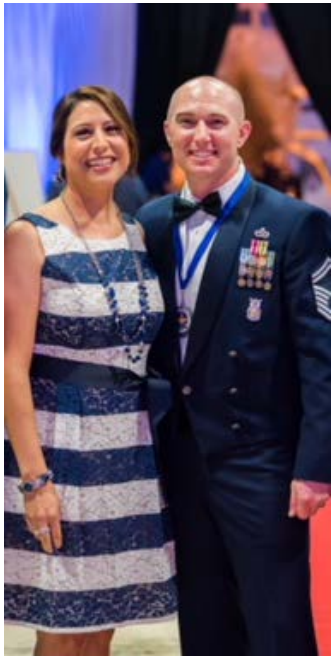
About Me

CISSP® Certified Information Systems Security Professional



CERTIFIED AUTHORIZATION CAP® PROFESSIONAL

INGALLS INFORMATION SECURITY

PROTECT YOUR INFORMATION℠

Future of Cyber Tools

"We are going to have to be able to take information from any platform, any sensor, and connect it at the strategic, operational, and tactical levels to bring effects anywhere on the planet, and I've got to be able to do that in fifteen minutes or less."

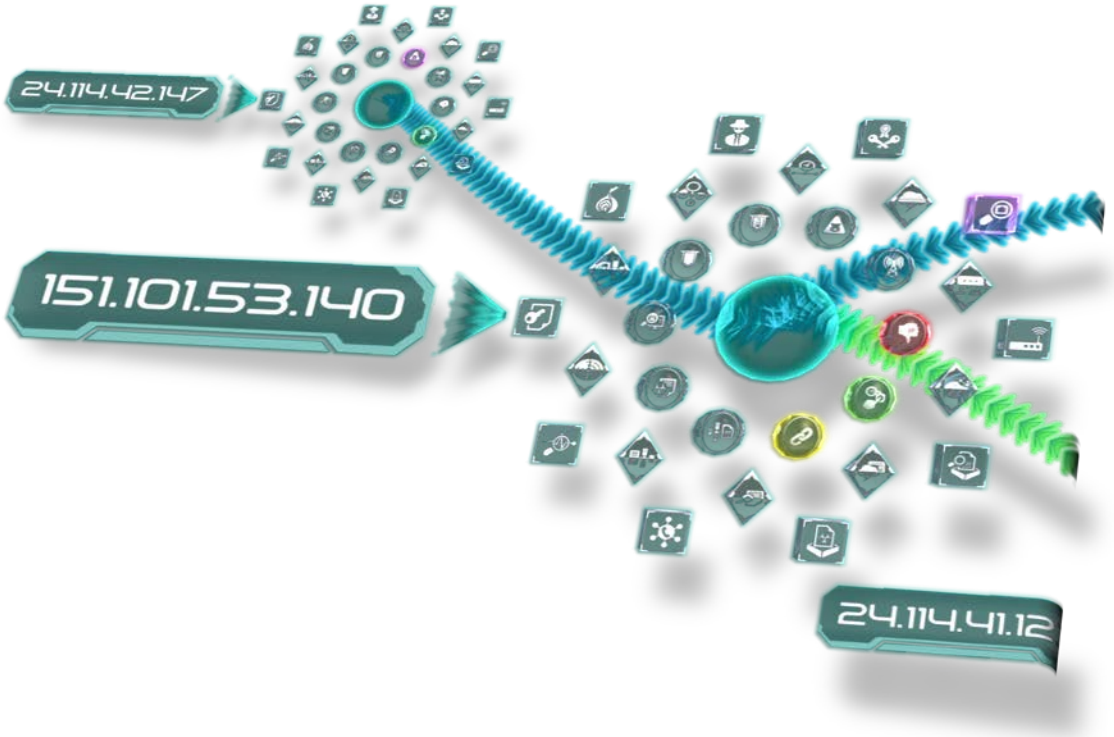
General Steven Wilson, VCSAF
Wright Dialogue with Industry
Dayton, Ohio, 18 July 2018

Solve Limiting Factors

Go From This:

	ClientIP	ClientPort	Duration	Filesize
200"""	10.10.1.253	50505	224 seconds	3510
200"""	10.10.1.253	52125	8 seconds	3653
200"""	10.10.1.253	51218	15 seconds	4680
200"""	10.10.1.253	63264	11 seconds	8048
200"""	10.10.1.253	62725	5 seconds	8048
200"""	10.10.1.253	62268	6 seconds	6694
200"""	10.10.1.253	62223	6 seconds	4295
200"""	10.10.1.253	64513	4 seconds	8048
	10.10.1.253	62000	4 seconds	804

To This (in 3D):

