ResearchSOC

Research Security Operations Center: The NSF Collaborative Security Response Center

September 26, 2018
2018 NSF CICI PI Meeting

Von Welch

The Team

Team members: Richard Biever (Duke), Michael Corn (UCSD), Tom Davis (IU), Inna Kouper (IU), Jim Marsteller (PSC), Sameer Patil (IU), Susan Sons (IU), Von Welch (IU)

Funded by NSF Grant 1840034.

ResearchSOC Goal

Serve as a Collaborative Security Response Center whose expertise and resources are leveraged by the entire research and education community to:

1. **Improve the cybersecurity posture of scientific cyberinfrastructure,** and
2. **Raise awareness of security threats facing the scientific community**.

ResearchSOC versus Trusted CI

ResearchSOC

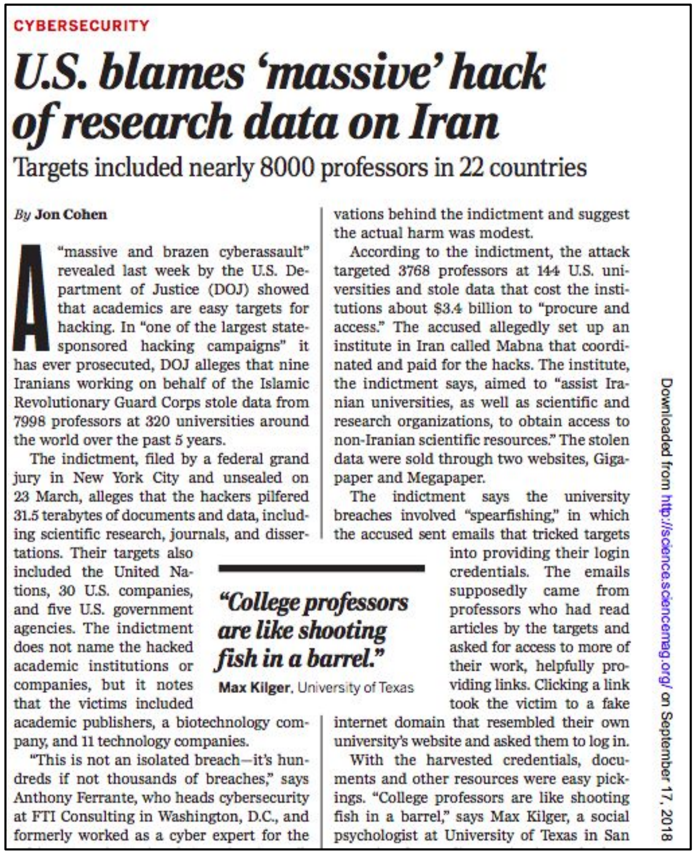
- Operational services and related training for NSF CI
- Community of Practice and Threat Intelligence Network
- Enabling Cybersecurity Research
- Outreach to Higher Ed Infosec regarding research CI

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

- Creating comprehensive cybersecurity programs
- Community building and leadership
- Training and best practices
- Tackling specific challenges of cybersecurity, software assurance, privacy, etc.

ResearchSOC Motivation

Protecting The Reputation of Research



CYBERSECURITY

U.S. blames 'massive' hack of research data on Iran

Targets included nearly 8000 professors in 22 countries

By **Jon Cohen**

A "massive and brazen cyberassault" revealed last week by the U.S. Department of Justice (DOJ) showed that academics are easy targets for hacking. In "one of the largest state-sponsored hacking campaigns" it has ever prosecuted, DOJ alleges that nine Iranians working on behalf of the Islamic Revolutionary Guard Corps stole data from 7998 professors at 320 universities around the world over the past 5 years.

The indictment, filed by a federal grand jury in New York City and unsealed on 23 March, alleges that the hackers pilfered 31.5 terabytes of documents and data, including scientific research, journals, and dissertations. Their targets also included the United Nations, 30 U.S. companies, and five U.S. government agencies. The indictment does not name the hacked academic institutions or companies, but it notes that the victims included academic publishers, a biotechnology company, and 11 technology companies.

"This is not an isolated breach—it's hundreds if not thousands of breaches," says Anthony Ferrante, who heads cybersecurity at FTI Consulting in Washington, D.C., and formerly worked as a cyber expert for the

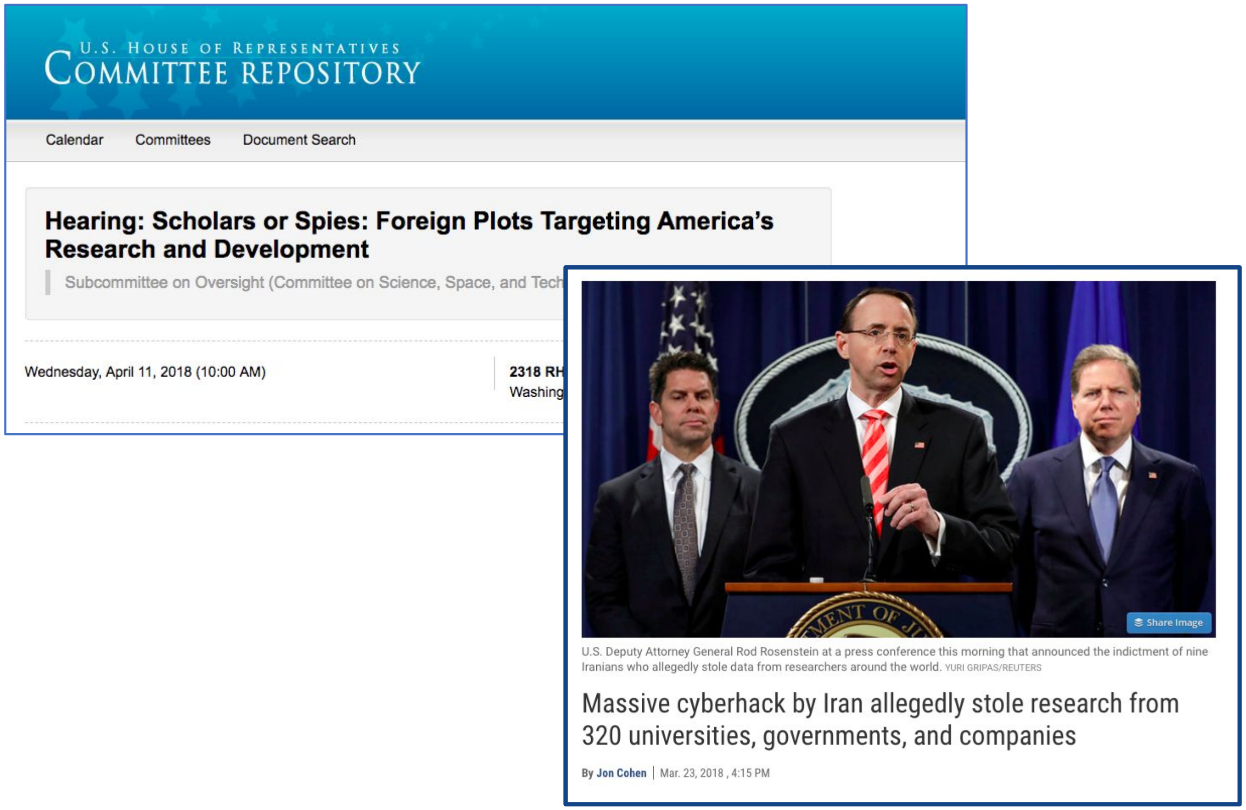
vations behind the indictment and suggest the actual harm was modest.

According to the indictment, the attack targeted 3768 professors at 144 U.S. universities and stole data that cost the institutions about $3.4 billion to "procure and access." The accused allegedly set up an institute in Iran called Mabna that coordinated and paid for the hacks. The institute, the indictment says, aimed to "assist Iranian universities, as well as scientific and research organizations, to obtain access to non-Iranian scientific resources." The stolen data were sold through two websites, Gigapaper and Megapaper.

The indictment says the university breaches involved "spearfishing," in which the accused sent emails that tricked targets into providing their login credentials. The emails supposedly came from professors who had read articles by the targets and asked for access to more of their work, helpfully providing links. Clicking a link took the victim to a fake internet domain that resembled their own university's website and asked them to log in.

