TCIPG

ANNUAL INDUSTRY WORKSHOP
NOVEMBER 12-13, 2014

CALIFORNIA ELECTRIC SYSTEMS FOR THE 21ST CENTURY (CES-21)

NOVEMBER, 12, 2014

DOUG RHOADES

CHIEF ENGINEER, CYBERSECURITY, SOUTHERN CALIFORNIA EDISON

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

CES-21

California Energy Systems for the 21st Century

CES-21 OVERVIEW

The objective of the CES-21 Program is to address challenges of cyber security and grid integration of the 21st century energy system for California through a Collaborative Research and Development Agreement (CRADA). The CES-21 Program utilizes a team of technical experts from Lawrence Livermore National Laboratory (LLNL) and three large Investor-Owned Utilities (IOUs) within the State of California.

Task 1 of the CRADA

- ***Machine to Machine Automated Threat Response (MMATR)***
  - The research is intended to develop automated response capabilities to protect critical infrastructure against emerging cyber-attacks.
  - Due to the time criticality of these cyber-attacks, the only way to effectively protect critical infrastructure will be through automated response capabilities.

CYBERSECURITY ECOSYSTEMS

- Administration Networks
  - Many providers
  - Endpoints and Gateways
  - Remediation via Filter
- ICS Systems
  - Exploits
  - Possible Vulnerabilities
  - Weak on Remediation

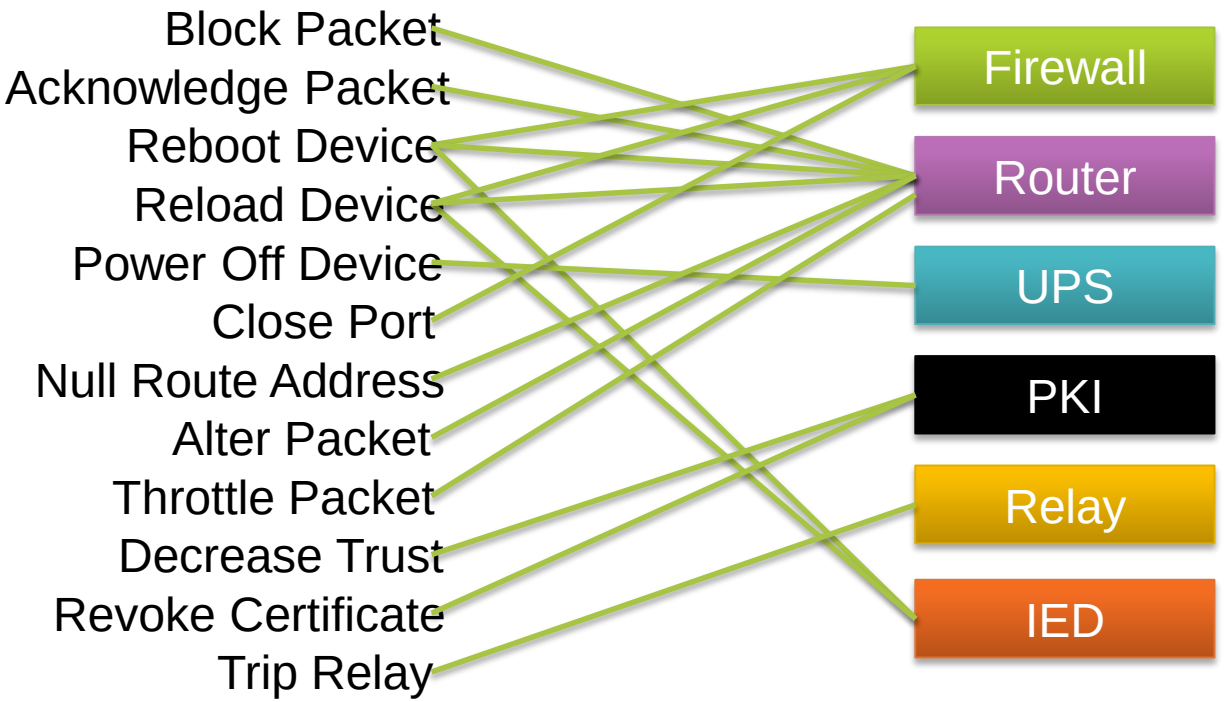
INDICATOR & REMEDIATION LANGUAGE (IRL)

- Complex ICS threats require a much richer descriptive syntax
- Major focus of MMATR is creation of Indicator and Remediation Language (IRL) for this purpose
  - Examine datastreams using powerful predicates
  - Discover IOCs
  - Specify remediations

