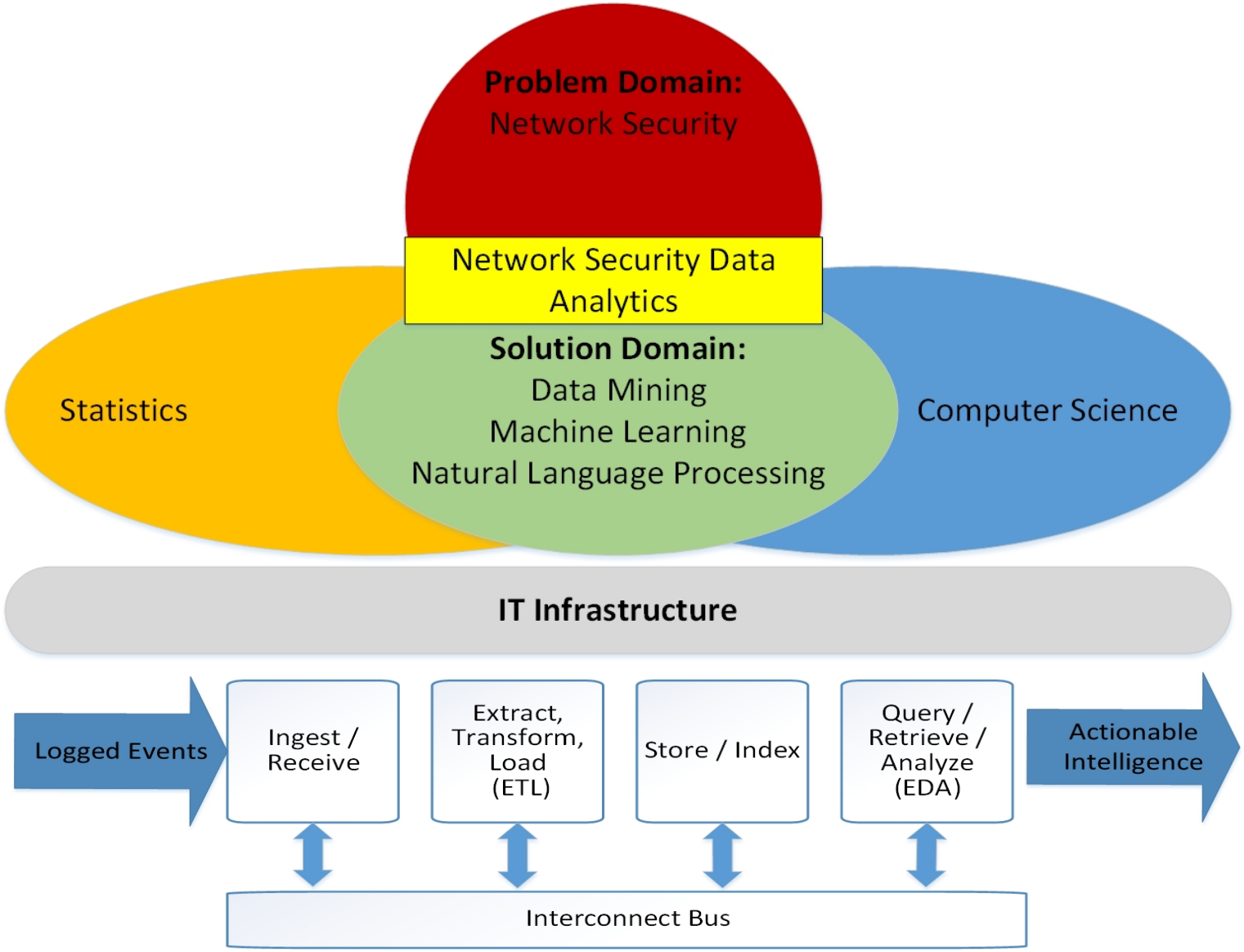
VirginiaTech
Invent the Future

Virginia Tech Information Technology