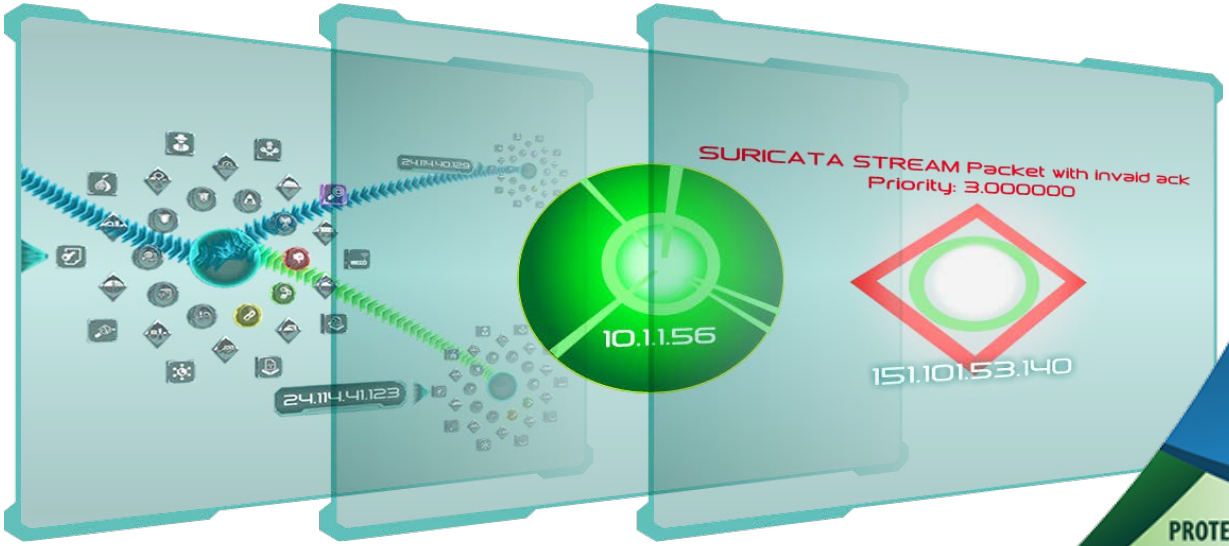


INGALLS INFORMATION SECURITY

PROTECT YOUR INFORMATION℠

Visualize Cybersecurity Data

- Data should have depth of focus:
  - General overview, metrics, and simple relationships can be thought of as a backdrop
  - Relevant information such as search results are better focused and delineated from the background
  - Critical data is presented in a way that is easily consumable
  - Ability to manipulate how data is displayed



INGALLS INFORMATION SECURITY

PROTECT YOUR INFORMATION℠

Augmented Reality

Augmented Reality overlays your vision with computer rendered graphics.

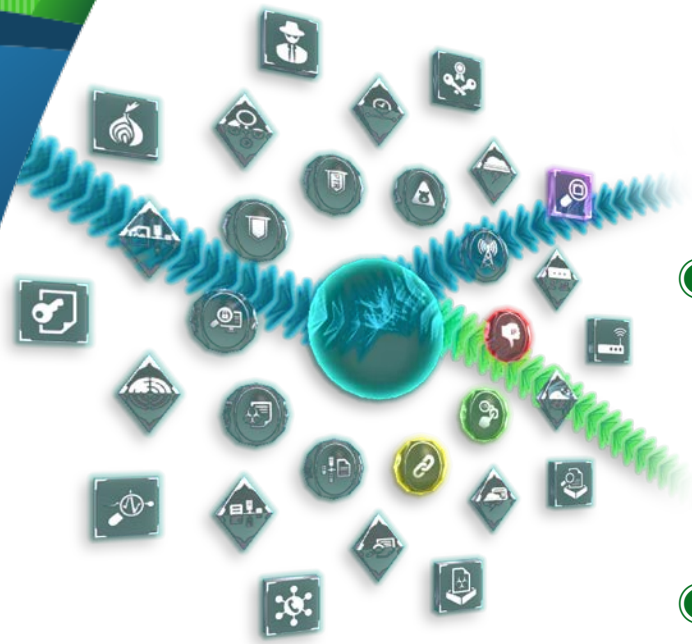
- This allows for many possibilities:
  - Share a single 3D visualization among a group of people (around a conference table, for example)
  - Provide briefings with substantive content in real-time
  - Training, auditing, and other group tasks

Source: getmeta.com

INGALLS INFORMATION SECURITY

PROTECT YOUR INFORMATION℠

Metadata: The Visualization Engine



- Using metadata allows us to:
  - Create situational awareness of the environment
  - Understand basic relationships clearly (client-server, proxy, etc.)
  - Identify patterns
  - Position interesting data to gain context
- Getting metadata is fairly easy:
  - Network events are captured in flow records, IDS, etc.
  - Access logs provide event metadata
  - Endpoint applications
- Storing/retrieving metadata is a challenge with lots of options:
  - NoSQL database clusters provide fast storage and search
  - Hadoop and other analytics platforms

Integrate and Optimize Cyber Ops

- Data visualization allows us to:
  - Provide orders of magnitude of more data in a relationship model
  - Create situational awareness of network states quickly
  - Alert and Identify abnormalities or patterns (draw the user's attention)
  - Reference additional information and overlay it in a given situation
    - Example: systems classified as handling PII, PHI, PCI data can be identified among systems with IDS alerts
- Analyst are able to:
  - Identify intrusions faster
  - Map them out faster
  - Provide Remediation teams with detailed information to clean up intrusions in shorter amounts of time and with less Risk
- Additionally, this technology is able to:
  - Serve as a training aid for entry-level analysts
  - Provide leaders with situational awareness, attacker pathway, and a breach map when dealing with Incident Response

Viewpoint - Objectives

- Allow modeling of security events that have occurred and intrusions that are discovered
- Defenders can cover more network area per Analyst
- Lower the technical barriers of analyst training
- Discuss security events among multi-discipline teams
- https://youtu.be/Lcw30z8I6Ck

INGALLS INFORMATION SECURITY

PROTECT YOUR INFORMATION℠

Questions?

My Contact Information:

Brandi Pickett, CISSP, CAP
SOC Manager/Risk Management Consultant
Brandi.pickett@iinfosec.com
501-515-1026

INGALLS INFORMATION SECURITY

PROTECT YOUR INFORMATION℠