

Improving Security Operations through the ES-ISAC

The ES-ISAC premise
and
Vuln Disclosure / Incident Coordination
Case Studies



The month I graduated high school

Presidential Decision Directive/NCS-63, May 22, 1998:

- “...owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center.”
- “Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC.”
- “...Under such a model, the ISAC would possess a **large degree of technical focus and expertise and non-regulatory and non-law enforcement missions**. it would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector”
- “Critical to the success of such an institution would be its **timeliness, accessibility, coordination, flexibility, utility and acceptability.**”

The Bad Guys

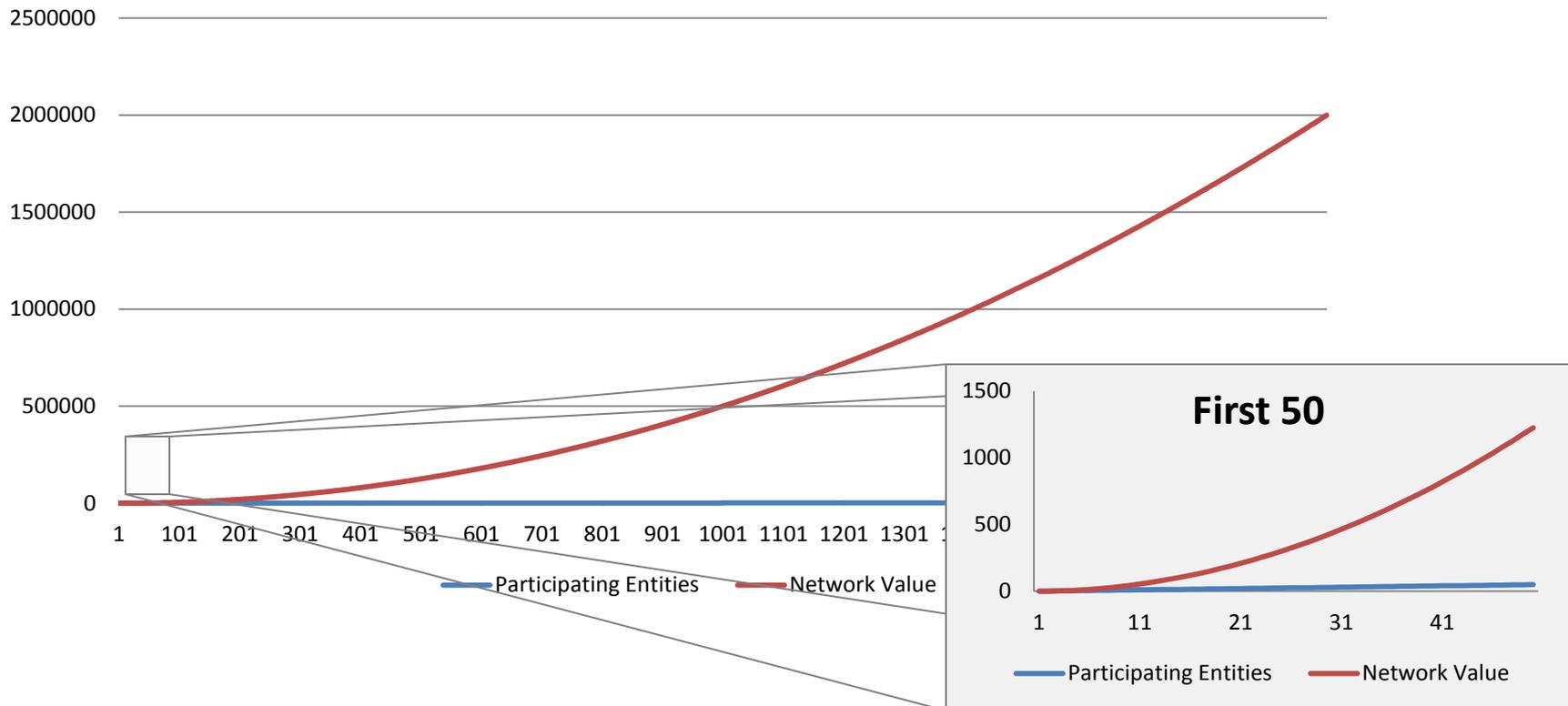
- Sustained Offensive Operations at a constant rate necessitate industry participation in sharing and analysis at a much higher level than when I graduated high school.
- Owner/operators don't necessarily have sustained defensive operations or visibility
- The ES-ISAC's goal is to fill the gap

