Validation and Measuring Automated Response (VMAR)

Idaho National Laboratory (INL)

Rita Foster and Jed Haile

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018
**Objective**

- Promote Automated Response Capabilities in nontraditional configurations

**Schedule**

- May 2016 – December 2019
- Milestones
  - September 2016 Partners/Models
  - November 2016 Evaluation Environment
  - February & September 2017 Capabilities Analysis
  - May 2018 Performance Scoring
- Response Capability where none existed prior

Summary: Validation and Measuring Automated Response

<table>
<thead>
<tr>
<th>Performer:</th>
<th>Idaho National Laboratory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partners:</td>
<td>San Diego Gas &amp; Electric</td>
</tr>
<tr>
<td>Federal Cost:</td>
<td>$1.4M</td>
</tr>
<tr>
<td>Cost Share:</td>
<td>$150K</td>
</tr>
<tr>
<td>Total Value of Award:</td>
<td>$1.6M</td>
</tr>
<tr>
<td>Funds Expended to Date:</td>
<td>85%</td>
</tr>
</tbody>
</table>
Advancing the State of the Art (SOA)

• In the Information Technology (IT), all in one Orchestrator command and control functionality

• More commonly in IT space, 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) space.

• 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 Kill Chain - done

- Huge shift in timing from respond (identify, create patch, test, and patch) to response (action taken: find, remove, block and log)

Challenge 2 – Latency Issues in Control for OT - done

- Provide performance views – Test Utility with performance metrics

Challenge 3 – Time to Test, Validate and Revert

- Design test concepts, measures and rollback

Challenge 4 – Standardization for unique configs - done

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

Challenge 5 – Dependencies - done

- Equipment availability, timing of partner involvement, leveraged coordination with other related projects
Major Accomplishments

- AR and orchestrator capabilities analysis mapped to NIST report – February 2017
- SDG&E Testbed May 2017 and other Vendors (SecurityMatters, Phantom)
- Collaborating with other sensor based projects in OE
- Instrumented 3 substation automation configurations for performance measures to evaluate potential latency issues – September 2017
- Tested 2 unique AR technologies on SDG&E configuration – October 2017
- Go/NoGo on Novel AR – November 2017
- Connected AR to existing SIEM for integration to IT creating a 3rd limited AR – September 2018
Major Accomplishments

• Indicate and Remediate Beyond IT Basics
  • COTS Based Automated Response
  • Prototyped Machine to Machine Automated Threat Response

• Heartbleed – Detection and Alert

• Full Indicator and Remediation Actions
  • Unknown Telnet – Kill session/block port – COTS and Threat Monitoring Appliance (TMA)
  • WannaCry and Industroyer- use of common attacker C2 channels
  • BlackEnergy – Wiper/Kill Disk
  • Industroyer – Breaker Open
  • SIEM – Failed Logins
COTS Automated Response

Filter to return non-whitelisted IP address
Structured Threat Intelligence Graph
Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Multiple pathways for technology transfer
  - Open source code for multiple asset owners
  - Technology Provider partnership
  - Asset Owner partnership

- What are your 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
Knowledge to end user

• April 2017 – Presentation: Performance Measures Design – ICSJWG

• September 2017 – Preliminary Performance Metrics Test Results to Utility Partners

• May 2018 – Paper and Presentation: Efficacy and Effectiveness of Measures for AR at ISA PowID

• June 2018 – Presentation to the Electric Sector Coordinating Council

• August 2018 – Demo of AR and measures to EnergySec

• September 2018 – Presentation/Demo to California Public Utilities Commission

• September 2018 – Paper Referenced: Sharable and Implementable Threat Intelligence

• January 2019 DistribuTech as part of California Energy System for the 21st Century
Path Forward

- Creation and Test of Novel Launch AR
- Final Performance Metrics Collection and Analysis
- Open Source Launch AR – host on repository
- Provide final publication - Metrics