Defending Energy Coops

Against Advanced Threat Actors

What are we going to talk about?

- The threat to rural and municipal grids from advanced threat actors (APTs)
- The motivations and tactics of APTs in the coop space
- How energy coops can defend against APTs in ways that are both cost effective and practical

But, before we do that…

A Little Background

Who are these guys?

- JJ Cummings – Intelligence Operations, Americas
- Joe Marshall – Outreach ICS/SCADA Systems

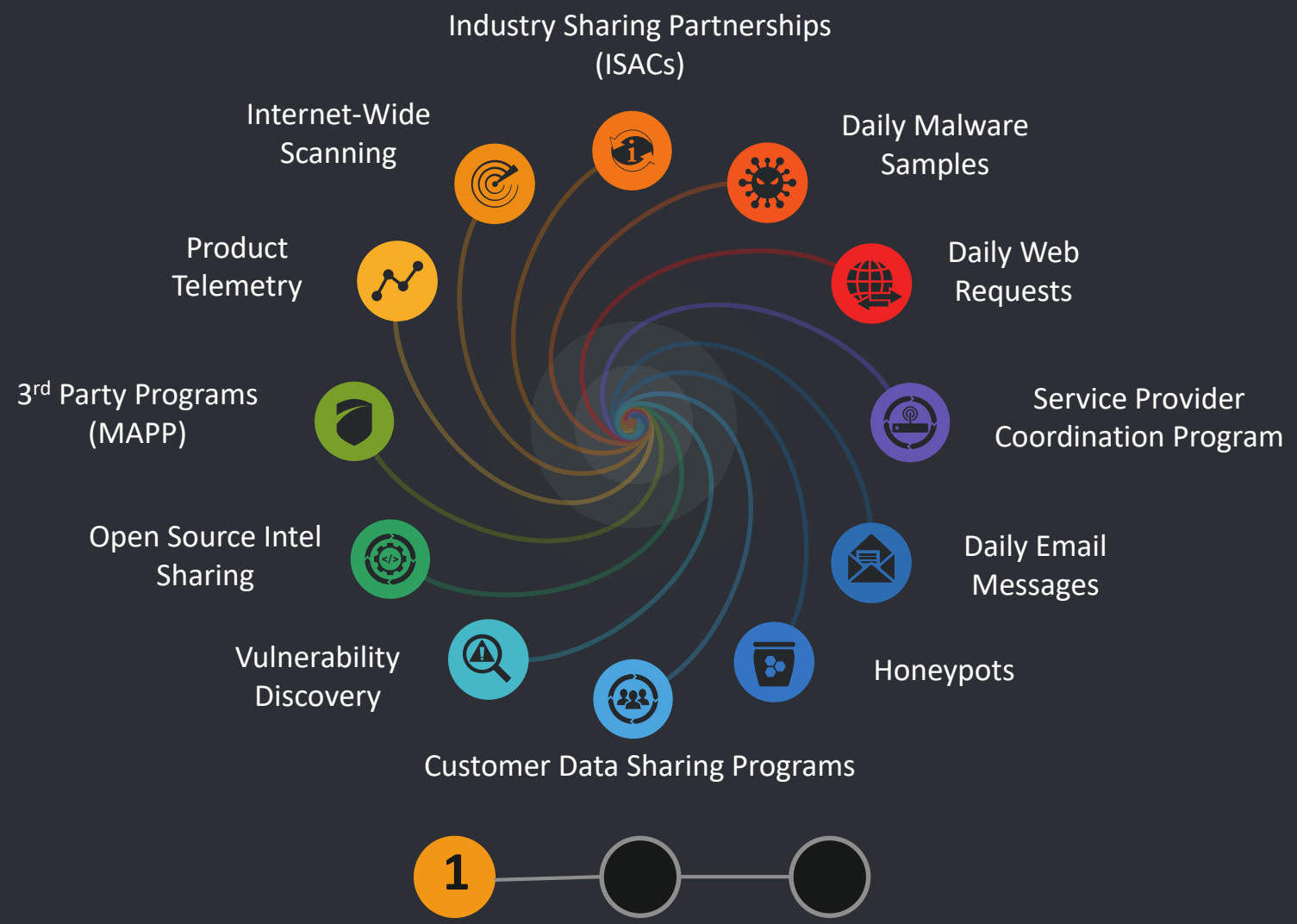
What is Talos?

