National Cybersecurity Center of Excellence

Energy Provider Community (EPC) Update

07/17/2018

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

- Welcome and Introductions
- Energy Sector Asset Management (ESAM) Project Update
- Summary of Energy Roundtable Discussion – IIoT / ICS Malware / BAS
- Questions, Open Discussion

OT Asset Management Attributes

- **Asset Discovery:** establishment of a full baseline of physical and logical locations of assets
- **Asset Identification:** capture of asset attributes, such as manufacturer, model, operating system (OS), Internet Protocol (IP) addresses, Media Access Control (MAC) addresses, protocols, patch-level information, and firmware versions
- **Asset Visibility:** continuous identification of newly connected or disconnected devices, and IP (routable and non-routable) and serial connections to other devices
- **Asset Disposition:** the level of criticality (high, medium, or low) of a particular asset, its relation to other assets within the OT network, and its communication (to include serial) with other devices
- **Alerting Capabilities:** detection of a deviation from the expected operation of assets

Energy Sector Asset Management Use Case

- Build Team Kickoff: June 2018
- Build Architecture: July / August 2018
- Implementation: start October / November 2018
- Draft ESAM Practice Guide (PG): January / February 2019
- Draft ESAM Public Release: March 2019

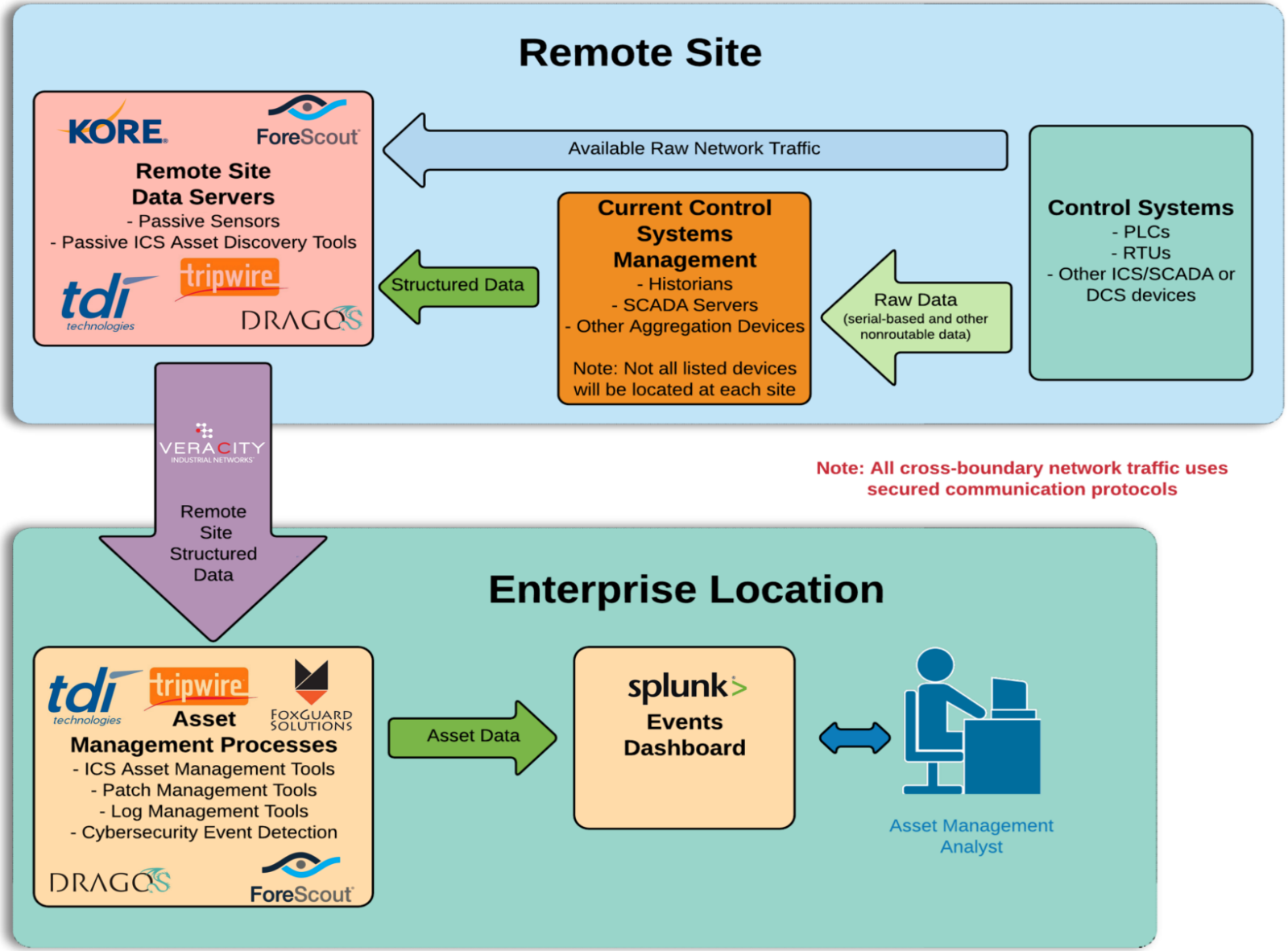
NCCoE ESAM Team: Contacts / Roles

- Jim McCarthy NIST / NCCoE – Principle Investigator
  - James.McCarthy@nist.gov or (301) 975-0228
- Michael Powell NIST / NCCoE – Project Engineer
  - Michael.Powell@nist.gov or (301) 975-0310
- Titilayo Ogunyale MITRE/NCCoE – Project Lead
  - TOgunyale@mitre.org or (301) 975-0219
- John Wiltberger MITRE/NCCoE – Lead Project Engineer
  - JWiltberger@mitre.org or (602) 499-3197
- Devin Wynne MITRE/NCCoE – Project Engineer
  - DWynne@mitre.org or (301) 975-0372
- Lauren Acierto MITRE/NCCoE – Outreach & Engagement
  - LAcierto@mitre.org or (301) 975-0295