With the harvested credentials, documents and other resources were easy pickings. "College professors are like shooting fish in a barrel," says Max Kilger, a social psychologist at University of Texas in San

> ***"College professors are like shooting fish in a barrel."***
> **Max Kilger**, University of Texas



U.S. House of Representatives
Committee Repository

Calendar Committees Document Search

Hearing: Scholars or Spies: Foreign Plots Targeting America's Research and Development

Subcommittee on Oversight (Committee on Science, Space, and Tech

Wednesday, April 11, 2018 (10:00 AM)

2318 RH
Washing

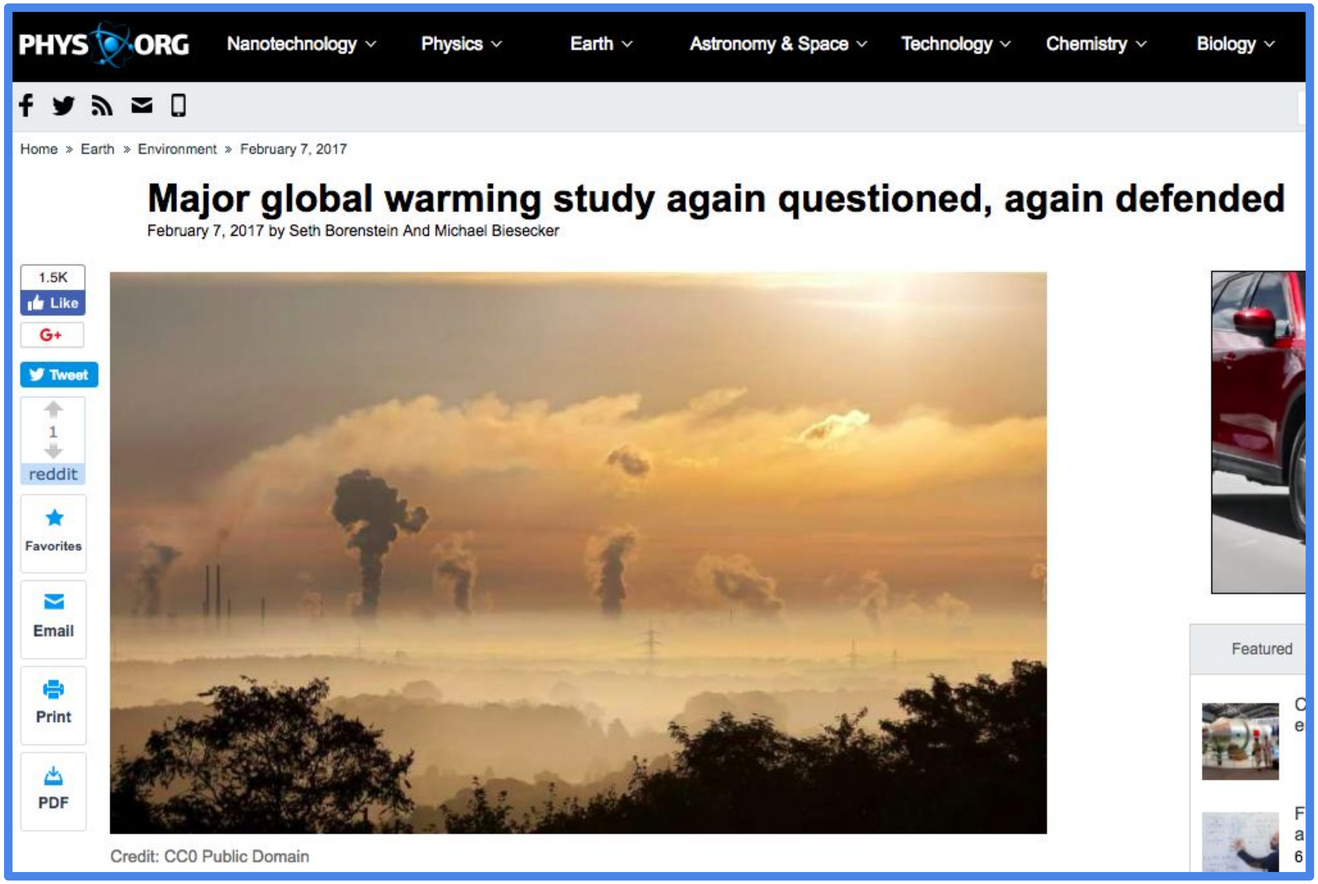
U.S. Deputy Attorney General Rod Rosenstein at a press conference this morning that announced the indictment of nine Iranians who allegedly stole data from researchers around the world. YURI GRIPAS/REUTERS

Massive cyberhack by Iran allegedly stole research from 320 universities, governments, and companies

By Jon Cohen | Mar. 23, 2018 , 4:15 PM

https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108175
http://science.sciencemag.org/content/sci/359/6383/1450.full.pdf

Protecting the Integrity of Research Data

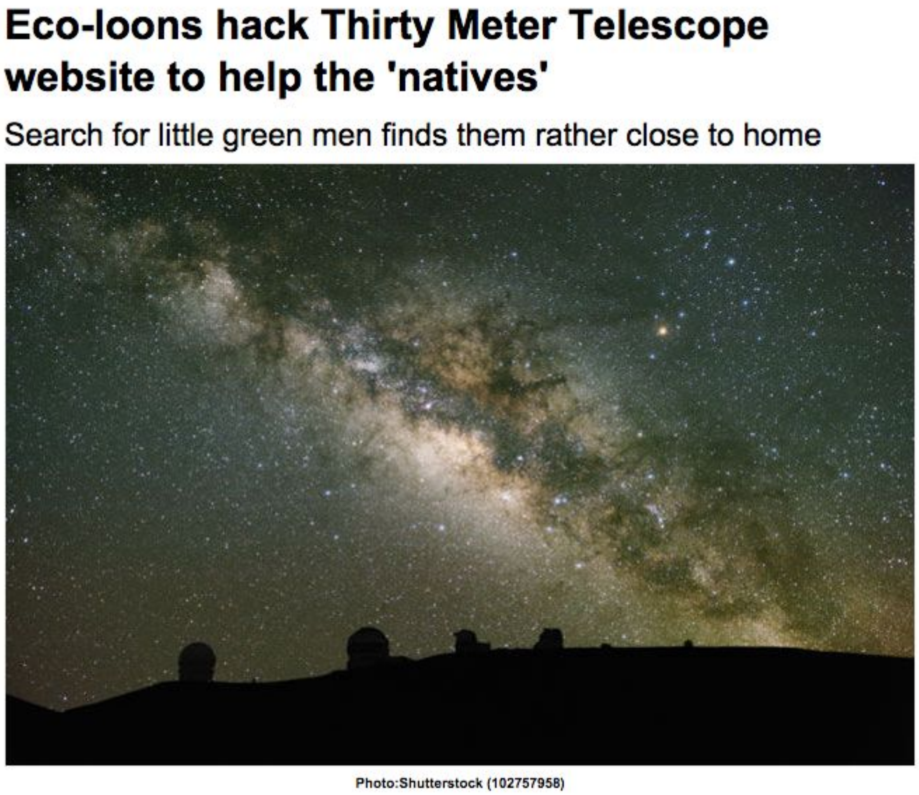


Major global warming study again questioned, again defended

February 7, 2017 by Seth Borenstein And Michael Biesecker

Credit: CC0 Public Domain

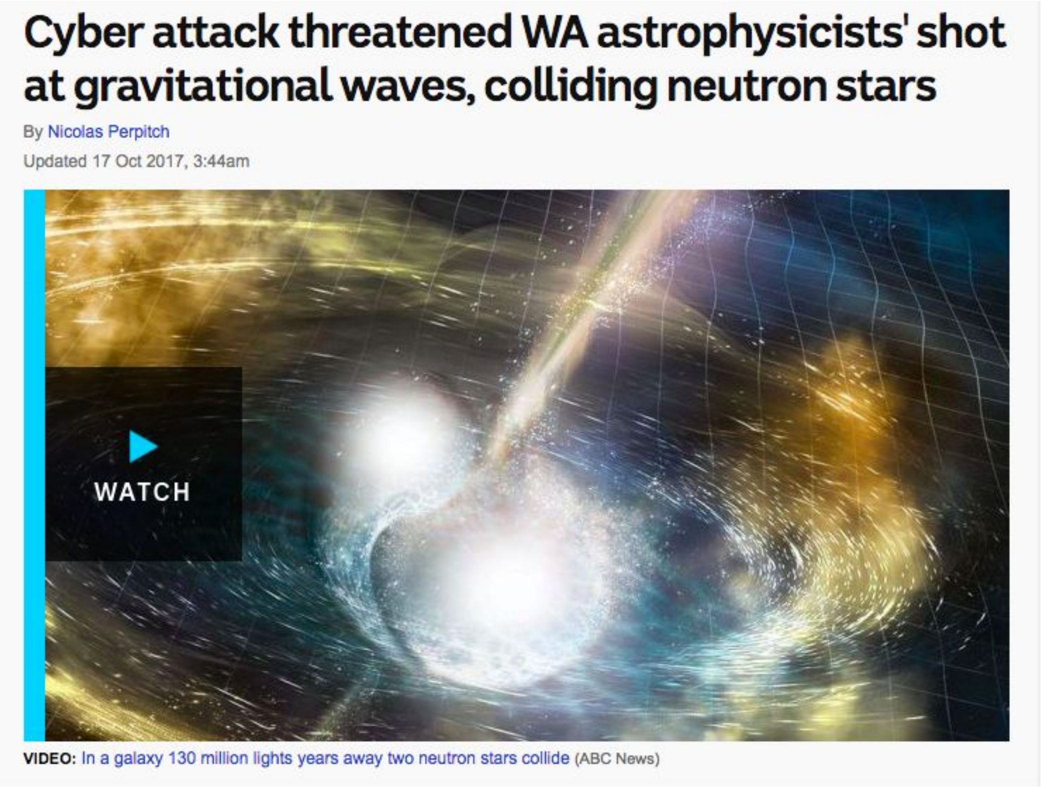
Protecting Productivity of Research



Eco-loons hack Thirty Meter Telescope website to help the 'natives'

