Trusted CI's TTP Program

Jim Basney
jbasney@ncsa.illinois.edu
September 14, 2023

*with contributions by:
Florence D. Hudson and Ryan Kiser

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Trusted CI:
The NSF Cybersecurity Center of Excellence

Our mission: to lead in the development of an NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and NSF's vision of a nation that is a global leader in research and innovation.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

NCSA

BERKELEY LAB

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

PITTSBURGH SUPERCOMPUTING CENTER

USA UNIVERSITY OF SOUTH ALABAMA

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://trustedci.org/

What is Cyberinfrastructure (CI)?

"The comprehensive infrastructure needed to capitalize on dramatic advances in information technology has been termed cyberinfrastructure (CI). Cyberinfrastructure integrates hardware for computing, data and networks, digitally-enabled sensors, observatories and experimental facilities, and an interoperable suite of software and middleware services and tools. "

-NSF Cyberinfrastructure Vision for 21st Century Discovery

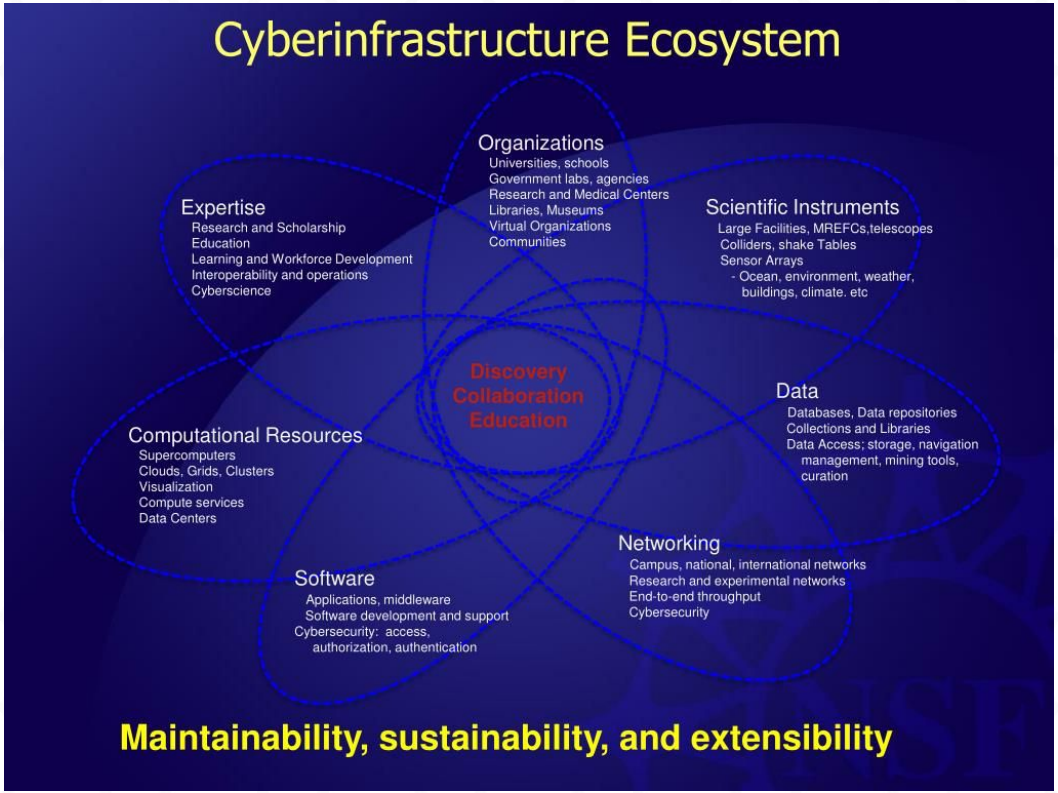


Image credit: NSF

Cybersecurity Transition to Practice (TTP)

Enabling researcher and practitioner collaboration to accelerate cybersecurity research to practice in academia, industry, government, or open source via

- Researcher/practitioner matchmaking
- Technical Readiness Level assessment
- TTP Canvas
- TTP Success Stories
- TTP Playbook

