Robert Caliva
Idaho National Laboratory
VMAR Project Manager
Rita Foster
Idaho National Laboratory
VMAR Technical Lead
Corey McClelland
San Diego Gas & Electric
CES-21 Program Manager

Validation and Measuring Automated Response (VMAR)

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

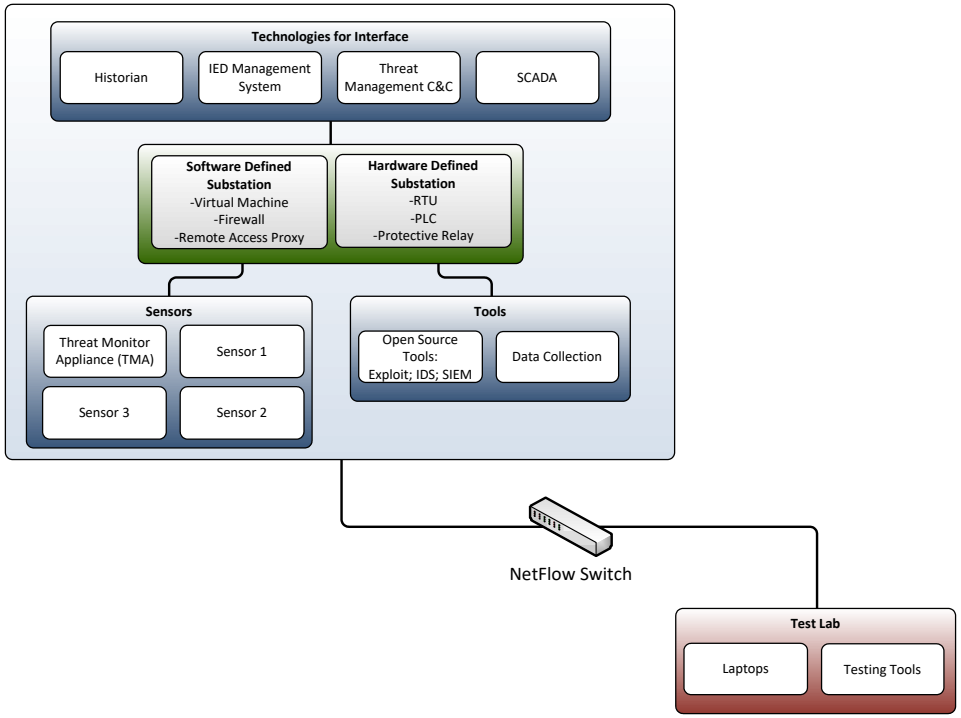
Summary: Validation and Measuring Automated Response

Objective

- Promote Automated Response Capabilities in nontraditional configurations and measure performance, security and resilience

Schedule

- May 2016 – December 2018
- Milestones
  - September 2016 Partners/Models
  - November 2016 Evaluation Environment
  - February 2017 Capabilities Analysis
  - May 2018 Scoring
- Response capability where none existed prior



Performer:	**Idaho National Laboratory**
Partners:	**San Diego Gas & Electric**
Federal Cost:	**$1.47M**
Cost Share:	**$150K**
Total Value of Award:	**$1.62M**
Funds Expended to Date:	**12%**

Advancing the State of the Art (SOA)

- In Information Technology (IT), all in one Orchestrator command and control functionality
- More commonly in IT, address blocking (blacklisting), adding new malware detection, and URL blocking can be automated. These features are emerging in some sectors, but not in the control system Operational Technology (OT)
- With a well defined OT configuration, tailored responses can be provided for automation
- To match the more state-like nature of control systems, provide reassurances to the latency concerns of operations and measure performance, security and resilience to trend over time
- Move beyond existing patch capability to create a novel response capability where none existed prior

Challenges to Success

Challenge 1 – Moving Left in Cyber Kill Chain

- Huge shift in timing from respond (identify, create patch, test, and patch) to response (action taken)

Challenge 2 – Latency Issues in Control for OT

- Provide performance views

Challenge 3 – Time to Test, Validate and Revert

- Design test concepts, measures and rollback

Challenge 4 – Standardization for unique configurations

- STIX, CybOX, OpenC2, performance scripts, open source tools

Challenge 5 – Dependencies

- Equipment availability, timing of partner involvement, leveraged coordination with other related projects/technologies/R&D

Progress to Date

Major Accomplishments

- Structured framework established linking VMAR to NIST
- Creating overall structure for automated response Capabilities Analysis
  - Capabilities vary widely – orchestrator to indicator/response
- Established a relationship and are collaborating with other sensor based projects in DOE-OE
- Identifying other partnerships (e.g., technology vendors)
- Substation hardware and virtualized components defined and being staged at SDG&E in preparation for shipment and configuration at INL

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user (Transition to Practice)

- Multiple pathways for technology transfer
  - Open source code for multiple asset owners
  - Technology Provider partnership
  - Asset Owner partnership
- Plans to gain industry acceptance
  - Heavy focus on measures and validation to prove out concepts for response and ensure no impact to operational system
    - Performance measures – bottleneck is traditionally latency of commands, but process, storage and networks will also be measured
    - Change in protection profile – adding response capability will change the security protection profile
    - Resilience of system – adding response capability increases agility, which is a key aspect of resilience

Path Forward

- Analyze response technologies
- Identify gaps needed for automated response
- Create measures for security protection profiles and apply resilience measures
- Build test and evaluation response capabilities of multiple techniques
- Collect data to prove out accuracy of measures
- Provide final publication
  - Open source code – targeted novel automated response
  - Metrics

Spectrum of Response

Passive Defense

- Basic security controls: firewalls, malware detection, patch management scanning, static honeypots and monitoring
  - Challenge – requires continual monitoring, updates and impacts OT

Active Defense

- Inoculate, contain and remove: Tarpits, Sandboxes, and Honeypots
- Indicator triggered suggestions to remediate provided
  - Challenge: requires eyes on glass, knowledgeable human interaction

Automated Response Does NOT exist in OT

- Pre-programmed scripts – Cyber Remedial Action Schemes
- Indicator triggered (threat or exploit) and remediation action
- Detect intrusion and deflect (Syn/Ack to Tarpit)
  - Challenge: latency, proof and ability to revert