Search for little green men finds them rather close to home

Photo:Shutterstock (102757958)



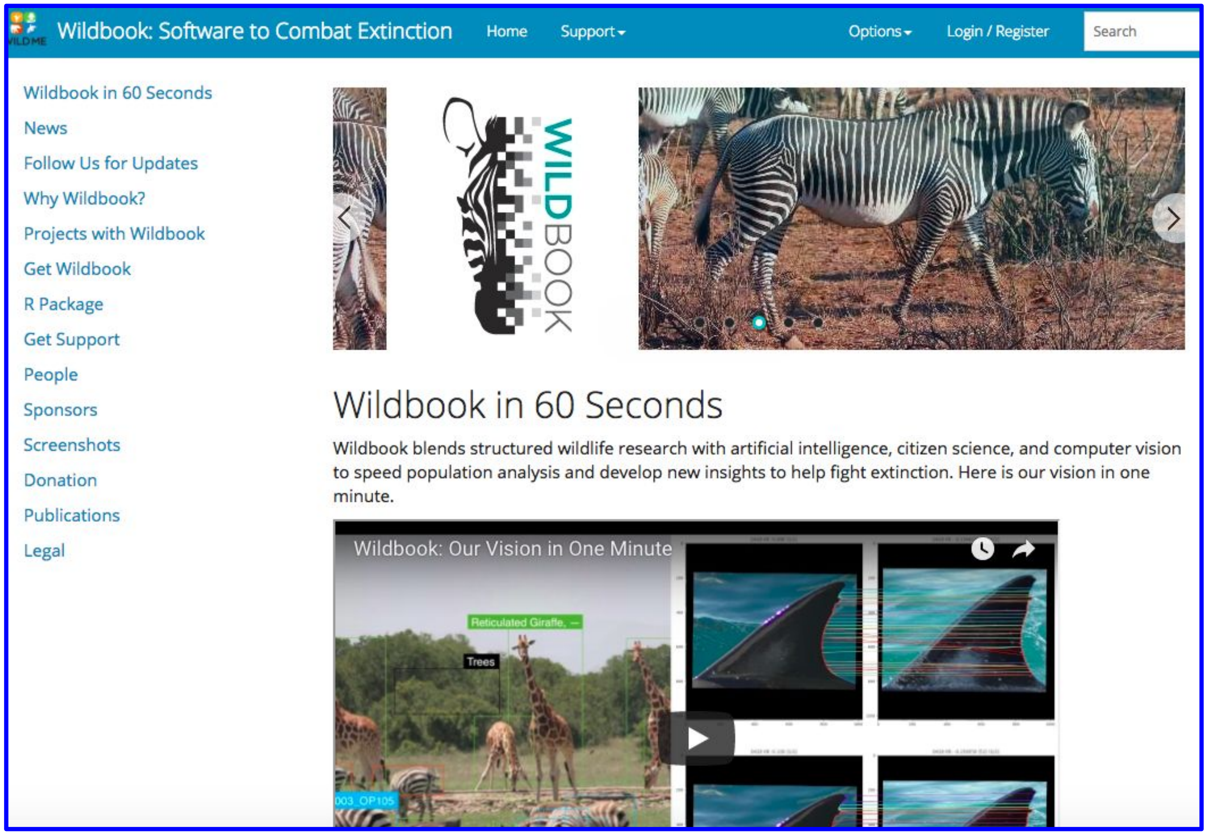
Cyber attack threatened WA astrophysicists' shot at gravitational waves, colliding neutron stars

By Nicolas Perpitch

Updated 17 Oct 2017, 3:44am

VIDEO: In a galaxy 130 million lights years away two neutron stars collide (ABC News)

Protecting the Subjects of Research



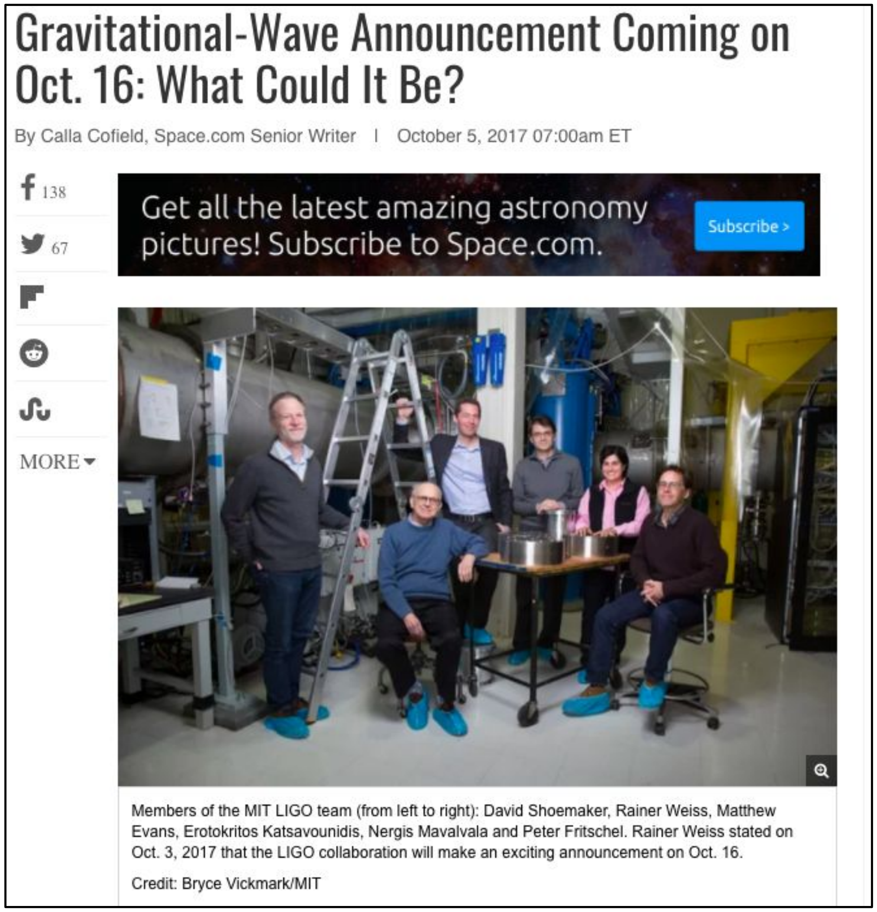
Wildbook: Software to Combat Extinction

- Wildbook in 60 Seconds
- News
- Follow Us for Updates
- Why Wildbook?
- Projects with Wildbook
- Get Wildbook
- R Package
- Get Support
- People
- Sponsors
- Screenshots
- Donation
- Publications
- Legal

Wildbook in 60 Seconds

Wildbook blends structured wildlife research with artificial intelligence, citizen science, and computer vision to speed population analysis and develop new insights to help fight extinction. Here is our vision in one minute.

Protecting Embargoed Research



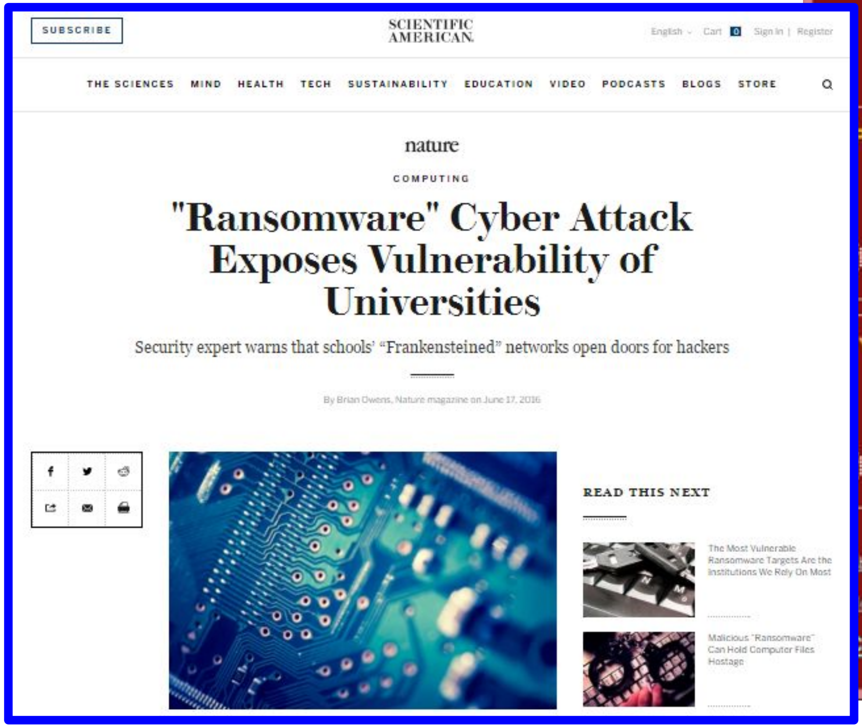
Gravitational-Wave Announcement Coming on Oct. 16: What Could It Be?

