2023 INTERNET2
TECHNOLOGY
exchange

Collaboration in the Security Community

Marina Krenz - REN-ISAC
Paul Howell – Internet2
Nick Lewis – Internet2

Agenda

- Who are we and why are we here?

- Collaborative successes

- Your feedback!

EDUCAUSE

EDUCAUSE

Conferences

- EDUCAUSE Cybersecurity and Privacy Professionals Conference – May 1–3, 2024 Minneapolis, MN! CFP will open in early January.

- EDUCAUSE Annual next month - October 9–12, 2023 in Chicago, IL

EDUCAUSE

- EDUCAUSE Cybersecurity and Privacy Workforce Survey will be released in October 2023

- The new EDUCAUSE Cybersecurity and Privacy Guide will also launch in October 2023

- Community Groups – Awareness and Education, GRC, CPO, Privacy, TOP, HECVAT, and 171 compliance

- EDUCAUSE QuickPolls, are one-day polls that rapidly gather, analyze, and share input from the EDUCAUSE community about specific emerging topics.

EDUCAUSE

HOME | LEARNING EXPERIENCE | REGISTRATION

Learning Lab | Creating a Campus Culture of Security and Privacy

Part 1: August 1 | 1:00–2:00 p.m.ET
Part 2: August 3 | 1:00–2:30 p.m. ET
Part 3: August 10 | 1:00–2:30 p.m. ET
Part 4: August 17 | 1:00–2:30 p.m. ET

Overview

As security and privacy have become increasingly intertwined, it's become critical to develop a campus culture that embraces both. A strategic awareness plan helps ensure that your efforts are successful. Attendees will participate in exercises to assess their audiences, develop messaging, identify needed assets (including campus partners), and build an effective plan.

Learning Outcomes:

NOTE: You will be asked to complete assignments in between the Learning Lab segments that support the learning outcomes stated below. You will receive feedback and constructive critique from course facilitators.

- Understand key elements and considerations in creating a security and privacy awareness plan

Regist

Space
now to

Particip
is enco
conten
be view

Career paths – find your path

The Four Pathways

The four pathways serve to guide professionals supporting and transforming higher education through the innovative use of technology.

Information Security

The Information Security Pathway is for higher education professionals whose primary role is to keep the campus community safe and protect institutional data across systems and for constituents, including students, faculty, staff, and partners.

LEARN MORE

Information Technology

The Information Technology Pathway is for leaders and professionals who support information technology systems and their strategy, management, budgets, and policy. The pathway guides those who manage the technology ecosystem comprising the systems and services that institutions use to store and manage data and processes, whether on campus, in the cloud, or through shared services.

LEARN MORE

Innovation

The Innovation Pathway is for professionals dedicated to the advancement of their institution's mission and strategic goals through the innovative and creative application of strategies and solutions. This pathway supports those tasked with leveraging data and technology in support of cross-institutional transformation.

LEARN MORE

Teaching & Learning

The Teaching and Learning Pathway guides those working to enhance or transform learning experiences and student success across the institution through the effective application of learning science and relevant data to guide the selection of pedagogies and technologies.

LEARN MORE

Positions and years spent at each professional level will vary.

2021 EDUCAUSE Horizon Report Information Security Edition

2021 EDUCAUSE Horizon Report®

- Cloud Vendor Managment • Endpoint Detection and Response
- Multifactor Authentication (MFA)/Single Sign-On (SSO)
- Preserving Data Authenticity/Integrity
- Research Security • Student Data Privacy and Governance

This report profiles important trends and key technologies and practices shaping the future of information security, and envisions a number of scenarios and implications for that future. It is based on the perspectives and expertise of a global panel of leaders from across the higher education landscape

Quicktalks…

Member QuickTalk | Core Data Service (CDS) Study Group

Online
June 07, 2022

Join our study group to connect with EDUCAUSE experts and your peers about how to get the most out of your CDS experience.