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

https://trustedci.org/ttp

Cybersecurity TTP Success Stories

- Boston University and the City of Boston with Secure Multi-Party Computation for gender pay gap analysis - Mayank Varia, BU
- Simplifying logon to cyberinfrastructure - Jim Basney, NCSA
- Securing payment card readers - Patrick Traynor, University of Florida
- Using machine learning to aid in the fight against cyberattacks - Jay Yang, Rochester Institute of Technology
- Exploring Unconventional Analog Computing - Shantanu Chakrabartty, Washington University in St. Louis
- The behavioral side of cybersecurity - Aunshul Rege, Temple University

Transition to Practice Success Story

CILogon 2.0 - Integrated IAM Platform for Science

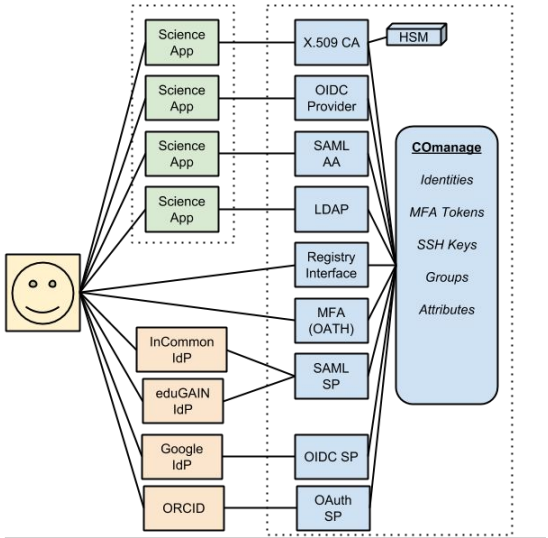
Challenges we sought to address

- Enable logon to scientific cyberinfrastructure (CI)
- Seamless IAM for academic research collaborations
- Use your campus identity
- Manage attributes/groups/roles for many research applications

Innovations we delivered

- Support for 2500+ identity providers, including international campus identity providers, GitHub, Google, and ORCID
- Multiple application APIs (OIDC, SAML, LDAP, X.509, SSH)
- voPerson attribute schema for Virtual Organizations (VOs)