Security Laboratory

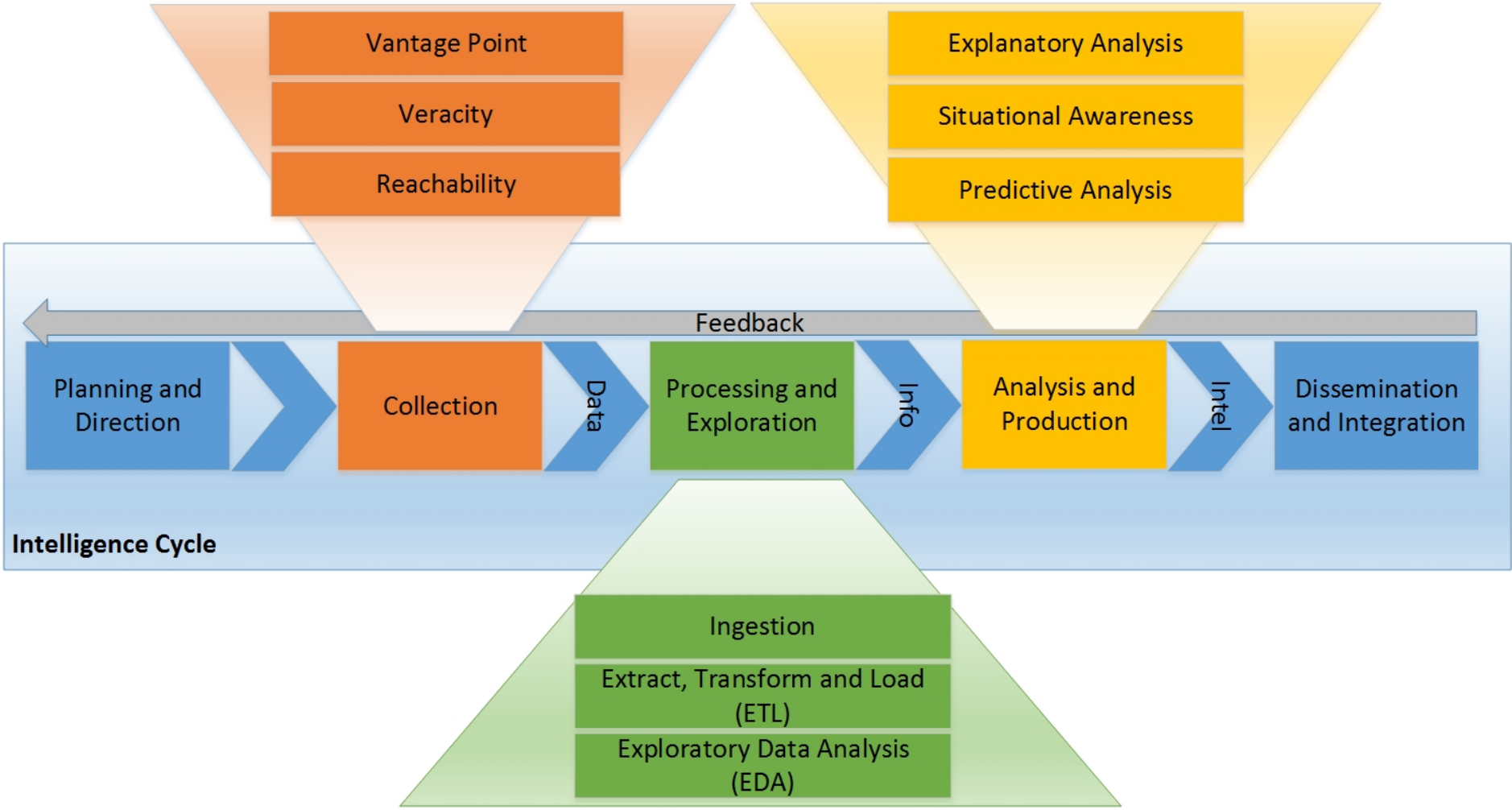
Virginia Tech Responds to Cybersecurity Challenges

