

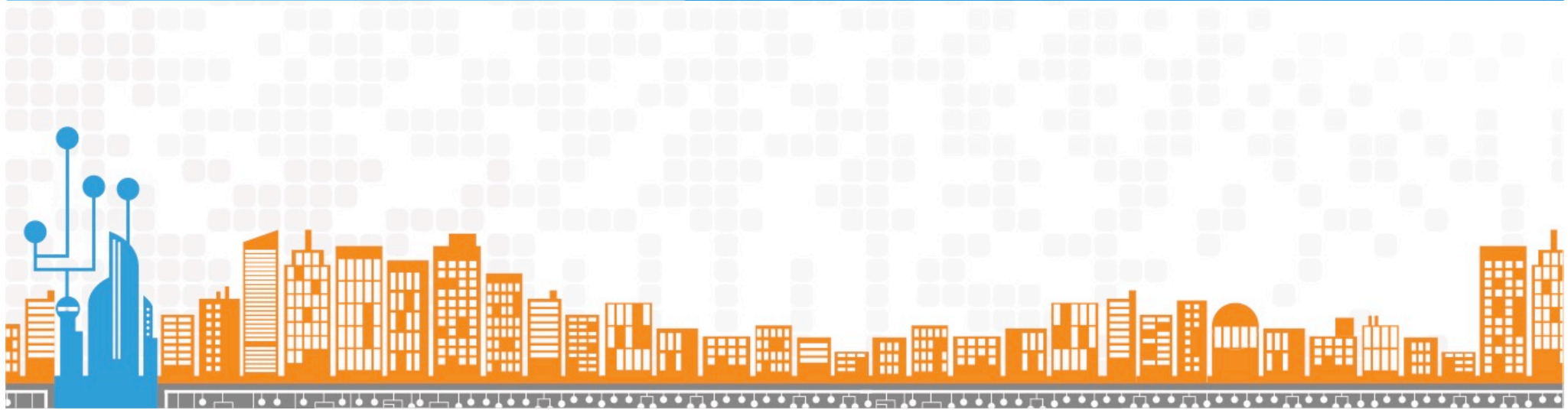
# 2019 S&T Cybersecurity and Innovation Showcase

