2019 S&T Cybersecurity and Innovation Showcase

Solutions Now I Innovations for the Future

Homeland Security
Science and Technology

A Federated Defense Community and Ecosystem in Practice

Thomas C Eskridge | Florida Institute of Technology

January 9, 2019

Homeland Security

Science and Technology

Team Profile

Florida Institute of Technology

Harris Institute for Assured Information

- Marco Carvalho, Ph.D. (PI)
- Thomas C Eskridge, Ph.D. (Tech Lead)
- William Nyfenegger, Shea Akerman
- Danny Metha, Shayesteh Talegahni

- DHS S&T PM: Edward Rhyne

Designated a **National Center of Academic Excellence in Information Assurance Research (CAE/R)** by the National Security Agency and the U.S. Department of Homeland Security.
For Academic Years 2014-2019

Florida Institute of Technology
Harris Institute for Assured Information

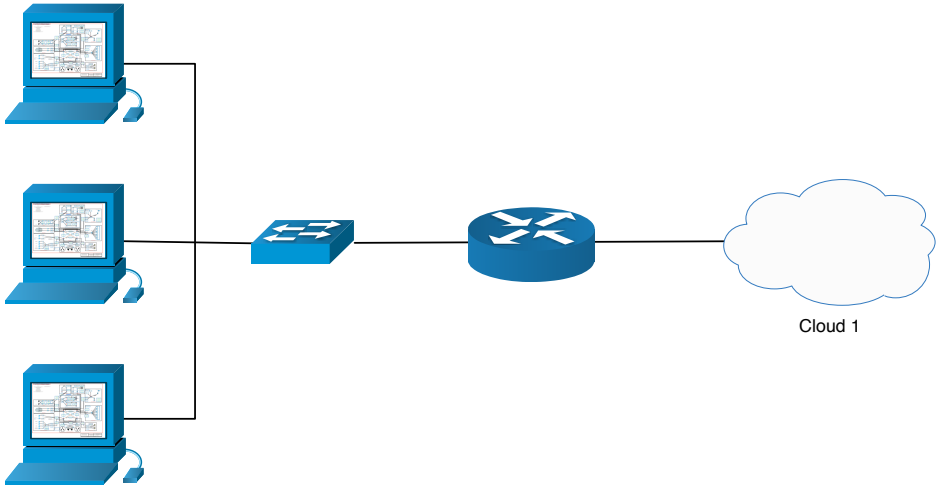
Sharing Information

- Organizations have several alternatives for sharing cyber threat information
- Mostly manual processes to ensure sharing policies are respected
- Information is not shared in a consistent, timely, and usable way