Hactivists, criminals, nation states

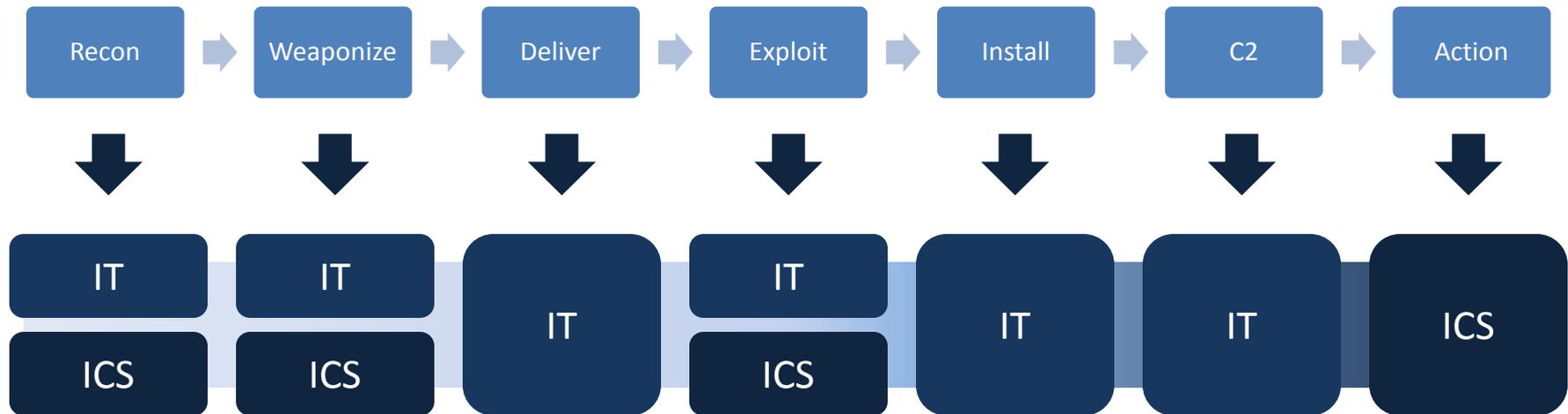
Economics of sharing

Metcalfe's Law: Value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2).