Cisco’s Threat Intelligence Arm

We do a lot of things, but what is most relevant for today?

Spoiler Alert: We don’t do sales…

Threat Intelligence



Threat Data Cycle

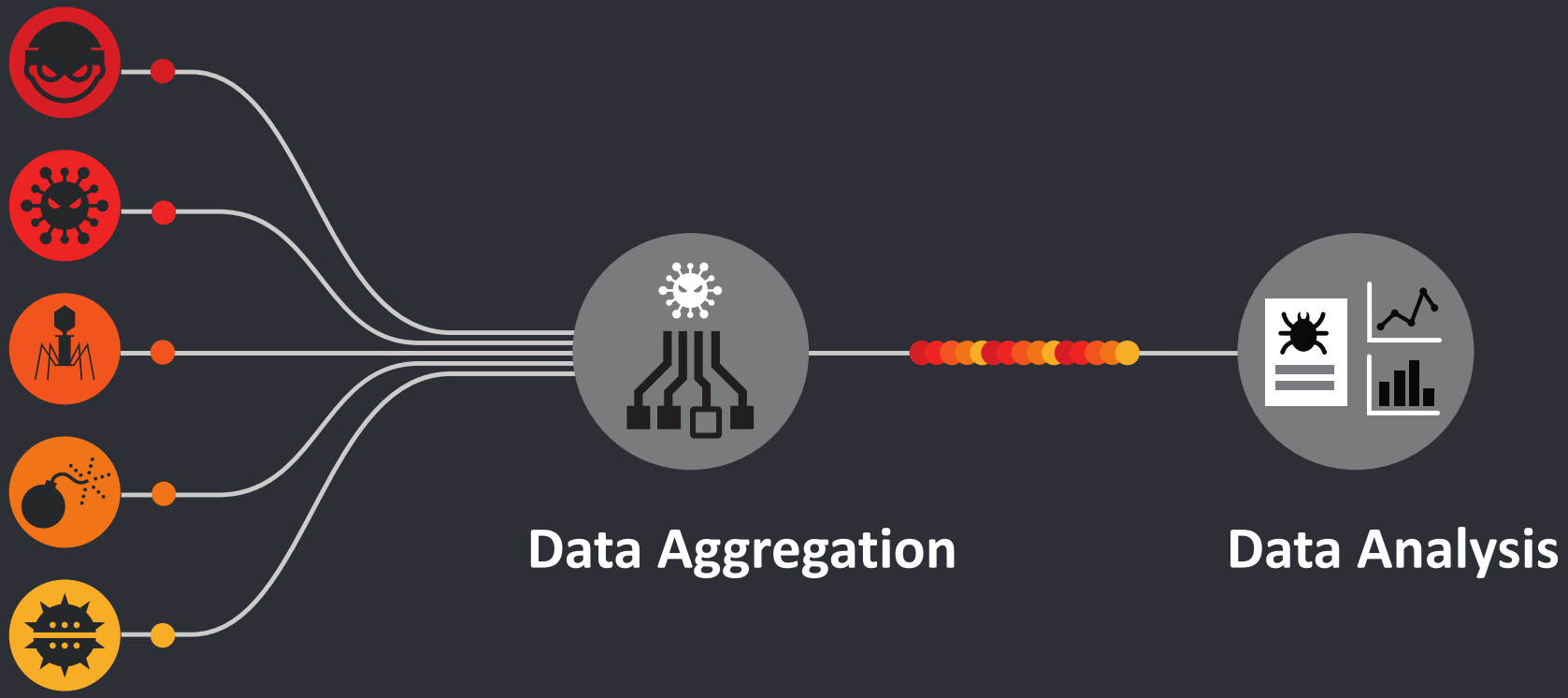
Talos pulls threat data from Cisco's telemetry, customer feedback, industry partnerships, and many other sources.

