MIDWEST RELIABILITY ORGANIZATION

Threat Intelligence and Threat Hunting 101

Brett Lawler, Threat Intelligence Consultant, Xcel Energy

Michael Meason, Senior Manager, Information and Security, Western Farmers Electric Cooperative

CLARITY | ASSURANCE | RESULTS

MIDWEST RELIABILITY ORGANIZATION

Threat Intelligence 101

Brett Lawler, Threat Intelligence Consultant, Xcel Energy

What is Threat Intelligence?

- Identify Risk
- Analyze and Communicate
- Mitigation Strategies

✓Protect People
✓Protect Assets
✓Protect Reputation

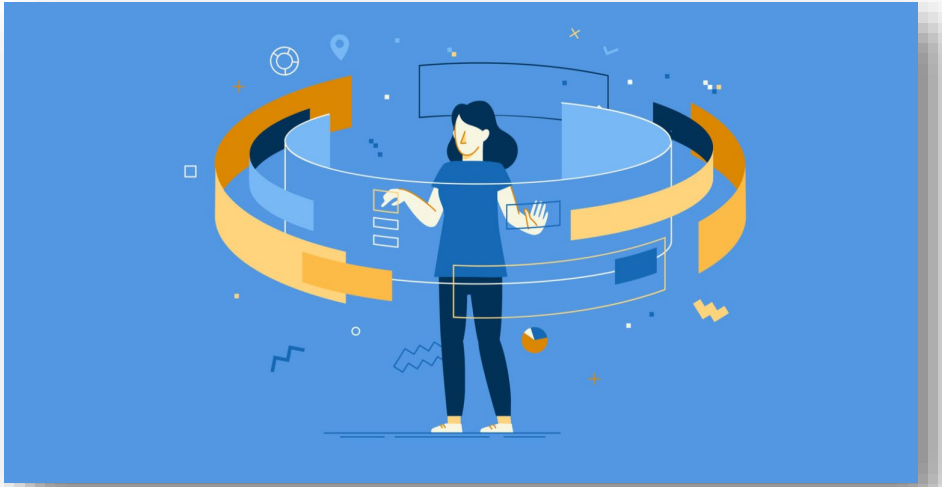
"The more we see, the more we understand, the more we understand, the better we are"

Communication is Key

- Products and Deliverables
  - How do you communicate intelligence?
  - What are you trying to accomplish?
  - “So What Factor”
  - Is it actionable?
- Coordination
  - Federal/State/ISACs
  - Peers
  - Internal Stakeholders

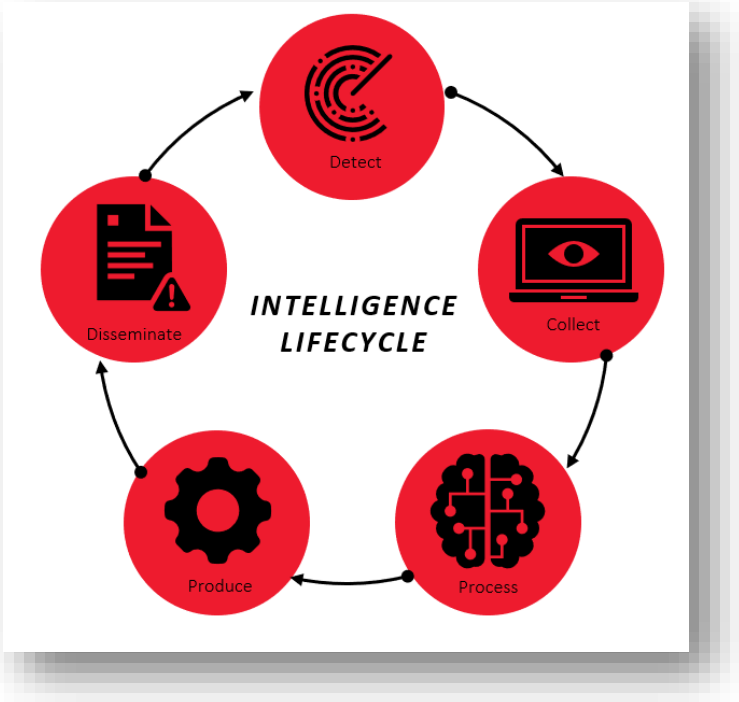
Collection Sources

- Federal/State Sources
- ISAC Sources
- Vendors
- Open Sources
- Passive Monitoring



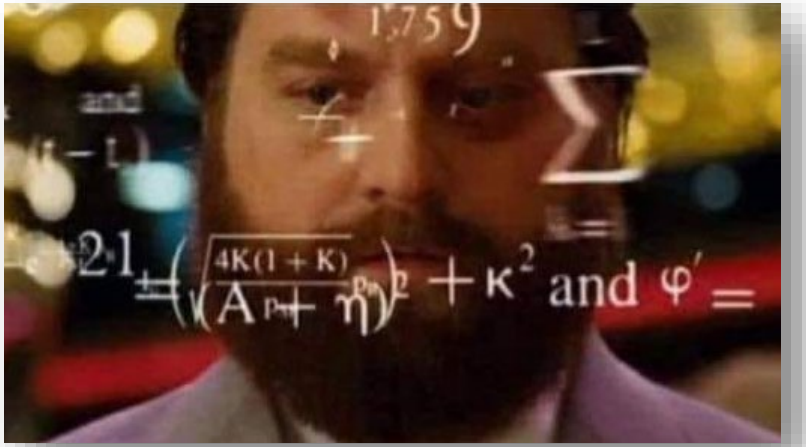
Intelligence Requirements

- What is a threat?
- Determine Intelligence Needs (INs)
- Playbook Strategy, if this….then…
- Who are my key stakeholders?
- Know your audience
- Constant Assessments



What Makes a Good Intelligence Analyst?

- Organized
- Communication Skills
- Analytical
- Investigative
- Knowledgeable
- Proactive
- Research Oriented



Questions

MIDWEST RELIABILITY ORGANIZATION

Threat Hunting 101

Michael Meason, Senior Manager, Information and Security,
Western Farmers Electric Cooperative

CLARITY | ASSURANCE | RESULTS

This is 101 Right?

- What is it?
- Why do we need it?
- How to get started?
- What is the value?

What is Threat Hunting or Proactive Hunting?

- Doing stuff (good) before stuff (bad) happens.
- Proactive
- Forward looking based on, intelligence, scenarios, risk, or analysis.

Why Do We Need It?

- Reactive = Too late
- Velocity of threats is too great
- Proactive provides value
- Provides granular knowledge

How To Get Started

- Scenario/Planned
- Ad-hoc

What is the Value?

- Deeper Understanding
- New Detection Capabilities
  - Uncovers New TTPs
- Lower Noise Floor
- Informs Operations

Utility Challenges

- Threat Intelligence
- Threat Hunting

Bringing It All Together

Questions