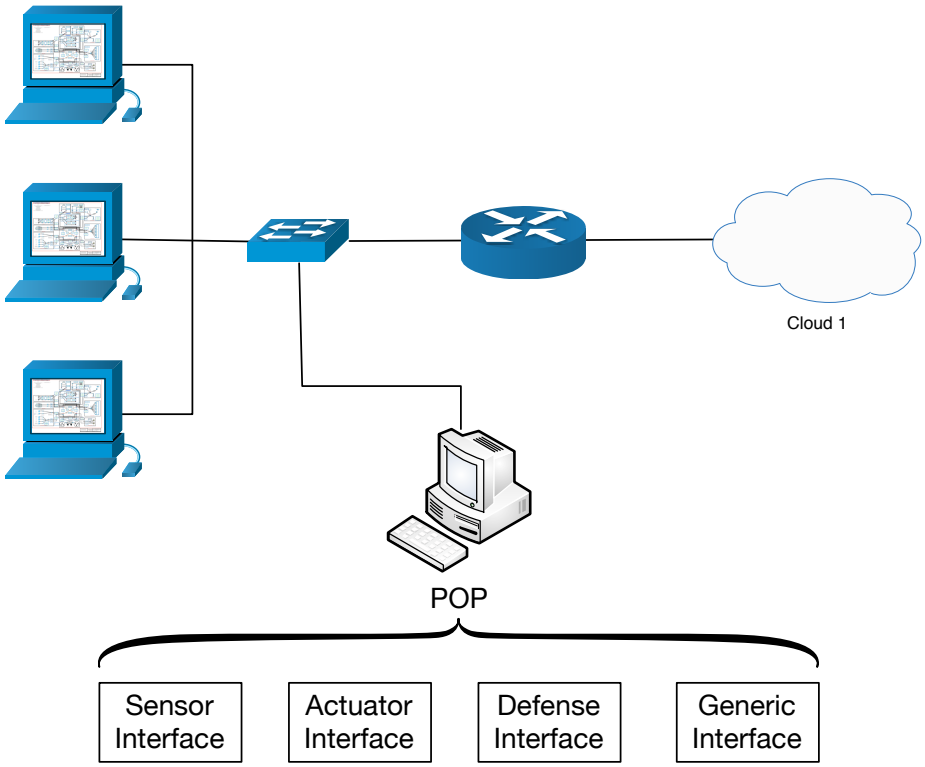
Sharing and Using Information

- The Federated Command and Control (FC2) program established
  - the technology to specify what is to be shared,
  - the mechanisms to automatically share it,
  - the capability to automatically use shared information