TALOS

Threat Intelligence

Threat Data

- Email Samples
- Web Samples
- Malware Samples

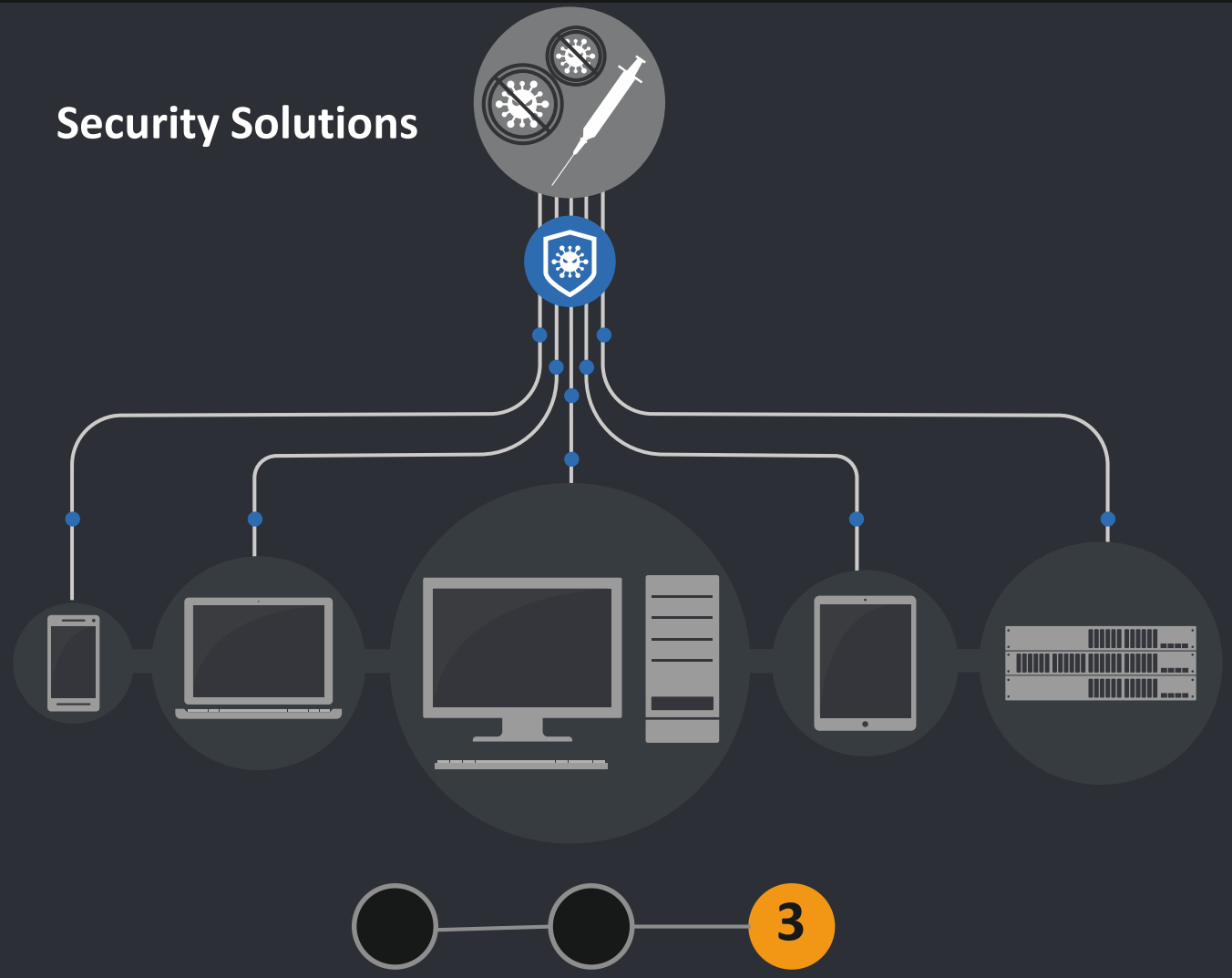


Threat data is aggregated and analyzed. Analysis of false negatives and false positives.

Threat Data Cycle