November 17, 2016

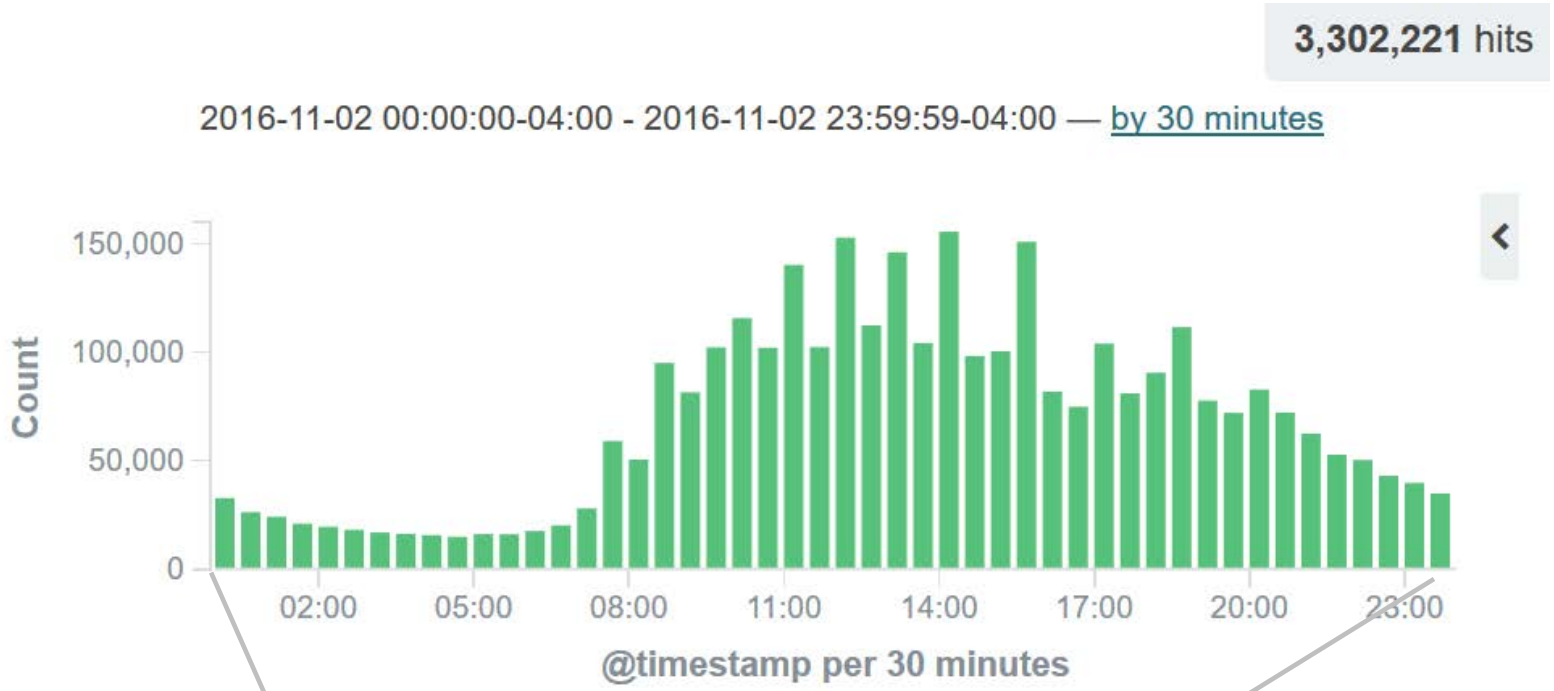
Network Security Analytics

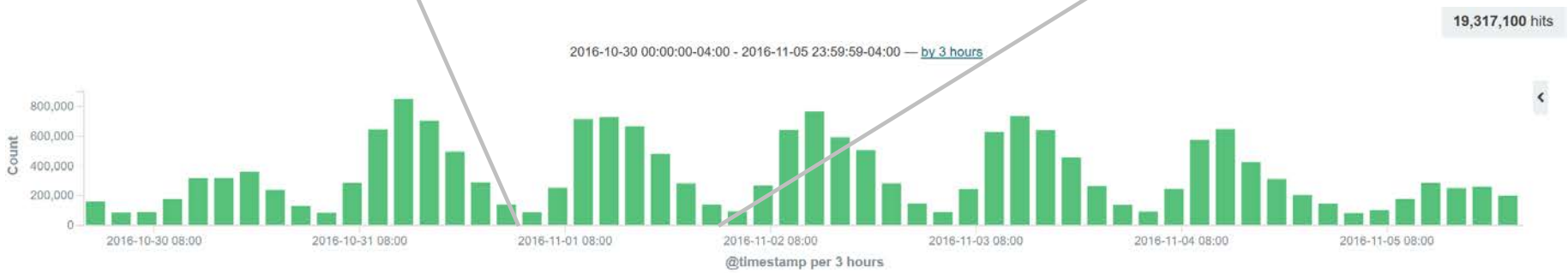


Operational Model



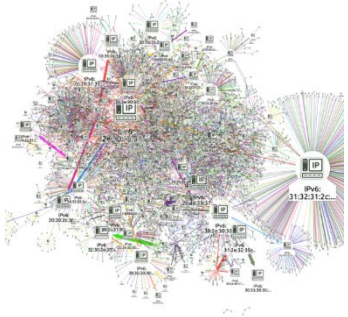
Example Data

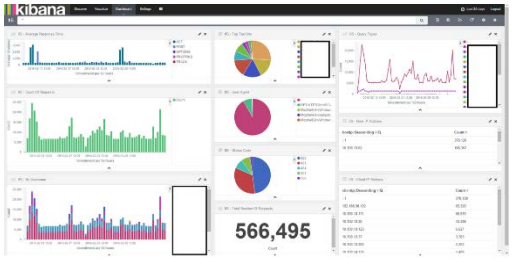




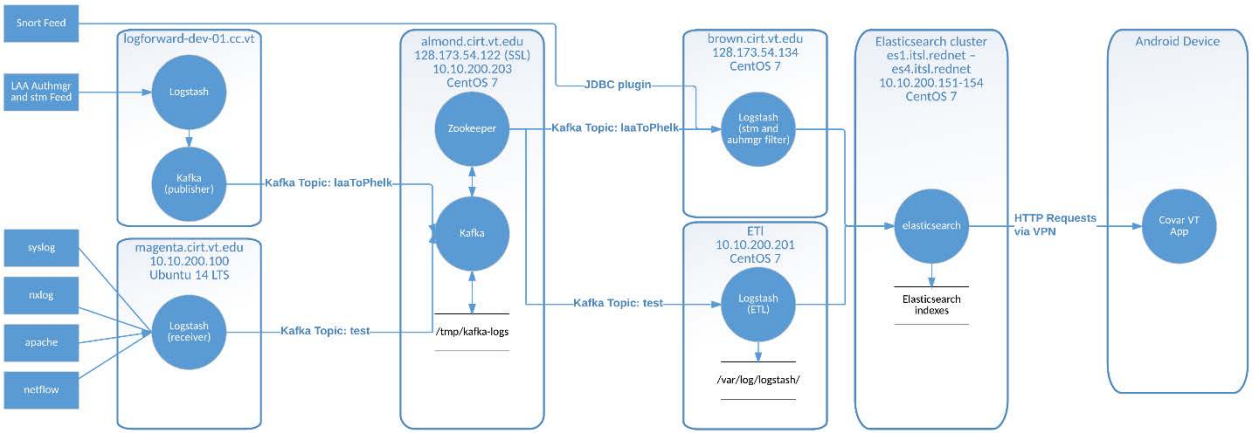
Visualizing the Future

