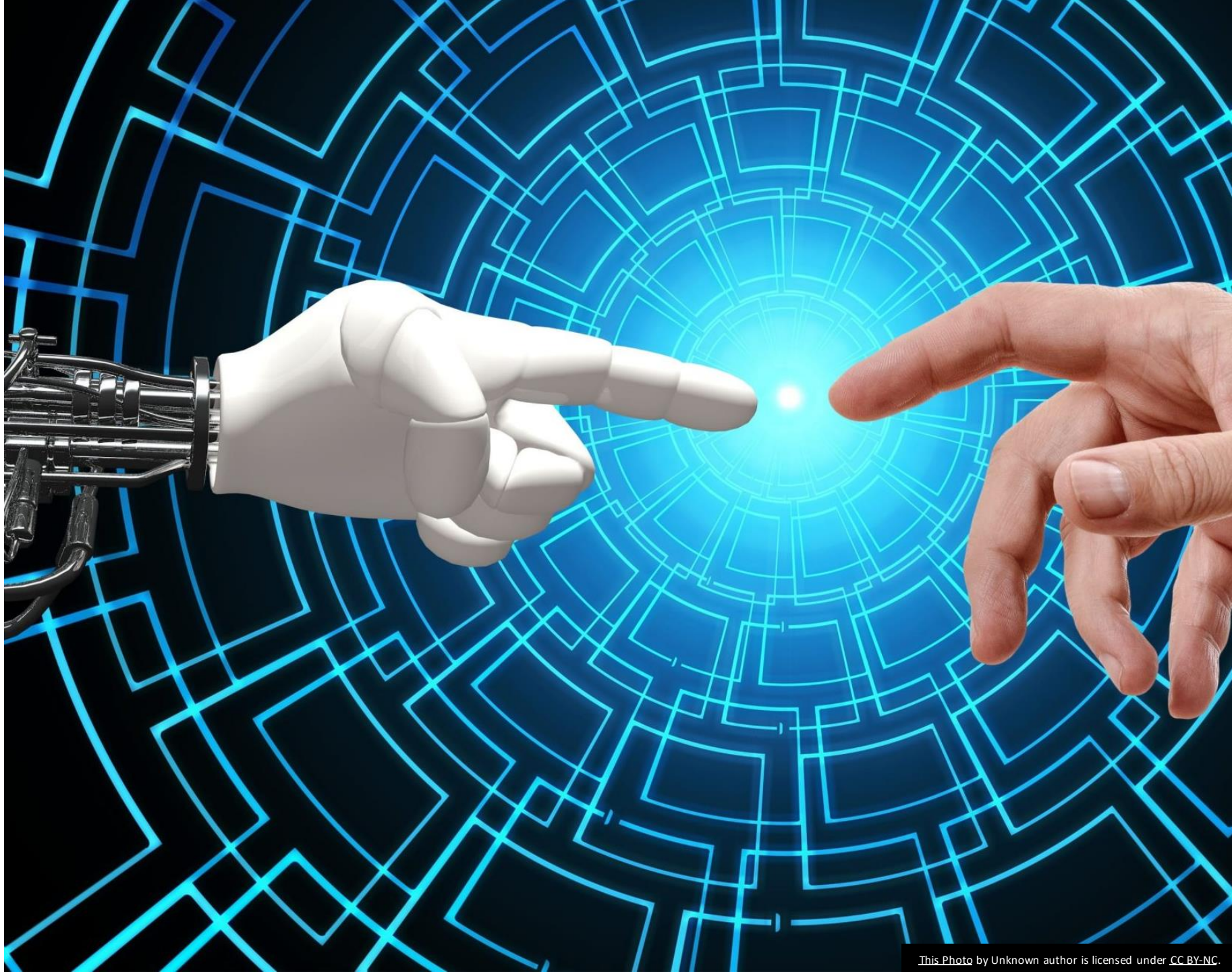
# Recommendations for improving Science Gateway Security