By Calla Cofield, Space.com Senior Writer | October 5, 2017 07:00am ET

Members of the MIT LIGO team (from left to right): David Shoemaker, Rainer Weiss, Matthew Evans, Erotokritos Katsavounidis, Nergis Mavalvala and Peter Fritschel. Rainer Weiss stated on Oct. 3, 2017 that the LIGO collaboration will make an exciting announcement on Oct. 16.

Credit: Bryce Vickmark/MIT

Protecting Research from Attacks That Don’t Care About Research



SUBSCRIBE
SCIENTIFIC AMERICAN.
English
Cart 0
Sign In | Register
THE SCIENCES MIND HEALTH TECH SUSTAINABILITY EDUCATION VIDEO PODCASTS BLOGS STORE
nature
COMPUTING

"Ransomware" Cyber Attack Exposes Vulnerability of Universities

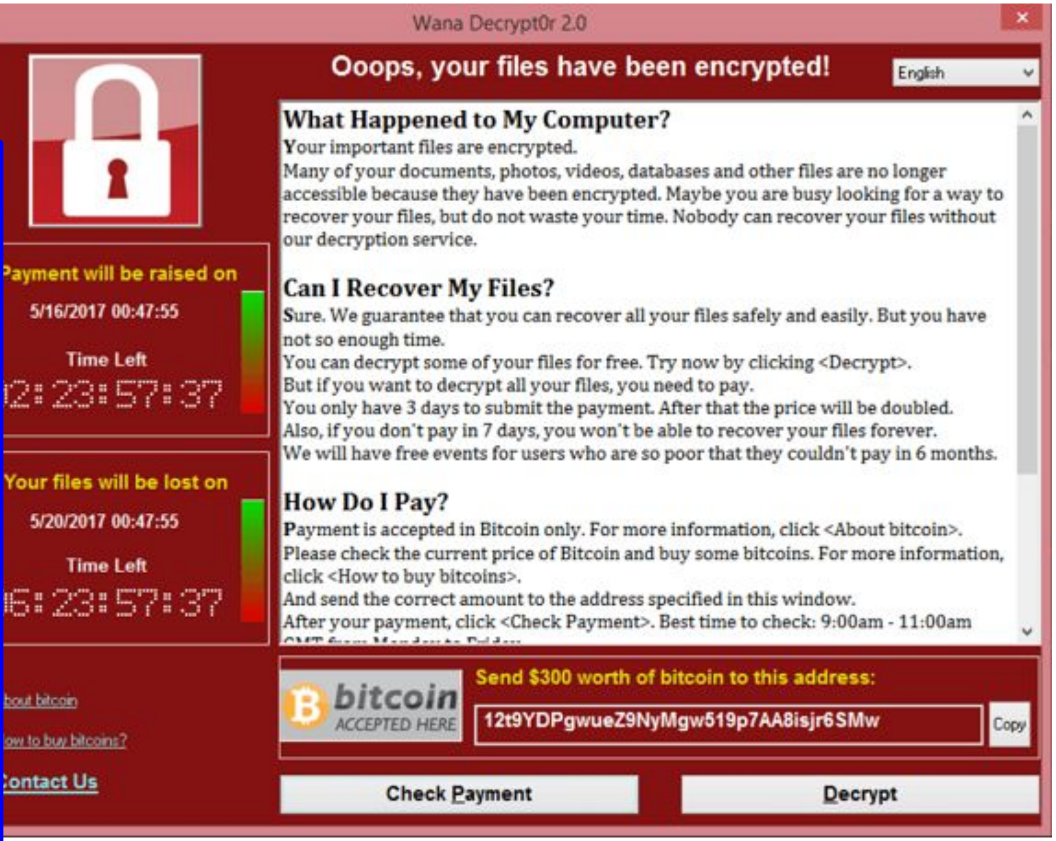
Security expert warns that schools’ “Frankensteined” networks open doors for hackers

By Brian Owens, Nature magazine on June 17, 2016

READ THIS NEXT

The Most Vulnerable Ransomware Targets Are the Institutions We Rely On Most

Malicious "Ransomware" Can Hold Computer Files Hostage



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
2:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
6:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

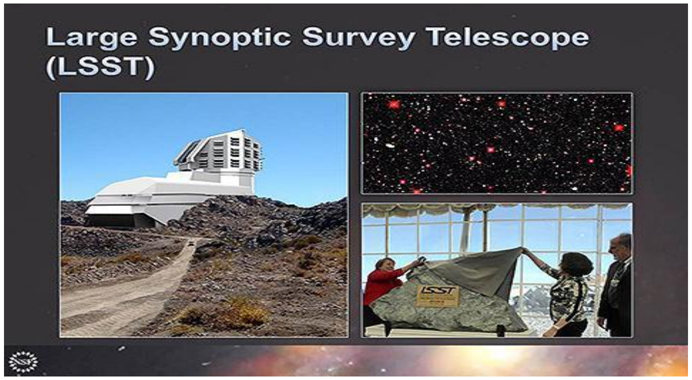
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

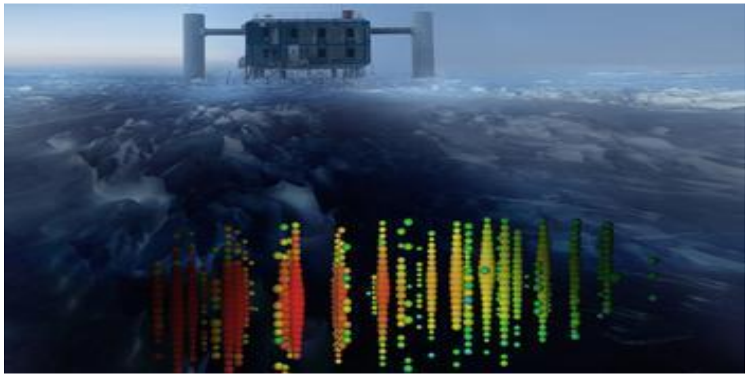
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

ResearchSOC Challenges

Scale of Science: Large Autonomous Facilities to...



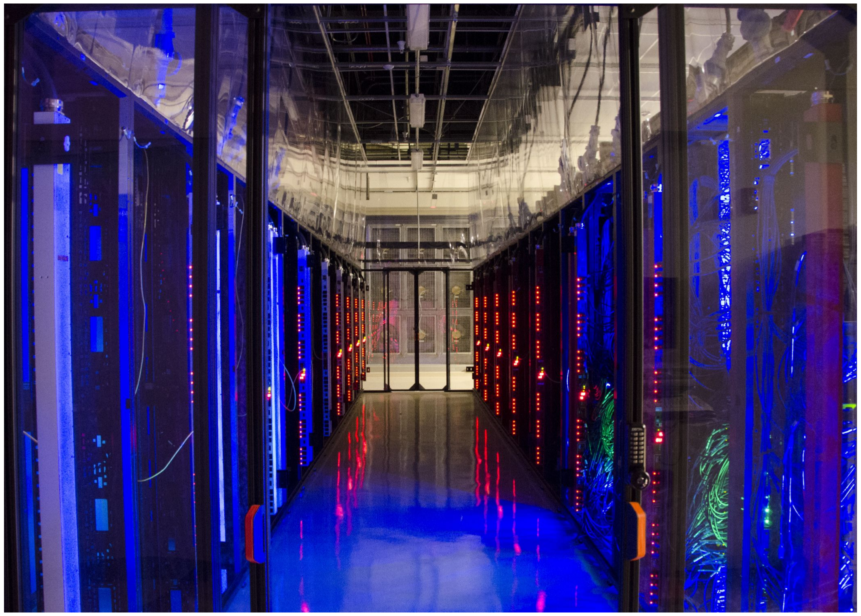
Large Synoptic Survey Telescope (LSST)



...Small-to-medium embedded projects

Credits, left-to-right: Marco Hatch, Western Washington University; Credit: Rob Beecham, photographer; Laura Stachel, executive director, WeCareSolar; Credit: Ramesh Balasubramaniam and graduate students, UC Merced, Cognitive Science; Credit: Clemson University

