Strategy for Cyber Threat Intelligence Capabilities in the Electric Sector

ROLAND E MILLER III / ANDREW BOCHMAN / 26 MARCH 2015

Background on Cyber Threat Intelligence

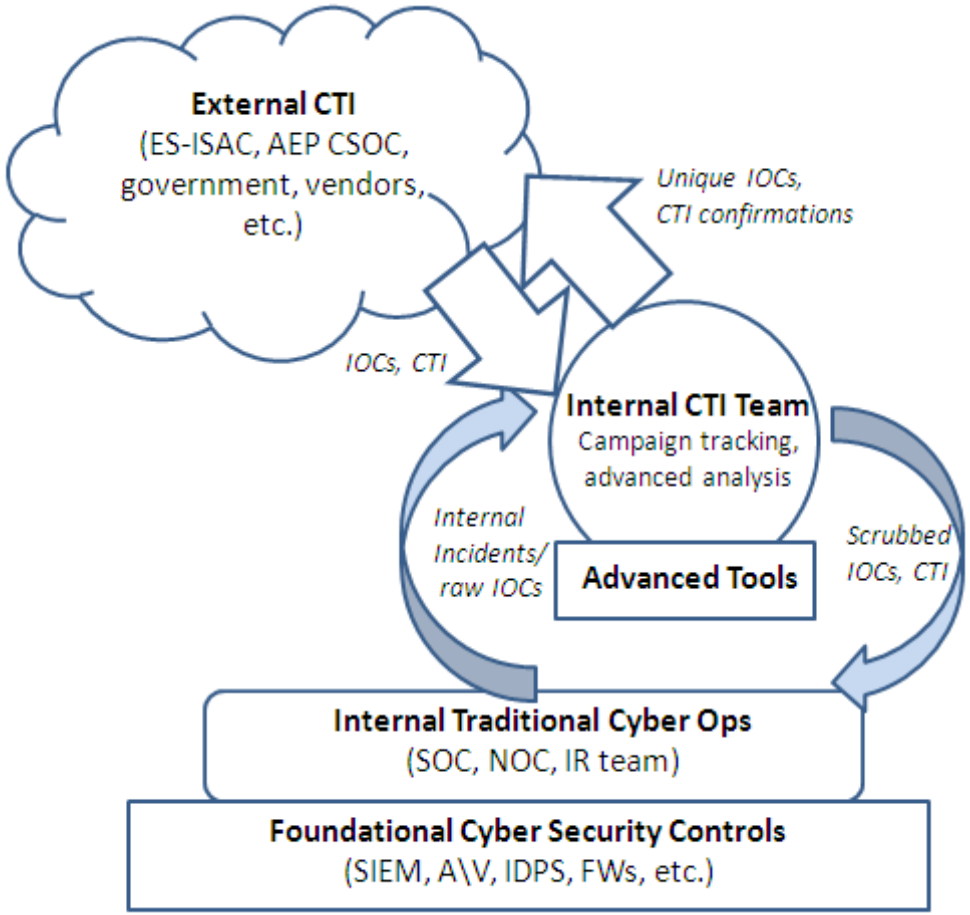
- Cyber Threat Intelligence (CTI) is the determination of the tactics, tools, and procedures (TTP) and associated indicators of compromise (IOC) that threat actors use, and sharing this information with other potential targets of the threat actors

- A CTI Ecosystem has both producers of CTI and consumers of it
  - The exchange of CTI is typically brokered by an Information Sharing and Analysis Center (ISAC)
  - In our sector this is the ES-ISAC

- Since there are different threat actors associated with different sectors, each sector can be thought of as a unique CTI ecosystem

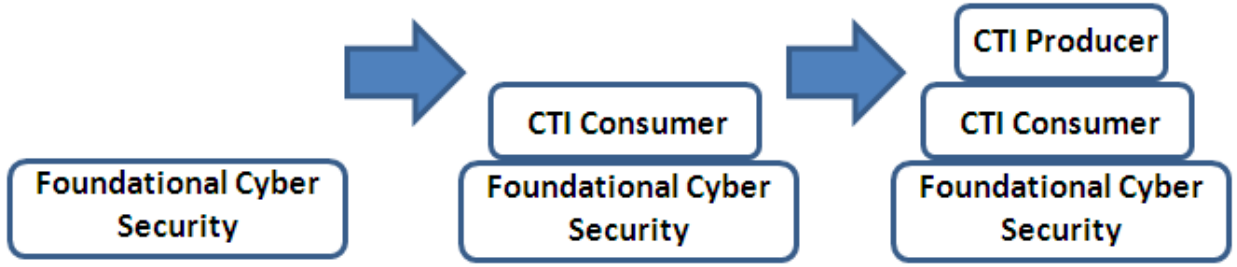
What Contributes to a Healthy CTI Ecosystem?