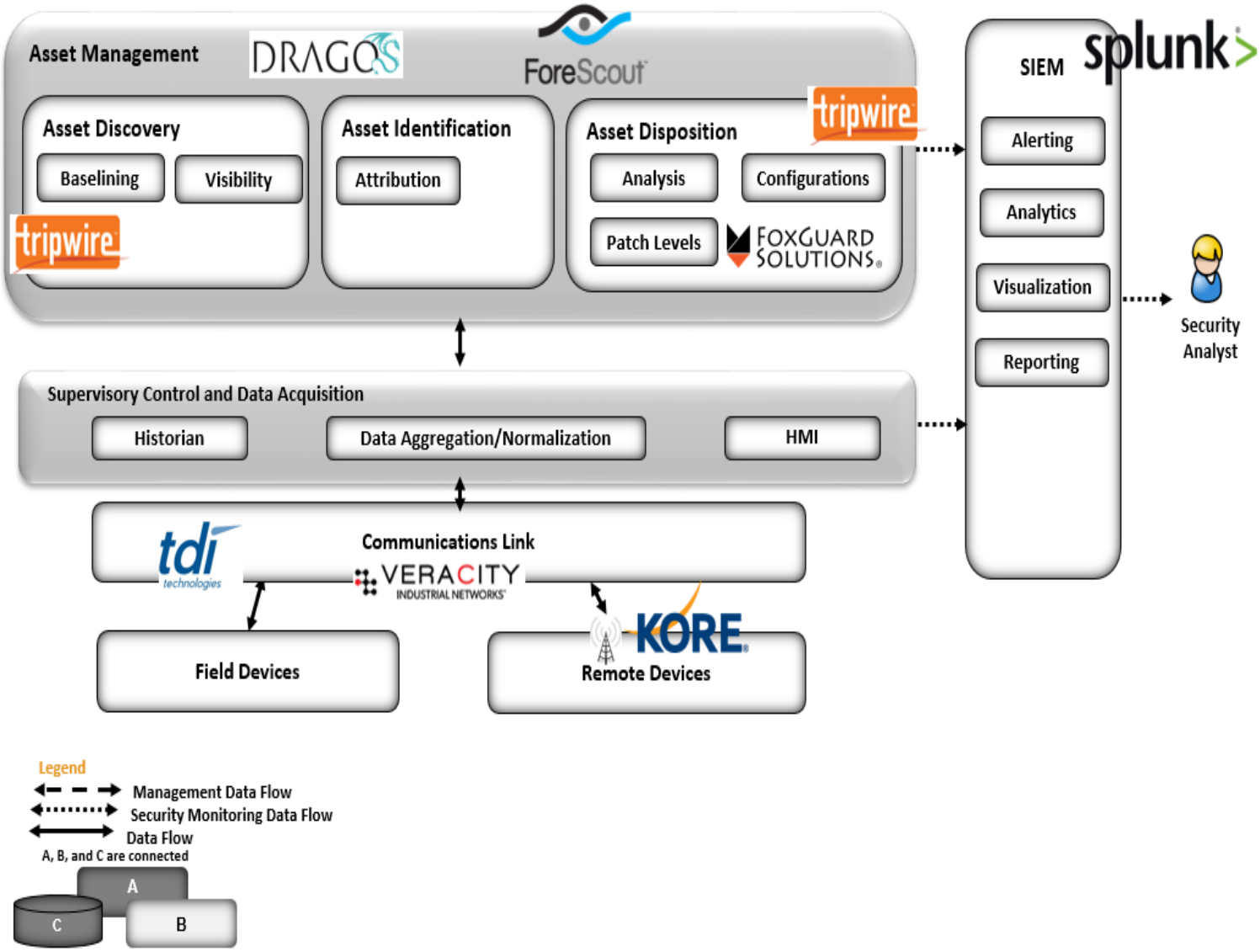
ESAM Build Team

- Dragos
- ForeScout
- FoxGuard Solutions
- Splunk
- KORE Wireless
- TDi Technologies
- Tripwire
- Veracity

ESAM Flow Diagram



ESAM Reference Architecture



Assets

- One set of assets from University of Maryland (facility provides 70 % of Electric, Steam and Chilled Water to campus)

- Actively pursuing other assets for build inventory

ENERGY ROUNDTABLE - 06/27/2018

- Gather group of SMEs from Industry, Government, Academia
- Topics: IIoT/ ICS Malware / Building Automation Systems (BAS)
- Key Observation: Industry is changing, application of Cybersecurity in certain areas is vague, but all realize it is necessary
- Discuss challenges in open, but generally framed context
- Develop project ideas which NCCoE can pursue, which will ultimately lead to a Cybersecurity project
- Vet these ideas to Community of Interest

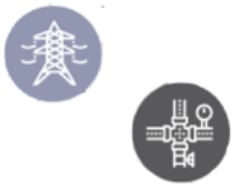
CHALLENGES

- Energy Sector Cybersecurity discussions consistently indicate IIoT is a focus area
- Industrial devices and networks are different than mainstream IT and pose unique challenges to operators / owners
- Industrial Cybersecurity landscape can be confusing to potential tech adopters
- IIoT generally understood but precise definitions vary and are nuanced based on implementation type (i.e. BAS, Water, Electric, Oil & Gas)
- Strengthen understanding of inter-connectedness of industrial networks, devices, and the need for Cybersecurity (especially ICS Malware mitigation)

INDUSTRIAL IOT EVOLUTION

Zuul

Legacy ICS



Legacy non-IP or unsecured/unmanaged IP systems connected to the Internet for business process optimization and analytics

