REN-ISAC

www.ren-isac.net • soc@ren-isac.net • 317.274.7228

What is an ISAC?

- Information Sharing and Analysis Centers
- Presidential Decision Directive-63 (PDD-63), signed May 22, 1998
  - The federal government asked each critical infrastructure sector to establish sector-specific organizations to share information about threats and vulnerabilities
  - Non-funded (will mention this later)
- Help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards.

OK so what is REN-ISAC?

- Private Trust Community
- CSIRT for .edu
- Sector ISAC
- R&D

REN-ISAC's Mission

The REN-ISAC mission is to aid and promote cyber security operational protection and response within the higher education and research (R&E) communities.

The mission is conducted within the context of a private community of trusted representatives at member institutions, and in service to the R&E community at-large.

REN-ISAC serves as the R&E trusted partner for served networks, the formal ISAC community, and in other commercial, governmental, and private security information sharing relationships.

Private Trust Community

A community of trusted security staff at R&E institutions sharing actionable information for operational protection and response; among the trusted R&E members, cross-sector, and with external trusted partners.

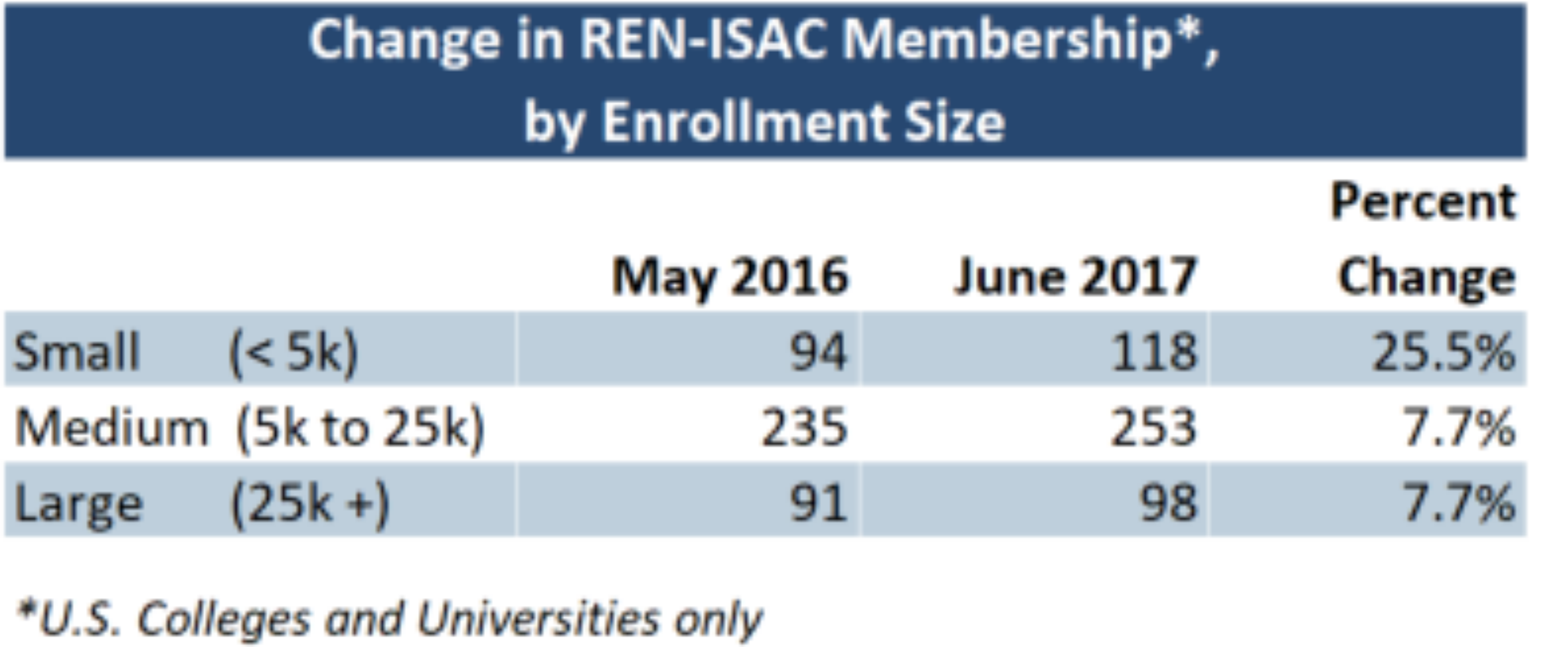
Membership

- Membership is open to:
  - Colleges and Universities
  - Teaching Hospitals
  - R&E Network Providers
  - Government-funded Research Organizations
  - Member Representative Eligibilty:
    - Very specific job responsibility requirements
      - Institution-wide operational protection and response (essentially the IT Security Office Security Engineers, Architects, and direct managers).
    - Tightly circumscribed to maintain a high level of trust and interaction among the representatives.
  - Two tiers, differing in eligibility criteria, trust vetting, sensitivity classification, and the commitment-level of the institution.