- Experience from the Defense Industrial Base (DIB) CTI ecosystem shows that a critical mass of CTI producers needs to be established to ensure that CTI that is relevant to the sector is being discovered and shared
- Equally important, is that the majority of the sector be setup to be a consumer of CTI
- Finally, a fully functional information broker needs to exist to share the CTI between the producers and the consumers
- To the right is a simple depiction of how a CTI Producer can interact internally and externally



CTI Roadmap for the Electric Sector

- While the Electric Sector has an active and engaged CTI broker (i.e., the ES-ISAC), most entities are not setup to be CTI Consumers, let alone being able to produce CTI for the sector's ecosystem
- The simple roadmap for an entity to become a CTI producer is shown below:



- While most entities should strive to become a CTI Consumer, the sector only needs a subset (a critical mass) of CTI Producers to become healthy and self-sustaining
  - There are less than a handful of entities in the sector that currently have the capacity and capability to be a CTI producer and they are all large public utilities that do not fully represent the sector's overall cyber threat footprint

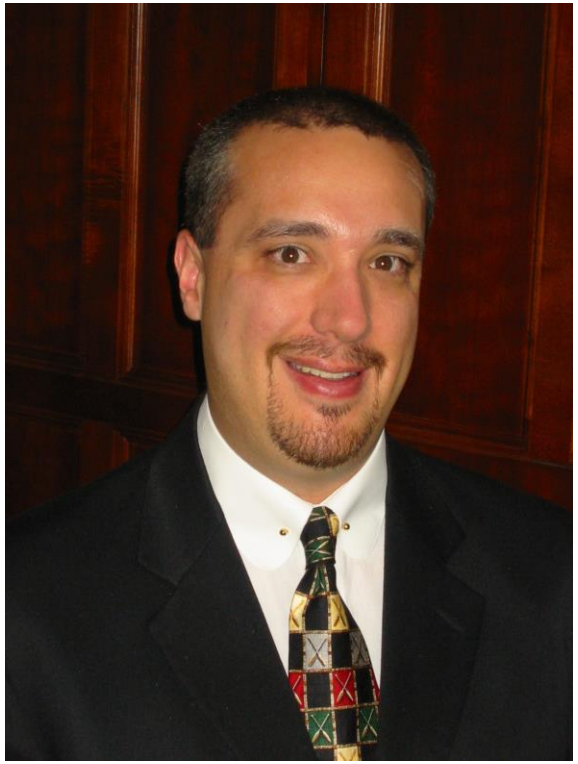
EAC Asks to DOE on the CTI Strategy

- ❖Best practices from other sectors with more mature CTI ecosystems (e.g. FS-ISAC, DSIE) should be identified and translated for the electric sector for considered adoption by ES-ISAC
- ❖Specific processes, vendor agnostic tools, capabilities, staffing capacity and personnel skillset recommendations should be developed
- ❖Specific steps to move from foundational security, to CTI consumer, to CTI producer should be outlined
- ❖A representative cross-section of the sector (a critical mass) should be seeded for development to become CTI producers
- ❖DOE should encourage more utility participants to join its Cybersecurity Risk Information Sharing Program (CRISP) program, and utilities already participating should take maximum advantage of CRISP-originated CTI sourced to them by the ES-ISAC

Roland E Miller III

Roland has over 18-years of experience in information security and has been providing strategic thought leadership in the discipline throughout his career. He has been involved with or chaired numerous groups responsible for strategy, policy, best-practices, and information sharing in information security throughout the years.

Roland is currently a senior manager responsible for cyber security strategy, architecture, and engineering at one of the nation's largest shareholder owned electric utilities.



Andy Bochman

Andy is Senior Cyber and Energy Security Strategist for Idaho National Lab's National and Homeland Security directorate.

A frequent speaker and adviser on topics at the intersection of grid modernization and national security, Andy has provided expert testimony and analysis on energy sector standards and gaps to FERC, NERC, DOE, DoD, NIST, NARUC and state utility commissioners.