Convolution

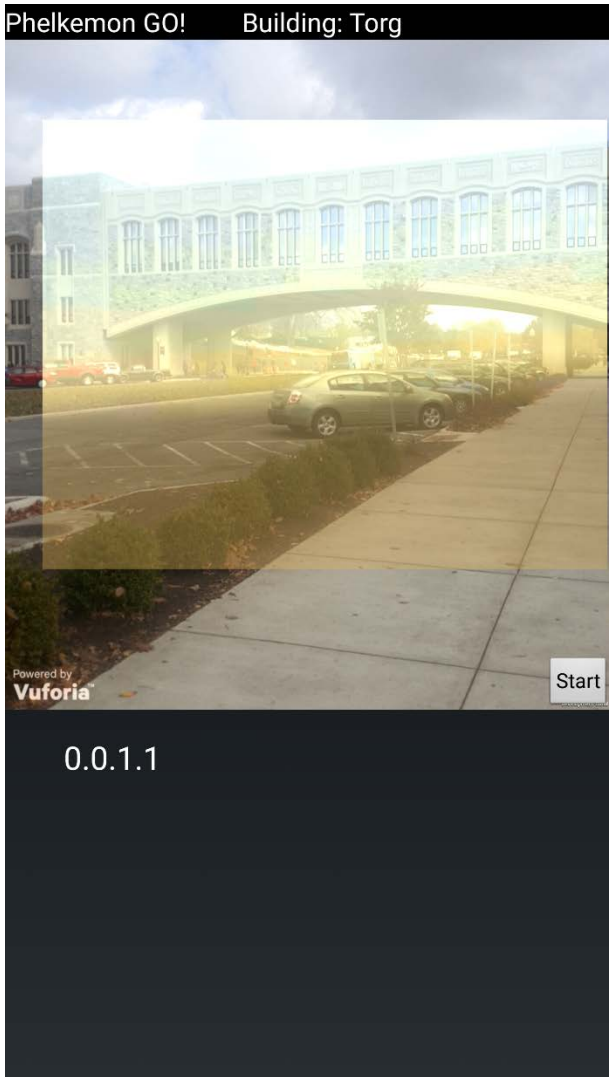


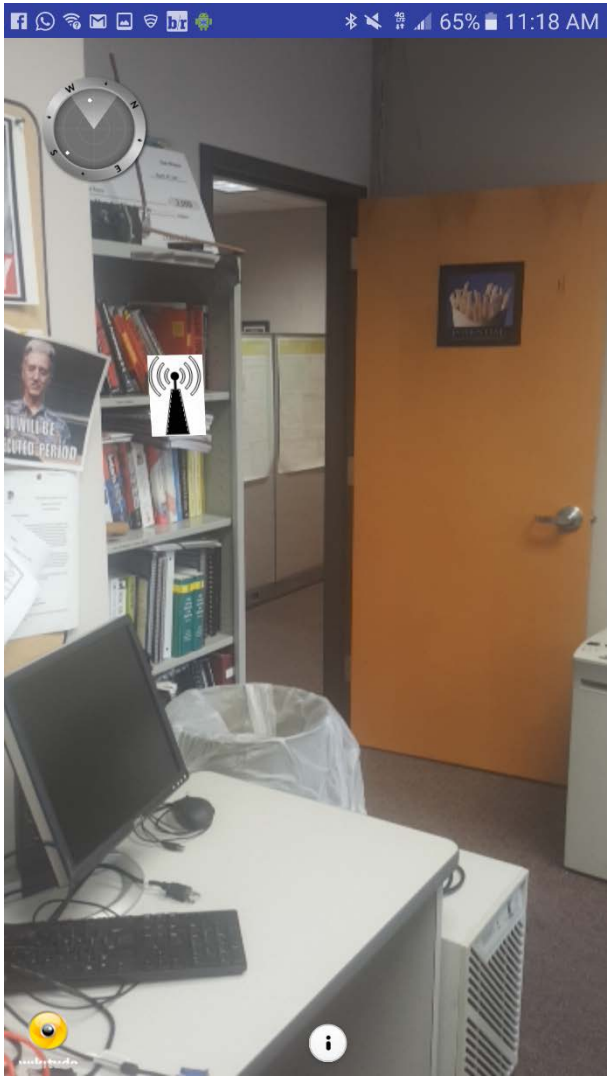


Intuition



Early Prototypes





Range Components

Courseware Repository

- ❑ Courses, modules, and exercises for use in HS, CC, and university cybersecurity curricula
  - Instructors/professors can select course content in full or *a la carte*
- ❑ Grants offered for courseware dev

Exercise Area

- ❑ Environment to run exercises as part of courses
- ❑ Team-based offensive and defensive, scenario-based cybersecurity exercises
- ❑ Cyber-physical system simulation (SCADA/IoT) for vulnerability exploration and analysis

