FMEA CONNECTIONS WORKSHOP

Cybersecurity for Utilities

CARTER MANUCY & PATRICK MILLER

Introduction

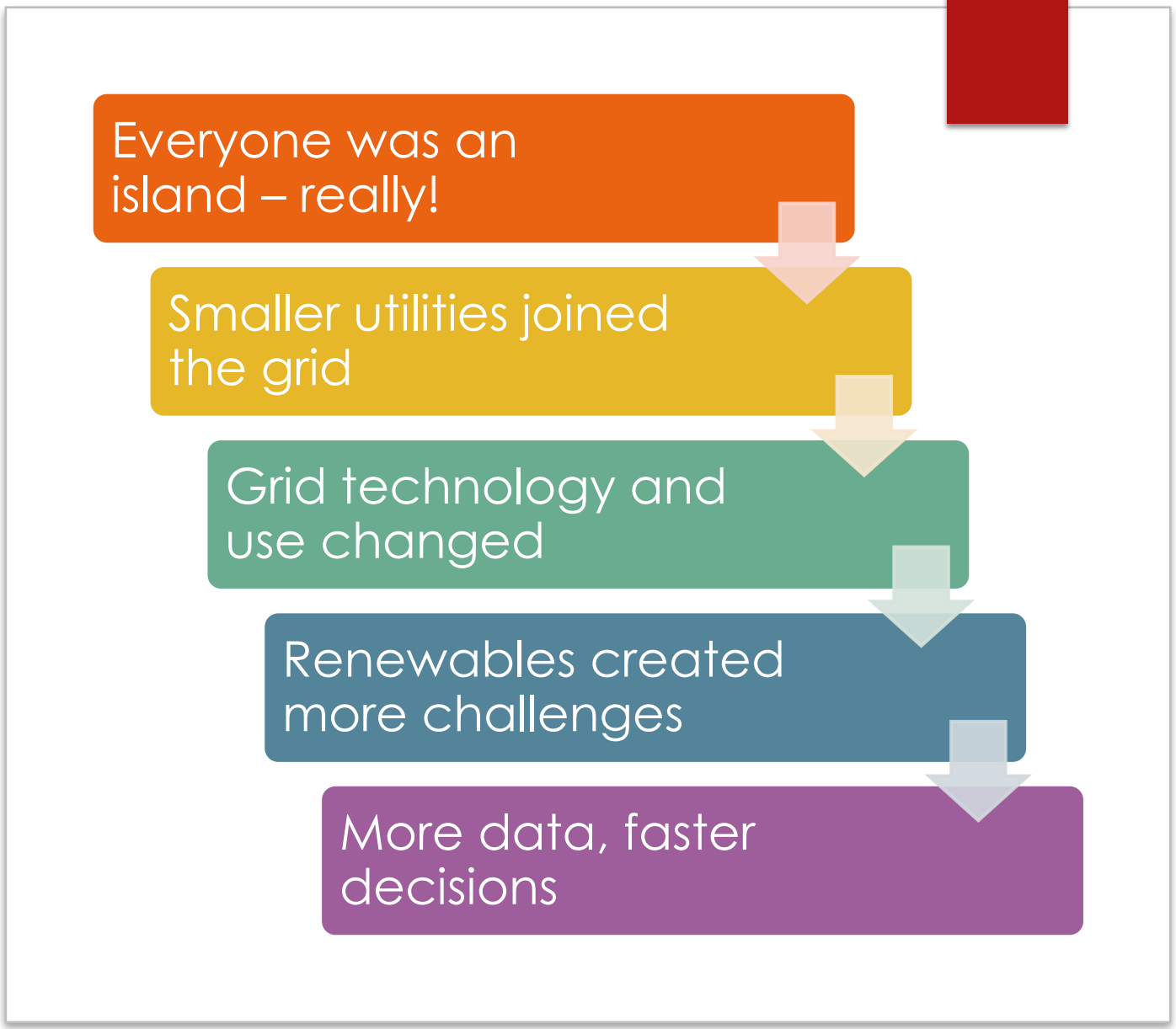
- Proven track record in IT Security
- NERC CIP experience - NERC CIPC, CSSWG, FRCC & SERC
- SANS GCIP Certified
- Designed state-wide secure networks
- Working with APPA
- Working with E-ISAC, DOE
- Current chair for Cyber Mutual Assistance

