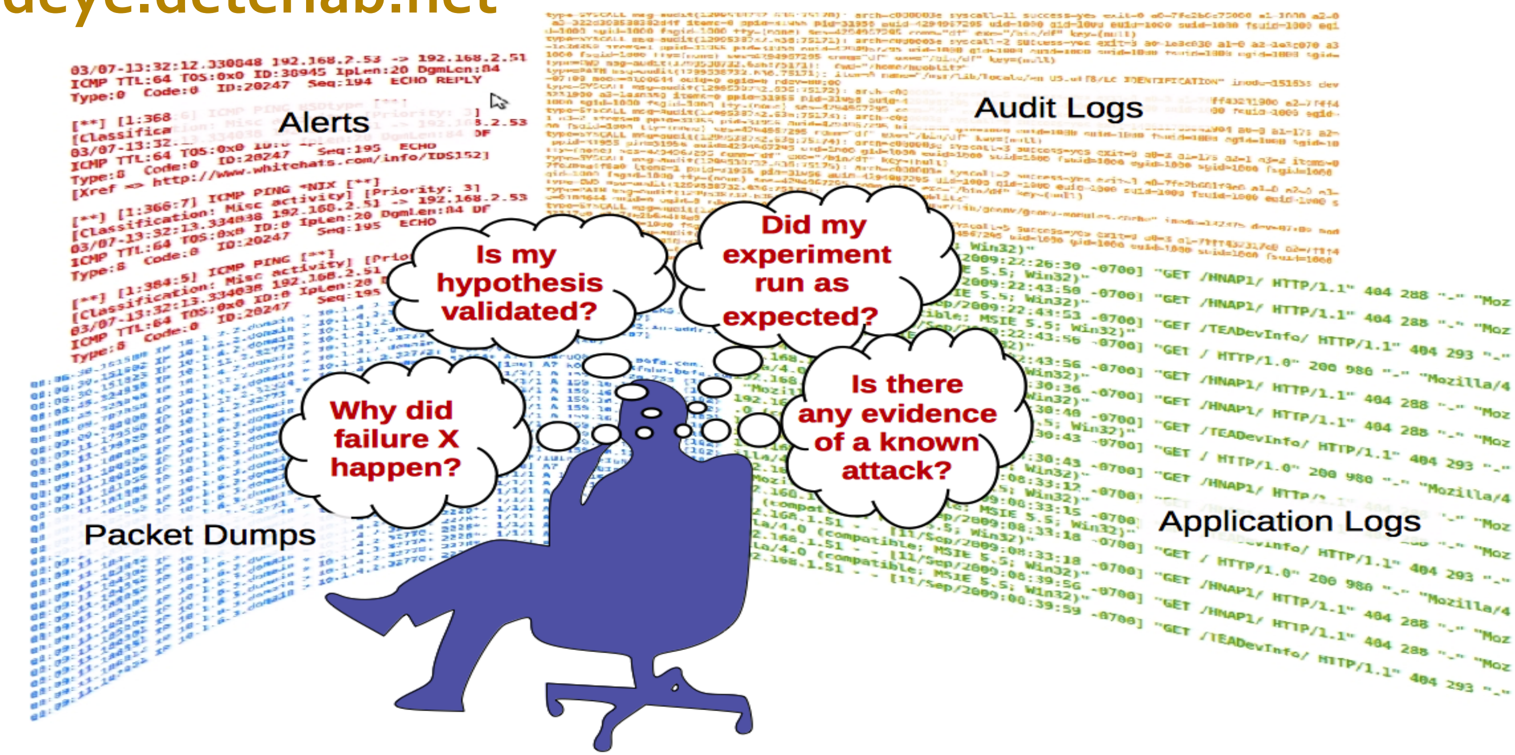
Nodes

Agents

Large Scale Data Analysis

- data → understanding

http://thirdeye.deterlab.net


Alerts
Audit Logs
Packet Dumps
Application Logs
Is my hypothesis validated?
Did my experiment run as expected?
Why did failure X happen?
Is there any evidence of a known attack?