Member QuickTalk | Showcase Coffee Shop: The Digital versus Brick-and-Mortar Balancing Game

Online
May 12, 2022

Grab your coffee and join us for an informal discussion on digital and physical work and learning spaces.

Member QuickTalk | Core Data Service (CDS) Study Group

Online
May 10, 2022

Join our study group to connect with EDUCAUSE experts and your peers about how to get the most out of your CDS experience.

EDUCAUSE

Jobs   .EDU Domain   EDUCAU

Hybrid Campus Showcase   Topics   Insights   Conferences & Learning   Community   Wh

Thursday, December 09 | 1:00PM–2:00PM ET | Online

Member QuickTalk | Cyber Insurance: Renewals, Rate Increases and Shared Strategies

Cyber Insurance has become an increasingly important topic for our members that is likely to continue evolving for higher education. As we look to 2022 and upcoming insurance renewals, we would like to provide members an opportunity to discuss their experiences and questions, as well as share strategies to address premium increases and new requirements imposed by underwriters and carriers.

To get the most from the QuickTalk experience, we encourage attendees to review the recently published **FAQ** on cyber insurance for higher education. This will be an interactive event and all are invited to contribute their questions and expertise.

QuickTalk Moderators

Aaron Baillio
CISO, University of Oklahoma

Brian Kelly
Director of the Cybersecurity Program, EDUCAUSE

Additional Resources

- **Frequently Asked Questions About Cyber Insurance**

INTERNET2

Cloud Services Updates

- Cloud Scorecard – over 50 service providers with many of interest to information security

- Institutional Profiles

- Vendor Risk Management service evaluation

- NET+ Miro now live!

- Service Evaluation for data migration tools

MY PORTFOLIO UPDATES

- CrashPlan (39), Duo (204), LastPass (69), Palo Alto Networks (3), Splunk (28) updates

  - MFA Community Report 2023 presentation this week!

  - Started NET+ LastPass Service Advisory Group

- Current Community Calls – CrashPlan (20) and Duo (60-120). Might restart PAN and Splunk.

- Vendor Risk Management and Vendor Management call?

- Exploring new service providers

InCommon

- [BaseCAMP](#) provides a workshop for those new to identity and access management (IAM), new to InCommon, or both, that focuses on the basics, an introduction to the InCommon Federation, and overviews and demonstrations of the community-developed identity and access management suite
- Participate in the [InCommon Academy for IAM training](#)
- Get involved in the [Community Success Program](#)
- Changes coming from NIH around potential areas of improvement in [identify proofing processes](#) for your campus.
- Get involved in the in the 2nd annual cybersecurity cooperation [exercise this fall](#)!
- InCommon kicked off Futures2, a [strategic planning project](#) being undertaken by the Steering Committee to help guide a vibrant future for InCommon

NATIONAL RESEARCH AND EDUCATION NETWORK UPDATES

Routing Integrity Initiative encourages the community's adoption of best practices that strengthen the resilience and reliability of data movement across the R&E network ecosystem to support our shared missions

- Routing Security as defined by Mutually Agreed Norms for Routing Security (see MANRS.org)
- Hardening of network devices (MFA authentication, regular review of firmware, logging, etc.)
- Detection and mitigation of DDoS attacks
- Resilient cloud connectivity
- IPv6 Deployment
- Routing Integrity Assessment service - contact manrs@internet2.edu
- Reports showing the accuracy of published routing policy for RENs
      https://github.internet2.edu/ssw/IRR-report
- Autonomous System Provider Authorization Working Group (ASPA-WG) is develop recommendations for its adoption by R&E networks