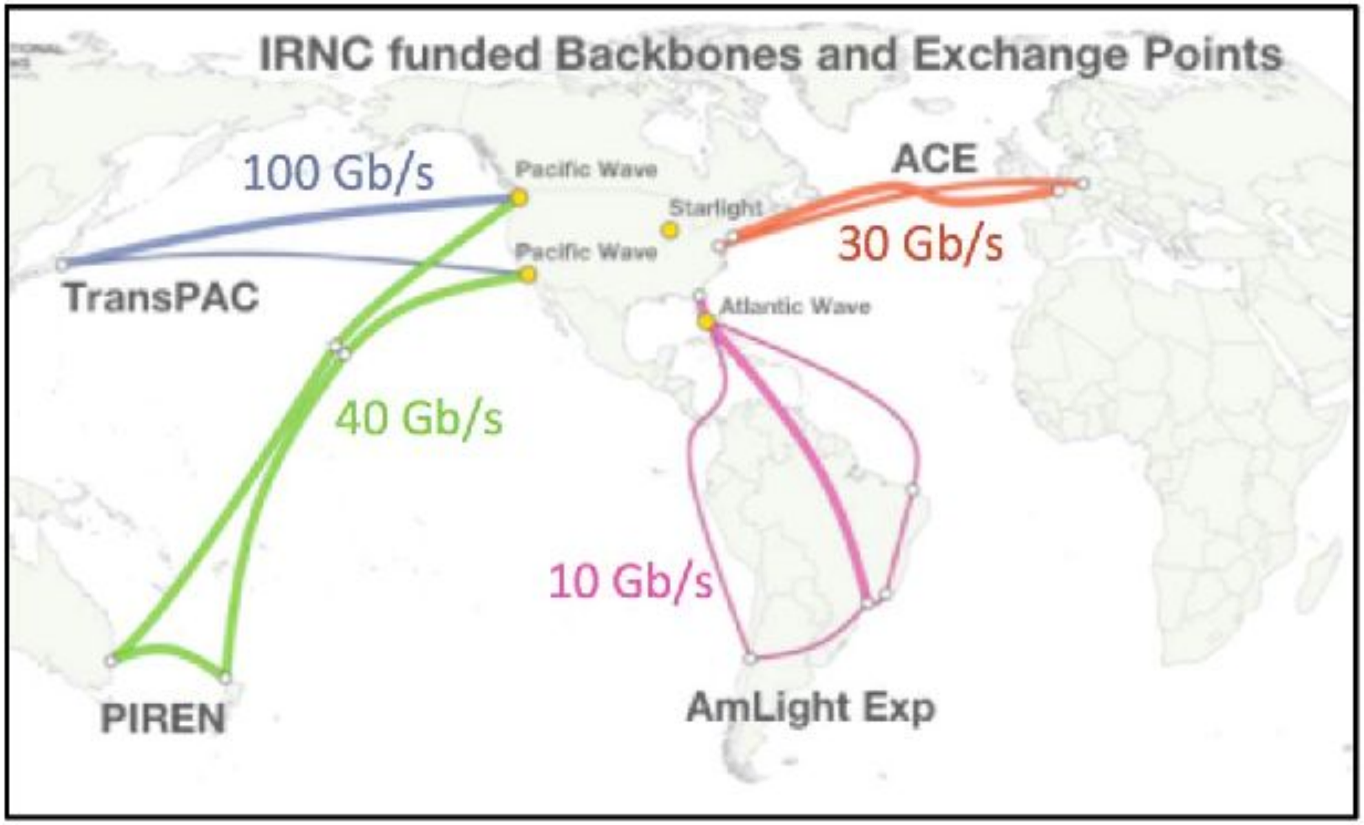
Cyberinfrastructure is Diverse



Credit: Chris Coleman, School of Computing, University of Utah

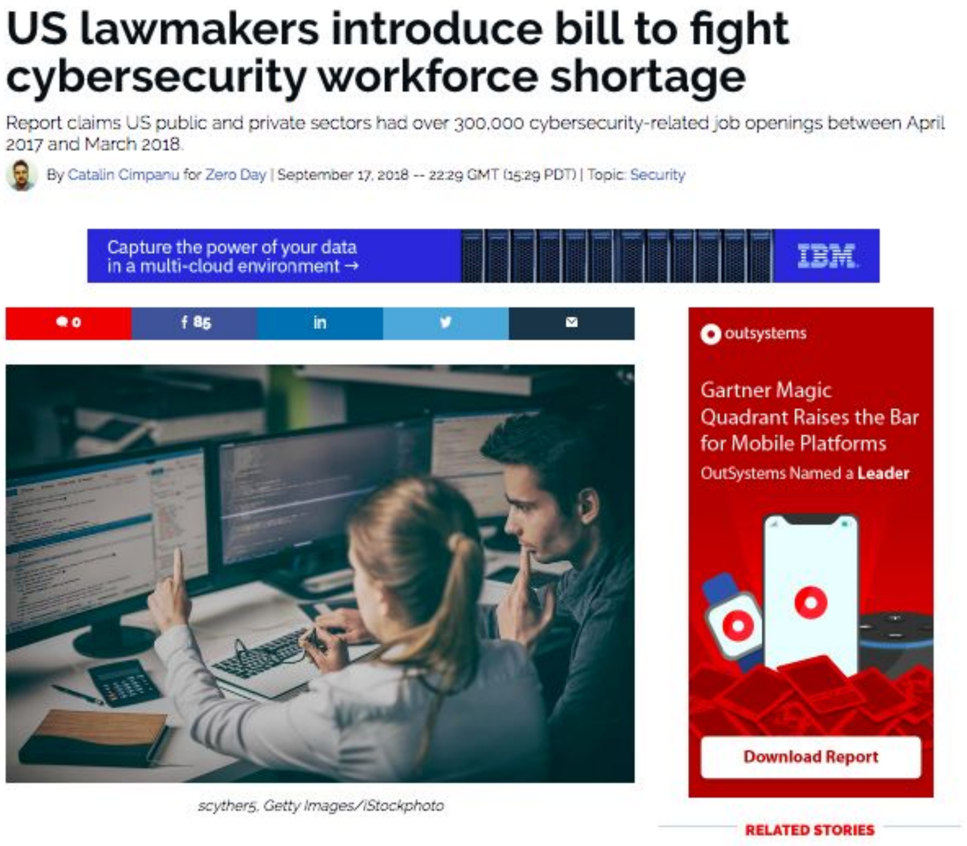
!=

Cyberinfrastructure is Highly Collaborative



Alberto Gonzalez, Jason Leigh, Sean Peisert, Brian Tierney, Edward Balas, Predrag Radulovic, Jennifer M. Schopf. 2017 IEEE International Congress on Big Data (BigData Congress) DOI:10.1109/BigDataCongress.2017.51

Intrusion Detection Requires Specialized Skills



US lawmakers introduce bill to fight cybersecurity workforce shortage

Report claims US public and private sectors had over 300,000 cybersecurity-related job openings between April 2017 and March 2018.

By Catalin Cimpanu for Zero Day | September 17, 2018 -- 22:29 GMT (15:29 PDT) | Topic: Security

scyther5, Getty Images/iStockphoto

RELATED STORIES

https://www.zdnet.com/article/us-lawmakers-introduce-bill-to-fight-cybersecurity-workforce-shortage/

The ResearchSOC Strategy

Existing Cybersecurity Services and Expertise

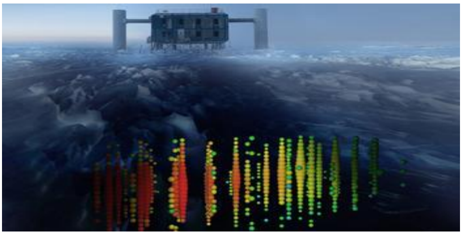
OmniSOC

STINGAR

3ROX
THREE RIVERS OPTICAL EXCHANGE

Existing Higher Ed Information Security Professionals

Awareness, Training, and Tailoring for CI



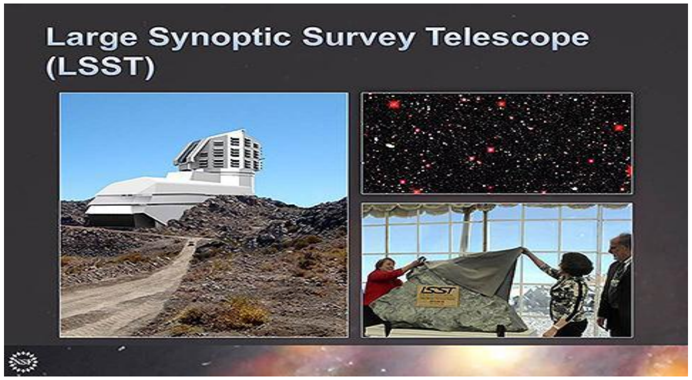
HIPAA Myths

- HIPAA compliance is a boolean = there is a threshold which, when crossed, makes you suddenly compliant
- HIPAA compliance is a one time deal
- You can have a qualified third party review your environment and certify your HIPAA compliant

