SUPPORTING GREATNESS. DEVELOPING OPPORTUNITIES.

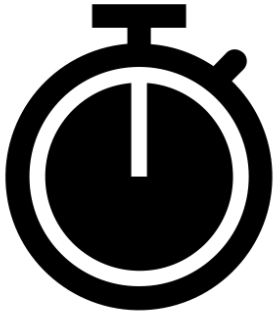
Cybersecurity for Utilities

- Carter Manucy, FMPA

December 10th, 2021

Agenda

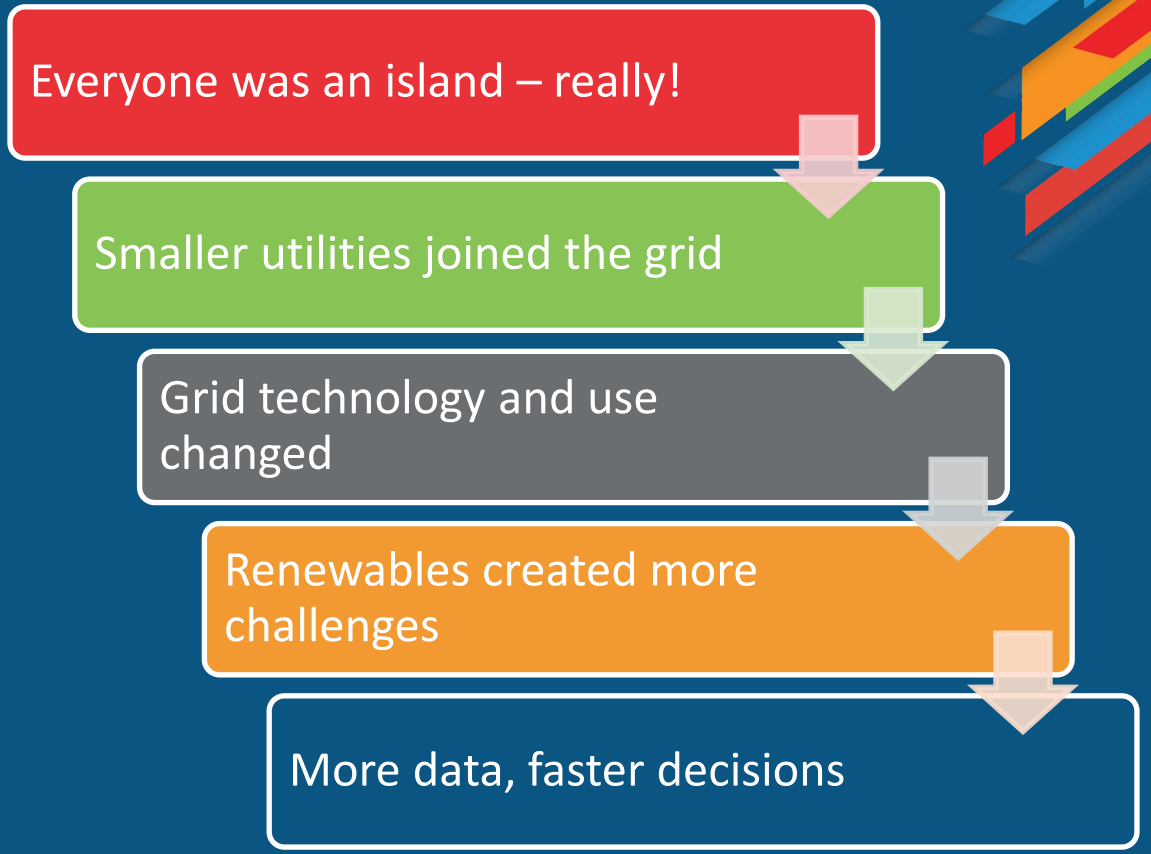
- Who I am
- Utilities and cybersecurity
- Challenges facing utilities
- Tools you can use to help fill gaps
- Funding & other help
- Cyber Mutual Assistance



Introduction

- Proven track record in IT Security
- Designed state-wide secure networks
- Partner with APPA on cybersecurity
- Working with E-ISAC, DOE, National Labs
- Current chair for Cyber Mutual Assistance
- Fight against the bystander effect
- SANS GCIP Certified
- Recipient of APPA Personal Service Award
- NERC RSTC Voting Member (`22)
- Previous NERC CIPC Voting Member
- Former NERC CSSWG chair
- Vice Chair for SERC CIPC, FRCC CIPS

How Did We Get Here?