INTERNET2 ROUTING INTEGRITY MILESTONES
MAY 2023

(A) = Routing Integrity Assessment
(R) = RPKI-ROV
(M) = MANRS Participant
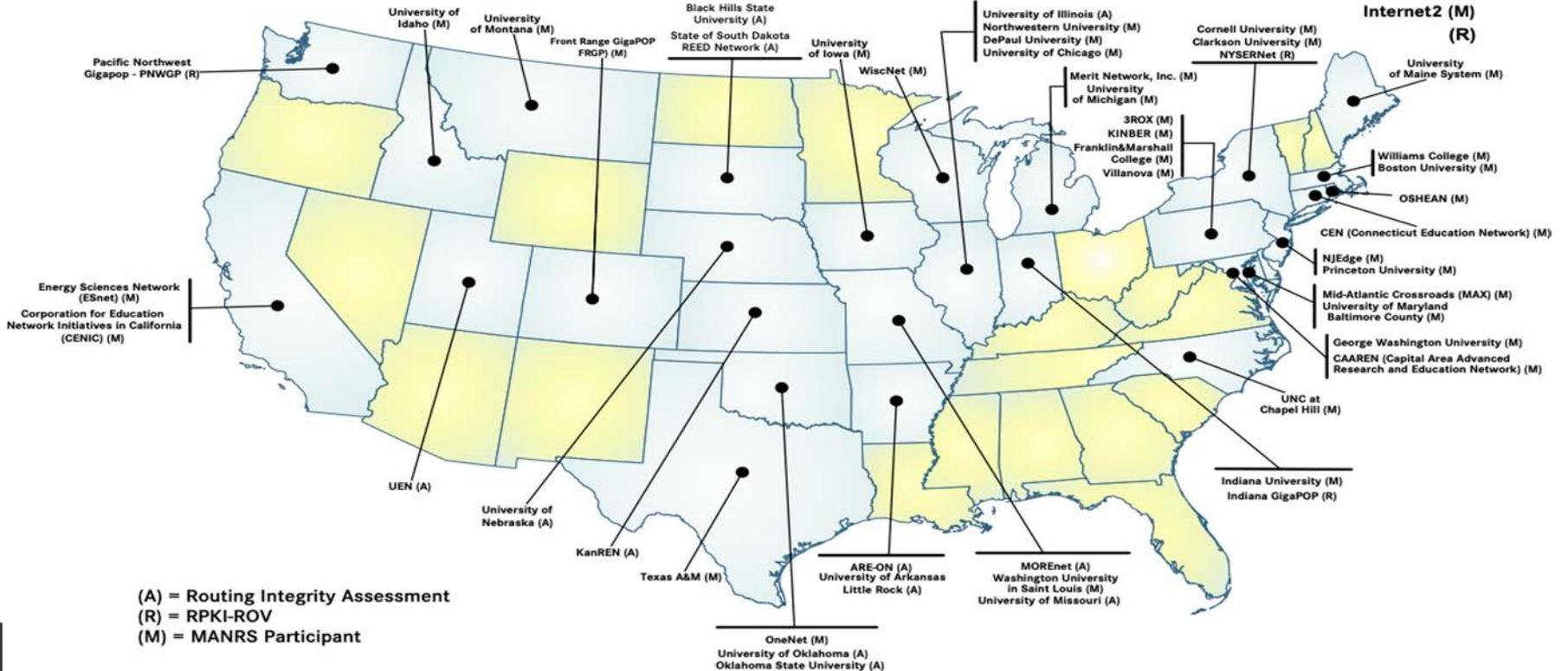
Nearly half of the US R&E IP addresses lack an ARIN agreement

What we see in the Internet2 R&E table:
- 2,203 ARIN direct IP address assignments
- 1,023 (46%) without an ARIN Agreement
- $1,876,124,160 Market value of IP numbers not covered by ARIN agreement!

Many mistakenly believe their IP addresses are covered by an ARIN agreement
- No agreement required to manage whois information (i.e., portal access doesn't require an agreement)
- You may be receiving and paying ARIN bills for other resources

Benefits of the ARIN agreement

- Access to routing security services:
    - Authenticated IRR
    - Hosted RPKI-ROAs
- Participation in ARIN's governance
- Better sleep knowing you have an agreement that specifies the registration services that announce to the Internet who holds your IP addresses

NOTE: Using ARIN Hosted RPKI-ROA service is, by far, the easiest way to mitigate the risk of outage due to route hijacking. No equipment changes required. It's only a bit more complicated than filling out a simple web form!

