CES21

CALIFORNIA ENERGY SYSTEMS FOR THE 21ST CENTURY

California Energy System for the 21st Century Overview and Accomplishments

Commissioner Committee Meeting

Emerging Trends Subcommittee

December 4, 2019

Glenn Haddox, Southern California Edison, Dir Cybersecurity & IT Compliance

David Lo, Pacific Gas & Electric, Cybersecurity Senior Manager

Nate Gleason, Lawrence Livermore National Laboratory, Cyber & Infrastructure Resilience Program Leader

TLP GREEN

CES21

CALIFORNIA ENERGY SYSTEMS FOR THE 21ST CENTURY

Note on Public Disclosure

The CES-21 Cybersecurity R&D effort is focused on the protection of critical infrastructure, therefore a secure process for reporting and a secure process for deliverables will need to be maintained. Detailed tactics, techniques, and procedures developed for use fall under DHS guidelines and will be marked and handled as:

"Protected Critical Infrastructure Information (PCII)"

and are not open to the public

CES-21 TLP Information Sensitivity Classifications

White	**Green**	**Amber**	**Red**
Public: approved for public release	Internal: not approved for public release but low risk if disclosed	Sensitive: moderate risk	Restricted: high risk to reputation, operations, personnel, safety, or security if disclosed

TLP GREEN

California Energy Systems for the 21st Century

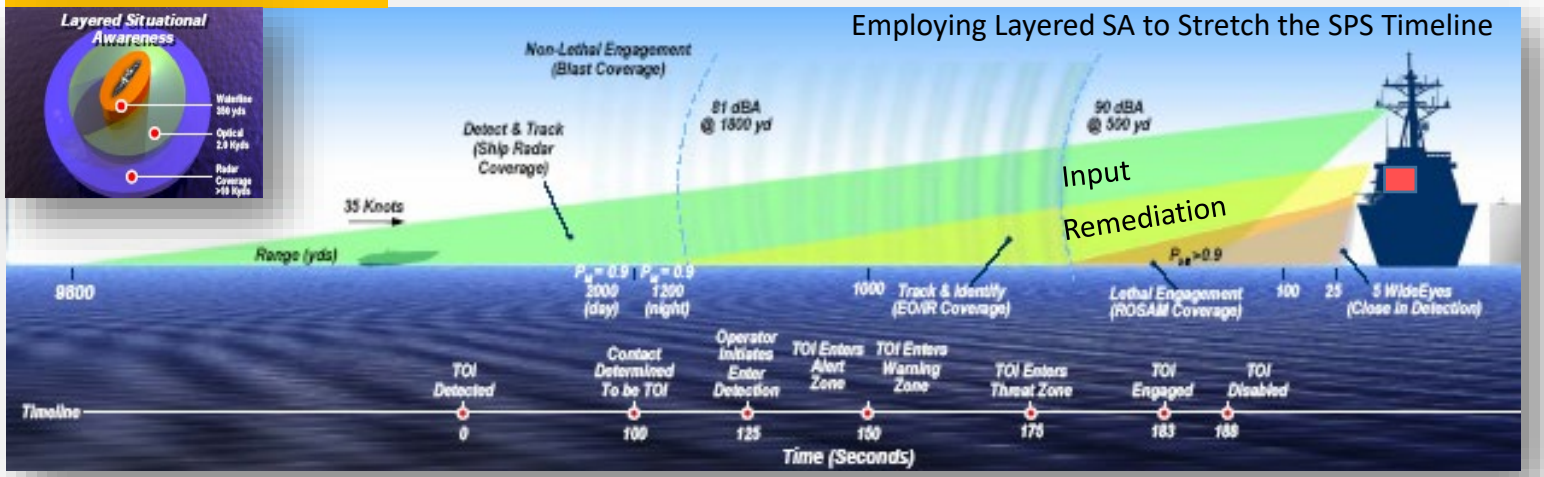
- CES-21 was a 5 year, $35M CPUC-authorized research and development program primarily focused on enhancing the security of California's electric grid against **cyber attack**
- **Collaborative** effort between California-based investor-owned utilities (IOUs) and Lawrence Livermore National Laboratory.
- CES-21 developed a visionary concept called "**Machine to Machine Automated Threat Response**" that provided a substantive starting point for future work
- CES-21 research concluded in October 2019 and has focused on developing technologies for automated detection and response to **identified threats to the electric transmission grid in California**