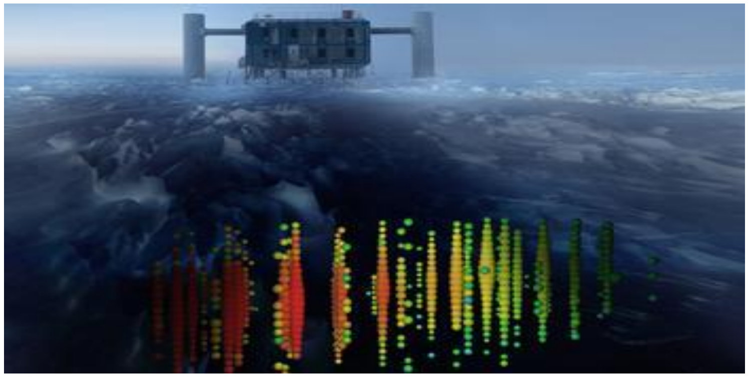
ResearchSOC

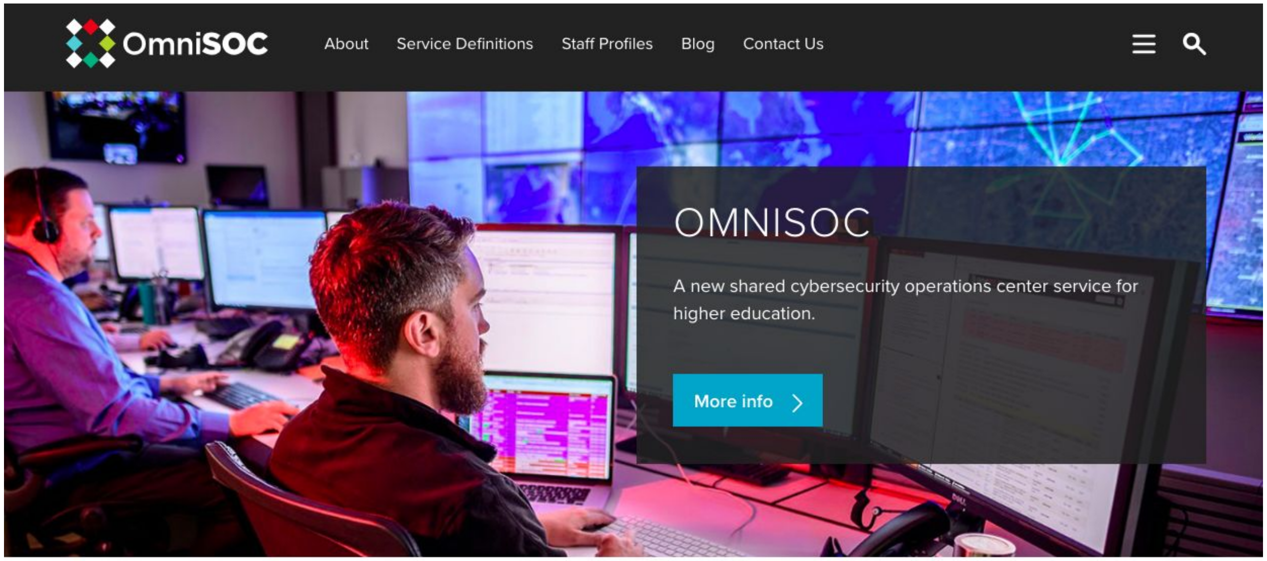
ResearchSOC Approach to Tackle...

Scale of Science: Large Autonomous Facilities to...



Large Synoptic Survey Telescope (LSST)





OMNISOC

A new shared cybersecurity operations center service for higher education.

- Process and Create Cyber Threat Intelligence
- Notify Member Incident Response Teams
- Communicate and Share Information
- Conduct Proactive Threat Hunting
- Analyze Security Events
- Monitor and Triage Security Events
- Provide Call Center Services

GlobalNOC

…extensibl

https://omnisoc.iu.edu/

Vulnerability Identification Service at the Three Rivers Optical Exchange (3ROX)

ReserachSOC will offer a Vulnerability Identification Service built upon the 3ROX service currently offered to members on a subscription basis. 3ROX is operated and managed by the Pittsburgh Supercomputing Center (PSC).

The service leverages the widely deployed open source ‘OpenVAS’ framework.

- Endpoint discovery exercises will be conducted to identify all assets in need of protection.
- The service detects and alerts vulnerable software versions or configurations and system weaknesses in networks or communications equipment.

ResearchSOC Approach to Tackle...

...Small-to-medium embedded projects

Credits, left-to-right: Marco Hatch, Western Washington University; Credit: Rob Beecham, photographer; Laura Stachel, executive director, WeCareSolar; Credit: Ramesh Balasubramaniam and graduate students, UC Merced, Cognitive Science; Credit: Clemson University

STINGAR

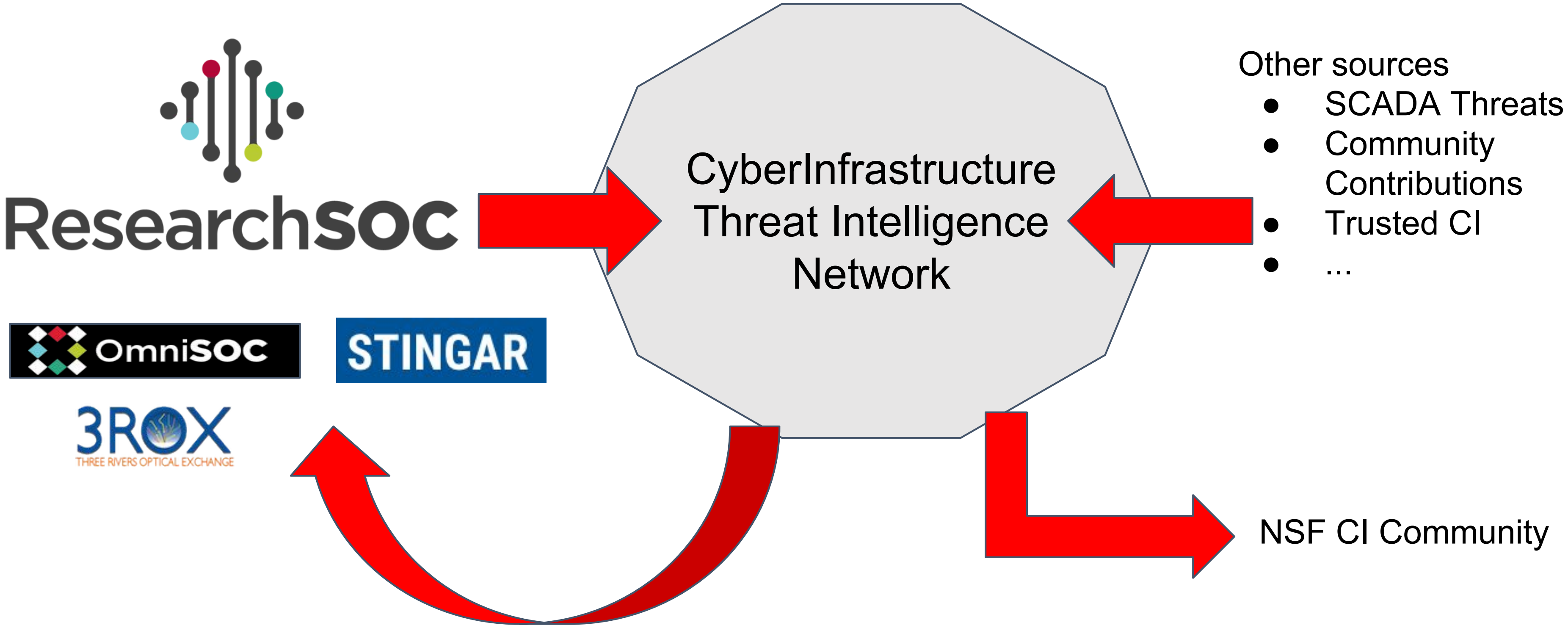
Threat intelligence for higher education

STRINGAR:
Sharing Threat Intelligence for Network Gatekeeping with Automated Response