Viswanathan, Husssain, Mirkovic, Schwab, Wroclawski
A Semantic Framework for Data Analysis in Networked Systems,
USENIX NSDI 2011

The **DETER** Project

Research Programs

- Advanced Testbed Technologies

  O(500) → O(100,000)

  http://containers.deterlab.net

- Experiment Control and Monitoring

  nodes → agents

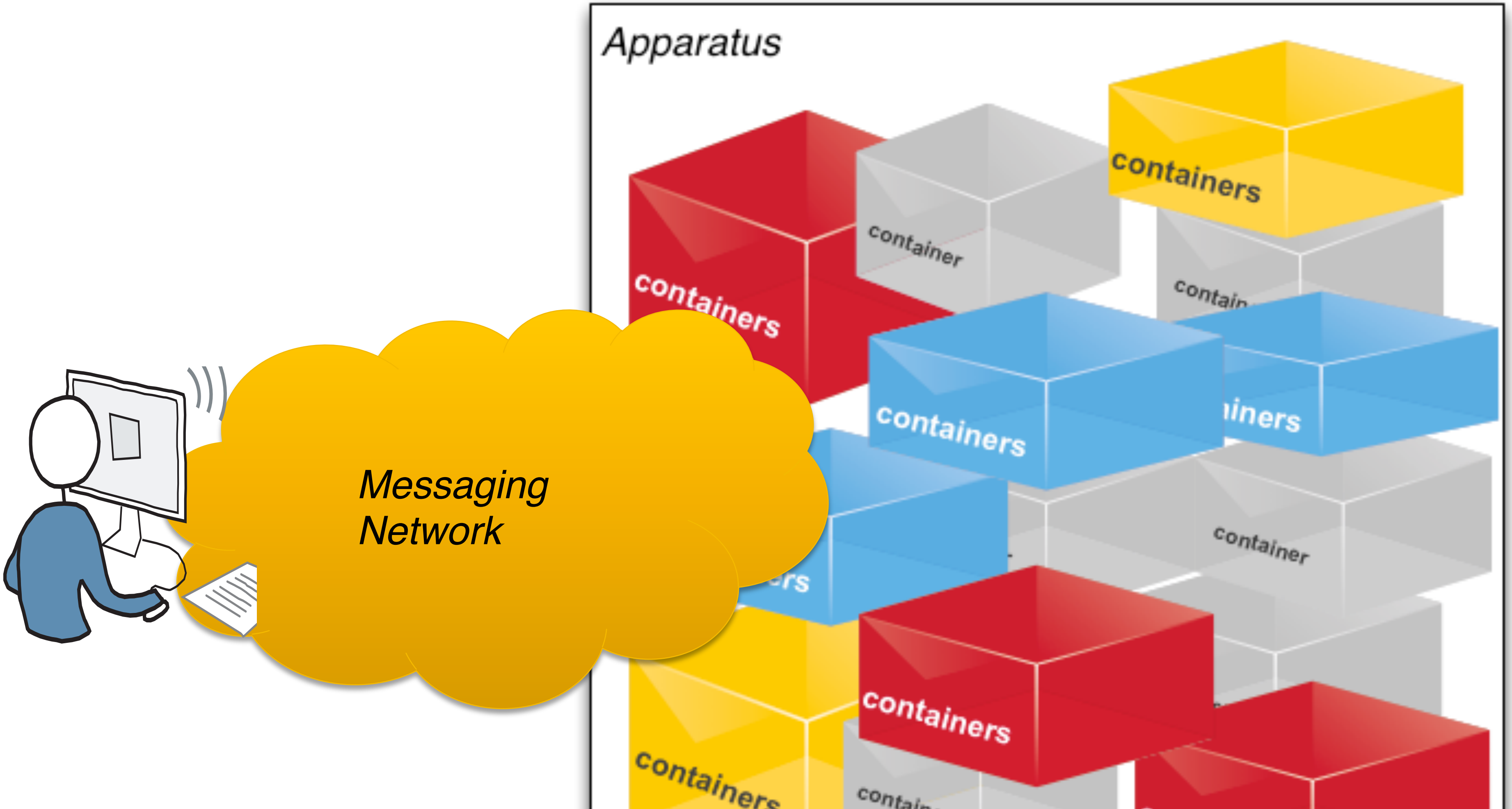
  http://montage.deterlab.net

- Large scale Data Analysis

  data → understanding

  http://thirdeye.deterlab.net

Frame of Reference



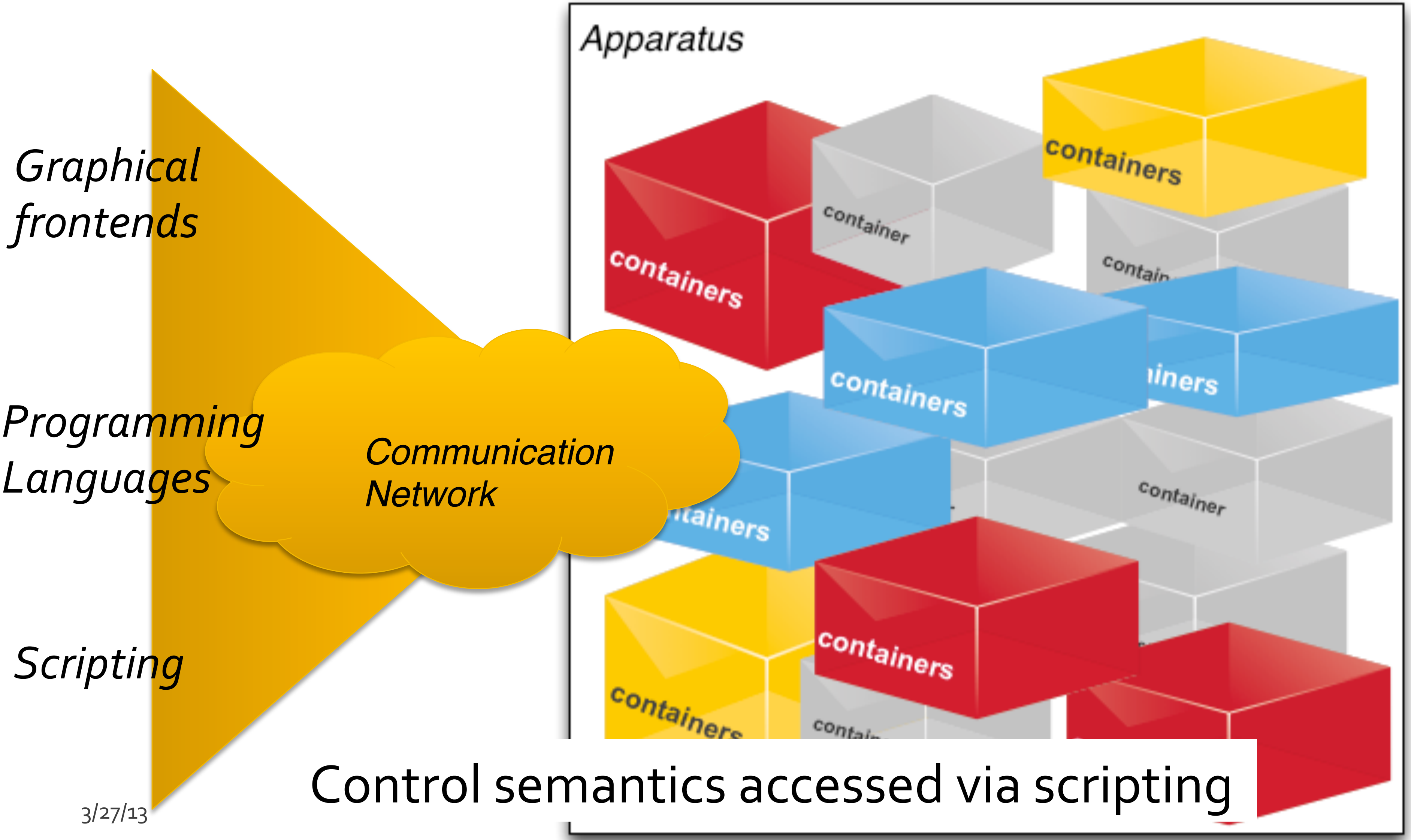
Define an instrumentation and control infrastructure

