CTSC

CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Cybersecurity for Gateways

Von Welch

Workshop on Trustworthy Scientific Cyberinfrastructure

PEARC 17

July 13, 2017

Science Gateways Cybersecurity
Three Key Aspects

1. Secure Software Development and Engineering
2. Identity and Access Control Management
3. Operational Cybersecurity

Science Gateways Cybersecurity
Three Key Goals

1. Maintain the trust of your resource providers
2. Maintain the trust of your community
3. Protect, as appropriate, the confidentiality, integrity, and availability of your key assets.

A Quick Overview of Resources…

Secure Software Development and Engineering

NSF “CI Framework for 21st century” (CIF21)

Software must be reliable, robust, and secure; able to produce trustable and reproducible scientific results;

…

https://www.nsf.gov/pubs/2012/nsf12113/nsf12113.pdf

Software Engineering
A Required Foundation

- Repositories/Hosting
- Testing
- Static Analysis
- Vulnerability Management
- Release & Delivery
- Coding/Project Tools
- Documentation

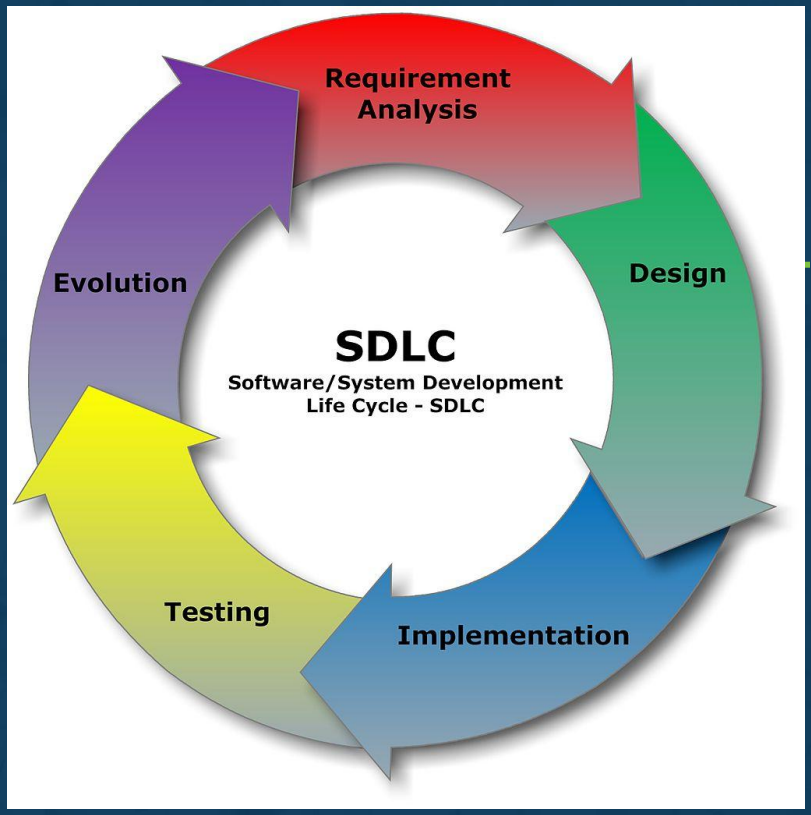
"Secure Software Engineering Best Practices"

Randy Heiland and Susan Sons

http://hdl.handle.net/2022/21322

Secure Coding

- Requirements
- Design
- Implementation
- Testing



Secure Coding Practices and Automated Assessment Tools
Prof. Barton P. Miller & Prof. Elisa Heymann

http://hdl.handle.net/2022/21325

CTSC

Identity and Access Control Management
Who can do what?

- Managing your community
- Different levels of access
- Who manages Groups/Communities/VOs?
- Local password or federated identity?
- User lifecycle

Federated Identity Management for Research Organizations
Jim Basney, Scott Koranda
http://hdl.handle.net/2022/21329

Facilitating Scientific Collaborations by Delegating Identity Management: Reducing Barriers & Roadmap for Incremental Implementation. Robert Cowles, Craig Jackson and Von Welch.
http://hdl.handle.net/2022/20357

Cybersecurity Operations
Keeping Everything Going

- Ongoing program to manage risks
- Patching, incident detection, incident response
- Knowing your upstream software providers?
- Communications with your community and resource providers.

"Developing Cybersecurity Programs for NSF Projects"
BoB Cowles, Craig Jackson, Jim Marsteller, Susan Sons
http://hdl.handle.net/2022/21327

Other Resources

"Science Gateway Security Recommendations"
J. Basney, V. Welch
http://www.ncsa.illinois.edu/People/jbasney/201309-gwsec.pdf

"SciGaP-CTSC Engagement Summary"
Randy Heiland, Scott Koranda, Von Welch
http://hdl.handle.net/2022/20926

"CyberGIS-CTSC Engagement Final Report"
Randy Butler, Terry Fleury, Jim Marsteller, Von Welch
http://hdl.handle.net/2022/16816

"The Open Science Cyber Risk Profile (OSCRP)."
Rich LeDuc, Sean Peisert, Karen Stocks and Von Welch.
https://dx.doi.org/10.6084/m9.figshare.4584256

SGCI and CTSC are here to Help!

Email lists, webinars, training, engagements.

sciencegateways.org / trustedci.org