Sustainability

- Membership fee, tiered $1250 – $2500 per institution per year
- Financial contributions from IU, LSU and Internet2, and in-kind support from EDUCAUSE
- Member contributions in projects, services, and activities

Membership Demographics



Change in REN-ISAC Membership*, by Enrollment Size

	May 2016	June 2017	Percent Change
Small (< 5k)	94	118	25.5%
Medium (5k to 25k)	235	253	7.7%
Large (25k +)	91	98	7.7%

**U.S. Colleges and Universities only*

Reach

- As of June 2017, there are over
  - 556 active Member institutions
  - 1763 active Member representatives

- A list of member institutions is on the Membership web page
  - https://www.ren-isac.net/membership/MemberList.html

- Currently 32 of the ~164 Pennsylvania Colleges/Universities are members of REN-ISAC

Benefits of Membership

- Receive and share actionable information among trusted peers
- Have access to threat indicator resources that can be used to identify local compromised machines, block known threats, and aid incident response (SES aka CIF)
- Information products (e.g. Daily Watch, Advisories, and Alerts)
- Benefit from REN-ISAC relationships in broad security community
- Benefit from REN-ISAC / vendor security cooperation relationships
- Participate in technical educational security webinars
- Participate in REN-ISAC meetings, workshops and training
- Access to the 24x7 REN-ISAC Watch Desk
- Develop relationships with known and trusted peers

Member Participation

- Member participation is a cornerstone of REN-ISAC
- Member contributions through participation:
  - Board
  - Technical Advisory Group
  - Microsoft Analysis Team
  - Membership Committee
  - Member Orientation and Engagement Committee
  - Technical webinars
  - Services development
  - Projects, e.g. sensor development
  - Special Interest Groups, e.g. SIEM, Forensics, Bro, etc.

CSIRT for .edu

- Daily notifications, directly and privately to abuse contacts at .edu institutions concerning compromised or vulnerable systems, credentials, and other incident involvement
  - In service to all of US .EDU regardless of membership, and international members in the five eyes as a best effort
  - Over 13,000 notifications per month
  - Over 1,800 institutions notified
- 24x7 Watch Desk
- Represent the sector in forums of private, commercial, and governmental CERT/CSIRTS

EDU Sector ISAC

- Trusted partner for the R&E community
- Member, National Council of ISACs
- Formal relationship with DHS/US-CERT
- Cross-sector information sharing
- Public alerts aimed at R&E security practitioners, CIOs and business officers

Relationships

- APWG (Anti-Phishing Working Group)
- DHS/US-CERT and other national CERTS and CSIRTS
- EDUCAUSE
- Global Research NOC at IU
- Higher Education Information Security Council
- Internet2
- LE (various)
- National Council of ISACs
- NCFTA
- Private threat sharing, analysis & mitigation communities (various)
- Other sector ISACs
- Vendors

R&D

- SES (visited later in the presentation)
- CSIRT Tools
  - RINO (Ren-Isac NOtification system)
    - Receives, collates, and distributes notifications concerning observed compromised or vulnerable systems
  - RIHF (Ren-Isac Human Filter)
    - Process notifications based on data that requires operator vetting and interaction.
- RINO and RIHF aren’t currently released open-source but we’re hoping to get there.

Selected Successes

- Rich and active sharing among the members
- Rich and high quality external relationships (to private, commercial, and governmental partners) brings substantial value to members
- High quality indicator information for threat mitigation and IR
- High quality and high volume remediation (CSIRT notifications of compromised machines) to entire .edu sector
- Substantial contribution to cleaning up .edu space (e.g. no longer an attractive location for miscreant C&C)
- Automated machine-based threat indicator sharing (SES aka CIF) within REN-ISAC and to external partners
- Participation of the sector (although there's more to be reached)

What’s Coming Next?

- SES v4
- Registry v2
- Expanded Participation
- New Notification System

Case Study: What is our actual reach?

- Two large credential lists were floating around
  - Anti-Public / Exploit.In
- Over 1 billion credentials total
  - Over 10 million were .edu related
- We were able to send out notifications on only about 4.5 million of the creds
- 1628 notificatons sent
  - ~4140 2 and 4 year degree granting institutions
  - So we're trying, but still aren't even at 50% reach yet

What can you do today?

- Get us your IP netblocks and domains
- We will add them to our internal contacts database and you'll start receiving notifications immediately after

Questions?

Scott Finlon
Principal Security Engineer
sfinlon@ren-isac.net

http://www.ren-isac.net

24x7 Watch Desk:
soc@ren-isac.net
+1 (317) 274-7228