Existing Technologies

- tevc event system
  - Primitives for start scripts
- SEER
  - GUI to configure, start and stop
- ad-hoc ssh scripts

Complexity and Scale of the experiment

Control Specification



Graphical frontends

Programming Languages

Scripting

Communication Network

Apparatus

Control semantics accessed via scripting

Taming Complexity

- Procedural Level Abstractions
  - Orchestrate coordinated event streams
  - Tools for Inter agent and Intra agent communication
- Explicit Feedback Mechanisms
  - synchronization primitive
  - reliability
  - experiment design agility

Matters of Scale

- O(500) → O(100,000) containers
  - Event Frequency

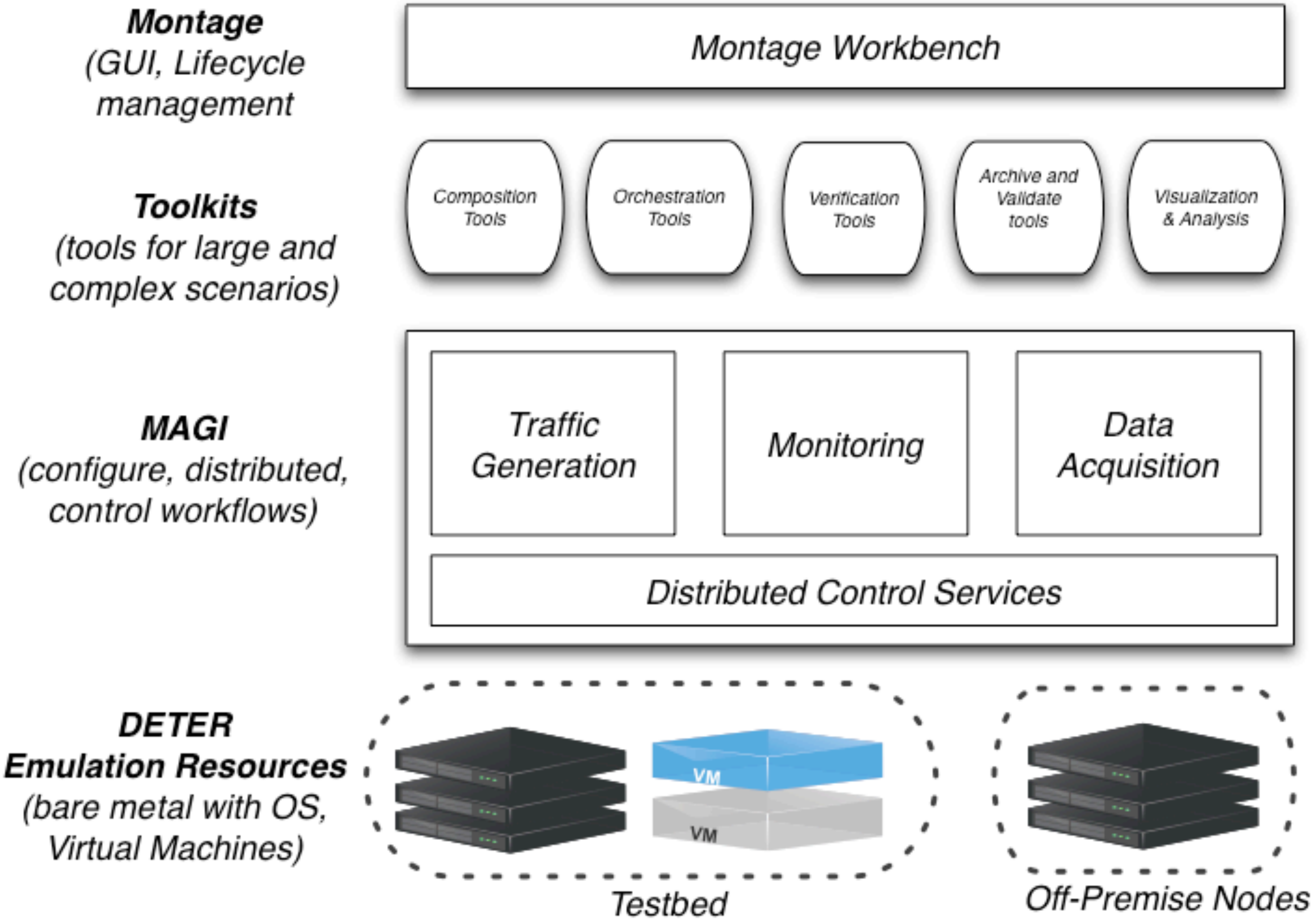
  100K host * 10 events/sec = 1M messages/sec