Solutions Now | 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

DRAFT



Homeland  
Security

Science and Technology





# Team Profile



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

- 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



*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







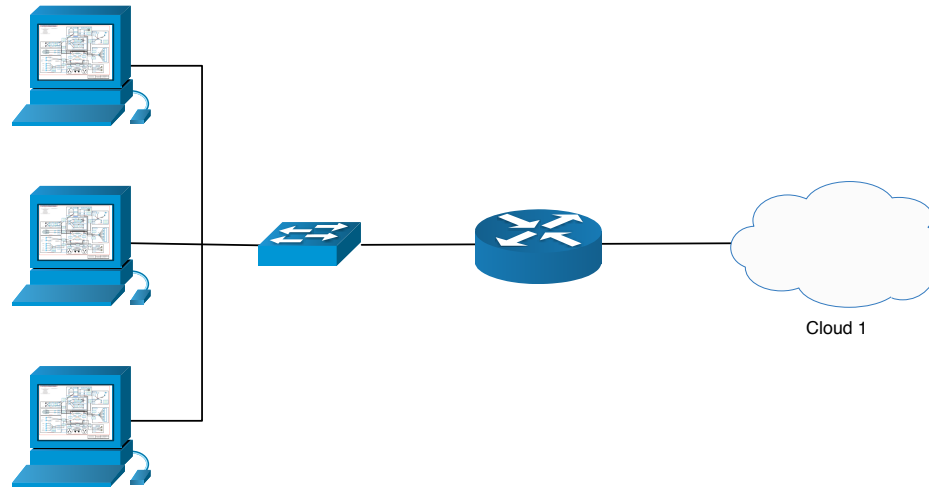
# Sharing and Using Information

- 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



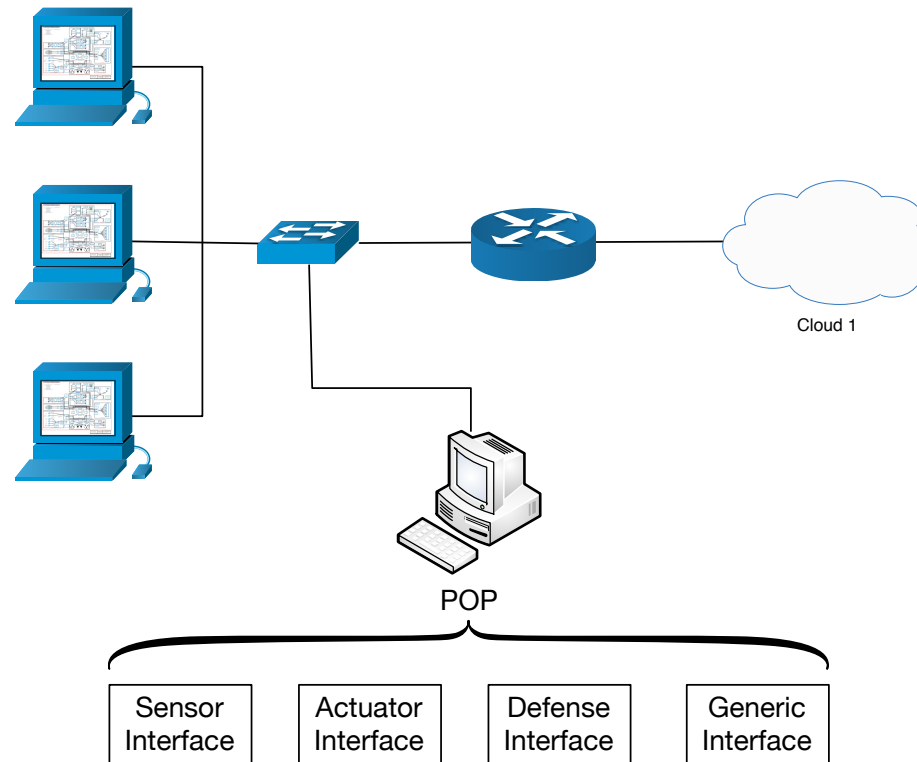


