All for One and One for All: EDUCAUSE, Internet2, and REN-ISAC's Collaborations in Cybersecurity
Presenters

- Brian Kelly, EDUCAUSE
- Nick Lewis, Internet2
- Todd Herring, REN-ISAC
Agenda

- Who are we and why are we here?
- Collaborative successes
- What’s going on?
- Who is steering the ship?
- Your feedback!
EDUCAUSE Cybersecurity Program

• Higher Education Information Security Council (HEISC)
• Annual Security Professionals Conference
• Information Security Guide
• Working Groups & Community Groups
• Security Matters blog column in EDUCAUSE Review
• Partnerships

https://www.educause.edu/security
EDUCAUSE Cybersecurity Program Staff

- Valerie Vogel is Senior Manager of the EDUCAUSE Cybersecurity Program.
- Brian Kelly is the Cybersecurity Program Director. He previously served as the CISO at Quinnipiac University before joining EDUCAUSE in March.
New/Updated HEISC Resources in 2019

- **7 Things You Should Know About Federated Identity**
- **Two-Factor Authentication (2FA) Lessons Learned**
- **2019 Information Security Almanac** with 2018 CDS data
- Revisions to the **Risk Management** and **Incident Management** chapters
- SOC Case Study (**Spring 2019**)
- Updates to **Phishing Simulation Programs** and **Password Managers** (**Spring/Summer 2019**)
- Security Professionals Conference 2020 CFP (**Fall 2019**)
- Security and Privacy Awareness Resources (**Fall/Winter 2019**)

#Security19
Internet2 Network Services

- Network security working group
- DDoS mitigation techniques
- Inter-domain routing security
- Investigate “Clean Pipe” services for NGI
- Leverage cyber threat intelligence feeds
- Improved attack detection
- Coordination with Global NREN security teams
- REN-ISAC and HEISC member
Guard Against Hijacks of Cloud Connections
Protect the R&E Ecosystem

Take MANRS Actions
Mutually Agreed Norms for Routing Security

Filtering
Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing
Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination
Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in common routing databases

Global Validation
Facilitate validation of routing information on a global scale

Publish your data, so others can validate
Internet2 Cloud Services Updates

• Duo, Splunk, GCP, others
• NET+ Duo MFA work with EDUCAUSE and NCSA
• Incorporating HECVAT into the program
• Cloud security working group
Internet2 Trust & Identity and InCommon

- Baseline Expectations and SIRTFI
- Getting infosec and IAM working together
- IoT SIG and engagement
REN-ISAC: What do we do?

Two primary roles:

**CSIRT** supporting the R&E community at-large, we serve the entire EDU space in the United States, including non-members. In this role, we work with trusted third parties to notify higher education institutions of infected hosts and suspicious network traffic.

REN-ISAC also serves over 620 member institutions in Australia, New Zealand, Canada, the UK, and the United States. For a modest annual fee, member institutions gain access to additional services and benefits.
REN-ISAC MEMBERSHIP: FROM THE BEGINNING

Count of Member Institutions: 2004 to Present

#Security19
## REN-ISAC Membership: 2018 to 2019

<table>
<thead>
<tr>
<th>Size (Active, colleges/universities only)</th>
<th>January 2018</th>
<th>January 2019</th>
<th>Difference</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Institutions</td>
<td>588</td>
<td>623</td>
<td>35</td>
<td>5.95%</td>
</tr>
<tr>
<td>Size</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>58</td>
<td>66</td>
<td>8</td>
<td>13.79%</td>
</tr>
<tr>
<td>Medium</td>
<td>173</td>
<td>185</td>
<td>12</td>
<td>6.94%</td>
</tr>
<tr>
<td>High</td>
<td>167</td>
<td>173</td>
<td>6</td>
<td>3.59%</td>
</tr>
<tr>
<td>Very High</td>
<td>115</td>
<td>119</td>
<td>4</td>
<td>3.48%</td>
</tr>
</tbody>
</table>

Size defined by total enrollment, as follows:
- **Small**: Up to 2,500
- **Medium**: 2,501 to 10,000
- **High**: 10,001 to 25,000
- **Very High**: 25,001 or more
Membership: Enterprise Participation

Changes to REN-ISAC guidelines allow new member representatives to join:

- Executives with a stake in InfoSec
- Security practitioners in roles such as IAM, risk management, ERP systems
New Services

• AuthFail, Passive DNS, SES v4
  • ren-isac.net/member-resources
• Blended Threat Workshops
  • ren-isac.net/workshops
• Peer Assessments
  • ren-isac.net/pas
## CSIRT Statistics, 2018