TALOS

Threat Intelligence



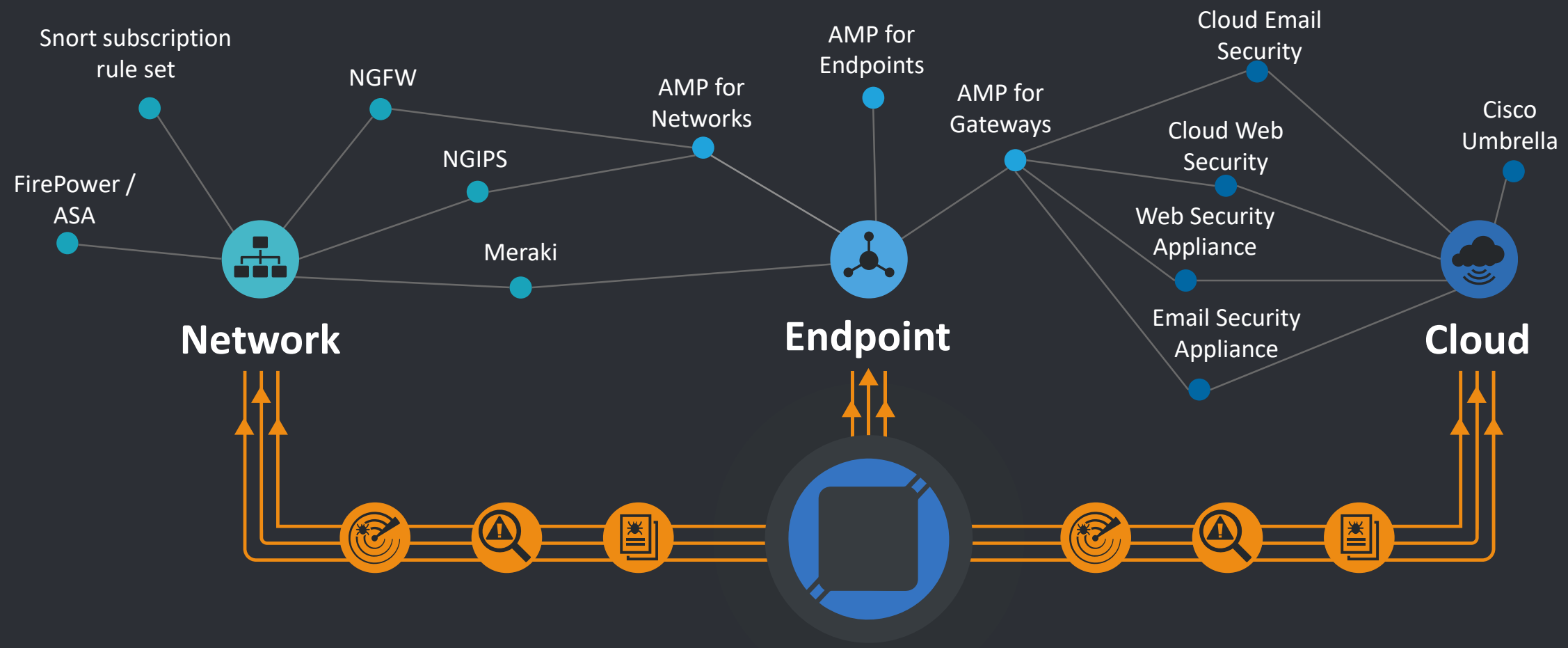
Threat Data Cycle

Security solutions are developed to prevent and address threats. These solutions and updates are pulled down by Cisco Security products.