If *Packet_type*$_a$ **between** *Addr*$_1$ **and** *Addr*$_2$ **occurs**
more than once every 100ms **then**
If *Message_field*$_a$ *varies by more than 10% in*
successive packets within 10s **then**
If *Message_field*$_a$ *varies from Message_field*$_b$
by more than 20% **then**
If *Power_draw*$_a$ *varies while Message_field*$_a$
stays constant in successive packets **then**
If *Message_field*$_a$ *varies by more than 10%*
from the rolling average **then**

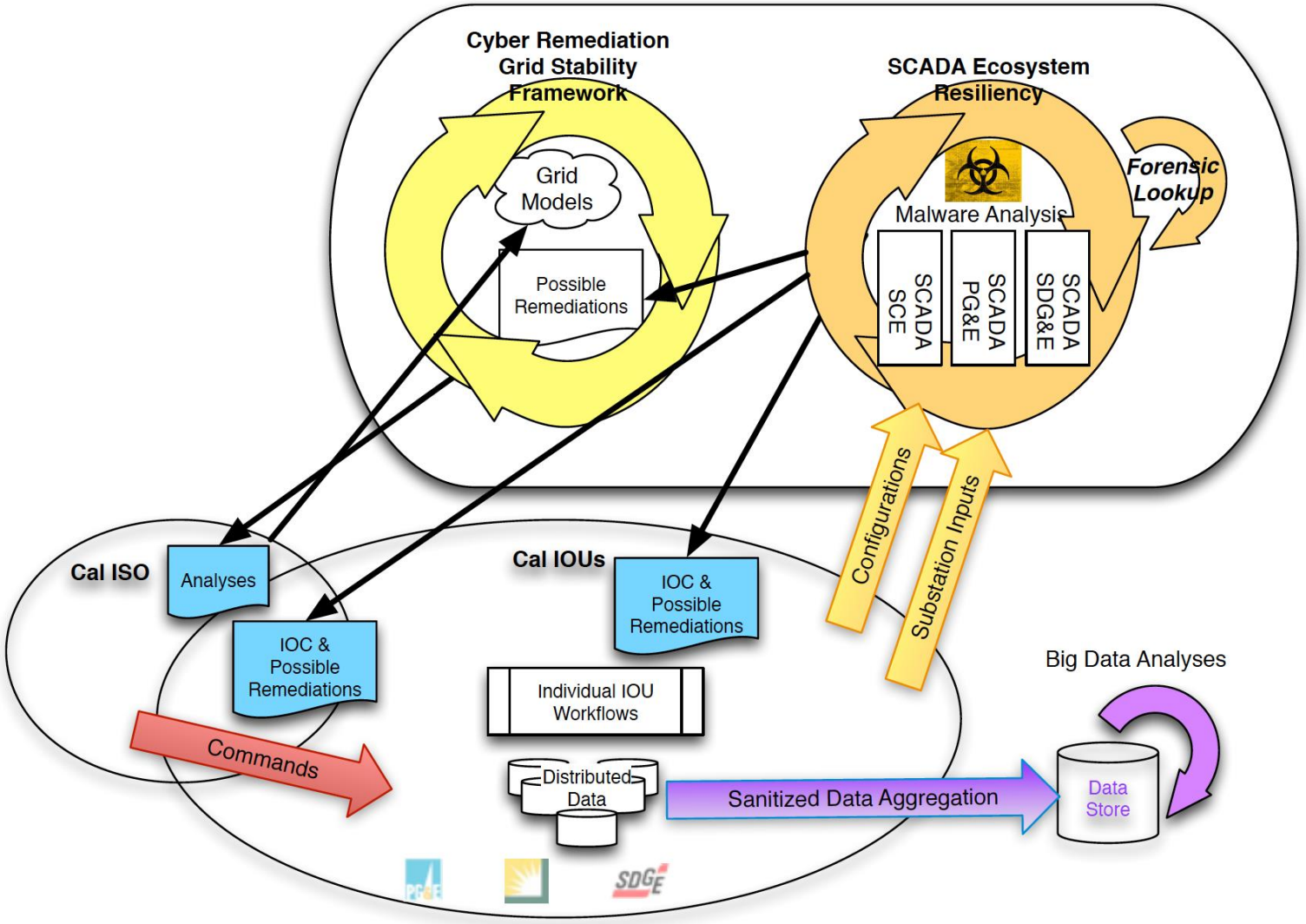
IRL EXECUTION

- Requires vendor buy-in to process standard IRL



- End result is a system that processes IRL packets from an authority, searching for the compromise and then executing the appropriate action(s)

MMATR INFORMATION FLOW



SUMMARY

- Public-Private Partnership
  - Lawrence Livermore National Laboratory leadership
  - Investor Owned Electric Utility Partners
- Open-Source Indicator of Compromise and Remediation Language (IRL)
  - Recognition of symptoms of a compromise
  - Specification of appropriate response(s)
  - Executable at “the edge”
- Creation of ecosystem for machine distribution and execution of ICS cybersecurity threat indicators and responses