Community of Purpose

- ❑ Consortium Governance
- ❑ Convene workshops to “teach the teachers” and share best practices
- ❑ Help expand NSA/DHS CAE certification among Virginia colleges and universities

Governance

- Consortium among participating institutions
  - Virginia Tech shall serve as the coordinating entity
  - Initial Consortium includes 2- and 4-year NSA/DHS Centers of Academic Excellence (CAE) in Cybersecurity Education and DoD Cyber Crimes Center Unit (DC3) National Centers of Digital Forensics Academic Excellence (CDFAE)
- Meet monthly to discuss way forward for the cyber range

- George Mason University (NSA/DHS CAE-CDE/R)
- James Madison University (NSA/DHS CAE-CDE)
- Longwood University (DC3 CDFAE)
- Lord Fairfax CC (NSA/DHS CAE-CDE 2Y)
- Norfolk State University (NSA/DHS CAE-CDE)
- Northern Virginia CC (NSA/DHS CAE-CDE 2Y)
- Radford University (NSA/DHS CAE-CDE)
- Tidewater CC (NSA/DHS CAE-CDE 2Y)
- Virginia Tech (NSA/DHS CAE-R)

Our Approach

- Hosted in the cloud
- Web portal for access to cyber range content
  - Role-based access
  - Login to see user-specific content
- Virtual environments will be dynamically created and destroyed as users start and finish exercises
- Large target networks can be replicated for multiple, simultaneous use