TALOS

Threat Intelligence

The Backbone of Cisco Security



Talos creates the threat detection content in all Cisco Security products, providing customers with comprehensive solutions from cloud to core.

TALOS

What's the Bottom Line?

Our daily work gives us unique visibility into advanced cyber threats around the globe

Which is what brings us here today…

TALOS

The Threat: Nation-State APTs (Apex Predators)

- Time is on their side
- Resources are vast (but not limitless)
- Advanced capabilities (but only use *just enough* to achieve their objectives)

We've been tracking this threat in the energy sector for years now…

TALOS

Talos Tracked The Threat

- BlackEnergy 3 – 2015, Destructive cyber attack conducted in Ukrainian's power grid
- Template APT – Late 2016 and early 2017, APT gained access to U.S. power grid by targeting supply chain and energy company partners
- Midwest Coop #1 – Mid-summer 2017, Talos confirmed nation-state APT intrusion into U.S. energy cooperative
- VPNFilter – Mid 2018, a vast, covert, network of compromised devices utilizing custom implants on SOHO equipment, including an ICS element for Modbus
- Midwest Coop #2 – Early/Mid 2018, Cisco Talos worked with LEO and IC elements to assist in triage and incident response for a compromised co-op

TALOS

APT Activity in a Rural Coop

Led Talos to Re-examine Our Assumptions

Assumptions

Assumption #1

Nation State APTs want to gain access to the U.S. power grid for two reasons:

1. Pre-position themselves to be able to conduct disruptive attacks if ordered to in the future

2. Signal U.S. leadership that they have this capability as a deterrent to U.S. interference with their national goals

Assumptions

Assumption #2

The goals of the disruptive attacks can be broken down into two main categories.

- Highly disruptive attack effecting large portions of the U.S. power grid, Likely crossing the line of an Act of War, More likely to escalate to a kinetic response
- Less disruptive attack to send a political message, Attempt to stay below the threshold of an Act of War, Less likely to escalate to a kinetic response

Assumptions

Assumption #3

Nation State APTs will try to stay below the threshold of an Act of War except in times of extreme tensions or actual war itself

- More likely that they will try to execute operations that have just enough impact to achieve their objectives but stay below that threshold

Assumptions Still Checked Out

So how do rural power cooperatives fit in to an APTs strategy?