Value through participation



Attack Kill Chain* versus BPS

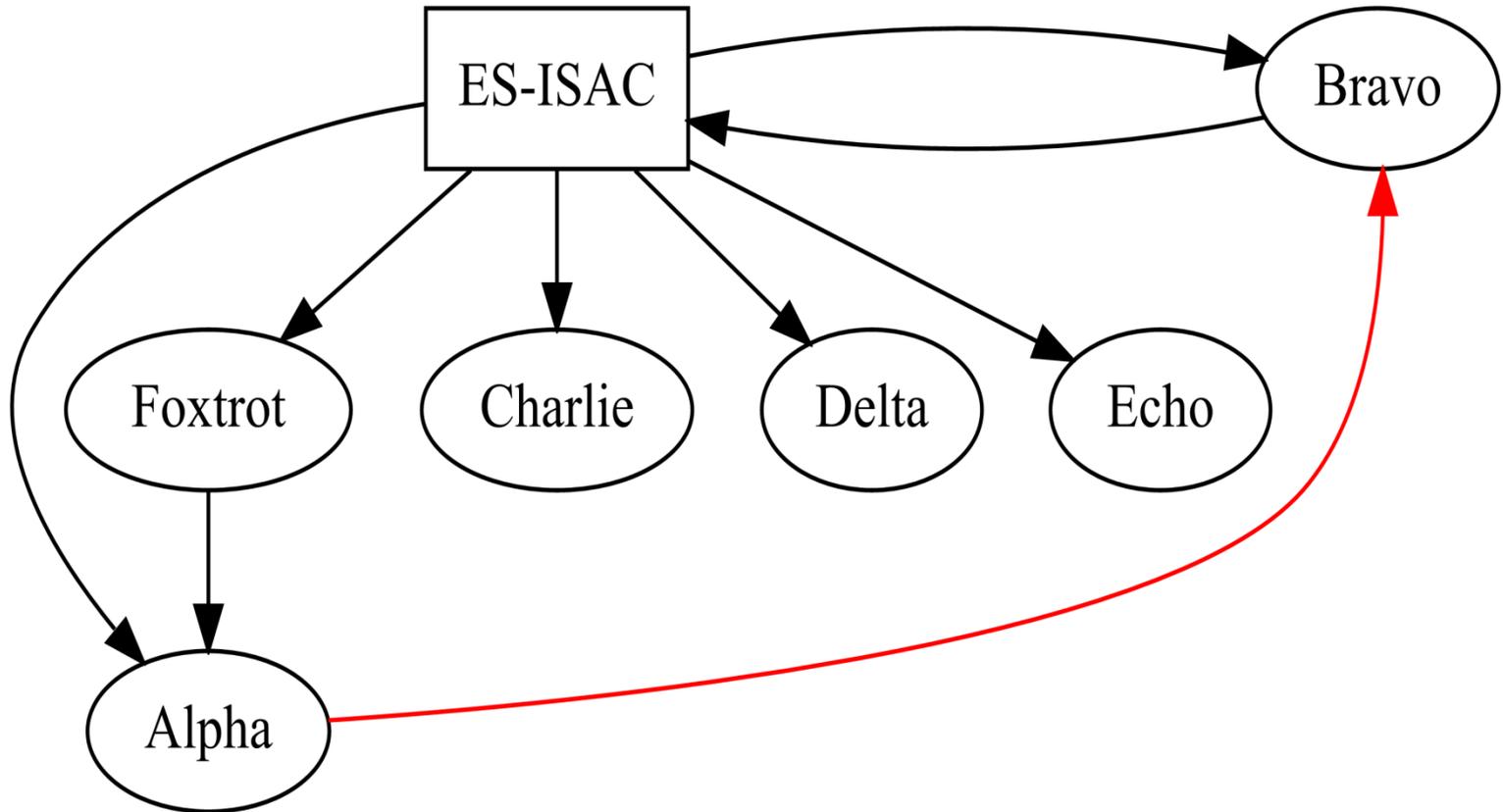


ES-ISAC's goal is to stop attacks before they progress towards exploitation.

&

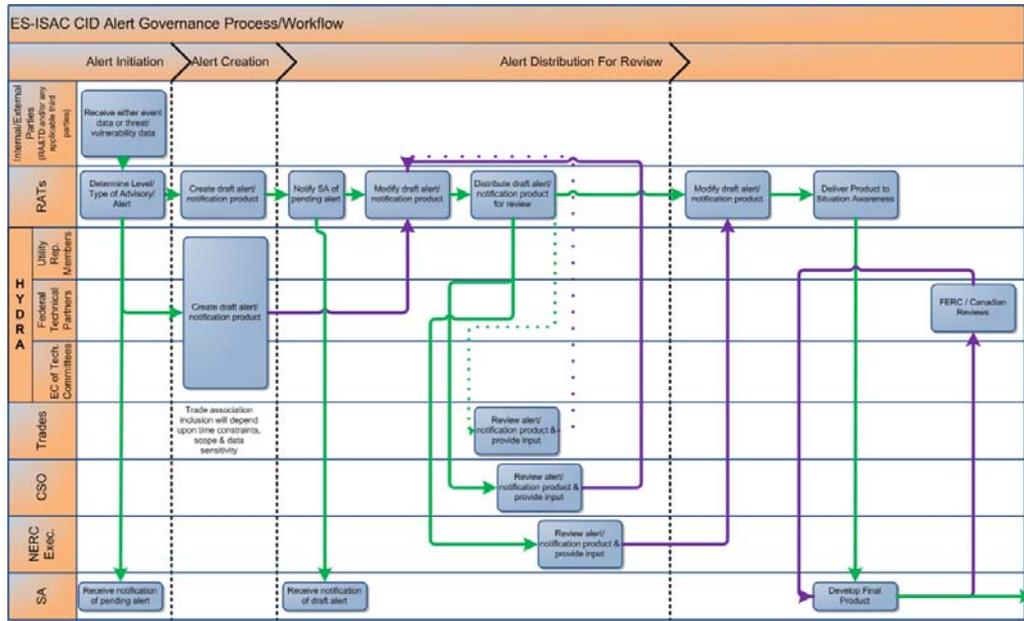
These campaigns require some level of sustained industry operation

Case Study #1



NERC Alerts

9 teams, 4 phases, 16 steps, 22 paths, with a 1wk – 6 month duration



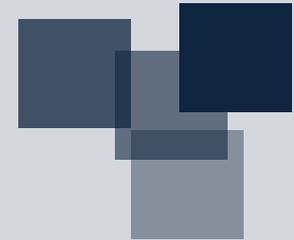
Case Study #2: PLC / Protocol Weakness vulnerability Disclosure

Thank you

Ben Miller // ES-ISAC // <http://www.esisac.com>
ben.miller@nerc.net

References:

- **Metcalfe's Law:** http://en.wikipedia.org/wiki/Metcalfe's_law
- **Attack Kill Chain:** tinyurl.com/3uepqs5 – (presented at the International Conference on Information Warfare and Security, 3/2010)
- **Verizon Data Breach Report:** <http://bit.ly/f5Dvjk>



Questions?