Solution Overview



NSF #1547268

PI: Jim Basney

Team: Flanagan, Fleury, Gaynor, Koranda, Oshrin

Email: jbasney@ncsa.Illinois.edu

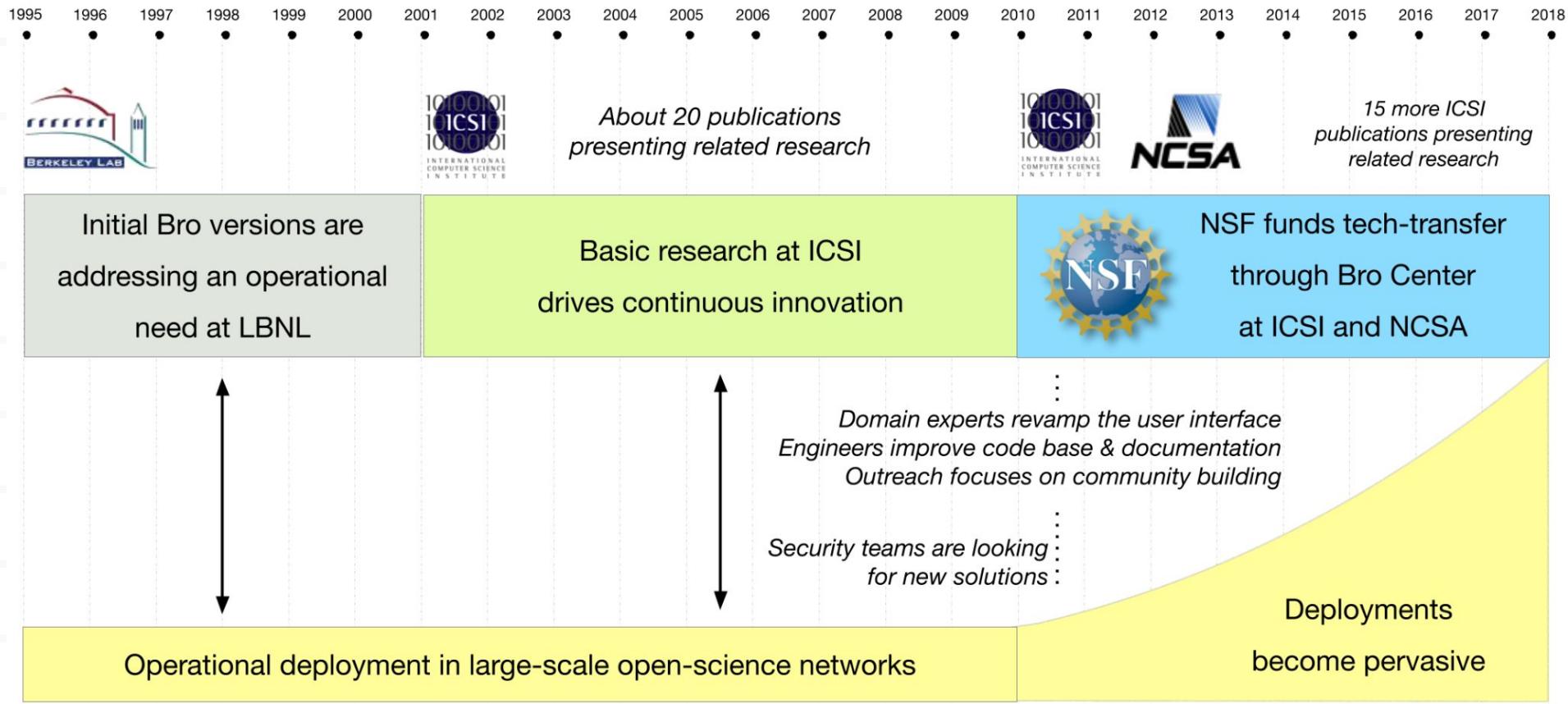
Value Proposition for users

- Researchers: federated auth for research applications
- CI operators: SaaS subscription
- Higher ed: open source IAM platform for campus research collaborations

TTP Best practices and key learnings

- TTP takes time! 10 years from first grant to first paying customer
- SBIR / STTR / I-Corps isn't the only way
- Talk to campus TTP office early
- Include TTP in grant milestones
- Program Income Fund → Self Supporting Fund
- Understand customer acquisition costs
- Get authorized signature on contracts

Zeek History



Credit: Robin Sommers' 2019 NSF Summit presentation

Trusted CI TTP Playbook

A resource for self-guided Transition to Practice (TTP) planning

A. TTP Technical Readiness Level (TRL) Assessment
B. TTP Canvas - Business model / sustainability model development

TTP Technical Readiness Level (TRL) Assessment Tool

- Based on the NASA Technology Readiness Level model
- A tool to assess the maturity of a given technology
- Intended to aid in planning future development efforts
- Used iteratively as development continues

TRL Explained

1. Research: Idea > Formalization > Proof of Concept
2. Development: Validation > Testing > Demonstration
3. Deployment: Pre-production > Production > Operations

TTP adaptations from the source material: definitions

1	Basic principles observed and reported
2	Technology concept or application formulated
3	Analytical and/or experimental critical function or characteristic proof-of-concept
4	Research validation in laboratory environment
5	Model or prototype demonstration in a relevant environment
6	Actual system completed and qualified through test and demonstration
7	Actual system proven through successful operations

TRL Worksheet: Subsystems and Components

- Subsystems = distinct categories of functionality needed
- Components = Functional pieces which deliver needed functionality
- Different components can have different TRL levels
- For example… a web application!
  a. Web interface frontend: subsystem made of javascript, an API, and web server components
  b. Data management: subsystem made up of database software, schema, and query components
  c. Core software: subsystem made up of Java software and a software interface layer