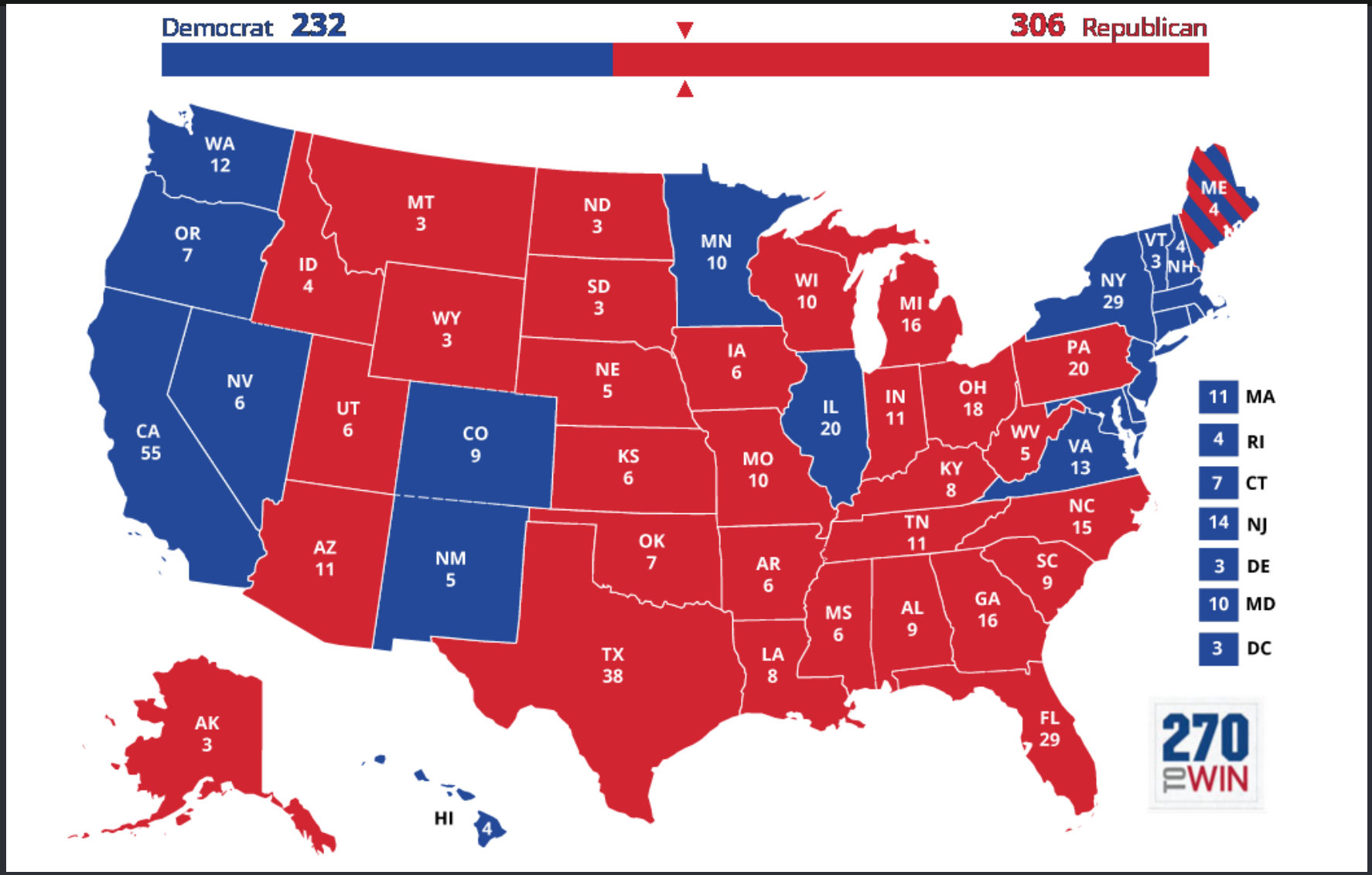
Why Target Rural U.S. Energy Cooperatives?