Collaboration

Military-Inspired Concepts Cyber Response

- What can be learned from military systems that have used automated threat responses for decades?
  - Organic radars augmented with automated identification system provide integrated surface picture
  - Science Applications International Corporation (SAIC) Blast Hailer & spotlight used for non-lethal engagement
  - Vision Technology video camera provides long range identification

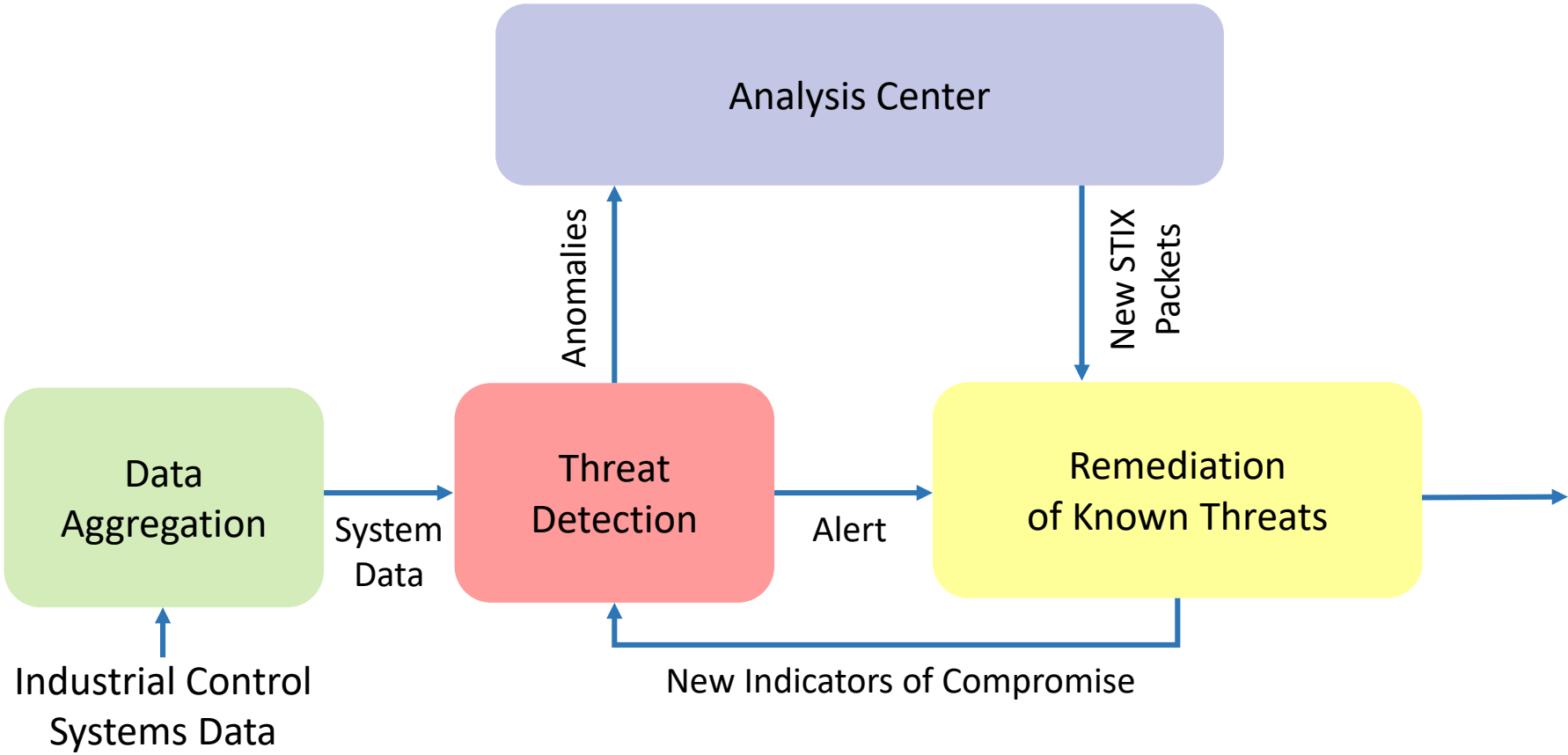
Pre-set "rules" or doctrine



TLP GREEN

Key Concept

- Machine to Machine Automated Threat Response (MMATR)