It’s Not All About OT…

Most threats come from IT

Ransomware and cryptocurrency

New community turned into a business model (RAAS)

More Challenges To Utilities

Staffing

- The great resignation
- Asking existing staff to do more
- Remote access becomes ubiquitous

Lack of visibility (Colonial pipeline!)

- Executive decision leads to shutdown

Secrets of Cybersecurity

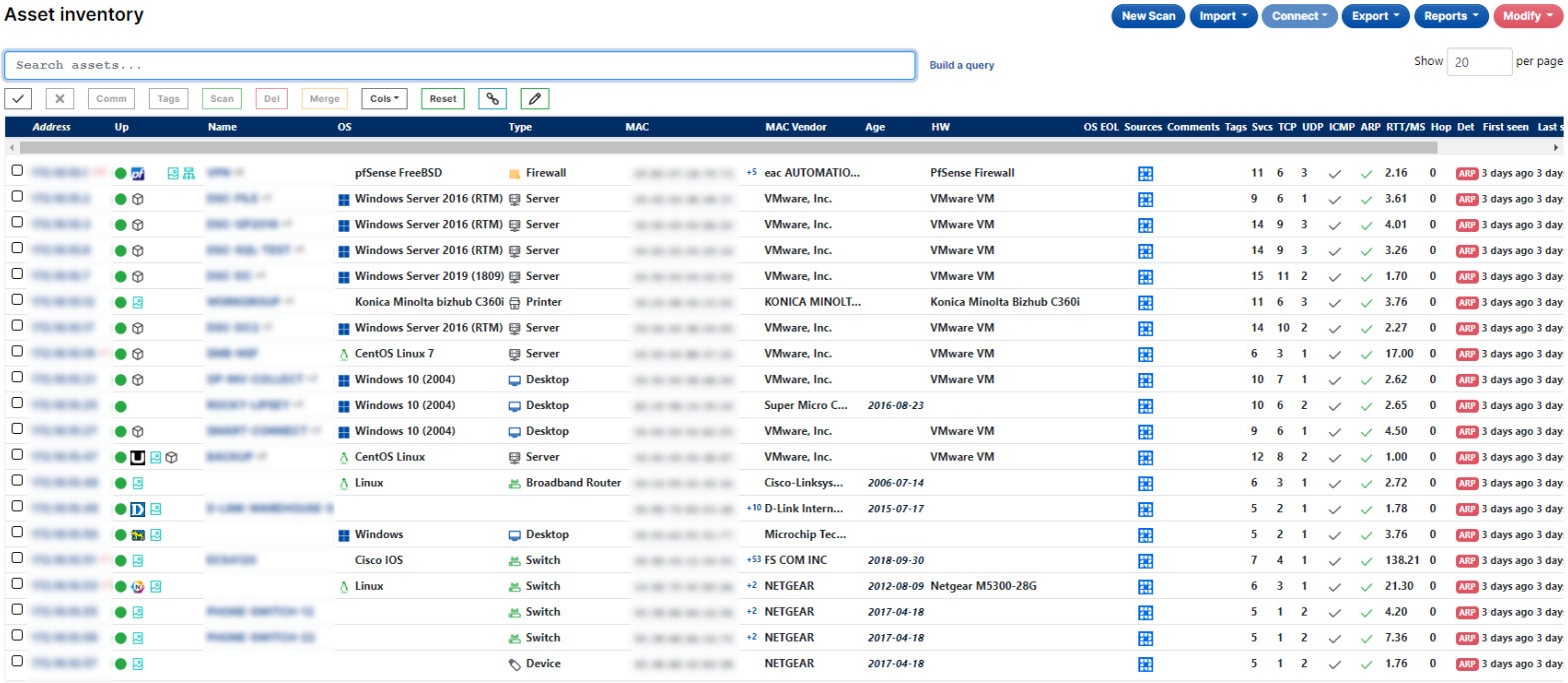
None of this is new

It’s hard to keep up

It takes a lot of time

Free and low cost resources are available

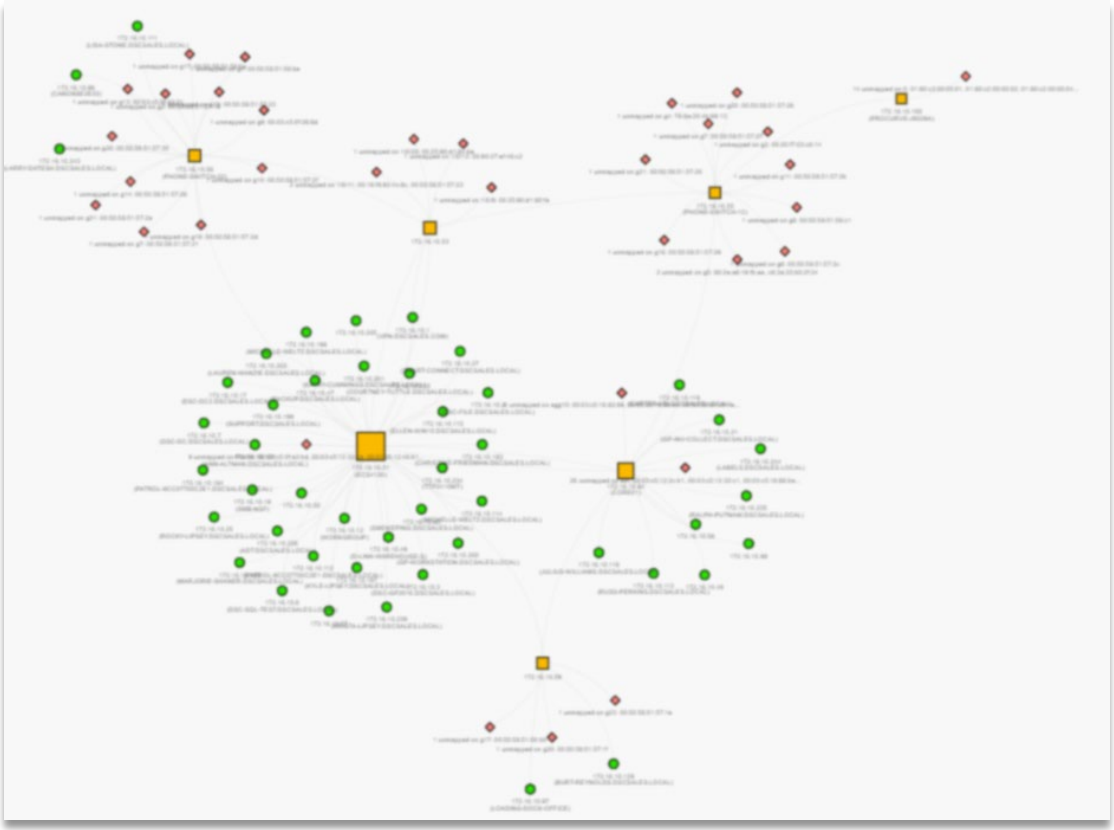
Inventory



Address	Up	Name	OS	Type	MAC	MAC Vendor	Age	HW	OS EOL	Sources	Comments	Tags	Svcs	TCP	UDP	ICMP	ARP	RTT/MS	Hop	Det	First seen	Last s
[redacted]	●	[redacted]	pfSense FreeBSD	Firewall	[redacted]	+5 eac AUTOMATIO...		PfSense Firewall				11	6	3	✓	✓	2.16	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	Windows Server 2016 (RTM)	Server	[redacted]	VMware, Inc.		VMware VM				9	6	1	✓	✓	3.61	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	Windows Server 2016 (RTM)	Server	[redacted]	VMware, Inc.		VMware VM				14	9	3	✓	✓	4.01	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	Windows Server 2016 (RTM)	Server	[redacted]	VMware, Inc.		