TTP TRL Worksheet Example: Web Interface Subsystem

Subsystem	Component	TRL	Justification	Implementation
Web Interface	Apache httpd	7+	This is widely used open source web server software. The installation is managed and supported by the hosting provider for the web server.	Provided by service provider
	API endpoint	4	Basic API calls have been tested successfully. Additional functionality is being developed and further testing is planned.	Custom httpd module written to provide REST API
	Web GUI	5	Web UI prototype is functionally complete and has been fully tested across two out of three target browsers. Ready to begin usability and accessibility testing.	Custom javascript UI built using open source library XYZ.

TTP Canvas - Template

1 Research problem

2 Technology innovations

3 Target users / customers

4 User operational challenges

5 Value delivered

6 Activities to deliver value

7 Resources required

8 Funding Model

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

TTP Canvas - Filled in for ASSERT

1 Research problem

- Generate and update cyber attack models in near-real-time without prior expert knowledge.
- Each attack model is a set of statistical summaries of intrusion alerts that are relevant in What, Where, When, and How the attack(s) transpired over time on a targeted network.

2 Technology innovations

- Unsupervised machine learning with non-parametric feature distributions from streaming data.
- Engineered features that are agnostic to specific networks and adversary behaviors.
- Entropy-based algorithms to account for rare yet critical features and model update in near-real-time.

3 Target users / customers

- SOC Analysts
- SOC Operation Management

4 User operational challenges

- Too many alerts, too little time.
- Common malicious activities vs. new or critical ones.
- Which alerts are related?

5 Value delivered

- Save time by enabling analysis of a small set of attack models instead of a large number of alerts.
- Valuable insights through distinctive (critical) attack models and sudden changes.
- Reference to alerts that are related to the same attack behavior.

6 Activities to deliver value

- Discover potential users and partners
- Extract user operational challenges.
- Identify and secure resources for software development and deployment.
- Develop partnership, relationship and some form of a contract.
- Deploy pilot with early partners / adopters and obtain feedback and evidences to demonstrate value added..
- Develop a strategy for agile realignment and development of prototype values for early partners / adopters.
- Cultivate channels for continuous and broader user engagement.
- Identify and develop additional value-added features for the users.

7 Resources required

- Client / partner outreach skills
- Client / partner assessment skills
- Client / partner engagement skills
- Researcher(s) and student(s)
- Developer(s)
- Operations/project management
- Systems integration and deployment skills
- Agile research and development pivoting skills
- Channel and funding venue development skills

8 Funding Model

- Grants
- Research partners
- Development partners
- Customers and sponsors

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

PI: S. Jay Yang, RIT

NSF TTP Programs

- Secure and Trustworthy Cyberspace (SaTC)
- Cybersecurity Innovation for Cyberinfrastructure (CICI)
- Small Business Innovation Research (SBIR)
- Small Business Technology Transfer (STTR)
- Innovation Corps (I-Corps)
- Convergence Accelerator
- Pathways to Enable Open-Source Ecosystems (POSE)
- Partnerships for Innovation (PFI)
- … and more from NSF's new Directorate for Technology, Innovation and Partnerships (TIP)

NSF Cybersecurity Summit

Hybrid meeting
Registration now open

October 23-26, 2023 at
Lawrence Berkeley National
Laboratory in Berkeley, CA

https://trustedci.org/summit/

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

DAY 1 Monday October 23, 2023 | Workshops/Trainings

	Track 1	Track 2	Track 3	Track 4
8:00AM	*Sign-In and Continental Breakfast*			
9:00AM–1:00PM (Refreshment break at 10:30)	Zeek Training: Hands-on Zeek Scripting	Zeek Training: Intermediate to Zeek	Jupyter Security Workshop	
1:00–2:00PM	*Lunch*			
2:00 PM–5:00 PM (Refreshment break at 3:30)	Zeek Training: Hands-on Zeek Scripting	Zeek Training: Intermediate to Zeek	Jupyter Security Workshop	WISE Community Workshop