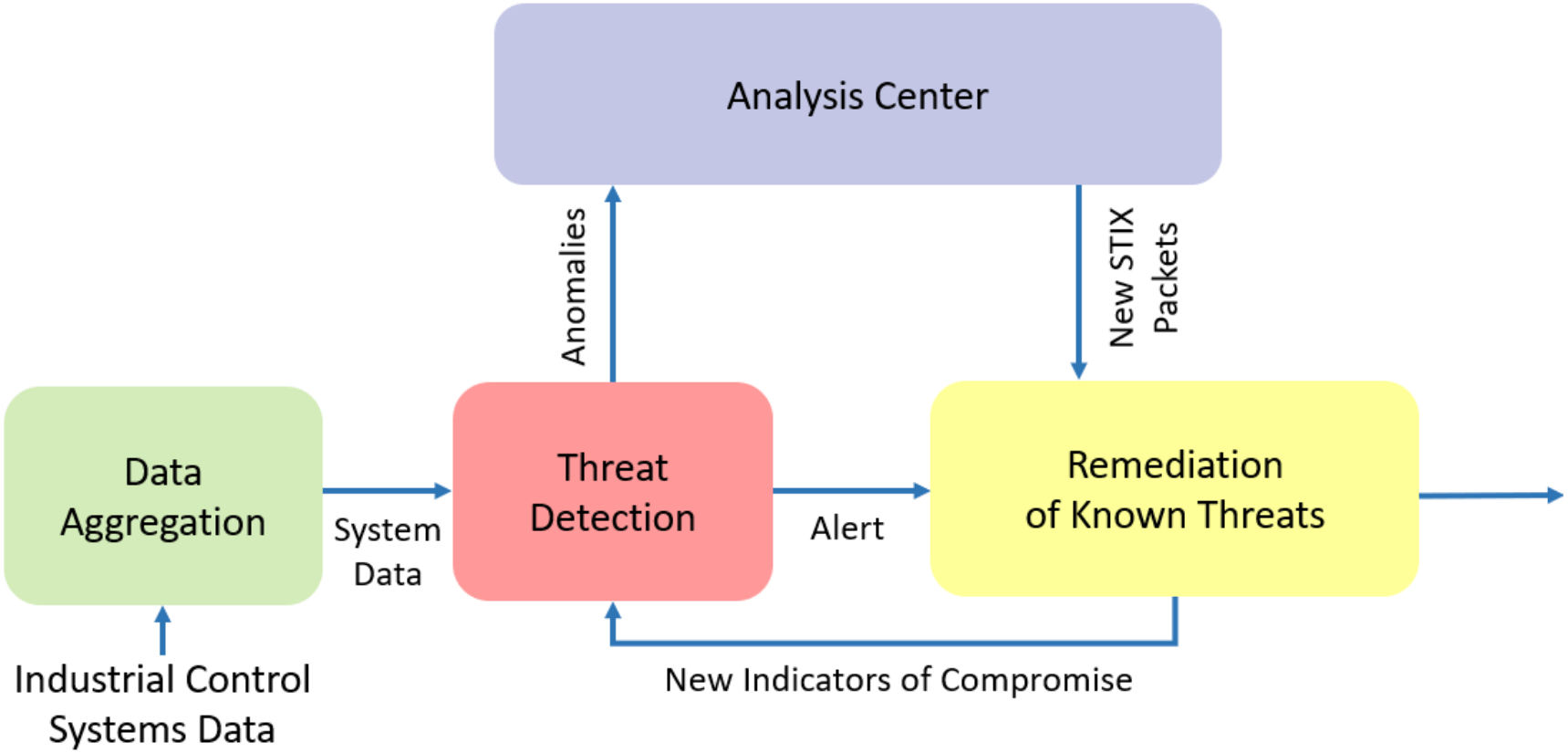


MMATR enables response to cyber attacks at machine speed

CES-21 Video

CES-21 Accomplishments:

Machine to Machine Automated Threat Response (MMATR)