1. Energy cooperatives serve a large, key portion of the U.S. population

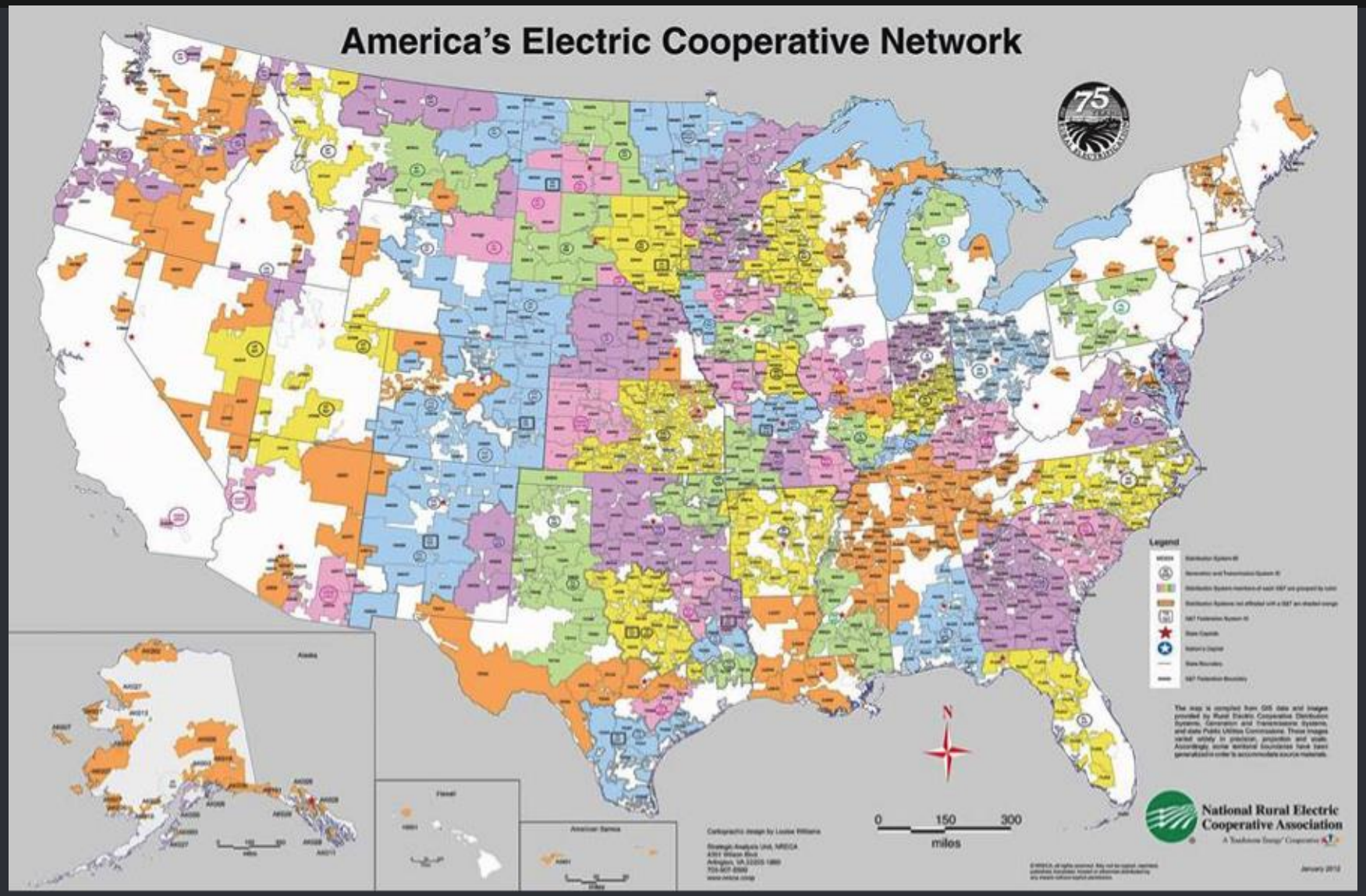
- Approximately 1 in 6 U.S. households and businesses
- Cooperative members span a wide range of individuals and verticals that are vital to U.S. national interest
- The cooperative map and the 2016 election map show heavy overlap

TALOS

2016 Election Results



2016 Electric Cooperative Map



Why Target Rural U.S. Energy Cooperatives?

2. Could fulfill a Nation State Actor's mission objectives

- Causing disruptions across multiple Coops could result in loss of power for hundreds of thousands of Americans

- They can tailor how many victims are affected to attempt to keep below the threshold of an Act of War

Why Target Rural U.S. Energy Cooperatives?