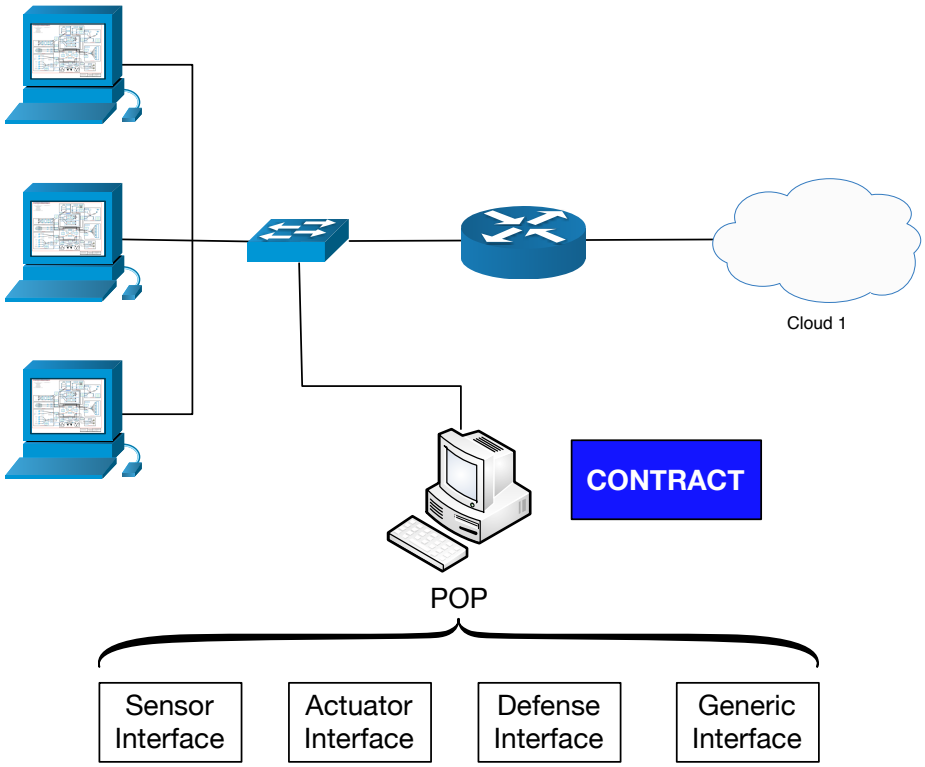
FC2 overview



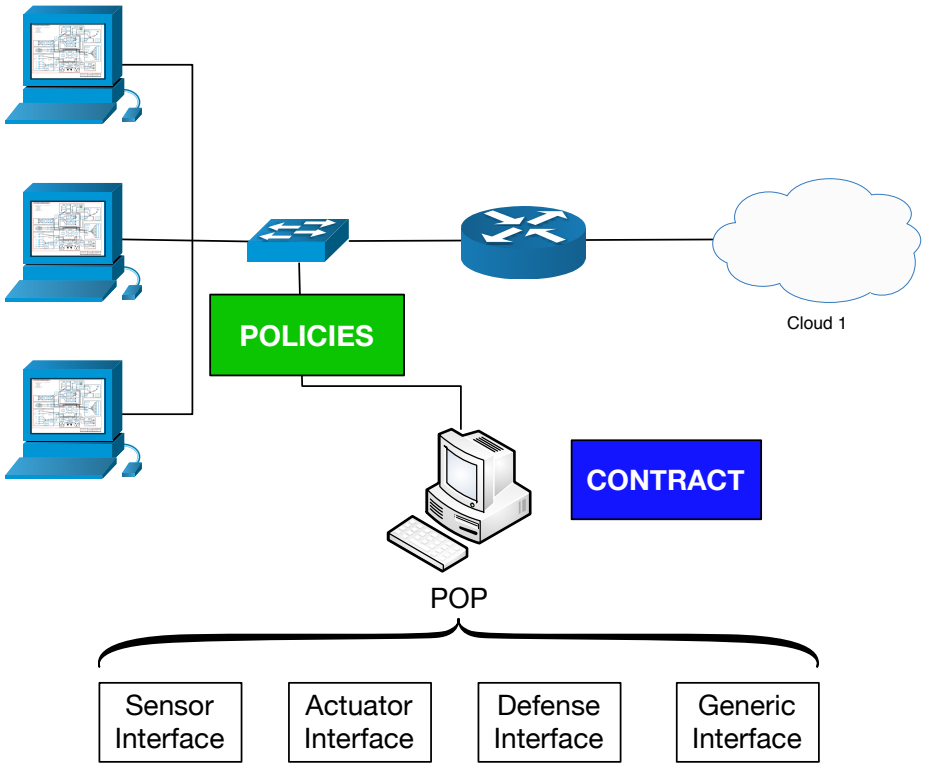
FC2 overview



FC2 overview



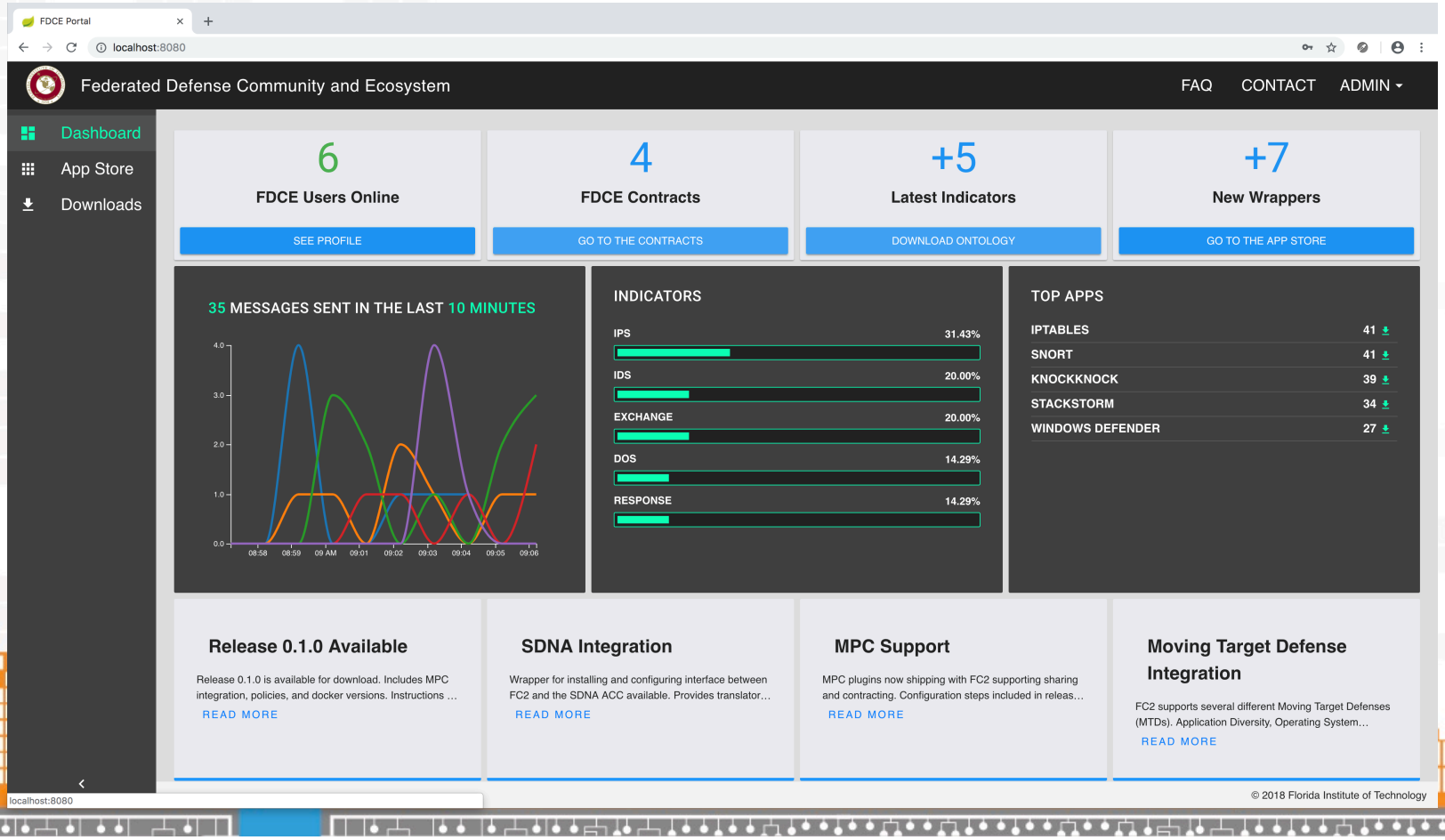
