An NSF Cybersecurity Center of Excellence to Support Research

Jim Basney, Tom Barton, and Kim Milford

Internet2 Global Summit
May 18 2016

trustedci.org
Agenda

Overview of CTSC (Jim)
Cybersecurity for Science: Challenges & Opportunities
  CTSC perspective (Jim)
  REN-ISAC perspective (Kim)
  University of Chicago perspective (Tom)
Discussion and Q&A
Overview of CTSC
Center for Trustworthy Cyberinfrastructure
The NSF Cybersecurity Center of Excellence

CTSC’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.
CTSC began with a 3-year NSF grant in 2013.

NSF 2015 Cybersecurity Innovation for Cyberinfrastructure (CICI) solicitation called for an NSF CCoE.

CTSC submitted a proposal and was awarded this honor.
NSF Cybersecurity Innovation for Cyberinfrastructure (CICI) Program

Also funds projects in the areas of Regional Cybersecurity Collaboration, Secure and Resilient Architecture, Secure Architecture Design, and Data Provenance for Cybersecurity.

https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505159
Vision for the NSF Science Community

1. For the NSF science community to understand fully the role of cybersecurity in producing trustworthy science.

2. For all NSF projects and facilities to have the information and resources they need to build and maintain effective cybersecurity programs appropriate for their science missions, and responsive to evolving risks and requirements.

3. For all Large Facilities to have highly effective cybersecurity programs.
## CTSC Activities

More information at trustedci.org

### Tailored Public Resources
- Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects;
- Identity Management Best Practices;
- Email Lists, Vulnerability Announcements

### Outreach
- Blog;
- Participation in LF Workshop;
- Int’l relationships

### Community Events
- Annual NSF Cybersecurity Summit,
- Monthly Webinars

### Training
- Developing Programs,
- Secure Coding,
- Incident Response

### Engagements
- LIGO, SciGaP, IceCube, Pegasus, CC-NIE peer review,
- DKIST, LTERNO, DataONE, SEAD, CyberGIS, HUBzero, Globus, LSST, NEON,
- U. Utah, PSU, OOI, U. Oklahoma, Gemini...
### New CTSC Activities as CCoE

<table>
<thead>
<tr>
<th>Activity</th>
<th>Web Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expanded situational awareness service</td>
<td><a href="http://trustedci.org/situational-awareness/">http://trustedci.org/situational-awareness/</a></td>
</tr>
<tr>
<td>Threat model for open science</td>
<td><a href="http://trustedci.github.io/OSCTP/">http://trustedci.github.io/OSCTP/</a></td>
</tr>
<tr>
<td>Annual community benchmarking survey</td>
<td></td>
</tr>
<tr>
<td>Tailoring resources for smaller / newer projects</td>
<td></td>
</tr>
<tr>
<td>Software assurance</td>
<td><a href="http://trustedci.org/software-assurance/">http://trustedci.org/software-assurance/</a></td>
</tr>
<tr>
<td>Identity and access management (IAM)</td>
<td><a href="http://trustedci.org/iam/">http://trustedci.org/iam/</a></td>
</tr>
</tbody>
</table>
CTSC Webinar Series

4th Monday of the month at 11am Eastern
Covering cybersecurity topics tailored to the NSF CI community

To view presentations, join the discuss mailing list, or submit presentation topics, visit:

http://trustedci.org/webinars
2016 NSF Cybersecurity Summit:

*August 16-18, 2016 - Arlington, Virginia*

http://trustedci.org/summit
Cybersecurity for Science:
Challenges and Opportunities
Challenges/Opportunities (Jim’s Perspective)

Understanding the cybersecurity needs/risks of CI across campus (including “Shadow CI”)
Enabling effective cooperation between science projects and IT security
Assessing CI security needs/risks beyond compliance
Leveraging community resources
    ACI-REF, Campus Champions, CTSC, Regional Cybersecurity Collaboration Centers
Community of trusted cybersecurity staff at R&E institutions

Sharing actionable information for operational protection and response

Confidentiality
## REN-ISAC

<table>
<thead>
<tr>
<th>Type</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>US College, Private for-profit</td>
<td>1</td>
</tr>
<tr>
<td>US College, Private not-for-profit</td>
<td>150</td>
</tr>
<tr>
<td>US College, Public</td>
<td>225</td>
</tr>
<tr>
<td>Medical Science/Medical Center</td>
<td>12</td>
</tr>
<tr>
<td>University Department</td>
<td>2</td>
</tr>
<tr>
<td>International College</td>
<td>29</td>
</tr>
<tr>
<td>Research Center</td>
<td>19</td>
</tr>
<tr>
<td>Network</td>
<td>8</td>
</tr>
<tr>
<td>Consortium</td>
<td>11</td>
</tr>
</tbody>
</table>
REN-ISAC

- CSIRT for .edu
  - 24x7 support
- Sector ISAC
- Cybersecurity research and development
- Education and training
- Automated threat intelligence sharing
Challenges/Opportunities (Kim’s Perspective)

- Understanding comprehensive risk management across campus
- Enabling effective cooperation between science projects and IT security
- Assessing CI security needs/risks beyond compliance
- Building a cohesive security program
- Confidentiality and privacy
- Leveraging community resources
  - REN-ISAC
Three Security Challenges for Campus Research CyberInfrastructure

Tom Barton
CISO
UChicago
1. Fragmentation of Traditional Discipline-Focused Research Support

- Dilutes ability to invest & improve
- Mainly outside of Physical and Biological Sciences
  - Social Sciences, Social Policy, Law, Business, Economics
- Institutional Review Boards need help too
  - UMich-style Data Usage Guide
  - Protocol-specific consultation
- Data Usage Agreements & potential liability
- NIST 800-171 as benchmark for UChicago approach
- Partnership of Offices of Legal Counsel, Medical Center Legal Affairs, University Research Administration, and IT Security
2. High Bandwidth Restricts Options

- Science DMZ and high end computing
  - 2x100G, multi-PB, O(10^5) cores
  - Large and international user community
- Concerns
  - Integrity of research data
  - DDoS potential
- Approach
  - Bro cluster & Bro community
  - Vulnerability management
  - Stakeholder agreement to limit reachable endpoints only to those necessary for the science
  - Interfederation, OSG, local access management
  - Seek help! Got any?
3. Maturing IT Security Operations

• Campus IT Security stresses importance of being notified when a compromise happens, so that they can determine complete footprint of attack and manage accordingly
• Slow recognition that we are embedded in an international federation which has analogous need
• Campus CI is a microcosm of that already
• Sirtfi: federated security incident response
  – Notification of recent access by compromised accounts
• REN-ISAC also must continue maturing support for research CI activities
Discussion
We thank the National Science Foundation (grant 1547272) for supporting our work.

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.