U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

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

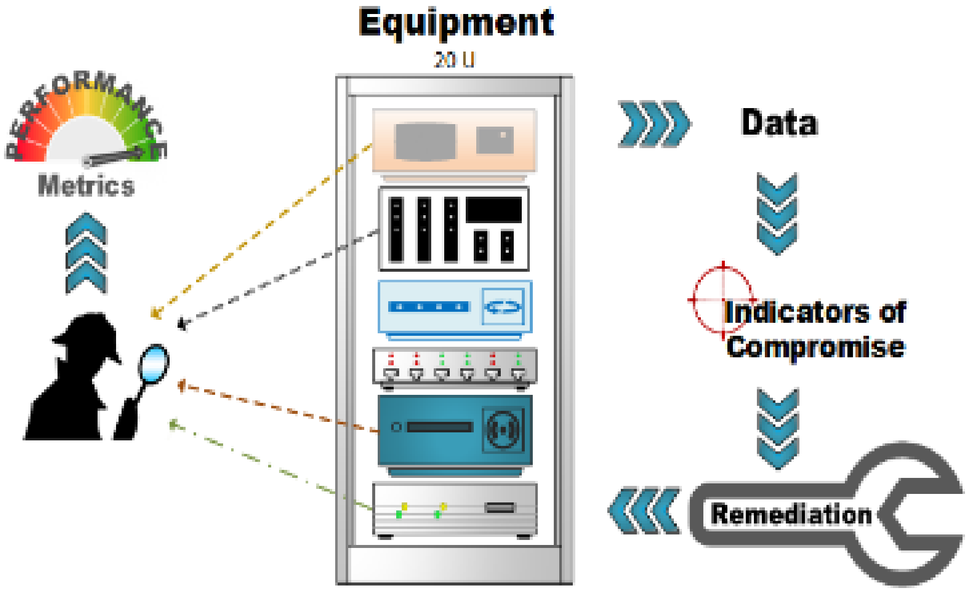
Summary: Validation and Measuring Automated Response

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



Performer:	Idaho National Laboratory
Partners:	San Diego Gas & Electric
Federal Cost:	$1.4M
Cost Share:	$150K
Total Value of Award:	$ 1.6M
Funds Expended to Date:	85%

Advancing the State of the Art (SOA)

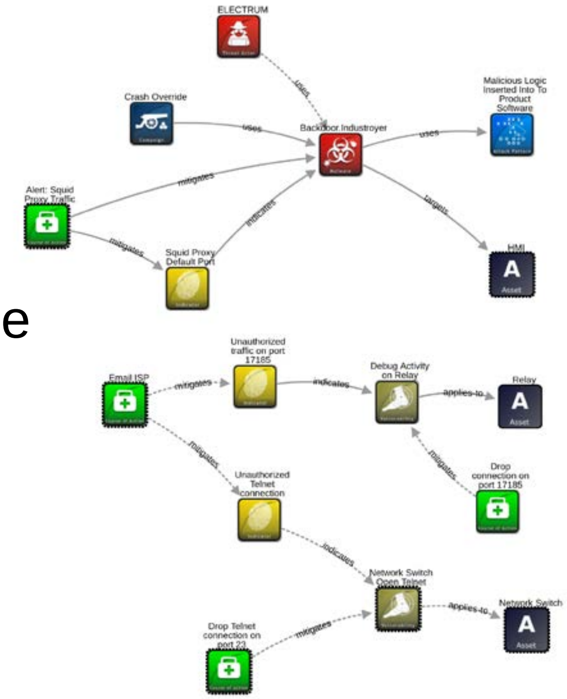
- In the Information Technology (IT), all in one Orchestrator command and control functionality

- 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.

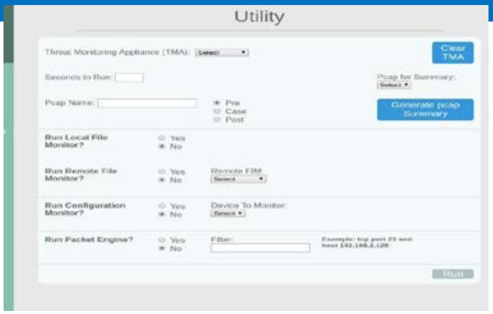
- With a well defined OT configuration, tailored responses can be provided for automation

- 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



Utility

Threat Monitoring Appliance (TMA): Select: ▾

Seconds to Run:

Pcap Name: ● Pre ○ Case ○ Post

Pcap for Summary: Select ▾

Run Local File Monitor? ○ Yes ● No

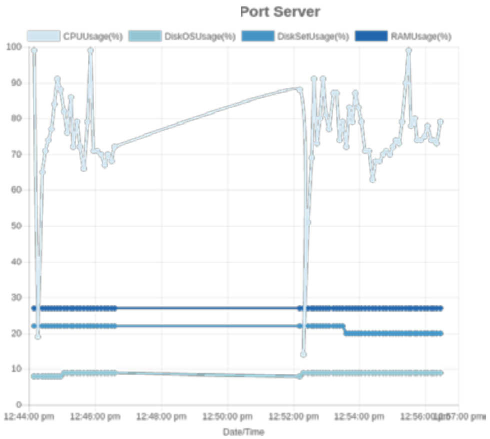
Run Remote File Monitor? ○ Yes ● No Remote FIM Select ▾

Run Configuration Monitor? ○ Yes ● No Device To Monitor: Select ▾

Run Packet Engine? ○ Yes ● No Filter: Example: tcp port 23 and host 192.168.2.120