IT vs OT

- IT priorities
  - Confidentiality
  - Integrity
  - Availability

- OT priorities
  - Availability (and safety)
  - Integrity
  - Confidentiality

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

Cybersecurity for Utilities

FMEA Connections Workshop – November 3 2021

INTRODUCTION

- Former utility staff (telecommunications, water & electric)
- First NERC CIP auditor in the US
- Drafter of NERC CIP standards and formal interpretations
- NERC CIP Supply Chain Working Group contributor
- Former Principal Investigator US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, Director and President Emeritus
- Centro de Ciberseguridad Industrial (CCI) US Coordinator
- Cybersecurity Advisory Team for State Solar, NARUC/NASEO
- Advisor to multiple industrial security product vendors
- GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP

THE HORSESHOE NAIL

- Small doesn’t mean lower probability target
- You will be automatically scanned/hacked if vulnerable
- Your resources (data, bandwidth, CPU cycles) = $$$
- Smaller is perceived as less security (easier to hack)
  - 43% of cyberattacks are aimed at small companies
  - Only 14% are prepared to defend themselves
  - 50% - 70% of all ransomware attacks are directed at small companies
- Launch point to larger targets
  - Connectivity
  - Trust relationships

WHAT WORKS?

- Do the “Top Ten” and reduce your risk by 80% or more
- Too many security products to track
- Too many frameworks to follow
- What works in the real world – your Muni world?
- Scientifically proven – ITPI, empirical results
- Operationally proven – CISA, INL, DOE, NERC
- Real world – 35+ years of experience
- You don’t have to eat the whole elephant at once

1. ASSET INVENTORY

- Not everything, but at least the important stuff
- If you don’t know what you have, you can’t protect it
- All the other key control areas are based on this
- Start with simple baseline elements
  - Make/model
  - Network and/or or host address
  - OS and/or firmware
  - All other software installed
  - Listening Ports (services)
  - Patches (or patch state; vulnerability)

2. PHASE OUT FRAGILE SYSTEMS

- Legacy systems
- Custom systems
- Unique systems
- That one “application” written by 3 engineers
- Brittle hardware
- Borrowed IT used as OT
- Applications that don’t play nice in the tech sandbox
- Applications that are the hardest to update
- Standardization will lower costs/risk and improve uptime

3. ARCHITECT FOR DEFENSE

- You should at least have a firewall between IT/OT
- Specific points for detection and visibility
  - Network boundary
  - Each network segment
  - Critical systems
  - Administrative & engineering systems
- Dependencies on outside systems
- Dependencies on outside business processes
- Intelligent islanding, shear-away networks & “turtle mode”

4. REMOTE ACCESS

- Is anything connected directly to the Internet?
- Remote administration
- Remote operations
- Vendor support
- Consider using a jump host
- Multi-factor authentication
- Monitor and alert

5. RESTRICT ACCESS

- Change all default accounts/passwords
- Unique user accounts wherever you can
- Eliminate shared accounts if possible
  - Where you can’t, track who has them
- Principle of least privilege
- Fewest administrator accounts/groups
- Different credentials for OT AD and IT AD
- Remove access ASAP for shared and unique users
- Use LONG passwords, not complex

6. VULNERABILITY MANAGEMENT

- Insecure by design
- First-to-market
- Patching vs. vulnerabilities
- Zero-days, forever-days
- Patching priority: perimeter first, then work inward
- Vulnerability “scanners”
  - Passive vs. active
- Role of configuration management