# FC2 overview



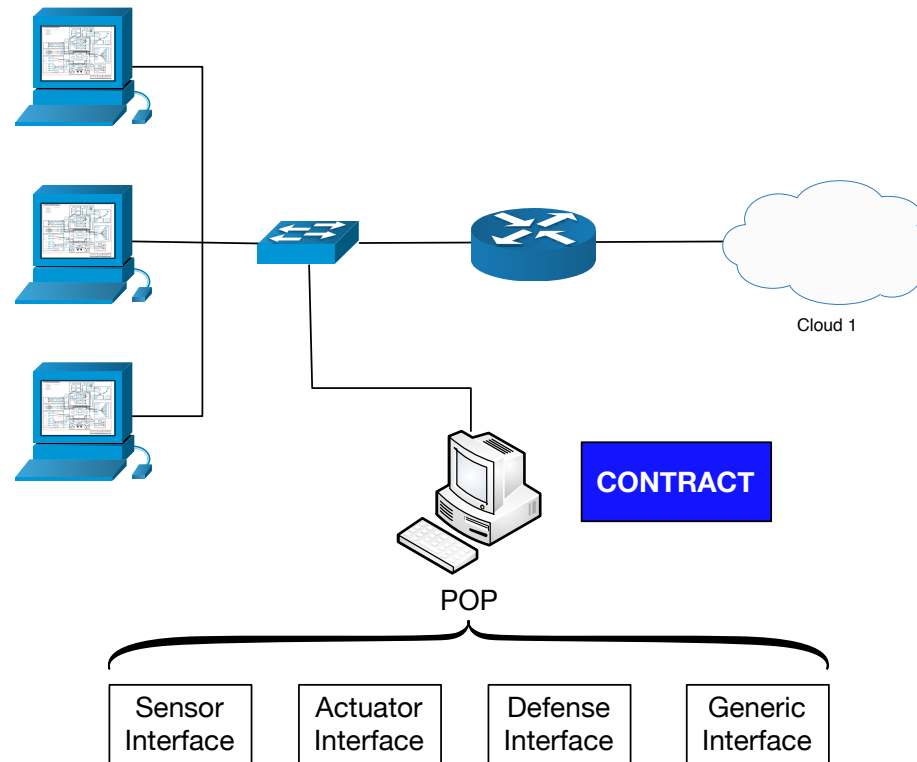


# FC2 overview





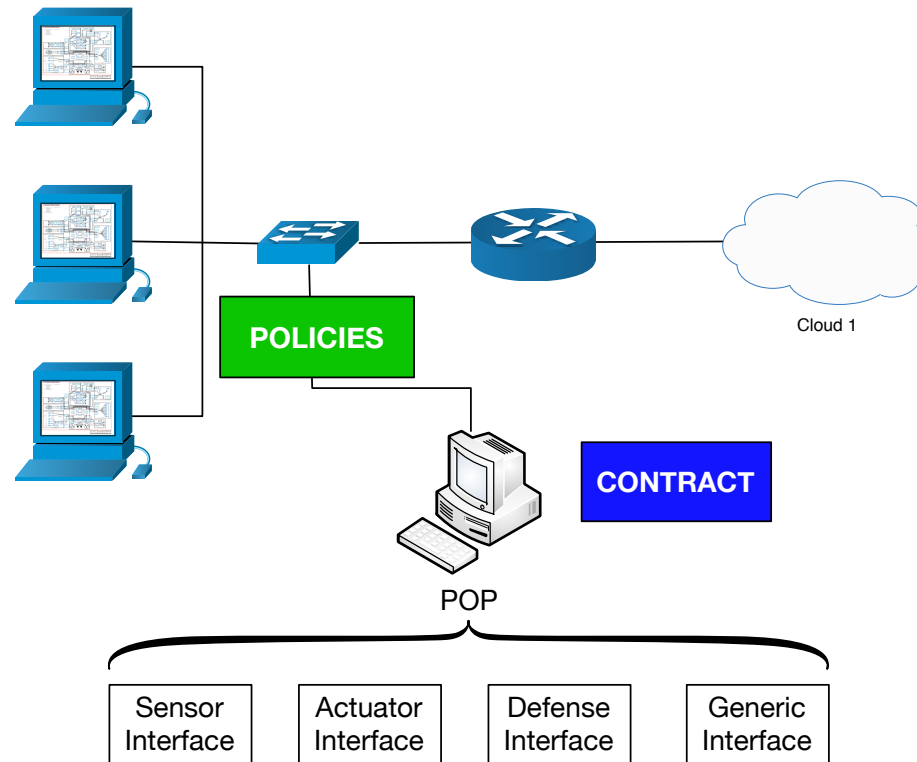
# FC2 overview







# FC2 overview





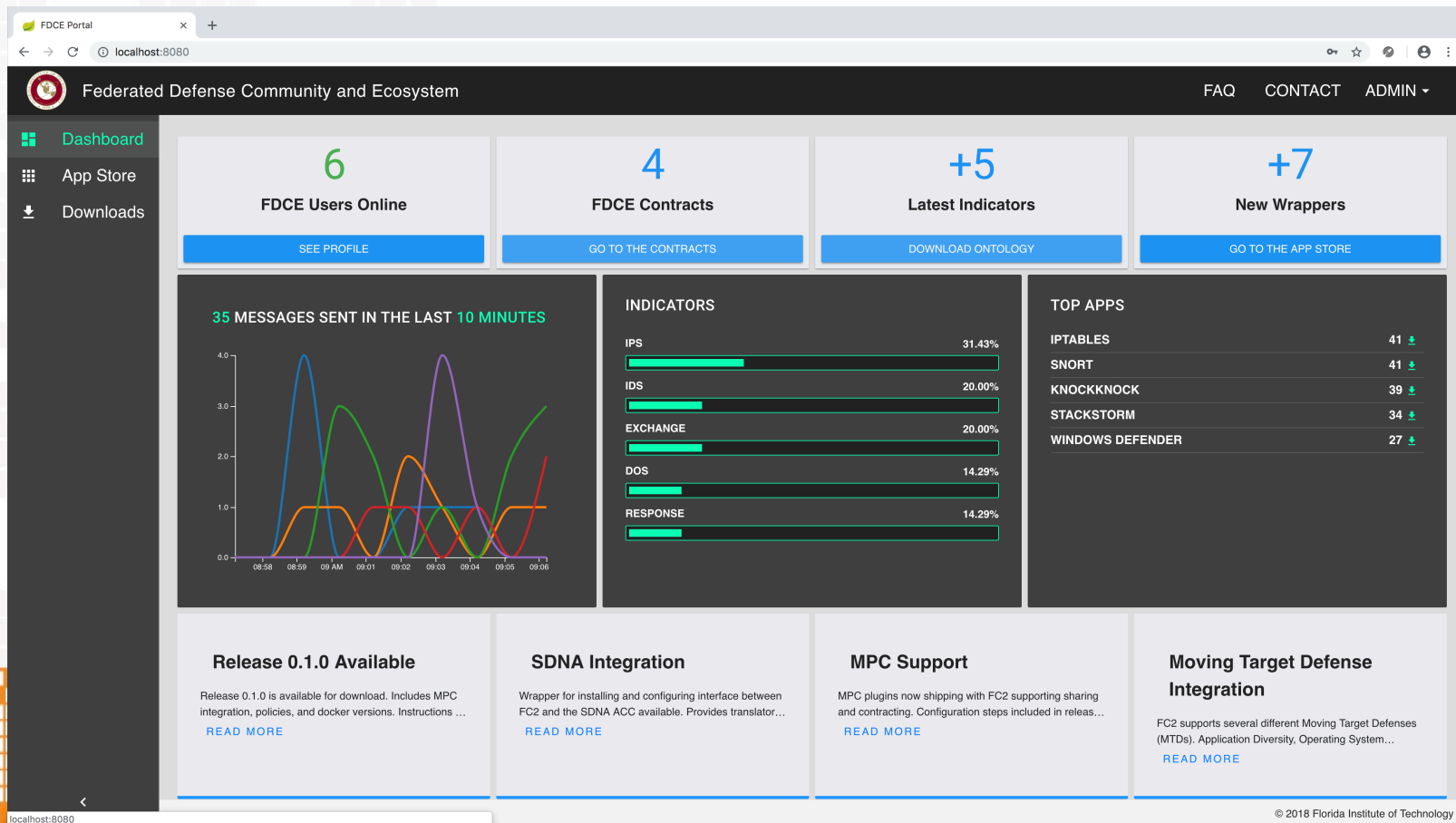
# Building Communities

- 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

FDCE Portal

localhost:8080/profile

☆ | 🔍 | 👤 | ⋮


 Federated Defense Community and Ecosystem


FAQ | CONTACT | ADMIN ▾


Dashboard


App Store

Downloads

 admin admin

 Harris Institute for Assured Information