VMware VM				14	9	3	✓	✓	3.26	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	Windows Server 2019 (1809)	Server	[redacted]	VMware, Inc.		VMware VM				15	11	2	✓	✓	1.70	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	Konica Minolta bizhub C360i	Printer	[redacted]	KONICA MINOLT...		Konica Minolta Bizhub C360i				11	6	3	✓	✓	3.76	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	Windows Server 2016 (RTM)	Server	[redacted]	VMware, Inc.		VMware VM				14	10	2	✓	✓	2.27	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	CentOS Linux 7	Server	[redacted]	VMware, Inc.		VMware VM				6	3	1	✓	✓	17.00	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	Windows 10 (2004)	Desktop	[redacted]	VMware, Inc.		VMware VM				10	7	1	✓	✓	2.62	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	Windows 10 (2004)	Desktop	[redacted]	Super Micro C...	2016-08-23					10	6	2	✓	✓	2.65	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	Windows 10 (2004)	Desktop	[redacted]	VMware, Inc.		VMware VM				9	6	1	✓	✓	4.50	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	CentOS Linux	Server	[redacted]	VMware, Inc.		VMware VM				12	8	2	✓	✓	1.00	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	Linux	Broadband Router	[redacted]	Cisco-Linksys...	2006-07-14					6	3	1	✓	✓	2.72	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]			[redacted]	+10 D-Link Intern...	2015-07-17					5	2	1	✓	✓	1.78	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	Windows	Desktop	[redacted]	Microchip Tec...						5	2	1	✓	✓	3.76	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	Cisco IOS	Switch	[redacted]	+53 FS COM INC	2018-09-30					7	4	1	✓	✓	138.21	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]	Linux	Switch	[redacted]	+2 NETGEAR	2012-08-09	Netgear M5300-28G				6	3	1	✓	✓	21.30	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]		Switch	[redacted]	+2 NETGEAR	2017-04-18					5	1	2	✓	✓	4.20	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]		Switch	[redacted]	+2 NETGEAR	2017-04-18					5	1	2	✓	✓	7.36	0	ARP	3 days ago	3 day
[redacted]	●	[redacted]		Device	[redacted]	NETGEAR	2017-04-18					5	1	2	✓	✓	1.76	0	ARP	3 days ago	3 day

https://Rumble.Run

Inventory



https://Rumble.Run

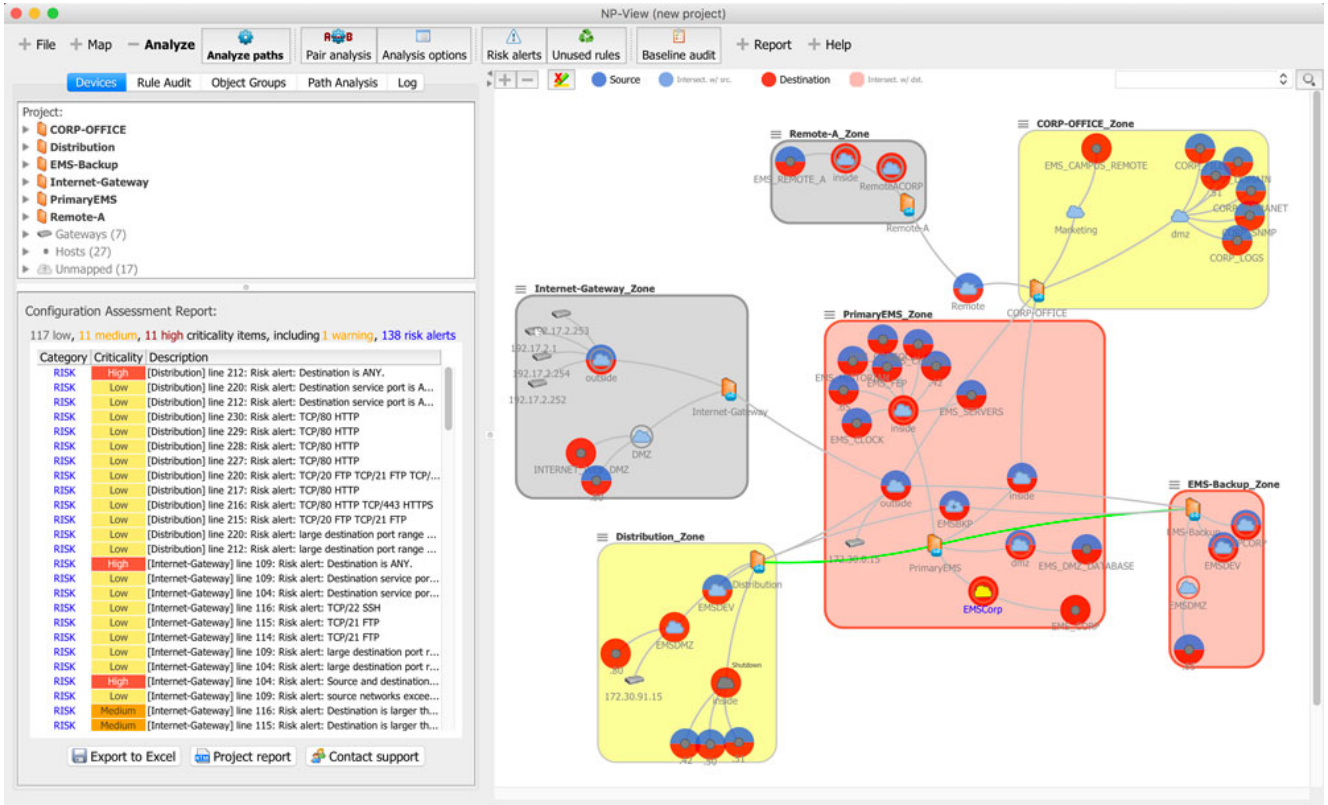
Know your limits!