7. CONTROL CHANGE

- Best defense against both accidents and malice…
- Establish a change control/review board
- Prepare for backing out any change
- Record all changes through baseline tracking
- Test changes, whenever/wherever possible

8. MONITOR

- Monitor as much as you possibly can
- Network monitoring
- System monitoring
- SIEM tools
  - Tuning
  - Monitoring and alerts
  - False positives
  - Integration with other tools
- OT-specific tools exist
- Can integrate with enterprise (most attacks start w/ IT)
- Neighborhood Keeper

9. KEEP IT SIMPLE

- Don’t over-buy security technologies
- Train your staff
- Complexity is the enemy of security
- Fewer places for attackers (or problems) to hide
- Reduces attack surface area
- Less expensive through volume purchase
- Easier on supply chain risk

10. RESPONSE AND RECOVERY

- Write down an Incident Response Plan (IRP)
- Keep it simple – something you can follow
- Public Power Incident Response Play Book
- Paper or table-top exercises
- NERC GridEx
- Cyber Mutual Assistance (CMA)
- Practice like it’s game day
- Are you sure you can recover?
- Have you actually tried to do it?

BONUS - REGULATION

- Compliance does not equal security
- Often necessary to establish a minimum bar
- Yes, hackers are faster than laws
- You can prescribe action, but not attitude
- “Transient Regulation”
  - Executive Orders
  - National Security Memorandum
  - Insurance
  - Contracts

BONUS - FRAMEWORKS & METRICS

- Where do you start? Is there a playbook?
- Pick one, apply it, and measure to it
- Perfection is the enemy of the good
- Most don’t need a gap assessment
  - Attach to existing initiatives, fold in more over time
- Suggest NIST-800-53 and 800-82
  - Fits within NIST Cyber Security Framework
  - Companion to ES-C2M2 (Cybersecurity Capability Maturity Model)
  - Will likely be the US standard for all critical infrastructure(s)
- Consistent measurement to demonstrate progress

BONUS – PEOPLE

- What if you installed 20 new security cameras and no one was watching them?
- Best tool in unskilled hands is a false sense of security
- Break down HR barriers
  - Entry level security talent
  - Higher rates for specific cyber skills or management
- Become a training path & be ok with them leaving
- Encourage conferences and networking for wide relationship connections

SUMMARY – PROVEN TO WORK

- Asset Inventory
- Phase out fragile systems
- Build a network you can defend
- Lock down all remote access
- Restrict user access
- Manage vulnerabilities and patches
- Change control and configuration management
- Monitor as much as possible
- Simplify: fewer security tools, less complexity in systems
- Practice response and recovery like it’s game day