- Make use of on-premise network sensors (honeypots)
- To identify and block:
  - attackers
  - compromised machines and accounts
- AND share:
  - threat intelligence with ResearchSOC to protect other customers

https://stingar.security.duke.edu/

Building A CI Threat Intelligence Network



CyberInfrastructure Threat Intelligence Network

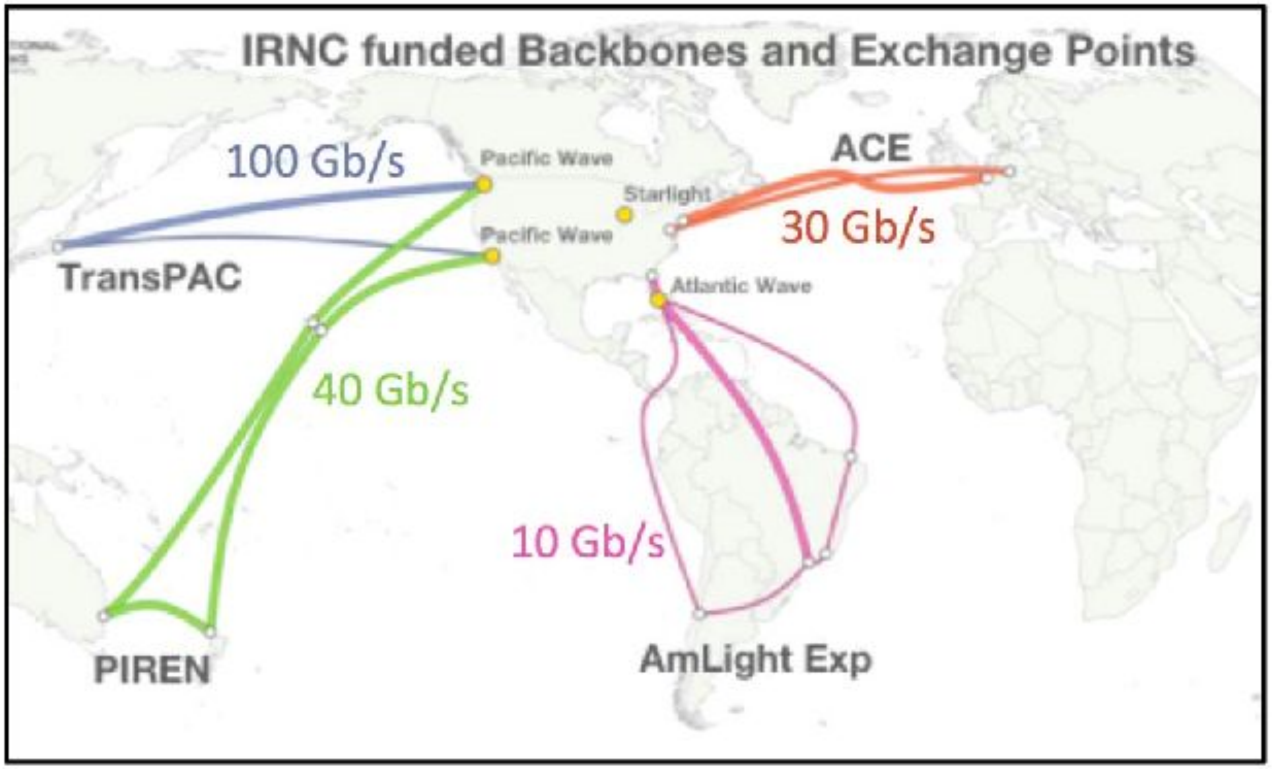
Other sources

- SCADA Threats
- Community Contributions
- Trusted CI
- ...

NSF CI Community

ResearchSOC Approach to Tackle...

Cyberinfrastructure is Highly Collaborative



Alberto Gonzalez, Jason Leigh, Sean Peisert, Brian Tierney, Edward Balas, Predrag Radulovic, Jennifer M. Schopf. 2017 IEEE International Congress on Big Data (BigData Congress) DOI:10.1109/BigDataCongress.2017.51

Engage Intrusion Capabilities By Enabling Research

The **operational data from security operations centers (SOCs) is of great value to cybersecurity research** as it can help with such challenging aspects of cybersecurity as false alarms, dynamic response metrics, and online risk assessment.

In reality, **privacy and security concerns prevent SOCs from sharing their cybersecurity and network data**. Redaction, anonymization, and other similar techniques decrease the utility of the data.

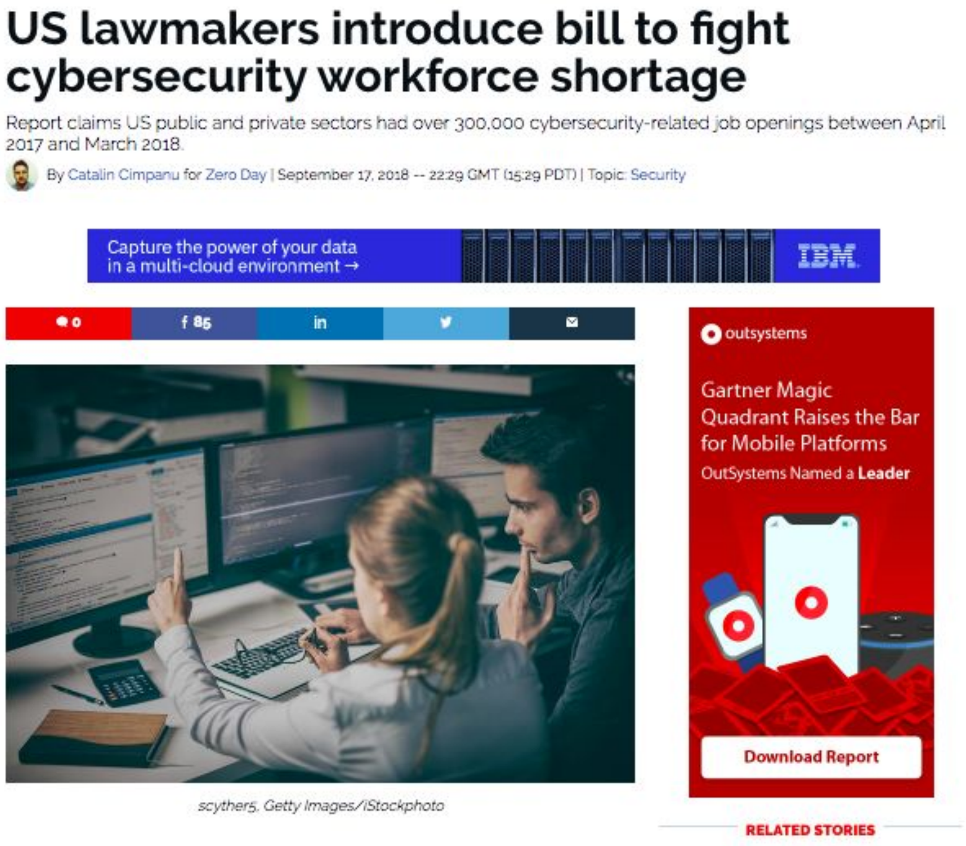
ResearchSOC Strategy

ResearchSOC will apply expertise developed by social, data, and computer scientists within the HathiTrust Research Center to make NSF data available to NSF researchers.

We will: (1) survey the needs of cybersecurity researchers, (2) curate and document the needed data, and (3) build awareness of the data and its potential (i.e., foster papers using the data).

ResearchSOC Approach to Tackle...

Intrusion Detection Requires Specialized Skills



US lawmakers introduce bill to fight cybersecurity workforce shortage

Report claims US public and private sectors had over 300,000 cybersecurity-related job openings between April 2017 and March 2018.

By Catalin Cimpanu for Zero Day | September 17, 2018 -- 22:29 GMT (15:29 PDT) | Topic: Security

scyther5, Getty Images/iStockphoto

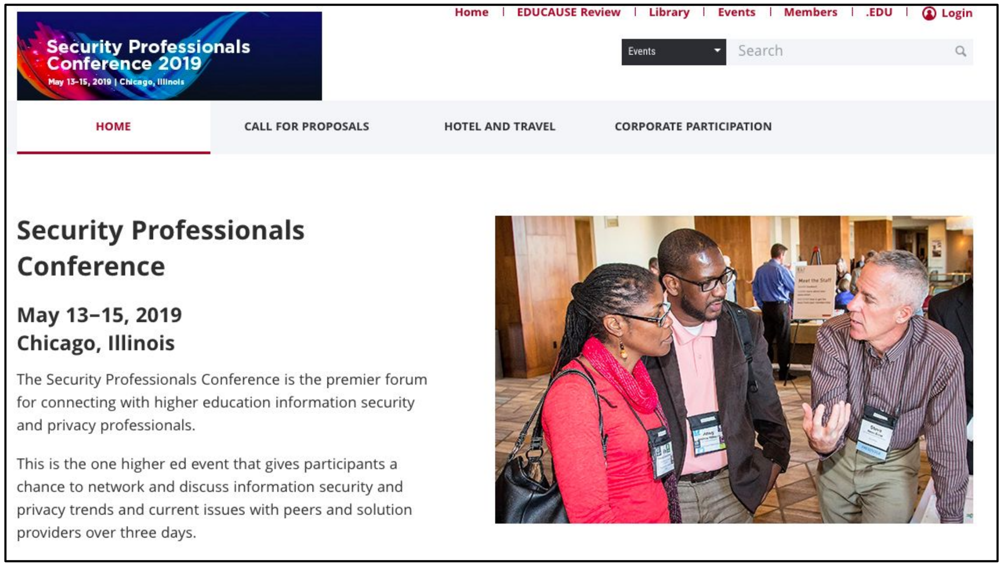
RELATED STORIES

https://www.zdnet.com/article/us-lawmakers-introduce-bill-to-fight-cybersecurity-workforce-shortage/

Approach #1: Enable Higher Education Information Security Offices to Serve Research

College and university information security offices (ISOs) are challenged in their understanding of the specialized needs of research projects.