By Mark Krenz, Trusted CI

SGCI Webinar
Sept 29, 2021




https://trustedci.org/

Trusted CI's mission is to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

PITTSBURGH SUPERCOMPUTING CENTER

THE UNIVERSITY of WISCONSIN MADISON

NSF

NCSA

BERKELEY LAB

UNIVERSITY OF SOUTH ALABAMA

# Who am I?

# Mark Krenz

- Chief Security Analyst at the Center for Applied Cybersecurity Research, Indiana University
- Deputy CISO for Trusted CI
- CISO for ResearchSOC
- 20+ years in system adminsitration
- 9+ years in Cybersecurity
- Programmer 0 and 1 over the years
- Creator of https://twitter.com/climagic

# Overview

- Goals
- Challenges
- Security requirements
- Recommendations
- Conclusion
- Questions

# Goals of most science gateways

- Create new interface to scientific resource
- Utilize latest technologies
- Work within limited budget
- Be very useful

# Challenges

- Limited funding
- Limited time
- Distributed team
- Limited security training

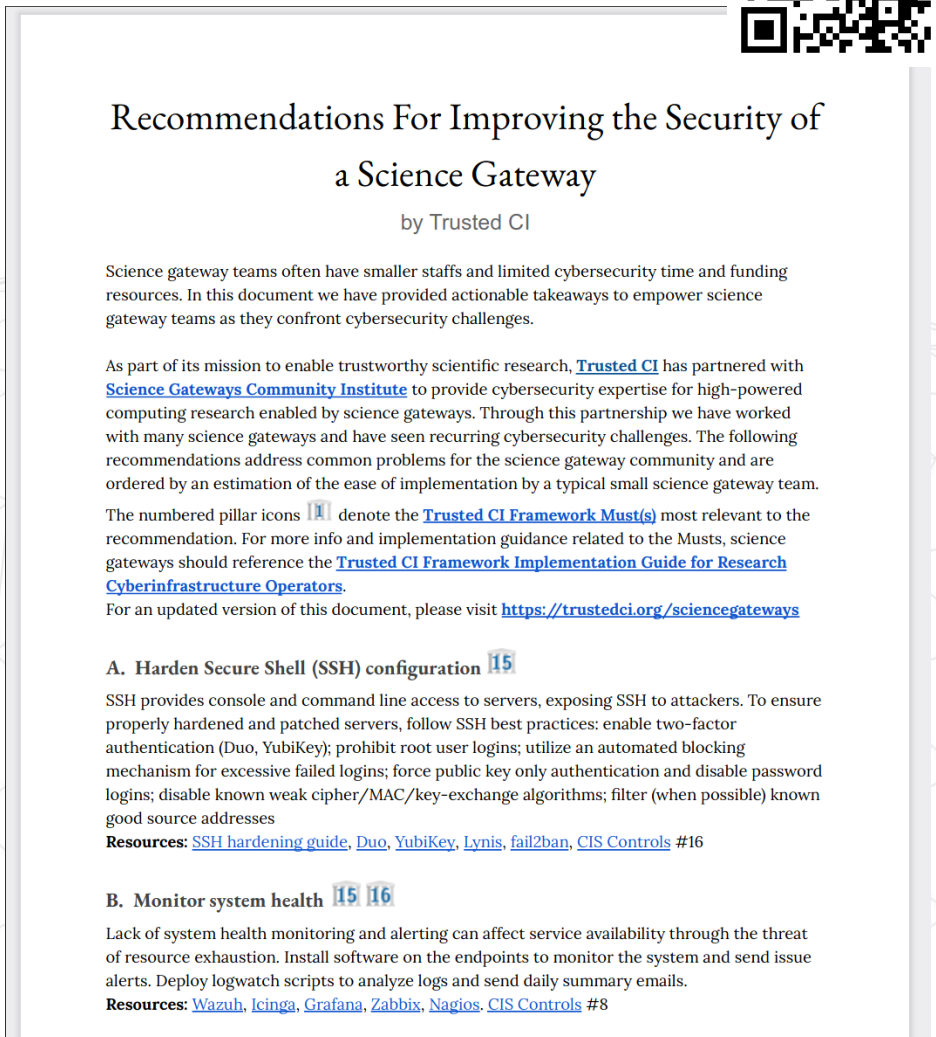
# Security requirements

- Where to start?
- What to do?
- What to prioritize?
- Start with low hanging fruit