CONTACT ME


@PATRICKCMILLER


LINKEDIN.COM/IN/MILLERPATRICKC


PMILLER@AMPERESEC.COM


WWW.AMPERESEC.COM


+15032721414

Secrets of Cybersecurity

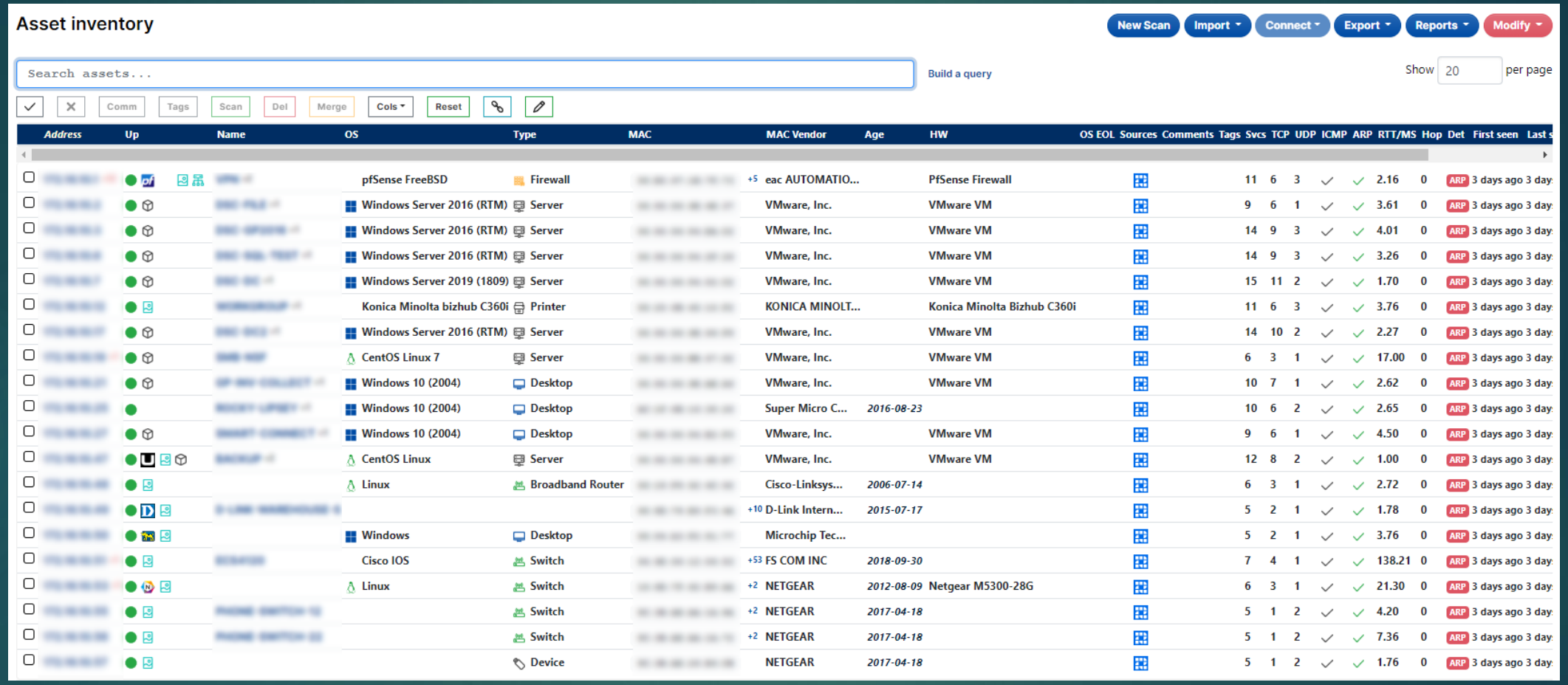
None of this is new

It's hard to keep up

It takes a lot of time

