Overview

- Graduate
- Apply for jobs
- Land a new job
- Get direction from your customer
- Do your job (the hands on part)
This job sounds perfect!
Land a new job

<table>
<thead>
<tr>
<th>Company</th>
<th>Three Geoff’s Network Consulting LLC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Title</td>
<td>Senior Network Scientist</td>
</tr>
<tr>
<td>Workcenter</td>
<td>Cyber Situational Awareness Cell</td>
</tr>
<tr>
<td>Job Description</td>
<td>Apply network science techniques and expertise to the Cyber Situational Awareness Cell of a multibillion dollar international corporation</td>
</tr>
</tbody>
</table>

Source: Rutgers.edu

Get direction from your customer

“We have thousands of computers connected all over the world, and we know all about them...but we don’t know how the network is behaving!!!.....HELP!”

Source: Youtube
Do your job

• Collect Netflow data
• Conduct Dynamic Network Analysis
• Gain better Cyber Situational Awareness
Data

- Netflow categorized into:
  1. Autonomic Inflow
     Bytes = 1 – 96, no flags, packets < 3
  2. Human Inflow
     Bytes = 97+, flags = AS/SA, packets >= 3
  3. Autonomic Outflow
     Bytes = 1 – 96, no flags, packets < 2
  4. Human Outflow
     Bytes = 97+, flags = AS/SA, packets >= 2
Collect Netflow Data

1. Go to casos.cs.cmu.edu

2. Click Get More Information

3. Click Reading List

Helpful Information:

- Reading List

4. Login with "si2016"

2016 Summer Institute Participant Portal

Please enter your password below to enter the portal to view our reading list and other information for Summer Institute.

June 13, 2016 - June 18, 2016

Login

Password: 

For questions relating to the 2016 Summer Institute, please email casos@cmu.edu.
Collect Netflow Data

5. Download Netflow samples

- 6.8 Case Study: Netflow Analysis
  - Netflow Samples
    - jun1_samp.csv
    - jun2_samp.csv
    - jun3_samp.csv
    - jun4_samp.csv
    - jun5_samp.csv
    - jun6_samp.csv
    - jun7_samp.csv

6. Unzip all to directory on Desktop
Collect Netflow Data

7. Open Import Wizard and select Table of network links

8. Name the Meta Network
Collect Netflow Data

9. Browse to files

10. Configure input data
Collect Netflow Data

11. Uncheck “Create a dynamic meta-network.”

Understand your data

- Describe your network data:
  - Undirected single mode network
  - Agent by Agent meta network
  - Bipartite graph
  - Flow records per day?
    - ~200,000
  - Links per day?
    - ~130,394
  - Nodes per day?
    - ~22,032
Perform Dynamic Network Analysis

1. Create a dynamic meta-network

```
Meta-Network Manager X
```

2. Fill in Date field

```
<table>
<thead>
<tr>
<th>Meta-Network Name</th>
<th>Date</th>
<th>Import as keyframe?</th>
</tr>
</thead>
<tbody>
<tr>
<td>jan1_samp</td>
<td>2016-06-01T00:00:00Z</td>
<td>✔</td>
</tr>
<tr>
<td>jan2_samp</td>
<td>2016-06-02T00:00:00Z</td>
<td>✔</td>
</tr>
<tr>
<td>jan3_samp</td>
<td>2016-06-03T00:00:00Z</td>
<td>✔</td>
</tr>
<tr>
<td>jan4_samp</td>
<td>2016-06-04T00:00:00Z</td>
<td>✔</td>
</tr>
<tr>
<td>jan5_samp</td>
<td>2016-06-05T00:00:00Z</td>
<td>✔</td>
</tr>
<tr>
<td>jan6_samp</td>
<td>2016-06-06T00:00:00Z</td>
<td>✔</td>
</tr>
<tr>
<td>jan7_samp</td>
<td>2016-06-07T00:00:00Z</td>
<td>✔</td>
</tr>
</tbody>
</table>
Perform Dynamic Network Analysis

3. Click Measure Charts

Perform Dynamic Network Analysis

4. Select the Dynamic Meta Network
Perform Dynamic Network Analysis

5. Select Custom: Density and Network Centralization, Total Degree

6. Add Measure, then view various results
**Gain Cyber SA**

- What could huge increase in Total Degree Centralization mean?
  - Malicious Scanning?
  - Cyber Attack?
  - Systems connecting to external update server?

**More Analysis?**

- Keep library of known nodes and compare against?
- Other measures that could provide better SA?
  - Weighted density?
  - In degree centralization on nodes inside the network?
    - Could identify targeted attacks
- Periodicity? Days of the week, etc