 admin@hi.ai.net

 [Reset Your Password](#)

Search

🔍

POINT OF PRESENCE

MESSAGES

Name ▾	# of Federations	# of Messages	Interests	Demographics
hi.ai	2	5	<a href="#">indicators</a> <a href="#">signatures</a>	<a href="#">university</a> <a href="#">computer-science</a>

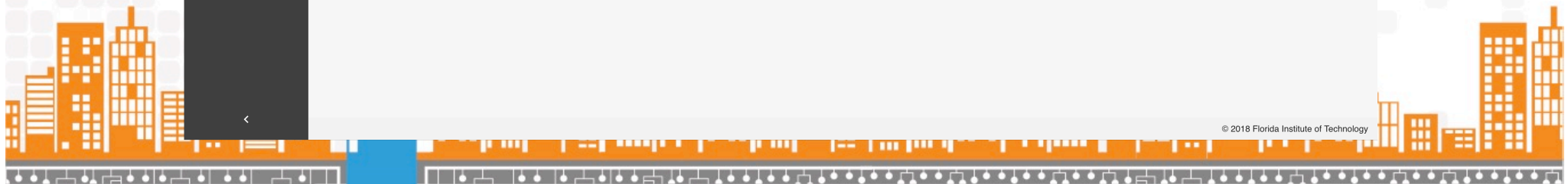
Name ▴	# Members	# Messages	Interests	State
federation1	4	3	<a href="#">indicators</a> <a href="#">signatures</a>	ACTIVE
federation2	5	2	<a href="#">responses</a> <a href="#">indicators</a>	ARCHIVED