Free and low cost resources are available

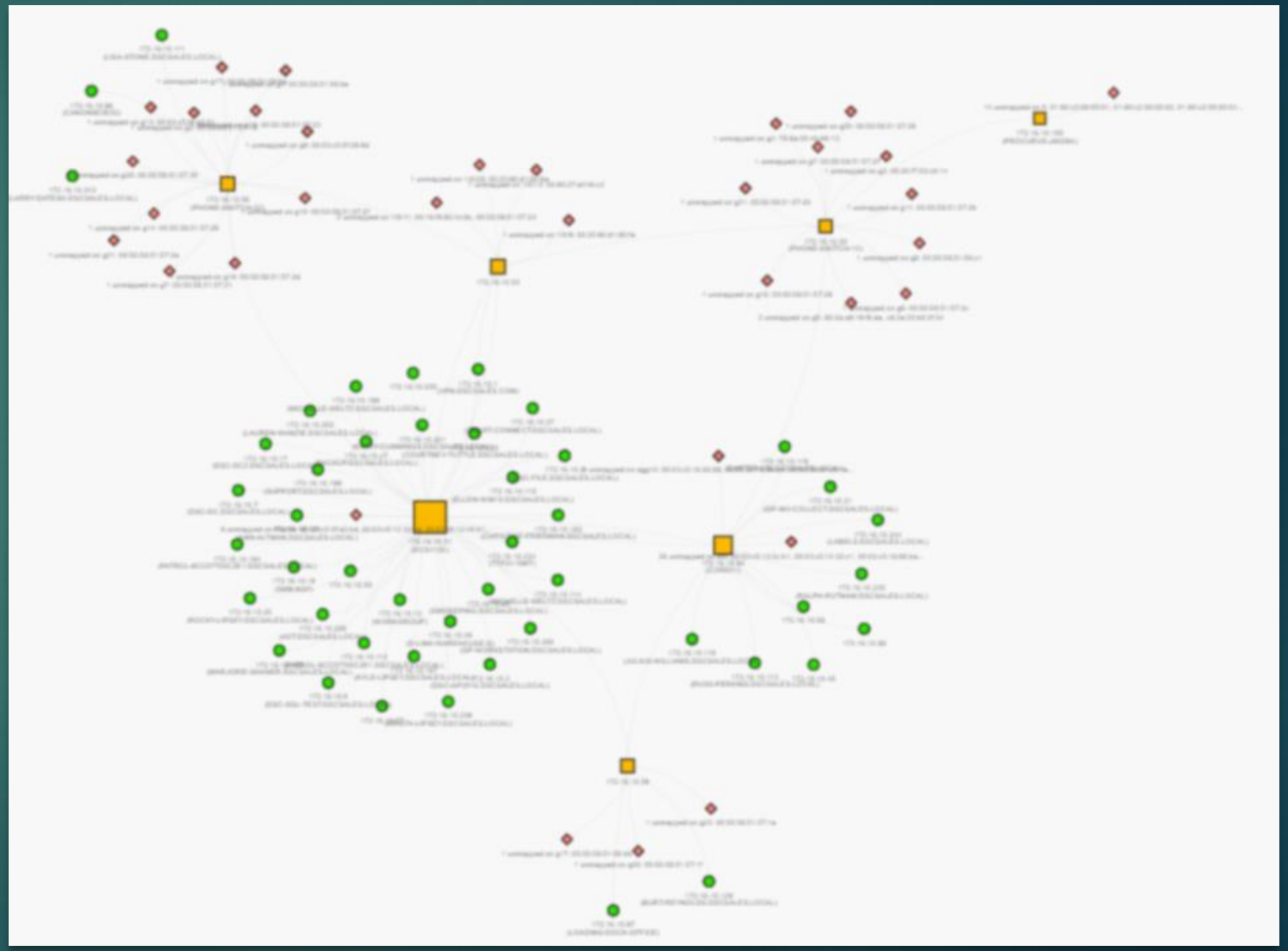
Inventory



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

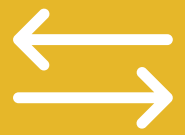
Inventory



https://Rumble.Run

Know your limits!