3. Lower risk for the Threat Actor

- Attempting a similar operation against heavily funded energy giants with large counter-cyber programs is a higher risk to threat actor TTPs

- An outage in a large energy company may affect too many people and businesses at once, which would risk escalating the event to an Act of War

Example Attack Scenario

After reconnaissance, gaining access, moving laterally and positioning in the network

1. Remote Disconnect: Abuse AMI to remote disconnect of all customers, circumventing safeguards for multiple disconnect protections, Achieve main objective
2. Disable Phones and Website: Abuse admin controls to disable phone system and website so customers cannot report outages, Extend effects of outages
3. Disable Substations: Abuse remote administration of substations to open all breakers, Extend effects of outages
4. Wipe Critical Network Devices: Unrecoverably encrypt all systems critical to business operations to eliminate easy recovery options

A True Apex Threat Will Tailor Their Attack to the Target

They will shape their attack to meet their mission objectives

How can anyone even hope to defend against this threat? (Nope… still not a sales pitch.)

You Don’t Need the Latest Magical Black Box

- Time and Energy of Security Personnel
- Disciplined Adherence to Security Plan

The most critical underinvestment that we’ve observed is in people, not technology

TALOS

Like with Football… Drill the Fundamentals

1. Password Policy: Have one, strictly enforce it
2. Network Segmentation: Operations, Finance, Field Network, Partner Systems, Phones, Security System
3. Reduce Attack Surface: Decommission unnecessary devices/networks, close unnecessary ports

More Fundamentals

4. Shelter AMI: Keep off the Internet, or use separate locked down computers for internet based AMI, also true for other critical systems

5. Patches and Updates: Apply ASAP, invest to ensure uptime

6. Cyber Emergency Response plan: Have one, practice it

Security Audits

1. Actively hunt for security issues on a regular schedule
2. Scan your network from the inside and outside
3. Review information posted on your company website and/or Cooperative publications

Security Audits

4. Check for compliance with security policies

5. Examine devices owned by partner organizations that have access to your network

6. Build a plan to action all the items you discovered as aggressively as you can with limited impact to operations

Monitor Network & Endpoint Activity

1. Set aside time to go through network logs and other telemetry, part of your routine

2. Doesn't need to be an extraordinary amount of time, but it's important to do it every day

3. You'll quickly develop an instinct for things that just don't look right and warrant further investigation

Having Visibility is the Key to Detect & Respond

Must have visibility into these three things at a minimum

1. Endpoint Activity: Sysmon, etc…
2. Network Traffic: Analyze netflow to identify anomalous connections, activity
3. DNS: Monitor DNS requests to hunt for unexpected domains

Centralized logging, offsite backups

Will Anything Really Stop an APT?

The short answer is, no…

So why go through all this work?

You Don’t Need to Be the Fastest

Just don’t be the slowest…

TALOS

Make Them Work For It: Contest the Battlespace

- Force them to spend more resources, take extra risks, and jeopardize more expensive capabilities
  - More likely they'll get caught
  - Less likely to accomplish their goals
- Mitigate the damage they can do, an event will be bad instead of catastrophic
- Frustrate them enough and they'll look for easier prey

Final Thoughts

The Concern

- Threat: Apex Predators
- Goals: Make a political statement, stay shy of Act of War
- Tendencies: Use tools just advanced enough to achieve goals to reduce cost and risk

What Can You Do?

- Take advantage of their tendencies, make them work
- Drill the fundamentals, you may be surprised how effective this can be
- Raise cost to the adversary, reduce their dwell time

Defender Objectives

- Deter: Make them look for an easier target
- Prevent: Don’t give them an easy way in, make them work for it
- Mitigate: Assume compromise, limit lateral movement, monitor to detect compromises early
- Recover: Be prepared with your response and recovery plan

This is not a war where you can keep them out of your castle 100% of the time...

Be prepared for breaches of your walls and repel the attackers to reclaim your ground

What Can You Do Right Now?

- Review your policies for credential management, eliminate shared credentials, tighten privilege levels
- Review AMI and other critical systems, are they internet connected, disconnect or locked down
- Build your plan to drill the fundamentals, conduct audits, and monitor your network (set achievable timetable for making them part of your routine)

TALOS

Beers With Talos Podcast - https://www.talosintelligence.com/podcasts

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity