California Energy Systems

For the 21st Century

PG&E SDGE

NEW CONTEXT

Using STIX and OpenC2 for Machine to Machine Automated Threat Response for Industrial Control Systems

TLP: WHITE SRC: New Context

This document is confidential to the parties engaged and cannot be consumed, distributed or used outside of the Investor Owned Utilities (IOU) CES21 working group without the express written consent of IOU legal counsel.

ABOUT CES-21

California Energy Systems For the 21st Century

- The main objective of CES-21 is to explore the next generation of Industrial Control Systems (ICS) cybersecurity, in the form of **machine-to-machine automated threat response** (MMATR) to protect electric grid infrastructure from emerging cyber-attacks.
- CES-21 is a cybersecurity research and development program directed by the California Public Utilities Commission and the California Legislature.
- Collaborative effort between California-based investor-owned utilities (IOUs) and Lawrence Livermore National Laboratory.
- $33 million over five years (2015-2019), enabled by California Senate Bill 96 and the CA Public Utilities Commission

SOUTHERN CALIFORNIA EDISON®
An *EDISON INTERNATIONAL*® Company

PG&E Pacific Gas and Electric Company®

SDGE
A Sempra Energy utility®

Lawrence Livermore National Laboratory

This document is confidential to the parties engaged and cannot be consumed, distributed or used outside of the Investor Owned Utilities (IOU) CES21 working group without the express written consent of IOU legal counsel.

ABOUT CES-21

California Energy Systems For the 21st Century

CES-21 is broken into a number of categories and deliverables.

- Indicator and Remediation Language (IRL)
- Advanced Threat Detection
- SCADA Ecosystem Resiliency
- Secure Systems Interfaces
- ICS Data Aggregation
- Simulation and Modeling

SOUTHERN CALIFORNIA EDISON®
An *EDISON INTERNATIONAL®* Company

Pacific Gas and Electric Company®

SDGE
A Sempra Energy utility®

Lawrence Livermore National Laboratory

ABOUT CES-21 IRL

Task 6 Indicator and Remediation Language (IRL)

- MMATR capability requires a machine readable language capable of describing indicators and remediation.
- IRL is a core component of MMATR capability

The language of choice for this program is STIX

Soon we will be adding OpenC2

This document is confidential to the parties engaged and cannot be consumed, distributed or used outside of the Investor Owned Utilities (IOU) CES21 working group without the express written consent of IOU legal counsel.

IRL LANGUAGE CHOICE

Task 6 Indicator and Remediation Language (IRL)

- In January 2015, New Context began evaluating existing threat framework languages
- Evaluated over a dozen existing frameworks
- We performed our analysis using a standard set of requirements that included:
  - Ability to express complex Indicators of Compromise (IOC)
  - Ability to express complex remediation steps
  - The frameworks must be in a machine readable format
  - The frameworks were evaluated against project defined use cases
- Used four rating metrics in order help provide a quantitative scoring to aid the research. Those metrics were:
  - Flexible: ability to support a wide range of use cases and information of varying levels of fidelity
  - Extensible: ability to take future growth into consideration
  - Readable: ability to be read “easily” by a human
  - Pervasive: measure of the acceptance and reputation within the community

ICS COMPLEXITY

Task 6 Indicator and Remediation Language (IRL)

- ICS and IT systems indicators and remediations are not alike
- The richness required to describe combinations of observed conditions that might indicate a compromise is difficult to represent in a machine executable format

ICS environments are heavily resource constrained and unable to host native monitoring capabilities

Devices typically must be observed via external data sources such as output logs, network traffic, HMI data

Physical characteristics monitoring such as current draw and heat dissipation

ICS COMPLEXITY

Pseudo language

Indicator pattern

If *Packet_type:a between Addr1 and Addr2 occurs more than once every 100s*

And if Message_field:a varies by more than 10% in successive packets within 10s

And if Power_draw:a varies while Message_field:b stays constant

Advanced Remediation

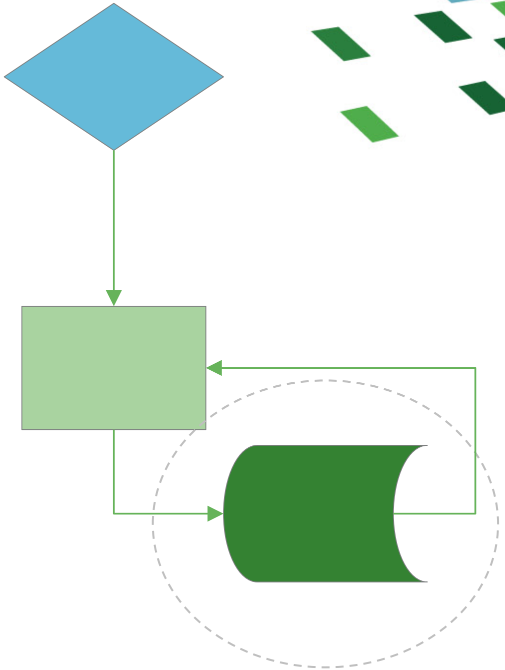
Alert operator

And Open_circuit:a and Close_circuit:b

And Load_program:23 on PLC:12

And Monitor_voltage on Transformer_monitor:a

And then if voltage on Transformer:a matches pattern 50 using 30ms window…



This document is confidential to the parties engaged and cannot be consumed, distributed or used outside of the Investor Owned Utilities (IOU) CES21 working group without the express written consent of IOU legal counsel.

STANDARDS DEVELOPMENT

Indicator and Remediation Language (IRL) Development

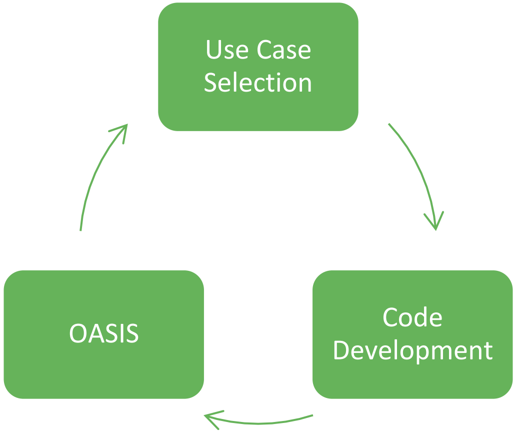
We first focused on indicator development

Important to first be able to detect IOCs

STIX 2 patterning was developed

Direct result of our ongoing work

- CES-21 research findings are submitted to the standards committees within OASIS
- Our research directly impacts and matures these frameworks



Use Case Selection

Code Development

OASIS

OpenC2 PLANS

Task 6 Indicator and Remediation Language (IRL)

- As our work moves toward a greater focus on automated remediation, our focus will be on OpenC2
- Complex multi step playbooks or remediation action schemes

1 Building a gap analysis of OpenC2 against use cases
Review of existing "verbs" to understand gaps
The scope is likely to go beyond Layer 3 "IT" actions like "restart" or "block"

Turn down a setting and monitor

2 We think may need additional expressiveness

If Register "X" then do "Y". Or If Register was set to "A" 2 hours ago, then Set Register to "B"

This document is confidential to the parties engaged and cannot be consumed, distributed or used outside of the Investor Owned Utilities (IOU) CES21 working group without the express written consent of IOU legal counsel.

About Me

NEW CONTEXT

Daniel Riedel

CEO, New Context

daniel@newcontext.com

@riedelinc

CES-21 Host

SOUTHERN CALIFORNIA EDISON®

An *EDISON INTERNATIONAL®* Company

Joy Weed

Cyber Outreach & Operations

Joy.Weed@sce.com

This document is confidential to the parties engaged and cannot be consumed, distributed or used outside of the Investor Owned Utilities (IOU) CES21 working group without the express written consent of IOU legal counsel.