FC2 overview



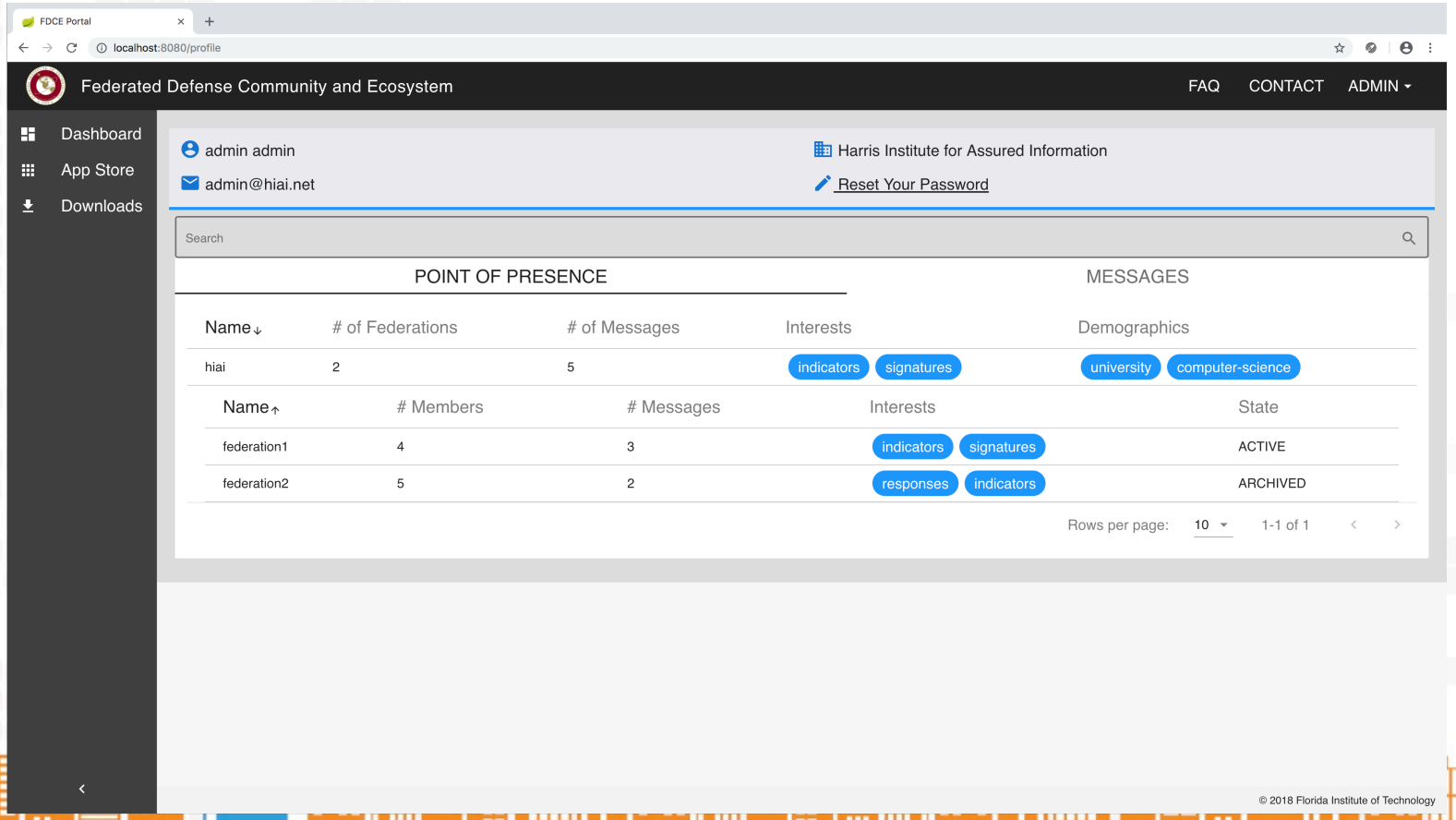
Building Communities

- FDCE Portal provides existing and potential members
  - Information on the status of the federations currently in force
  - Historical information of the effectiveness of information sharing
  - Download of FC2 system
  - Download of FC2 apps
  - News and updates