ARIN agreement fee changes (for legacy resources)

For legacy resources in 2023, ARIN's fees are $175/yr. That's $175/yr for any number of legacy resources. **Signing an agreement this year locks in fee increases of $25/yr**.

Waiting until next year (or longer) to sign an ARIN agreement will result in fees subject to ARIN's normal fee schedule. For a single /16, the current fee schedule is $4,000/yr (22 times higher than the legacy fee schedule).

Across the Internet2 community, this difference adds up to **$2M/yr** in fees for agreements signed after 2023, vs **$75K/yr** in fees for agreements signed this year.

Questions?   Go to the ARIN table or email manrs@internet2.edu

REN-ISAC

REN-ISAC

Research & Education Networks
Information Sharing & Analysis Center

REN-ISAC - What Are We Seeing?

- Ransomware Tracker

- CSIRT Metrics

- Security Event System (SES)

- pDNS

Adobe Stock

2022-2023 Stats by Ransomware Group

RW Group	Count of RW Group	% of overall
Vice Society	9	21%
AvosLocker	7	16%
AlphVM (BlackCat)	4	9%
LockBit 3.0	3	7%
Unknown	3	7%
Hive	3	7%
LockBit 2.0	3	7%
Suncrypt	2	5%
BianLian	2	5%
Snatch	1	2%
Quantum	1	2%
BlackByte	1	2%
Conti	1	2%
54bb47h (Sabbath)	1	2%
REvil	1	2%
Royal	1	2%
Grand Total	43	100%

Mean Enrollment	8310.34	
Median Enrollment	3231	
RI Members Affected	19.00%	

RW Group	Count of RW Group	% of overall
Vice Society	11	21.57%
Clop	10	19.61%
LockBit 3.0	7	13.73%
AvosLocker	4	7.84%
Royal	3	5.88%
Nokoyawa	3	5.88%
Snatch	2	3.92%
Akira	2	3.92%
Rhysida	2	3.92%
BianLian	2	3.92%
AlphVM	1	1.96%
Trigona	1	1.96%
Medusa	1	1.96%
Play	1	1.96%
MONTI	1	1.96%
Grand Total	51	100.00%

Mean Enrollme	10606.26	
Median Enrollm	7452	
RI Members Aff	16.36%	

CSIRT ACTIVITY in 2023

| Master File: Current CSIRT Data 2023	Jan	Feb	Mar	Q1	Apr	May	Jun	Q2
Compromised Machines	3570	5137	4643	13,350	2,858	4,313	4,244	11,415
Compromised Credentials	6791	9977	5995	22,763	1,893	3,947	9,234	15,074
Spam or Phish	15	12	10	37	9	19	3	31
Vulnerable Machines	0	67	445	512	0	0	0	0
Open Recursive Domain Resolvers	75	68	99	242	61	71	76	208
Open Mail Relays	0	0	0	0	0	0	0	0
SSH Scanning	0	0	0	0	0	0	0	0
Other Misc Notifications	7	3	8	18	3	8	3	14
Total:	10,458	15,264	11,200	36,922	4,824	8,358	13,560	26,742
SOC Interactions								
notification questions	10	31	9	50	55	58	22	135
password related	90	7	2	99	0	0	4	4
notifications	33	57	40	130	48	49	12	109
other	7	261	198	466	134	160	165	459
total interactions:	140	356	249	745	237	267	203	707
SOC non-interactive tickets	1,026	498	278	1802	163	192	222	577
Unique institutions contacted per period*	2,060	2,189	1,953	N/A	1,099	1,606	2,061	N/A

Security Event System Stats

Top SES Data Providers by Unique Indicators Submitted in the Past Seven Days (Updated Hourly)

