

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





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





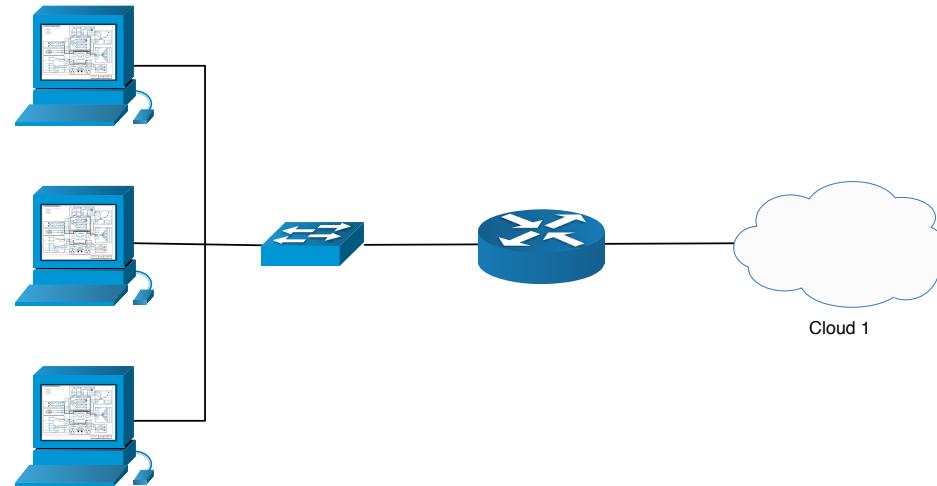
Sharing and Using Information

- 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



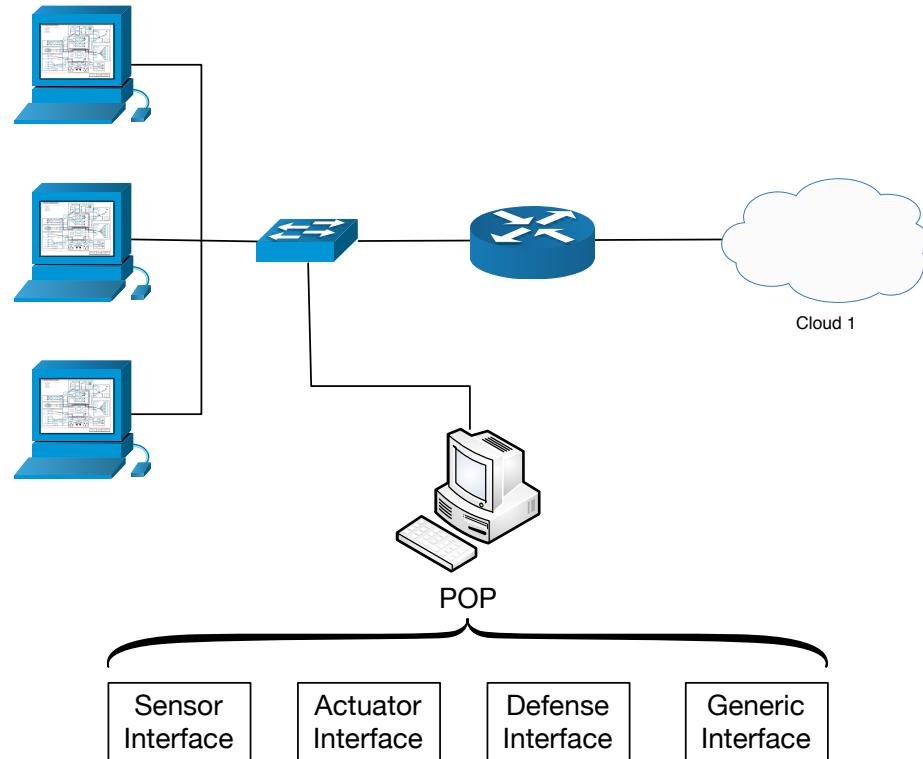


FC2 overview



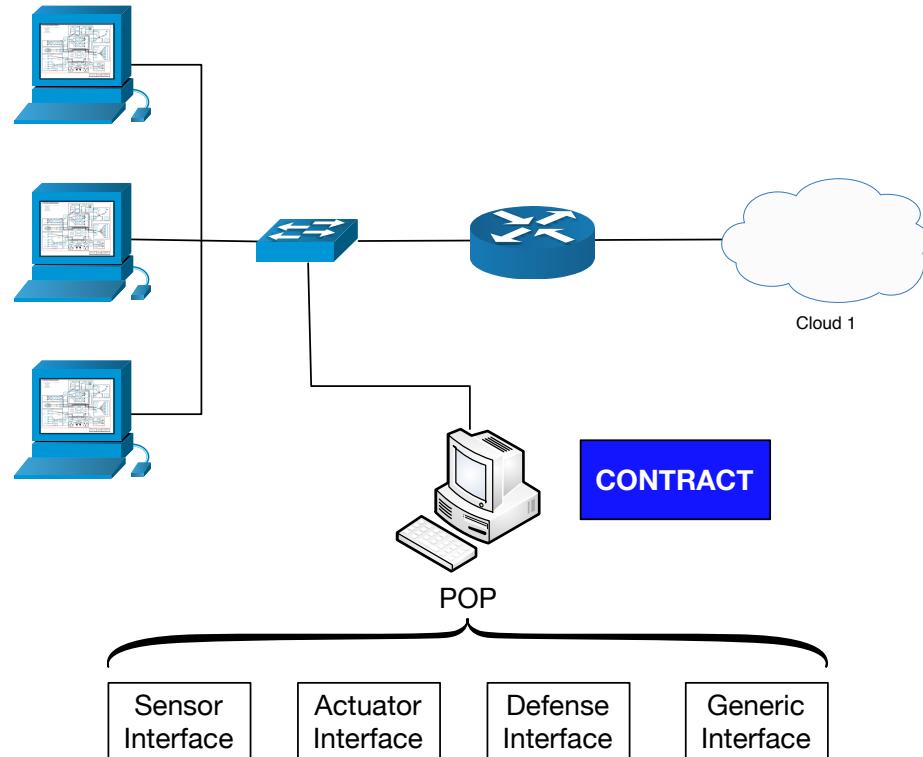


FC2 overview



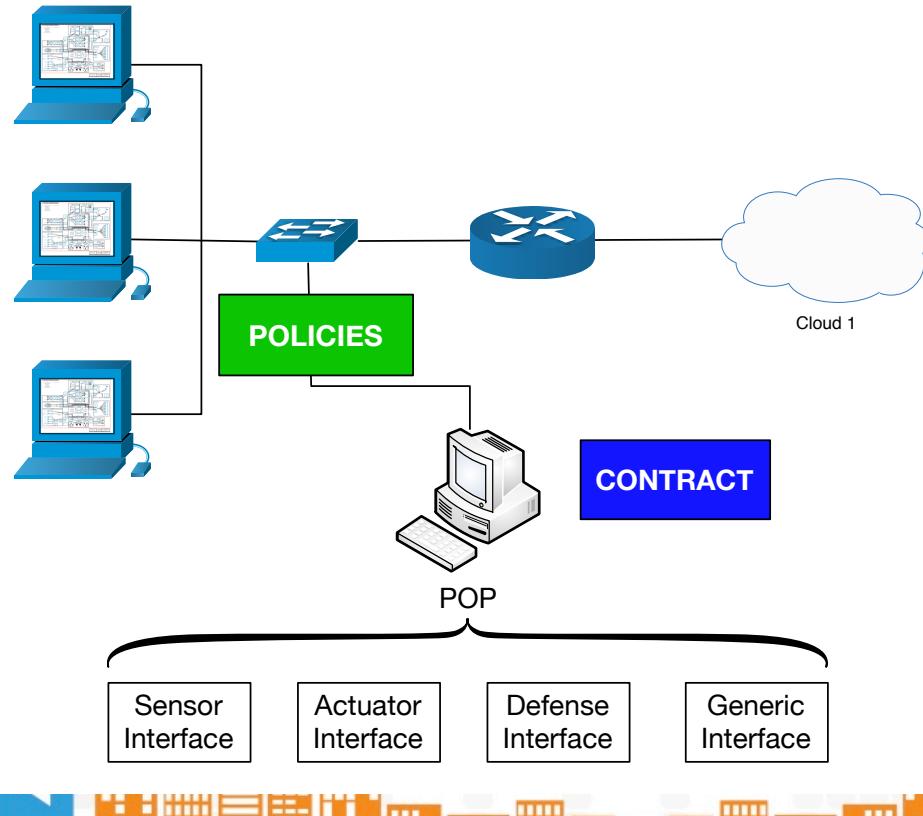


FC2 overview





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

Federated Defense Community and Ecosystem

FAQ CONTACT ADMIN ▾

Dashboard App Store Downloads

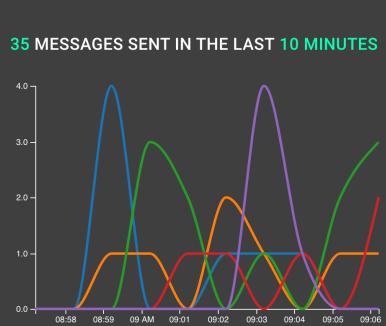
FDCE Users Online: 6 SEE PROFILE

FDCE Contracts: 4 GO TO THE CONTRACTS

Latest Indicators: +5 DOWNLOAD ONTOLOGY

New Wrappers: +7 GO TO THE APP STORE

35 MESSAGES SENT IN THE LAST 10 MINUTES



INDICATORS

Indicator	Percentage
IPS	31.43%
IDS	20.00%
EXCHANGE	20.00%
DOS	14.29%
RESPONSE	14.29%

TOP APPS

App	Count
IPTABLES	41 ↗
SNORT	41 ↗
KNOCKKNOCK	39 ↗
STACKSTORM	34 ↗
WINDOWS DEFENDER	27 ↗

Release 0.1.0 Available

Release 0.1.0 is available for download. Includes MPC integration, policies, and docker versions. Instructions ...

[READ MORE](#)

SDNA Integration

Wrapper for installing and configuring interface between FC2 and the SDNA ACC available. Provides translator...

[READ MORE](#)

MPC Support

MPC plugins now shipping with FC2 supporting sharing and contracting. Configuration steps included in releas...

[READ MORE](#)

Moving Target Defense Integration