# Security help

https://trustedci.org/science-gateways

- Developed for Science Gateways
- Prioritized recommendations
- References to Trusted CI Framework
- Curated list of resources



Recommendations For Improving the Security of a Science Gateway

by Trusted CI

Science gateway teams often have smaller staffs and limited cybersecurity time and funding resources. In this document we have provided actionable takeaways to empower science gateway teams as they confront cybersecurity challenges.

As part of its mission to enable trustworthy scientific research, **Trusted CI** has partnered with **Science Gateways Community Institute** to provide cybersecurity expertise for high-powered computing research enabled by science gateways. Through this partnership we have worked with many science gateways and have seen recurring cybersecurity challenges. The following recommendations address common problems for the science gateway community and are ordered by an estimation of the ease of implementation by a typical small science gateway team.

The numbered pillar icons [1] denote the **Trusted CI Framework Must(s)** most relevant to the recommendation. For more info and implementation guidance related to the Musts, science gateways should reference the **Trusted CI Framework Implementation Guide for Research Cyberinfrastructure Operators**.
For an updated version of this document, please visit **https://trustedci.org/sciencegateways**

**A. Harden Secure Shell (SSH) configuration** [15]

SSH provides console and command line access to servers, exposing SSH to attackers. To ensure properly hardened and patched servers, follow SSH best practices: enable two-factor authentication (Duo, YubiKey); prohibit root user logins; utilize an automated blocking mechanism for excessive failed logins; force public key only authentication and disable password logins; disable known weak cipher/MAC/key-exchange algorithms; filter (when possible) known good source addresses
**Resources:** SSH hardening guide, Duo, YubiKey, Lynis, fail2ban, CIS Controls #16

**B. Monitor system health** [15] [16]

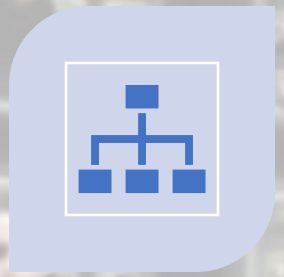
Lack of system health monitoring and alerting can affect service availability through the threat of resource exhaustion. Install software on the endpoints to monitor the system and send issue alerts. Deploy logwatch scripts to analyze logs and send daily summary emails.
**Resources:** Wazuh, Icinga, Grafana, Zabbix, Nagios. CIS Controls #8

# Know your limits

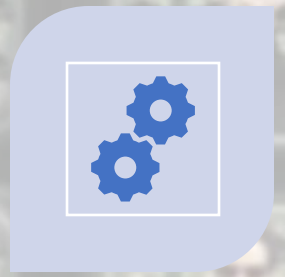
**[C]** Implement a maintainable system architecture