DAY 2 Tuesday October 24, 2023 | Plenary and Workshops/Trainings

7:00 AM	*Sign-In and Continental Breakfast*		
8:00 AM	*Welcome & NSF Address*		
8:30 AM	*Berkeley Welcome & ESNet Welcome*		
9:00 AM	*Trusted CI Update*		
9:30 AM	*Keynote #1 (TBA)*		
10:00 AM	*Keynote #2 (TBA)*		
10:30 AM	*Refreshment Break*		
11:00 AM	*Plenary Session	Implementing NIST 800-171 in a both distributed and centralized environment*		
11:30 AM	*Plenary Session	Unmasking Shadows: Investigating MICI-BICA, an Incident Involving IRC-Based Malware Deployment, Rootkit Stealth, and Self-Hiding Cryptominers*		
12:00 PM	*Plenary Session	Black Hole Locker Ransomware : Affiliate program*		
12:30–2:00 PM	*Lunch*			
	Track 1	Track 2	Track 3
2:00–5:00 PM (coffee break at 3:30)	*Securing your Code with Better Coding Practices and Tools*	*Jupyter Network Monitoring with Zeek Workshop*	*Security intrusion at the Zebra Scientific Alliance*
5:30-7:30 PM	**Social night -Residence Inn Study hall rooftop**-2121 Center St, Berkeley,		

DAY 3 | Wednesday October 25, 2023 | Plenary and Workshops/Trainings /BoFs/Project Mtgs

7:00 AM	*Sign-In and Continental Breakfast*			
8:00 AM	*Plenary Session	Principles of Decentralized Cyberinfrastructure*			
8:30 AM	*Plenary Session 5	(TBA)*			
9:00 AM	*Plenary Session 6	(TBA)*			
	Track 1	Track 2	Track 3	Track 4/Project Meetings
9:30 am–12:30 PM (coffee break at 10:30)	Deep Machine Learning for Intrusion Detection in Cyber-Physical Critical Infrastructures	Physical Security is important Um'k	Regulatory Compliance for Research: DFARS/CMMC, HIPAA, GDPR, NSPM-33	SAFER Member Meeting (Members Only)
12:30–2:00 PM	*Lunch*			
2:00 PM	Catch Me If You GPT: Tutorial on Deepfake Texts	BOF: Research Security Compliance collaborations to support PI research	The Trusted CI Framework: Strategies for Getting Started	ACCESS CONECT Cybersecurity Group and invited guests. 20 people (2:00-4:00 PM)
3:30 PM	*Refreshment Break*			
4:00 PM	Catch Me If You GPT: Tutorial on Deepfake Texts	BoF: NICE Workforce Framework Adoption: Cybersecurity Teaching Innovations	The Trusted CI Framework: Strategies for Getting Started	SAFER Member Meeting CONTINUED (Members Only)
5:00 PM	*Conclude*			

DAY 4 | Thursday October 26 - Plenary and Workshops/Trainings/BoFs

7:00 AM	*Sign-In and Continental Breakfast*		
	Track 1	Track 2	Track 3
8:00 AM	[TLP:RED] How we failed to handle a triple-combo attack against the R&E HPC community worldwide...in the middle of a pandemic	Trusted CI Framework Community of Practice (CoP) Quarterly Meeting (8:00 – 11:00 AM)	Security Log Analysis (8:00 – 11:00 AM)
8:30 AM	[TLP:RED] Monero mining, with love, from space		
9:00 AM	[TLP:RED] Reserved		
9:30 AM	[TLP:RED] Reserved		
10:00 AM	[TLP:RED] Reserved		
10:30 AM	pDNSSOC: Correlating DNS logs with threat intel from MISP as a poor man's SOC. (10:30-12:00 PM)		
11:00 AM	Experiences from SIO (CCRV) and OSU (RCRVs) in Cybersecure-by-Design Ship Design and Construction (11:00 AM-12:00 PM)		
12:00–1:30 PM	*Lunch*		
1:30 PM	**Plenary Session	US Academic Research Fleet (ARF) Cyber Risk Management Program (CRMP)**		
2:00 PM	**Plenary Session	Cyber Forensics In Everyday Business**		
2:30 PM	***Poster Session / Ice Cream Break /Refreshment***		
3:30 PM	***Plenary Session	Trusted CI Fellows Panel***		
4:00 PM	***Plenary Session	(TBA)***		
4:30 PM	***Summit Observations and feedback***		
5:00 PM	***Adjourn***		