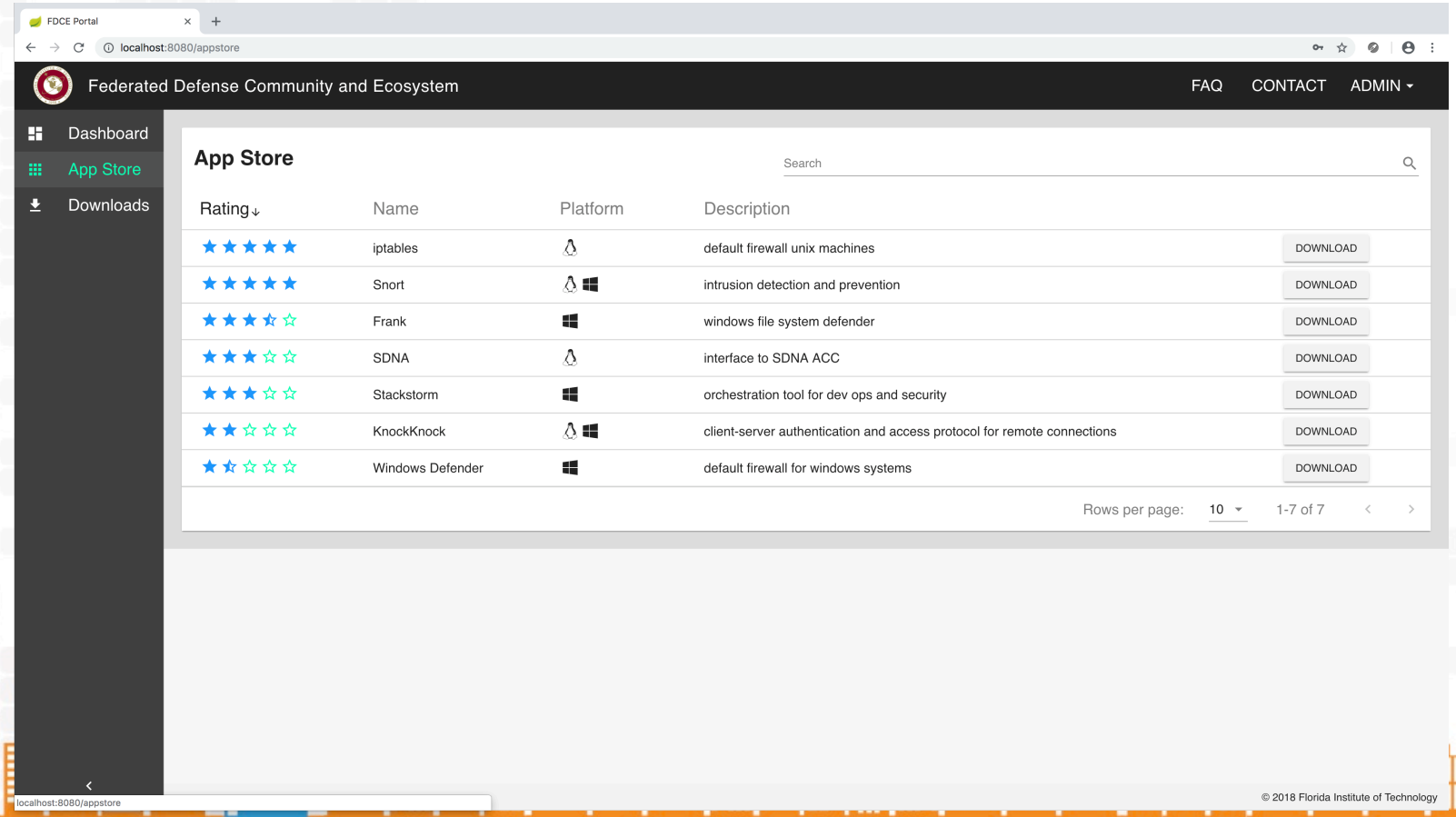
Building Communities



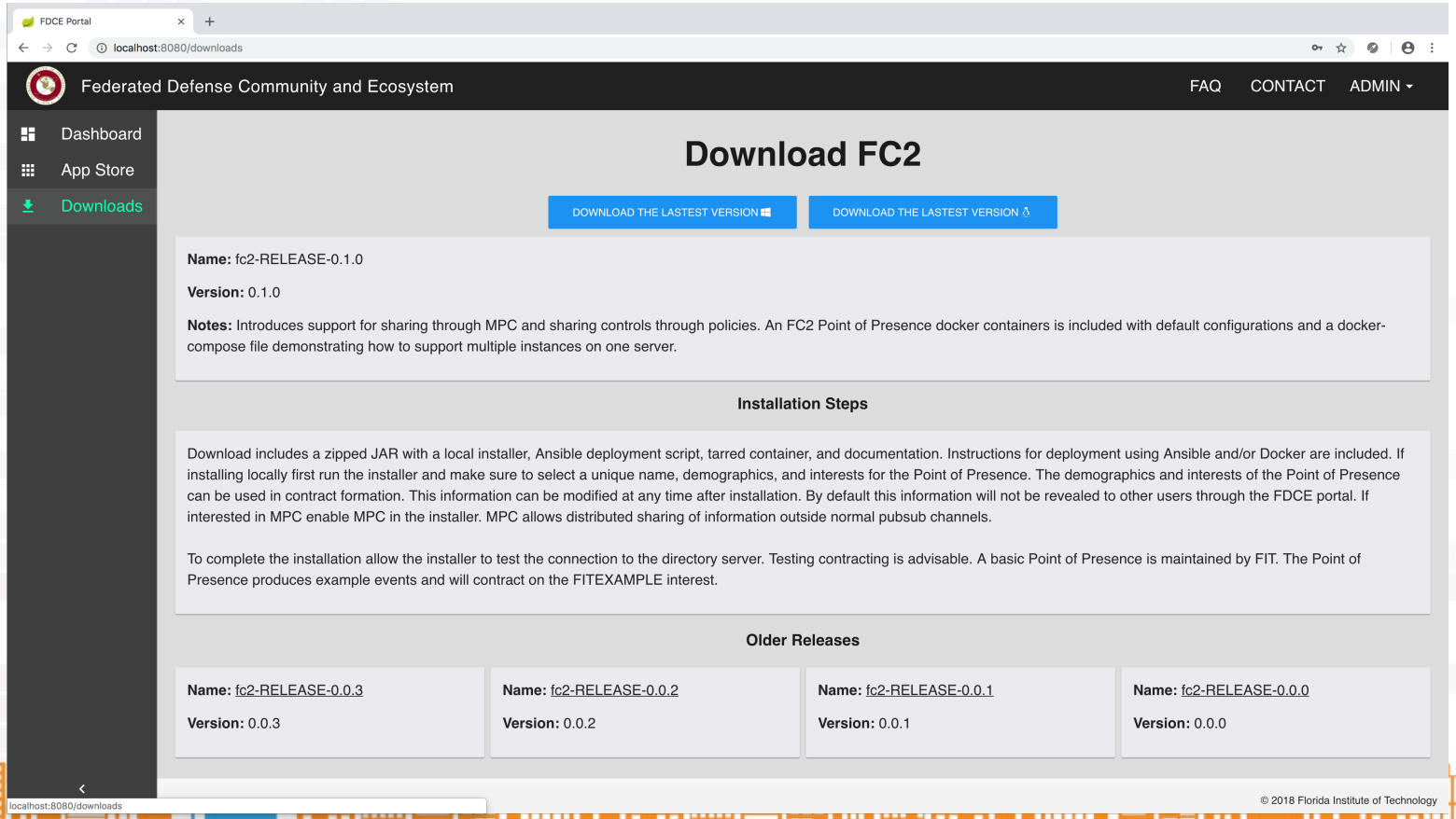
Building Communities



Building Communities



Building Communities



Growing and maintaining communities

- FDCE Portal will be the principal means of communicating with the community
- Use cases, performance reviews, enhancements
- Core and app updates, new app availability
- Upcoming workshops

Benefits

- Organizations will see
  - automatic population and sending information on contracted information
  - automatic use of incoming information
  - expanded sensor network
- Community to support customizable, contextual, and actionable information sharing

Alternative Sharing Services

- Sharing indicators
- Sharing observations
- Sharing responses

Current Status

- Packaged FC2 for delivery and installation
  - docker containers for POP
  - app store for sensors and defenses
    - 14 sensors and actuators
    - 8 advanced defenses

Current Status

- Developing the organization portal
  - User registration
  - Aggregate reporting from members
  - Member profile pages
  - FC2 Core download
  - App store downloads

Current Status

- Recruiting new members
- Adding new FC2 apps
- Developing training materials
- Planning end of year workshop

Lessons Learned

- Simplicity
- Anonymity
- Predictability and feedback

Contact Info

Marco Carvalho (PI)
Florida Institute of Technology
Harris Institute for Assured Information
mcarvalho@fit.edu
321 674 8767

Thomas C Eskridge
teskridge@fit.edu
321 674 7455

2019 S&T Cybersecurity and Innovation Showcase

Solutions Now I Innovations for the Future

Homeland Security
Science and Technology