Consumer IoT & Cloud IIoT

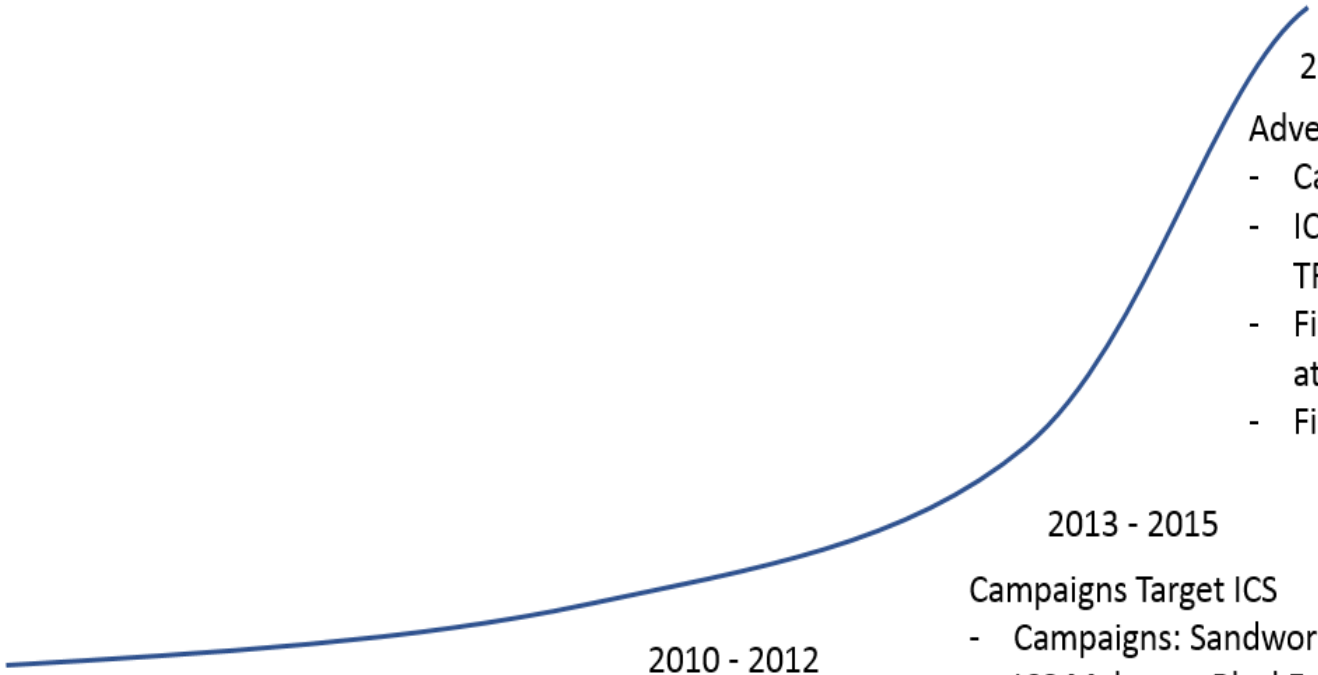
Consumer & non-critical Industrial Systems managed by manufacturer (Device-aaS or DaaS). Provides Cloud integration with Enterprise Authorization and Analytic Systems. **No secure local access support for emergency operations**

Mission Critical IIoT (Next-Gen ICS)

Modernized IP based IIoT systems for Mission Critical industrial use. Requires Hybrid Cloud/Enterprise integration options AND support for **secured local Device Enclave access** during emergency/COOP operations.