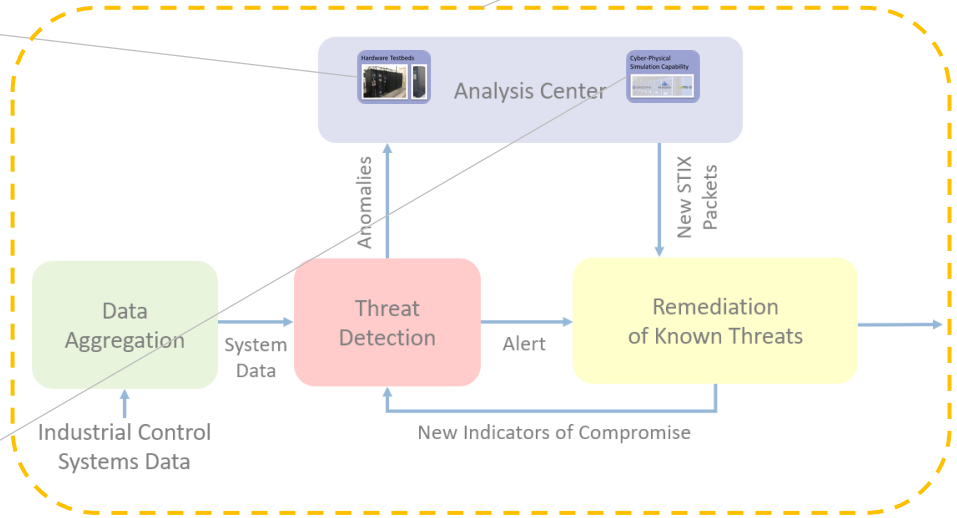


CES-21 Accomplishments: Tools

Hardware Testbeds

Cyber-Physical Simulation

Secure SCADA Protocol for the 21st Century

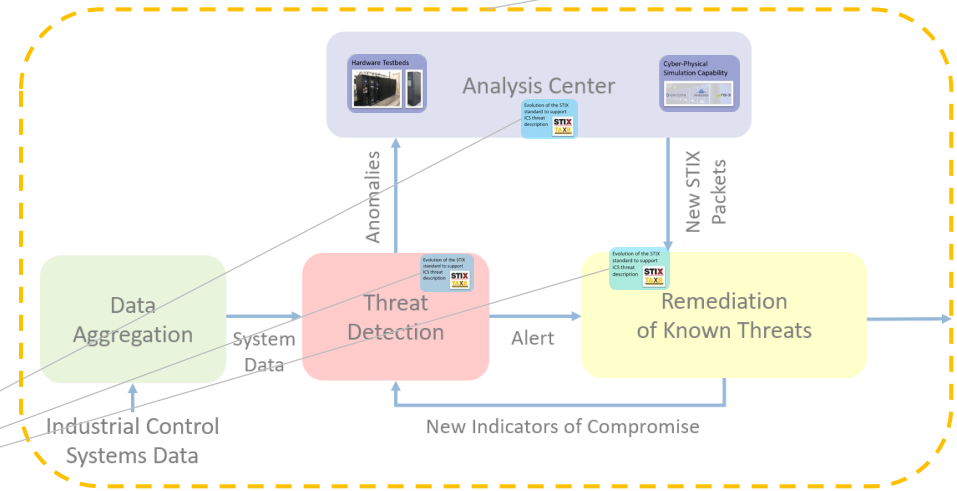


CES-21 Accomplishments: Standards

SSP-21 protocol specification

Evolution of the STIX standard to support ICS threat description

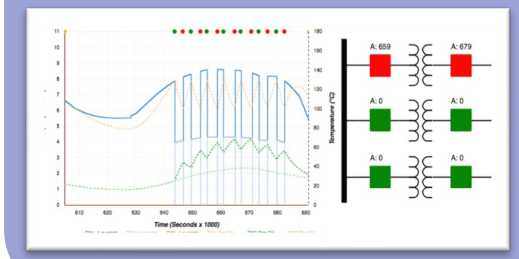
STIX TAXII

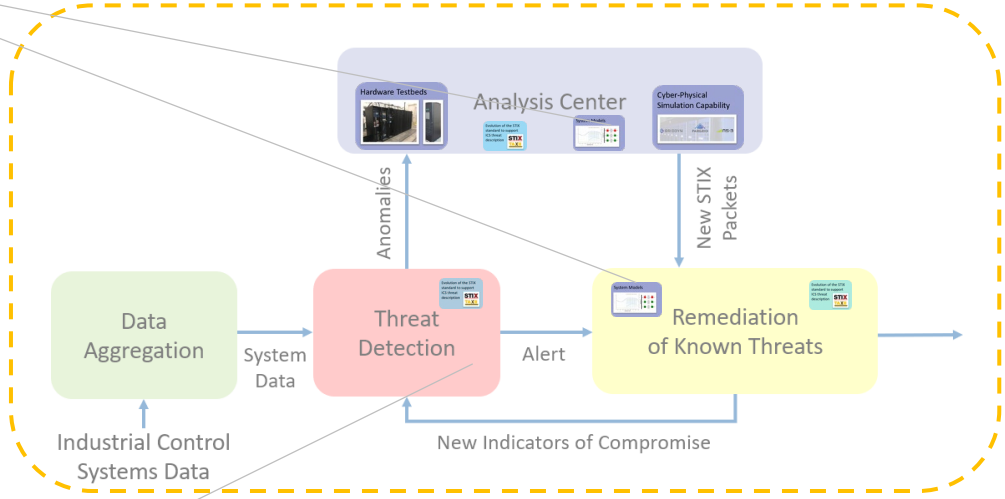


TLP GREEN

CES-21 Accomplishments: Impact Analysis

System Models





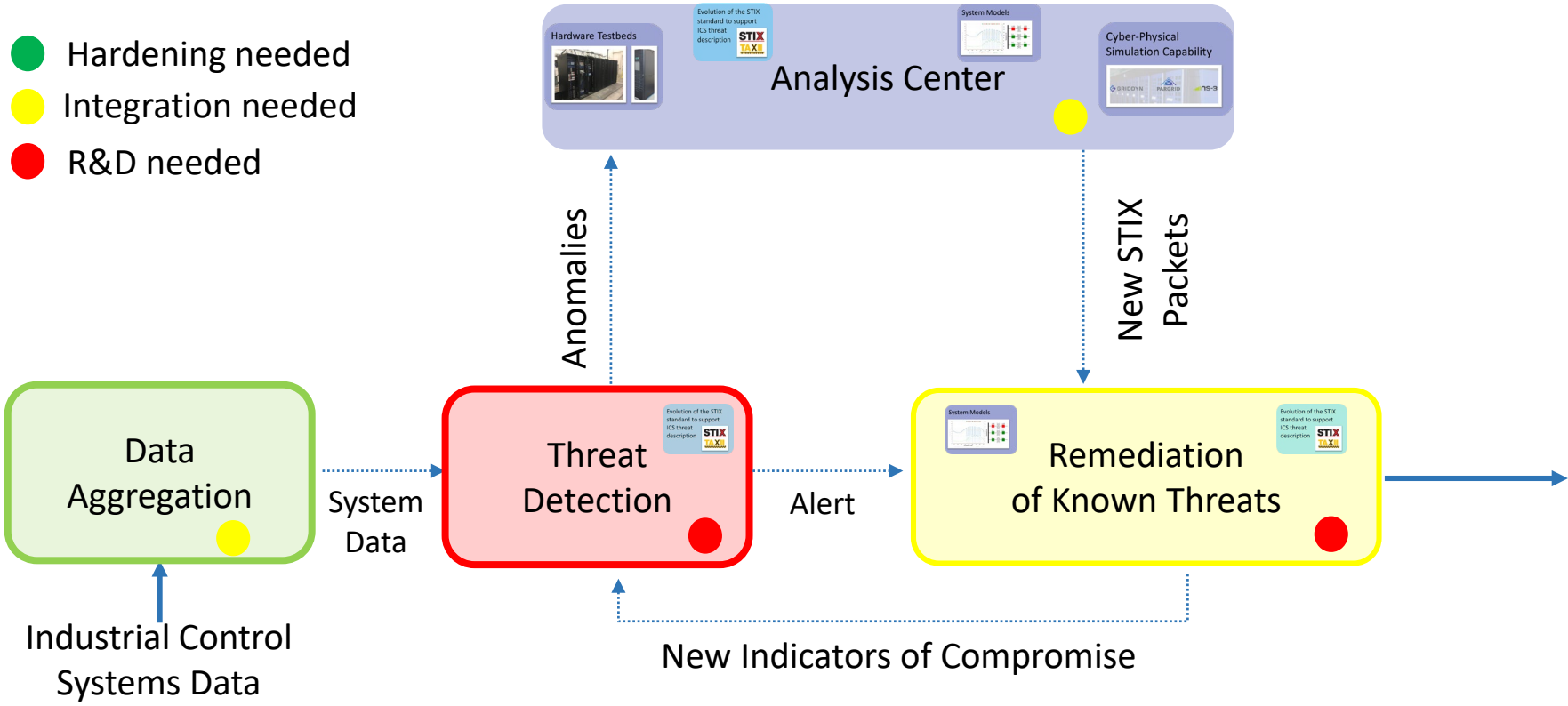
Threat Scoring and Prioritization

TLP GREEN

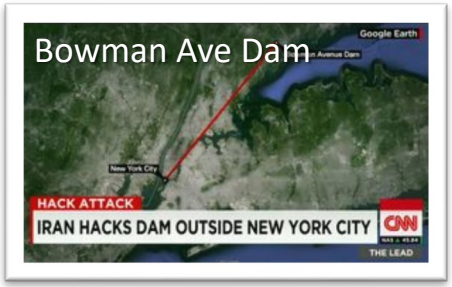
Remaining Gaps:

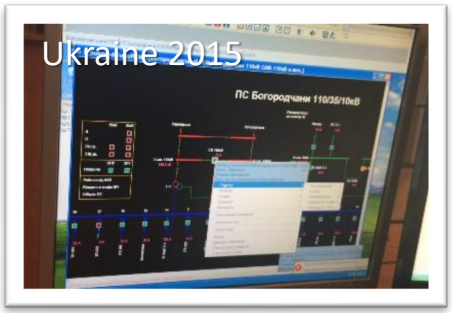
Machine to Machine Automated Threat Response (MMATR)

Additional work is needed to enable MMATR operational capability



Since the program began five years ago, the cyber threat has evolved….





- Cyber attacks on the grid have been conducted – these are no longer just hypothetical events
- In California, the growing use of automation (e.g., smart meters, inverters) is increasing the cyber attack surface substantially
- Highly sophisticated nation-state actors who are constantly innovating are driving urgency for solutions for today and research to address emerging needs in cyber defense