<table>
<thead>
<tr>
<th></th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th>Grand Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromised machines</td>
<td>16,083</td>
<td>14,228</td>
<td>16,615</td>
<td>16,448</td>
<td>63,374</td>
</tr>
<tr>
<td>Compromised credentials</td>
<td>5,008</td>
<td>2,613</td>
<td>5,098</td>
<td>2,796</td>
<td>15,515</td>
</tr>
<tr>
<td>Spam or phish</td>
<td>78</td>
<td>78</td>
<td>51</td>
<td>62</td>
<td>269</td>
</tr>
<tr>
<td>Vulnerable machines</td>
<td>-</td>
<td>12</td>
<td>1</td>
<td>2</td>
<td>15</td>
</tr>
<tr>
<td>Open recursive DNS resolvers</td>
<td>612</td>
<td>564</td>
<td>543</td>
<td>504</td>
<td>2,223</td>
</tr>
<tr>
<td>Open mail relays</td>
<td>14</td>
<td>15</td>
<td>11</td>
<td>8</td>
<td>48</td>
</tr>
<tr>
<td>SSH scanning</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Other</td>
<td>22</td>
<td>11</td>
<td>11</td>
<td>4</td>
<td>48</td>
</tr>
<tr>
<td><strong>Total Notifications:</strong></td>
<td><strong>21,817</strong></td>
<td><strong>17,521</strong></td>
<td><strong>22,330</strong></td>
<td><strong>19,824</strong></td>
<td><strong>81,492</strong></td>
</tr>
</tbody>
</table>
## CSIRT Statistics, 2018 Compared to 2016

<table>
<thead>
<tr>
<th>REN-ISAC CSIRT Activity</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th>Grand Total</th>
<th>2016!</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromised machines</td>
<td>16,083</td>
<td>14,228</td>
<td>16,615</td>
<td>16,448</td>
<td>63,374</td>
<td>67,104</td>
</tr>
<tr>
<td>Compromised credentials</td>
<td>5,008</td>
<td>2,613</td>
<td>5,098</td>
<td>2,796</td>
<td>15,515</td>
<td>2,197,745</td>
</tr>
<tr>
<td>Spam or phish</td>
<td>78</td>
<td>78</td>
<td>51</td>
<td>62</td>
<td>269</td>
<td>2,309</td>
</tr>
<tr>
<td>Vulnerable machines</td>
<td>-</td>
<td>12</td>
<td>1</td>
<td>2</td>
<td>15</td>
<td>53</td>
</tr>
<tr>
<td>Open recursive DNS resolvers</td>
<td>612</td>
<td>564</td>
<td>543</td>
<td>504</td>
<td>2,223</td>
<td>2,768</td>
</tr>
<tr>
<td>Open mail relays</td>
<td>14</td>
<td>15</td>
<td>11</td>
<td>8</td>
<td>48</td>
<td>148</td>
</tr>
<tr>
<td>SSH scanning</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Other</td>
<td>22</td>
<td>11</td>
<td>11</td>
<td>4</td>
<td>48</td>
<td>10</td>
</tr>
<tr>
<td><strong>Total Notifications:</strong></td>
<td><strong>21,817</strong></td>
<td><strong>17,521</strong></td>
<td><strong>22,330</strong></td>
<td><strong>19,824</strong></td>
<td><strong>81,492</strong></td>
<td><strong>2,270,137</strong></td>
</tr>
</tbody>
</table>
SANS / REN-ISAC Partnership

- Special discounts are available from **June 1, 2019 – July 31, 2019**.
- Save more than 50% on SANS online technical courses
- Save up to 70% on SANS Security Awareness training
- Visit [www.sans.org/partnership/education](http://www.sans.org/partnership/education) for more information, to generate quotes and place an order
COLLABORATION
AREAS OF COLLABORATION

- EDUCAUSE Security Professionals Conference
- Working Group
- HECVAT & CBI
- NCSAM
- Program Committees
- Feedback on each others’ projects
Tell Us About It!

• What do you need?
• What is not getting done?
• Where do you see our coordination opportunities?
THANKS!

QUESTIONS AND FEEDBACK?
Session Evaluations

There are two ways to access the session and presenter evaluations:

1. In the online agenda, click on the “Evaluate Session” link.

2. From the mobile app, click on the session you want from the schedule > then click the associated resources > and the evaluation will pop up in the list.

#Security19