ResearchSOC will reach out to ISOs to educate them on the motivations and techniques for engaging with and protecting research projects on their campuses.


Home | EDUCAUSE Review | Library | Events | Members | .EDU | Login
Security Professionals Conference 2019
May 13–15, 2019 | Chicago, Illinois
Events
Search
HOME
CALL FOR PROPOSALS
HOTEL AND TRAVEL
CORPORATE PARTICIPATION

Security Professionals Conference

May 13–15, 2019
Chicago, Illinois

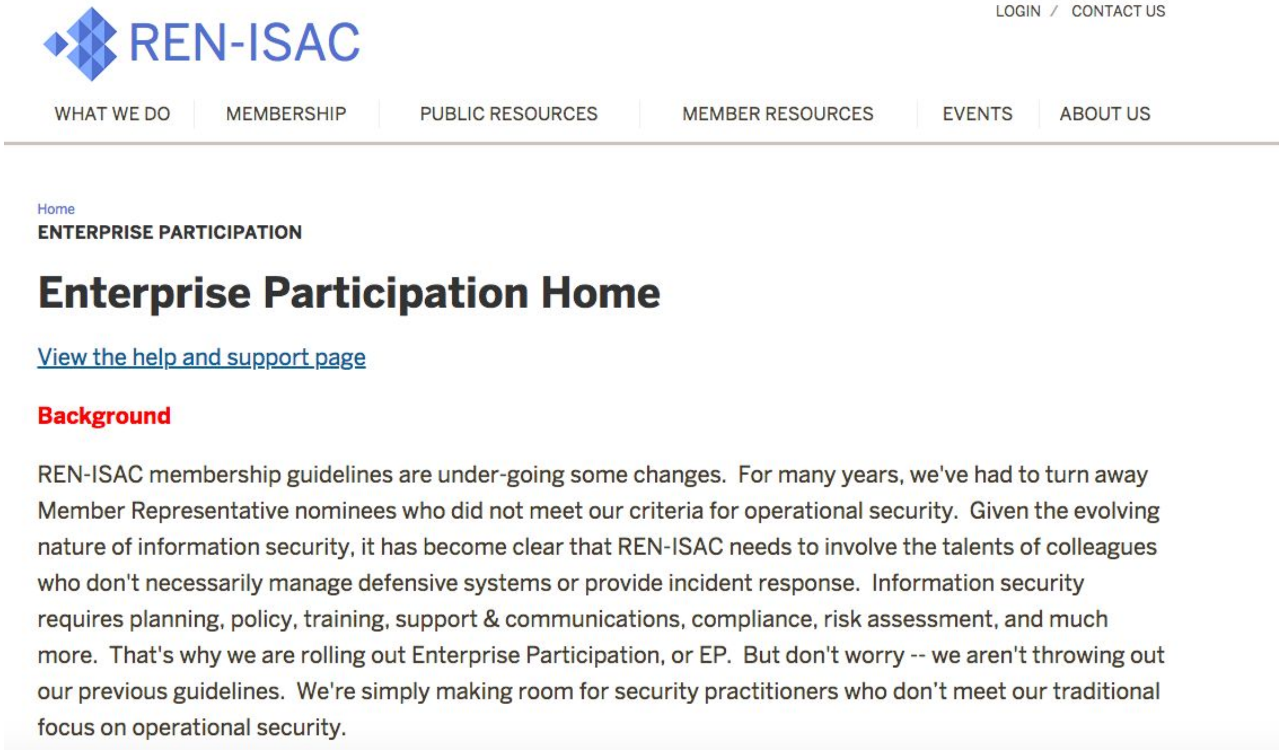
The Security Professionals Conference is the premier forum for connecting with higher education information security and privacy professionals.

This is the one higher ed event that gives participants a chance to network and discuss information security and privacy trends and current issues with peers and solution providers over three days.

https://events.educause.edu/security-professionals-conference/2019

Look for ResearchSOC at EDUCAUSE SPC 2019!

Approach #2: Build a Community of Research Cybersecurity Particitioners



ENTERPRISE PARTICIPATION

Enterprise Participation Home

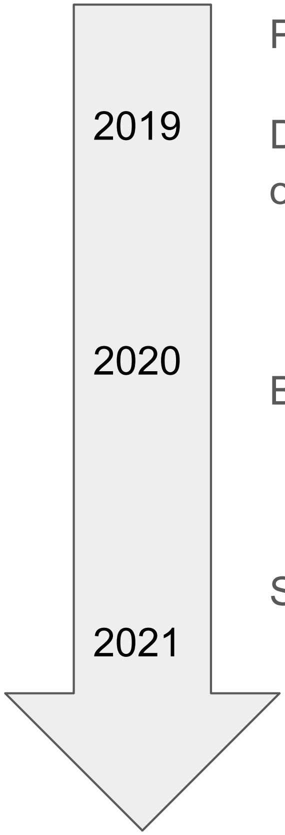
View the help and support page

Background

REN-ISAC membership guidelines are under-going some changes. For many years, we've had to turn away Member Representative nominees who did not meet our criteria for operational security. Given the evolving nature of information security, it has become clear that REN-ISAC needs to involve the talents of colleagues who don't necessarily manage defensive systems or provide incident response. Information security requires planning, policy, training, support & communications, compliance, risk assessment, and much more. That's why we are rolling out Enterprise Participation, or EP. But don't worry -- we aren't throwing out our previous guidelines. We're simply making room for security practitioners who don't meet our traditional focus on operational security.

https://www.ren-isac.net/ep/index.html

Timeline and Initial Clients



Project start

Development of tech and contracts;
outreach to InfoSec and Researchers

Beta Testing

Sustainability and for-fee services

NRAO

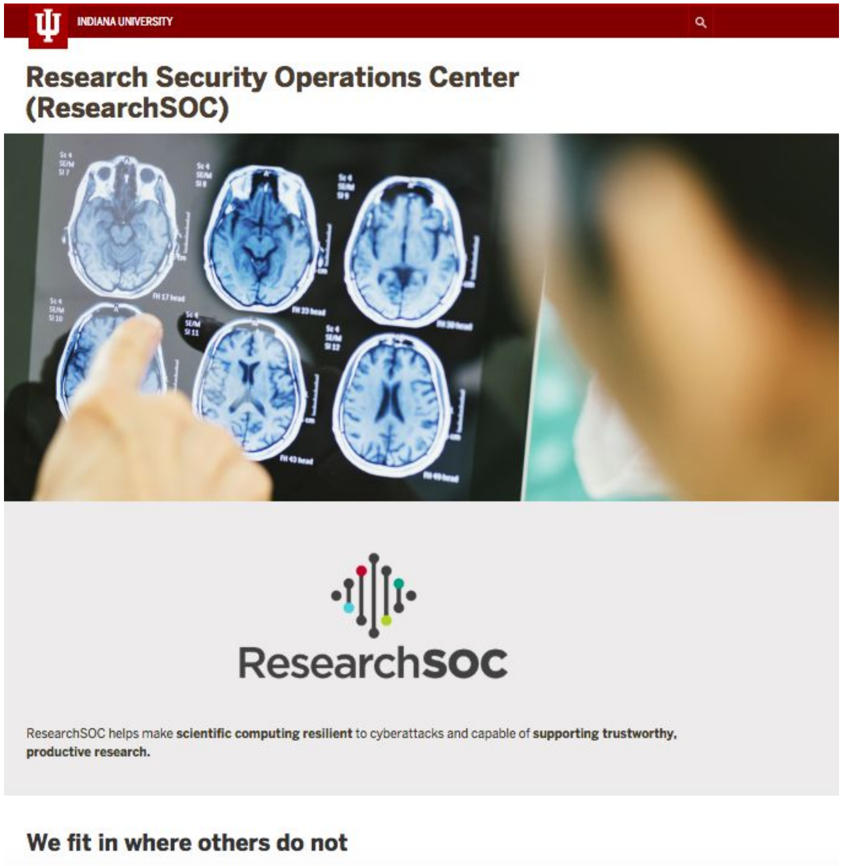
GAGE

UNAVCO

NATIONAL RESOURCE FOR TRANSLATIONAL
AND DEVELOPMENTAL PROTEOMICS

Have opening for one more early adopter.

For More Information



INDIANA UNIVERSITY

Research Security Operations Center (ResearchSOC)

ResearchSOC

ResearchSOC helps make **scientific computing resilient** to cyberattacks and capable of **supporting trustworthy, productive research.**

We fit in where others do not

rsoc@iu.edu

https://researchsoc.iu.edu/

The ResearchSOC is supported by the National Science Foundation under Grant 1840034.

The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.