Trusted CI Partners

https://trustedci.org/partners

Monthly Webinars

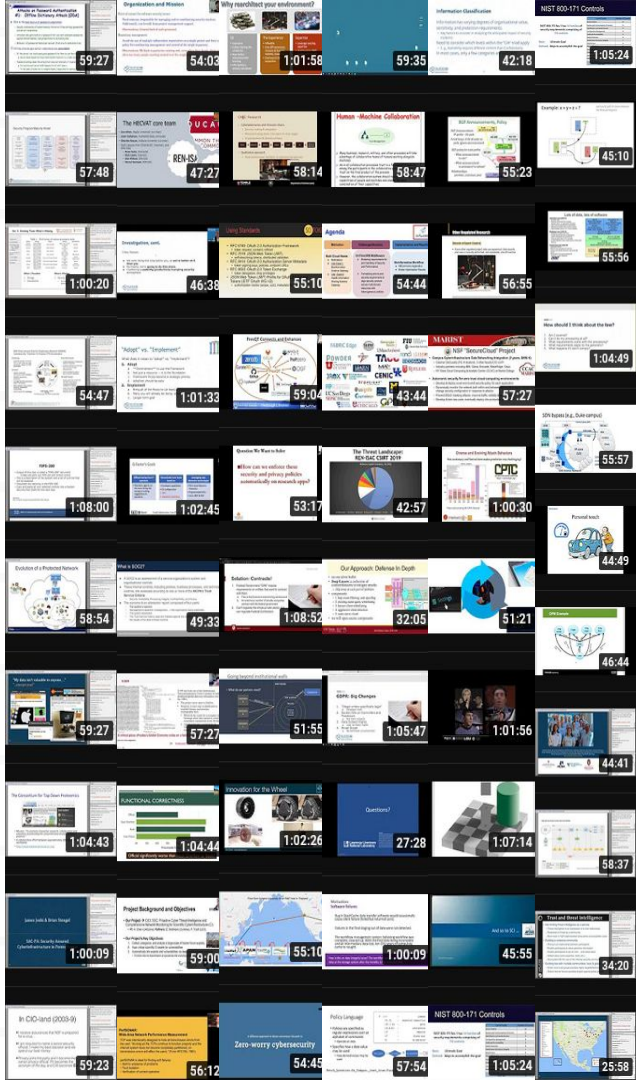
Cybersecurity for Cyberinfrastructure

Community presentations about cybersecurity research results, operational practices, lessons learned, etc.

4th Monday of the month at 11am Eastern

https://www.trustedci.org/webinars

https://www.trustedci.org/trustedci-email-lists



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Staying Connected with Trusted CI

Trusted CI Webinars

4th Monday of month at 11am ET.

https://trustedci.org/webinars

Email Lists

Announce and Discuss

https://trustedci.org/trustedci-email-lists

Follow Us

https://trustedci.org

https://blog.trustedci.org

Ask Us Anything

No question too big or too small.

info@trustedci.org

Slack

Email ask@trustedci.org for an invitation.

Cyberinfrastructure Vulnerabilities

Latest news on security vulnerabilities tailored for cyberinfrastructure community.

https://trustedci.org/vulnerabilities/

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Acknowledgments

Trusted CI is supported by the National Science Foundation under Grants 1234408, 1547272, 1920430, & 2241313. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.

Trusted CI activities are made possible thanks to the contributions of a multi-institutional team:

https://trustedci.org/who-we-are/

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Q & A

https://trustedci.org/ttp

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE