Information Sharing

Objectives

- Discuss what ISACs are
- Explore information sharing

Sharing is Caring!

- Information sharing is nothing new
- Unfortunately not many like to share
- Why?
  - competition
  - reluctance
  - lack of reciprocation
  - lack of having something to share
- Sharing information helps us take on the bad guys

ISACs

- Information Sharing and Analysis Centers (ISAC) started as a concept in 1998
- Groups of like industries banding together to share information
- Typically share threat information
- Most ISAC’s run 24/7
- Information that is shared is usually highly actionable

Well known ISACs

- FS-ISAC – Financial
- MS-ISAC – US states
- REN-ISAC – Research and Education
- Other industries as well
  - Retail
  - Real Estate
  - Automotive
  - Utilities

REN-ISAC SES

- REN-ISAC anticipates that each member institution can realize value from leveraging SES in some of the following ways:
- To aid in REN-ISAC members incident response process
- To facilitate the sharing of cyber threat intelligence with other REN-ISAC members for operational protection and response
- To aggregate REN-ISAC members observations regarding cyber threat data for the purpose of increasing or decreasing the confidence level/severity of any individual data point within SES
- To facilitate the sharing of cyber threat intelligence with trusted partners for the purpose of threat mitigation and remediation
- To facilitate the sharing of cyber threat intelligence with law enforcement
- To provide feeds of cyber threat data to be used in REN-ISAC members local protections, such as IDS signatures, flow monitoring, and sinkholes

Other sources of information

- Many more information sharing services
- Have I been pwned?
- Shadow server
- Google
- US Cert
- Dorkbot
- Phishtank
- Others

SAFES

- The ability to store events or logs from multiple locations
- Process different types of events
- Process different input sources
- Normalize timestamps and key fields
- Alert on specific data
- Analyze data while combing internal and external data inputs
- Provide historical SAFES alert information