1990 2000 2010 2020

The Industrial Threat Landscape



1998 - 2009

Lack of Collection
- Campaigns: APT1
- ICS Malware: None

2010 - 2012

New Interest in ICS
- Campaigns: Cleaver
- ICS Malware: Stuxnet

2013 - 2015

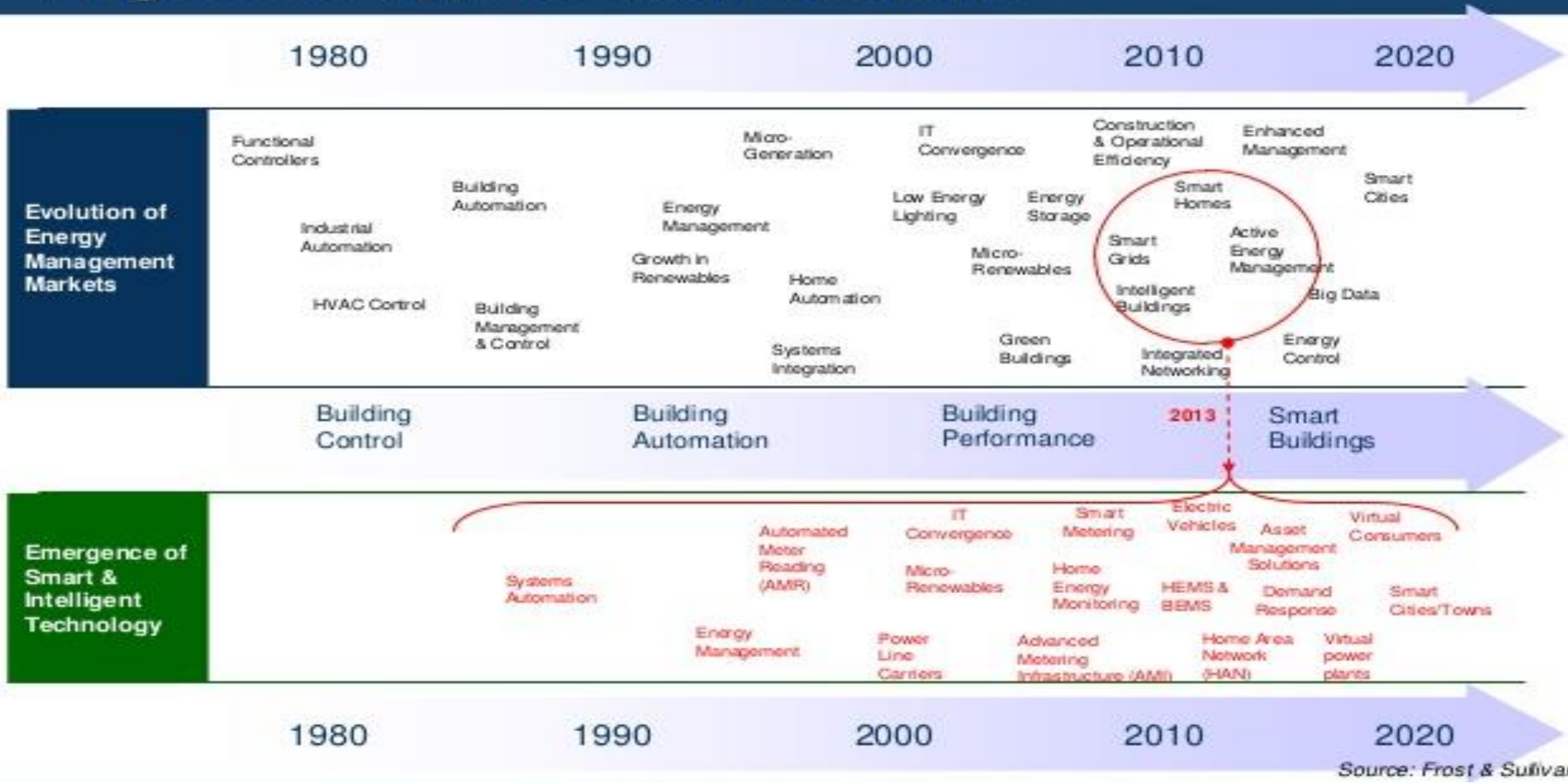
Campaigns Target ICS
- Campaigns: Sandworm and Dragonfly
- ICS Malware: BlackEnergy 2 and Havex
- First attack to cause physical destruction on civilian infrastructure (German Steel)

2015-2017

Adversaries Disrupt ICS
- Campaigns: 8 from 5 Teams
- ICS Malware: CRASHOVERRIDE and TRISIS
- First and second ever electric grid attacks that disrupt power
- First malware to target human life

DRAGOS

Building Energy Management
Progression Towards Smart Solutions



Source: Frost & Sullivan

NCCOE ENERGY SECTOR UPCOMING ACTIVITIES

- **Publication Finalized July 2018**
  - **NIST SP 1800-2 Identity & Access Management (IdAM)**

- **Fall 2018**
  - **GridSecCon2018: Training Session (4 Hours)**
    October 16 – 19, 2018, Las Vegas, NV
    Presenting NCCoE Energy Sector projects (such as ESAM) to session attendees

Contact Us

Jim McCarthy, Senior Security Engineer

Energy Sector Lead

James.McCarthy@nist.gov

301-975-0228

Energy_NCCoE@nist.gov

http://nccoe.nist.gov

301-975-0200

nccoe@nist.gov

Engagement & Business Model

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the practice guide

About NCCoE

Collaborative Hub

The NCCoE assembles experts from businesses, academia, and other government agencies to work on critical national problems in cybersecurity. This collaboration is essential to exploring the widest range of concepts.

As a part of the NIST cybersecurity portfolio, the NCCoE has access to a wealth of prodigious expertise, resources, relationships, and experience.