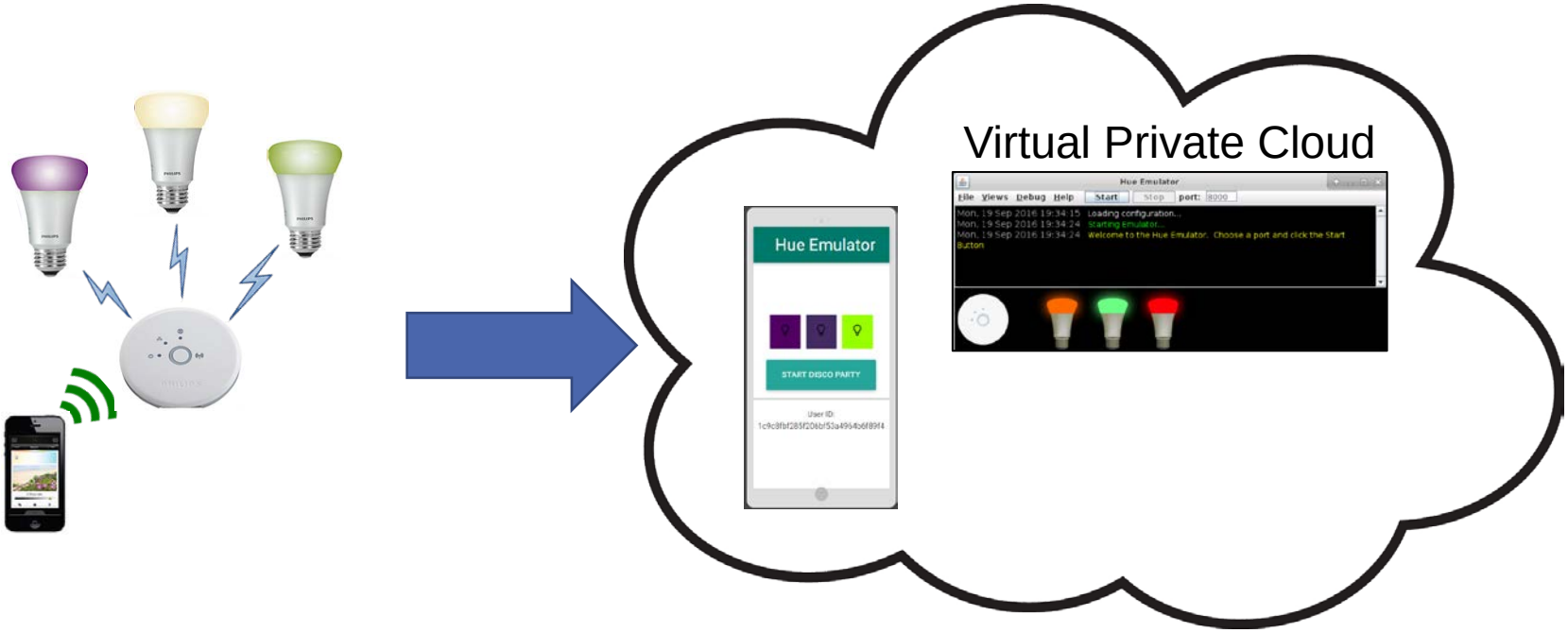
Example Cybersecurity Topics

- Introduction to Cybersecurity
- Introduction to Networking
- Secure Network Configuration
- Network Defense
- Digital Forensics
- Network and Memory Forensics
- Reverse Engineering
- Cryptography
- Incident Response
- Penetration Testing
- Security Data Analytics
- Mobile Devices and IoT
- SCADA and Industrial Control Systems
- Cyber Policy and Law

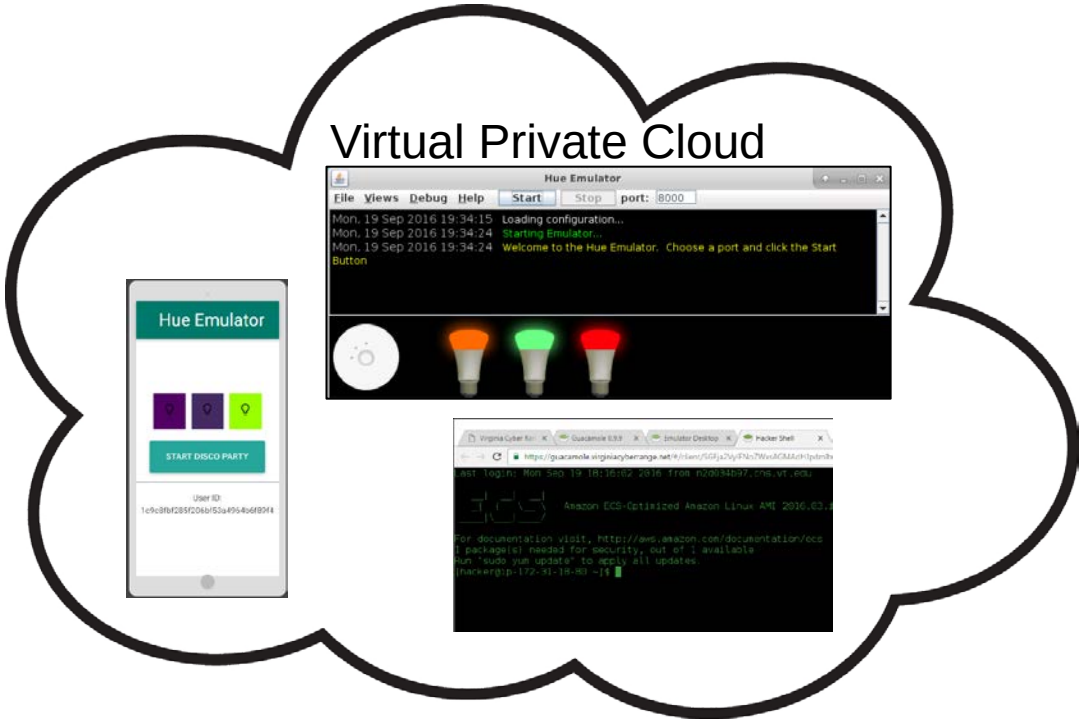
virginiacyberrange.org

Our Simulation (1)

- Virtual machines are used to replicate typical IoT scenario
  - One VM emulates lighting system (wireless bridge and bulbs)
  - Another VM simulates an authorized user of the system using a smartphone



VIRGINIA
CYBER RANGE

Our Simulation (2)

- A malicious actor can eavesdrop on wireless communications
  - Captures information that lets her impersonate the authorized user
  - Impersonates user to
    - Control lights
    - Create new users
    - Delete existing users
  - ***These actions let the attacker take complete control of the target system!***