  - Event Bandwidth

  4KB/message = 4GB/sec

- Group Communication and Aggregation Mechanisms

MAGI Architecture



Montage
(GUI, Lifecycle management

Montage Workbench

Toolkits
(tools for large and complex scenarios)

Composition Tools

Orchestration Tools

Verification Tools

Archive and Validate tools

Visualization & Analysis

MAGI
(configure, distributed, control workflows)

Traffic Generation

Monitoring

Data Acquisition

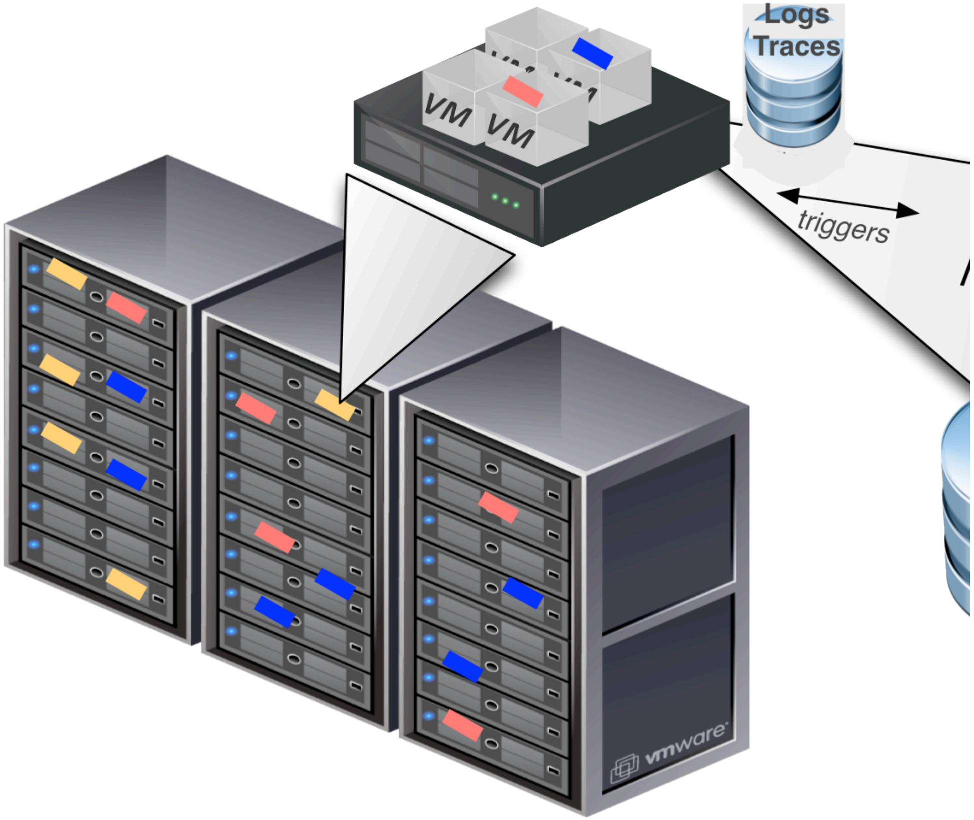