Rows per page: 10 ▾

1-1 of 1

< >

© 2018 Florida Institute of Technology






# Building Communities

FDCE Portal

localhost:8080/appstore

 Federated Defense Community and Ecosystem

FAQCONTACTADMIN










Dashboard

App Store

Downloads

App Store

Search

Rating↓	Name	Platform	Description	
★★★★★	iptables		default firewall unix machines	DOWNLOAD
★★★★★	Snort	 	intrusion detection and prevention	DOWNLOAD
★★★★☆	Frank		windows file system defender	DOWNLOAD
★★★★☆	SDNA		interface to SDNA ACC	DOWNLOAD
★★★★☆	Stackstorm		orchestration tool for dev ops and security	DOWNLOAD
★★★★☆	KnockKnock	 	client-server authentication and access protocol for remote connections	DOWNLOAD
★★★★☆	Windows Defender		default firewall for windows systems	DOWNLOAD

Rows per page: 10 1-7 of 7

localhost:8080/appstore

© 2018 Florida Institute of Technology






# Building Communities

FDCE Portal

localhost:8080/downloads

 Federated Defense Community and Ecosystem

FAQCONTACTADMIN ▾

Dashboard

App Store

Downloads

## Download FC2

DOWNLOAD THE LATEST VERSION ▾

DOWNLOAD THE LATEST VERSION ▴

**Name:** fc2-RELEASE-0.1.0

**Version:** 0.1.0

**Notes:** Introduces support for sharing through MPC and sharing controls through policies. An FC2 Point of Presence docker containers is included with default configurations and a docker-compose file demonstrating how to support multiple instances on one server.

### Installation Steps

Download includes a zipped JAR with a local installer, Ansible deployment script, tarred container, and documentation. Instructions for deployment using Ansible and/or Docker are included. If installing locally first run the installer and make sure to select a unique name, demographics, and interests for the Point of Presence. The demographics and interests of the Point of Presence can be used in contract formation. This information can be modified at any time after installation. By default this information will not be revealed to other users through the FDCE portal. If interested in MPC enable MPC in the installer. MPC allows distributed sharing of information outside normal pubsub channels.

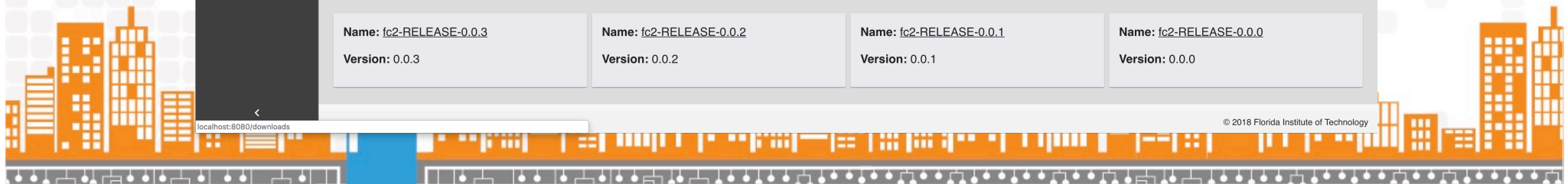
To complete the installation allow the installer to test the connection to the directory server. Testing contracting is advisable. A basic Point of Presence is maintained by FIT. The Point of Presence produces example events and will contract on the FITEXAMPLE interest.

### Older Releases

<p><b>Name:</b> <a href="#">fc2-RELEASE-0.0.3</a></p> <p><b>Version:</b> 0.0.3</p>	<p><b>Name:</b> <a href="#">fc2-RELEASE-0.0.2</a></p> <p><b>Version:</b> 0.0.2</p>	<p><b>Name:</b> <a href="#">fc2-RELEASE-0.0.1</a></p> <p><b>Version:</b> 0.0.1</p>	<p><b>Name:</b> <a href="#">fc2-RELEASE-0.0.0</a></p> <p><b>Version:</b> 0.0.0</p>
------------------------------------------------------------------------------------	------------------------------------------------------------------------------------	------------------------------------------------------------------------------------	------------------------------------------------------------------------------------

localhost:8080/downloads

© 2018 Florida Institute of Technology





# 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](mailto:mcarvalho@fit.edu)

321 674 8767

**Thomas C Eskridge**

[teskridge@fit.edu](mailto:teskridge@fit.edu)


321 674 7455



*Florida Institute of Technology*

Harris Institute for Assured Information





# 2019 S&T Cybersecurity and Innovation Showcase

Solutions Now | Innovations for the Future



Homeland  
Security

Science and Technology