Provider	%
partner11.ren-isac.net	15%
stopforumspam.com	15%
threatview.io	15%
dataplane.org	13%
infoblox-iid	10%
intel.ren-isac.net	10%
apwg.org	5%
partner6.ren-isac.net	3%
partner13.ren-isac.net	3%
openphish.com	3%
spamhaus.org	3%
phishtank.com	
majestic.com	
tranco-list.eu	
viriback.com	
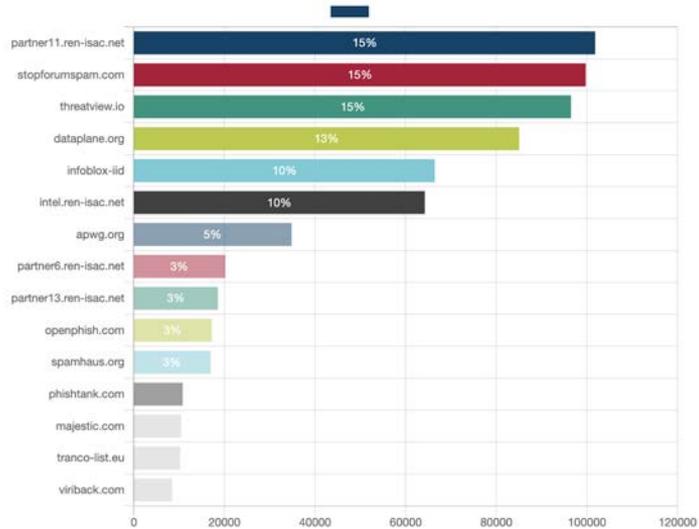
*partnerXX.ren-isac.net are anonymized contributors

Top Threat Indicator Types Reported in the Past Seven Days (Updated Hourly)

Legend: ipv4, fqdn, url, email, md5, sha256, ssdeep, sha1, ipv6, uuid

ipv4: 50%
fqdn: 41%
url: 6%
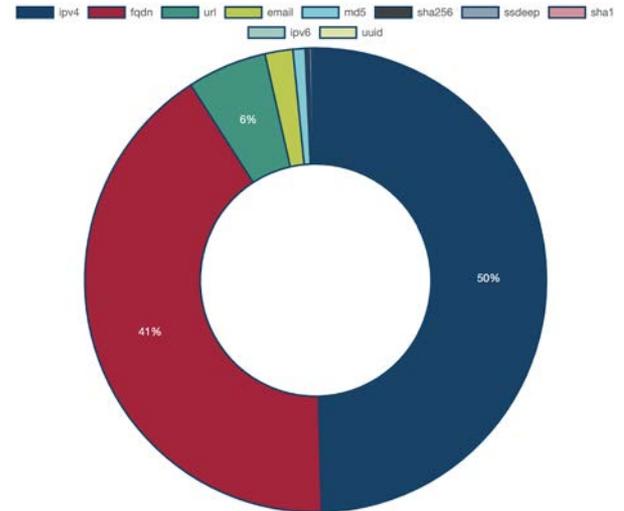
https://www.ren-isac.net/member-resources/SES/SES_Data_Feed.html

Security Event System Stats 2022-2023

31MM+   ALL indicators

10MM+   High confidence indicators

7,7MM+   High confidence indicators from .edu providers

72% of High Confidence indicators are from .edu providers

REN-ISAC - What Are We Doing?

- SES
- pDNS
- Active Discussion Lists
- Collaboration with other ISACs
- CSIRT Activities - all EDUs
- Alerts/Advisories/Best Practices
- The REN-ISAC Hub
- Peer Assessment
- PEN testing

REN-ISAC - How Can We Help?

info@ren-isac.net

COLLABORATIONS

AREAS OF COLLABORATION

- Conference planning
- Working Groups
- HECVAT
- 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

CONTACT INFORMATION

- Krenz, Marina, REN-ISAC – <mvkrenz@iu.edu>
- Joseph Potchanant - jpotchanant@educause.edu
- Paul Howell – phowell@internet2.edu
- Nick Lewis – nlewis@internet2.edu