Distributed Control Services

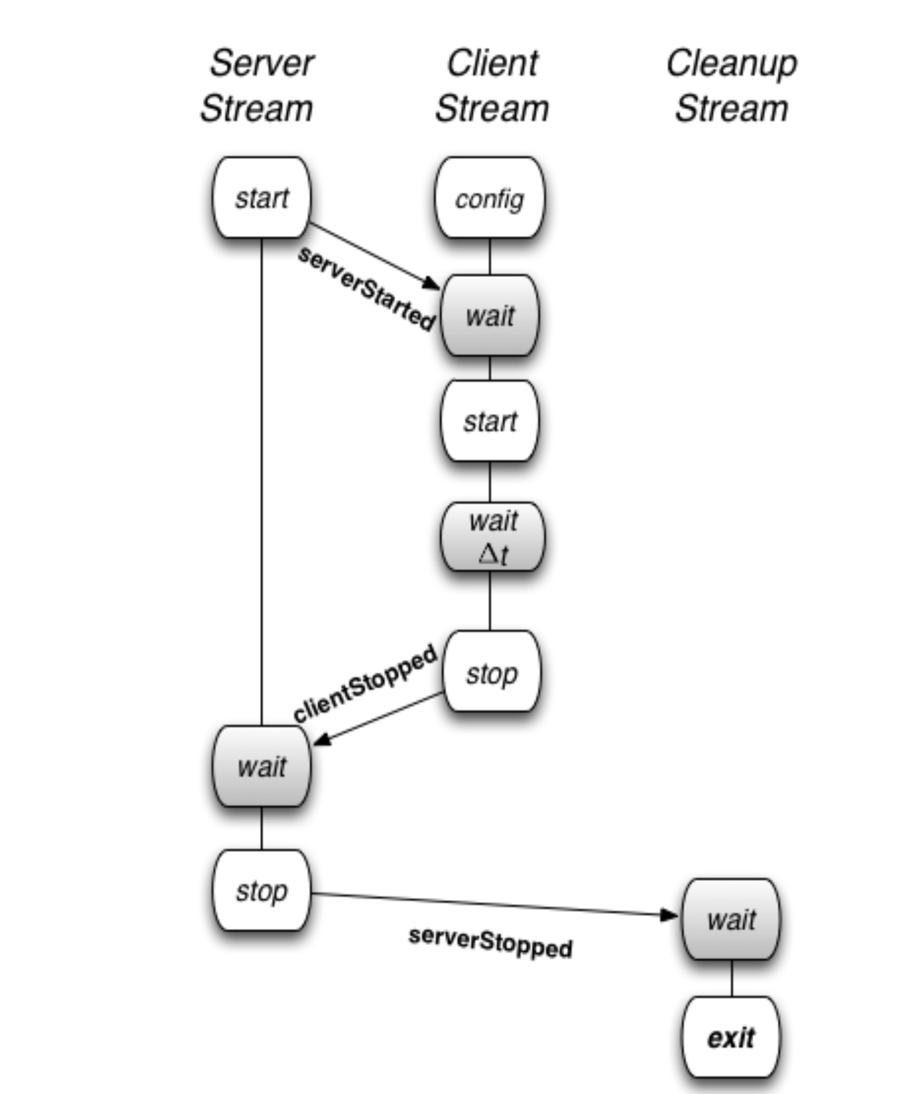
DETER Emulation Resources
(bare metal with OS, Virtual Machines)

Testbed

Off-Premise Nodes

MAGI


Logs
Traces
VM
VM
triggers
vmware


Server Stream
Client Stream
Cleanup Stream
start
config
serverStarted
wait
start
wait Δt
stop
clientStopped
wait
stop
serverStopped
wait
exit

Demo

Thank you

- MAGI Beta Release users.isi.deterlab.net:/share/magi/v09/

Contact: Alefiya Hussain

hussain@isi.edu