Don’t run “IT Tools” on OT systems

- What hasn’t changed?
- What are we working around?
- New employees: What don’t you like?
- What are your customers saying?

Computers don’t have sell-by dates

Network Security



[NP-View]

Remote Access

One of the biggest risks to your organization

Please use a VPN (and a good one at that)

Oldsmar
-> TeamViewer

Getting Help – The NSC 100 Day Plan

- Who is the ESCC?
- Dragos Neighborhood Keeper
-NRECA's Essence
- Funding & Grant opportunities

Funding

- IOU’s vs Municipals
- DOE CEDS Grants
- Infrastructure Investment and Jobs Act- $1.3B for Cybersecurity Grant Program

Risk Reduction

Training

- Phishing
- Exercises
  - Be prepared!

Exercises

- CISA Table Top Exercise Package
- GridEx
- NUARI
- MS-ISAC (CIS)

CMA (Cyber Mutual Assistance)

- ✓ Typically “no-notice”
- ✓ No clear beginning and end
- ✓ Not geographically bounded

“Am I next? Am I ready to respond?”

TRADITIONAL MUTUAL AID

Types of Assistance

- Short-term advisory assistance, including services, personnel, and/or equipment.
- Assistance can be provided remotely and when:
  - Significant threats or critical system vulnerabilities have been identified
  - A cyber incident causes the disruption of electric or natural gas service

CMA PROGRAM STATISTICS

- Approximately:
  - **80%** of US electricity customers
  - **80%** of US domestic natural gas customers
  - **1.25 million** electricity customers in Canada

- **175** Participating Entities in the US & Canada:
  - Public Power
  - Federal Entities
  - Cooperatives
  - Investor-owned
  - RTOs/ISOs

Proxies

- Not all organizations have the resources to fully participate in all meetings
- Proxies can be designated to represent other utilities
- Proxies must already have an NDA in place
- Proxies do not make commitments on behalf of the entity but help establish quorum

How to Participate

The CMA Program is open to electric and natural gas companies

Participation is covered by a non-disclosure agreement, and is voluntary and confidential

To join, or for more information:

- **Website** www.electricitysubsector.org/cma
- **Email** cma@electricitysubsector.org

Action Plan

1. Get a checkup
2. Exercise!
3. Talk to people who understand your business model to make sure solutions are right-sized for your utility
4. Get involved with CMA
5. Work with your JAA to see what kind of member services or joint action opportunities exist!

Contact Information

Carter Manucy
IT/OT & Cybersecurity Director
Florida Municipal Power Agency
Carter.Manucy@fmpa.com
321-239-1032

ECG
ECOGA.ORG