Don't run "IT Tools" on OT systems

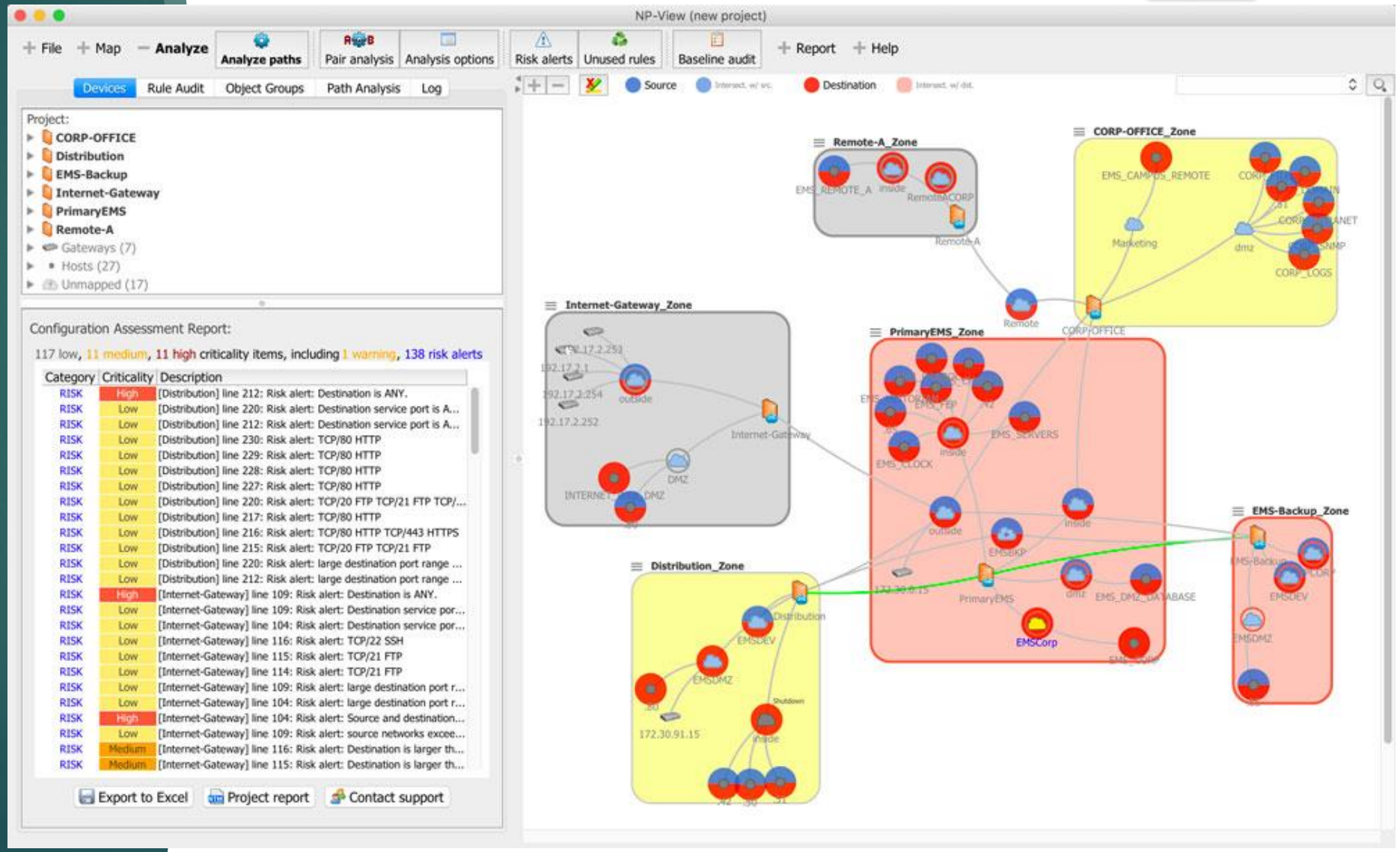


- What hasn't changed?
- What are we working around?
- New employees: what don't you like?
- What are your customers complaining about?

Computers don't have sell-by dates

Network Security

- No shortcuts ;(
- NP-View



Remote Access

One of the biggest risks to your organization

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

Oldsmar
-> TeamViewer

Vulnerability Management

Patching philosophies

- Now: drop everything, this is bad
- Never: doesn't apply to us or our systems
- Next: important, plan for it

Assessment tools (Qualys, Tenable)

- Point-in time
- Should be repeated on a periodic basis

100 Day Plan

- ESCC
- Dragos Neighborhood Keeper
- NRECA's Essence
- Funding

Funding

- IOU's vs Municipals
- DOE CEDS Grants
- INVEST Act - $1.86B (?)

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

PROGRAM STATISTICS

- **174** Participating Entities in the US & Canada:
  - Public Power
  - Federal Entities
  - Cooperatives
  - Investor-owned
  - RTOs/ISOs
- Approximately:
  - **80%** of US electricity customers
  - **80%** of US domestic natural gas customers
  - **1.25 million** electricity customers in Canada

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!