Ivezic, Marin. **Cyber Kinetic Attacks**. *http://ivezic.com/cyber-kinetic-book/*

TLP GREEN

Layered Defense Strategy for the Electric Grid

NIST	Low-tier Adversaries	Mid-tier Adversaries	Sophisticated-tier Adversaries
Identify			
Protect			
Detect			
Respond	USE vulnerabilities	DISCOVER vulnerabilities	CREATE vulnerabilities
Recover			
Endure			

Framework for resilient energy infrastructure

	Low-tier Adversaries	Mid-tier Adversaries	Sophisticated-tier Adversaries
Identify	Risk Assessment, Asset Inventory and Identification, Critical failure analysis		
Protect	Basic Security Protections (firewalls)	Encryption and Network Isolation	Supply chain verification
Detect	Known Threats Only (antivirus)	Anomaly Detection	Advanced cross-domain data analytics
Respond	Manual Response After Event	Automated response to known threats	Real time automated response to unknown threats
Recover	Pre-Planning Only, Manual Recovery	Post-Event Analysis and Event Reconstruction	Optimized strategies for blackstart leveraging DERs
Endure	Manual Event Isolation	Basic Automation for Real Time Isolation	Decentralization

Commercially available products | CES-21 Focus | Gaps to be addressed

CES21

CALIFORNIA ENERGY SYSTEMS FOR THE 21ST CENTURY

Collaboration & Impacts

- Briefed to Governor of California Jerry Brown in 2017 and 2018
- Briefed to Deputy Secretary of Department of Energy (DOE) Dan Brouillette
- Briefed to multiple Assistant Secretaries in Department of Energy and Department of Homeland Security
- Referenced in **April 4, 2017 U.S. Senate Hearing** to receive testimony on examining efforts to protect U.S. energy delivery systems from cybersecurity threats :

*"...**California Energy Systems for the 21st Century (CES-21)** program's Machine-to-Machine Automated Threat Response (MMATR) project has strong potential to accelerate alerts for specific categories of threat information to near real time."* – Andy Bochman, Idaho National Laboratory

- Presented at major conferences: DistribuTECH, S4, SANS ICS Security Summit

CES-21 made significant impact across multiple aspects of cybersecurity for the power grid and established strong relationship between California Utilities and DOE National Laboratories enhancing the collaboration between state of California and federal government.

THANK YOU & QUESTIONS