**[D]** Determine acceptable cybersecurity risks

# Know thyself



**[E]** CREATE AND MAINTAIN ARCHITECTURE DIAGRAMS



**[F]** CREATE AND MAINTAIN A DATA FLOW DIAGRAM

**[M]** USE A SECURITY ASSESSMENT TOOL

**[N]** PREPARE AN ASSET INVENTORY

# Keep watch

**[B]** Monitor System health

# Be ready for action

[G] Adopt an Incident Response Plan

# Use best practices

[A] Harden Secure Shell (SSH) configuration

[I] Harden docker/container configurations

[J] Train staff in secure coding

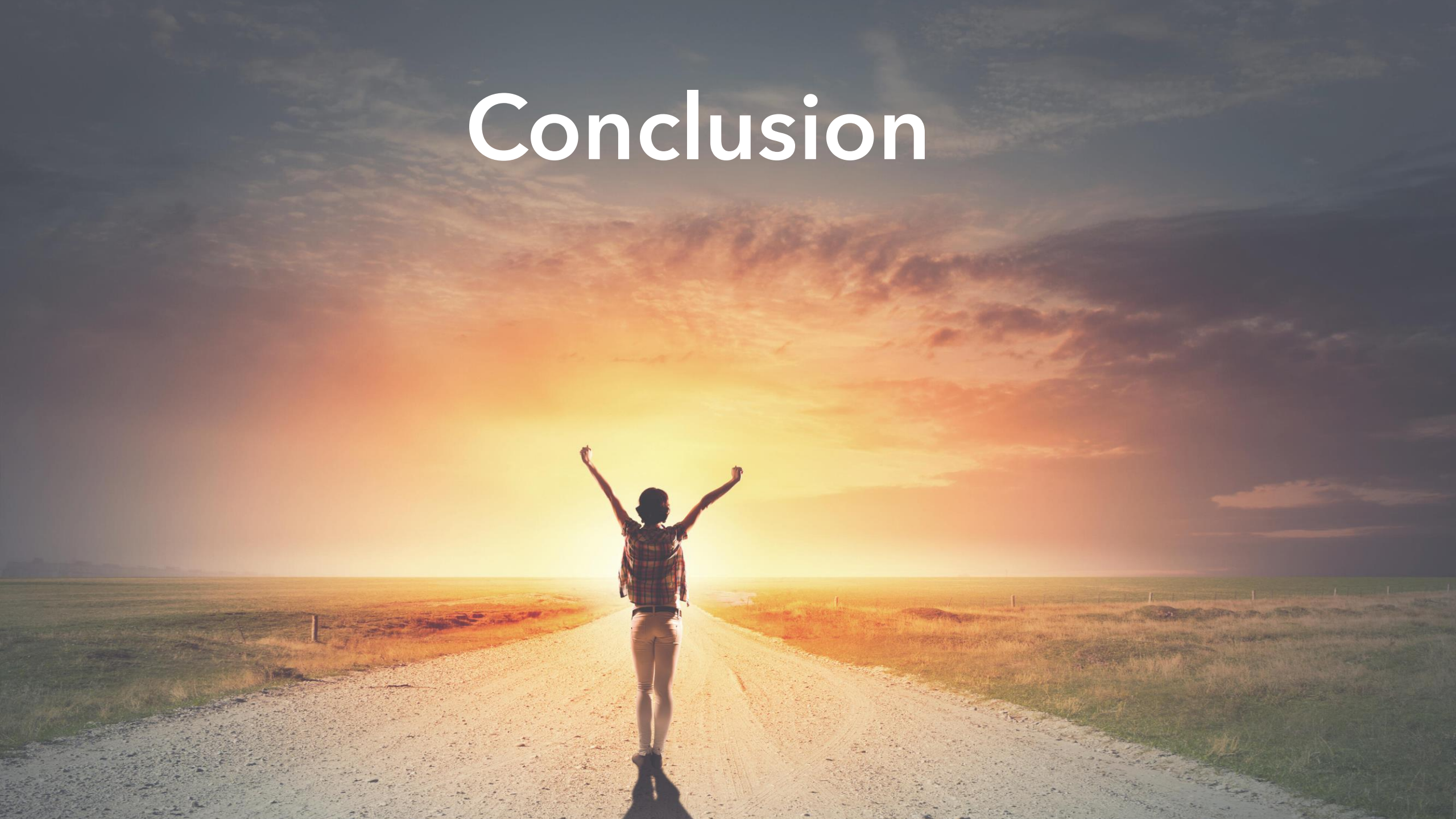
[L] Perform cloud security best practices

# Know your friends

**[O]** Use institutional resources

**[K]** Use HPC and Science Gateway resources

# Conclusion



# Upcoming Event:
# NSF Cybersecurity Summit

- Plenary: October 12–13
- Trainings: October 15
- Workshops: October 18–19

- REGISTRATION CLOSES October 4th
- Register at: https://www.trustedci.org/

We thank the National Science Foundation (grant 1920430) for supporting our work.

# Questions