FC2 supports several different Moving Target Defenses (MTDs). Application Diversity, Operating System...

[READ MORE](#)

localhost:8080

© 2018 Florida Institute of Technology

Building Communities

The screenshot shows a web browser window for the FDCE Portal at localhost:8080/profile. The page has a dark header with the title "Federated Defense Community and Ecosystem". On the left is a sidebar with links: Dashboard, App Store, and Downloads. The main content area displays user information: "admin admin" and "admin@hiai.net", along with a link to "Harris Institute for Assured Information" and a "Reset Your Password" button. Below this is a search bar and a table titled "POINT OF PRESENCE". The table has two sections: "MESSAGES" and "Demographics". The "MESSAGES" section shows data for "hiai" (Name, # of Federations: 2, # of Messages: 5) with interests "indicators" and "signatures" and demographics "university" and "computer-science". The "Demographics" section shows data for "federation1" (Name, # Members: 4, # Messages: 3) with interests "indicators" and "signatures" and state "ACTIVE", and for "federation2" (Name, # Members: 5, # Messages: 2) with interests "responses" and "indicators" and state "ARCHIVED". At the bottom of the table are pagination controls: "Rows per page: 10", "1-1 of 1", and navigation arrows.

POINT OF PRESENCE				MESSAGES	
Name ↓	# of Federations	# of Messages	Interests	Demographics	
hiai	2	5	indicators signatures	university computer-science	
Name ↑	# Members	# Messages	Interests	State	
federation1	4	3	indicators signatures	ACTIVE	
federation2	5	2	responses indicators	ARCHIVED	

Building Communities

The screenshot shows a web browser window titled "FDCE Portal" at the URL "localhost:8080/appstore". The page is titled "Federated Defense Community and Ecosystem" and features a navigation menu on the left with options: Dashboard, App Store (which is selected), and Downloads. The main content area is titled "App Store" and displays a table of applications. The table has columns for Rating, Name, Platform, Description, and a "DOWNLOAD" button. The applications listed are:

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

At the bottom of the table, there are pagination controls: "Rows per page: 10", "1-7 of 7", and navigation arrows.

At the very bottom of the page, there is a footer bar with the text "localhost:8080/appstore" and "© 2018 Florida Institute of Technology".

Building Communities

The screenshot shows a web browser window titled "FDCE Portal" at "localhost:8080/downloads". The page is titled "Download FC2". It features a sidebar with "Downloads" selected. The main content area displays information for "fc2-RELEASE-0.1.0" and "fc2-RELEASE-0.0.1".

fc2-RELEASE-0.1.0

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

Name	Version
fc2-RELEASE-0.0.3	0.0.3
fc2-RELEASE-0.0.2	0.0.2
fc2-RELEASE-0.0.1	0.0.1
fc2-RELEASE-0.0.0	0.0.0

© 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

321 674 8767

Thomas C Eskridge

teskridge@fit.edu

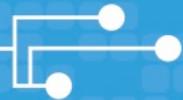
321 674 7455



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