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

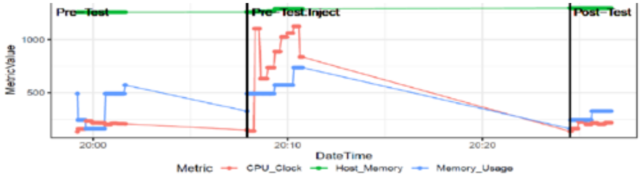
- Provide performance views – Test Utility with performance metrics

<u>Challenge 3 – Time to Test, Validate and Revert</u>

- **<u>Design test concepts, measures and rollback</u>**

Challenge 4 – Standardization for unique configs - done

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



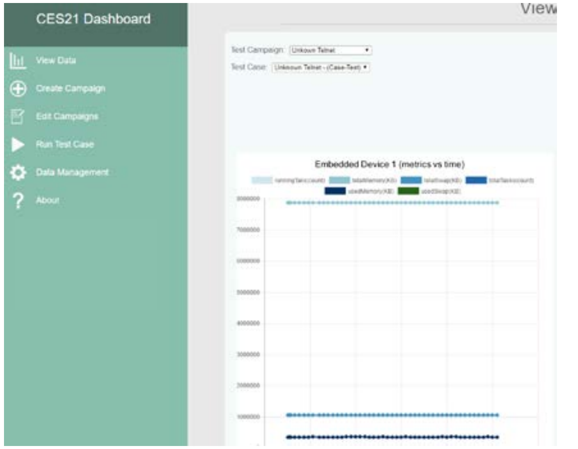
Challenge 5 – Dependencies - done

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

Progress to Date

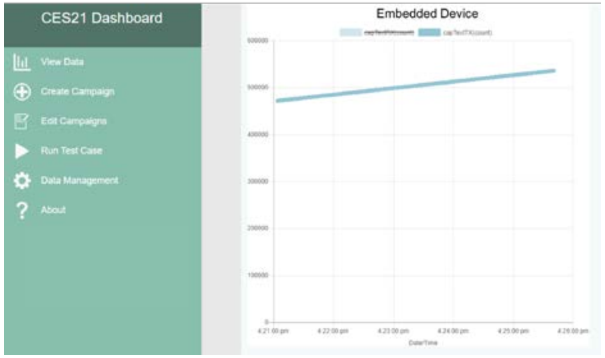
Major Accomplishments

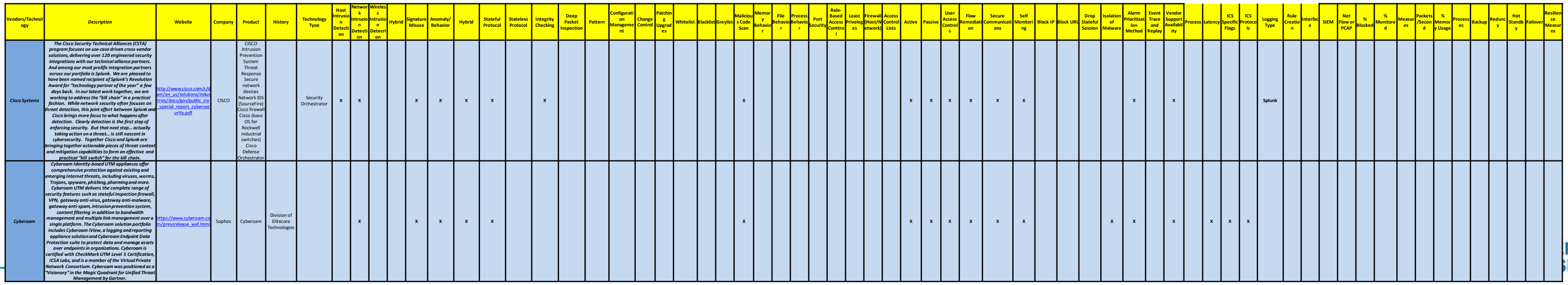
- AR and orchestrator capabilities analysis mapped to NIST report – February 2017
- SDG&E Testbed May 2017 and other Vendors (SecurityMatters, Phantom)
- Collaborating with other sensor based projects in OE
- Instrumented 3 substation automation configurations for performance measures to evaluate potential 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



Test Campaign: Unkown Telnet

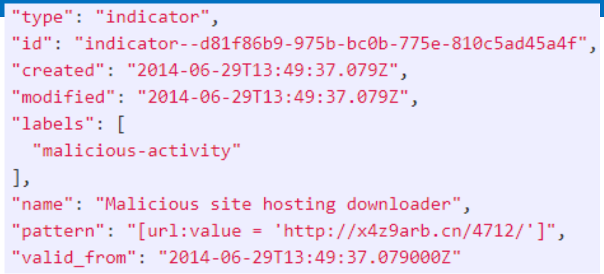
Test Case: Unknown Telnet - (Case-Test)





Vendors/Technology	Description	Website	Company	Product	History	Technology Tyoe	Host Intrusion Detection	Network Intrusion Detection	Wireless Intrusion Detecrion	Hybrid	Signature Misuse	Anomaly/Behavior	Hybrid	Stateful Protocol	Stateless Protocol	Integrity Checking	Deep Packet Inspection	Pattern	Configuration Management	Change Control	Patching Upgrades	Whitelist	Blacklist	Greylist	Malicious Code Scan	Memory Behavior	File Behavior	Process Behavior	Port Security	Role-Based Access Conttrol	Least Priveleges	Firewall (Host/Network)	Access Control Lists	Active	Passive	User Access Controls	Flaw Remediation	Secure Communications	Self Monitoring	Block IP	Block URL	Drop Stateful Session	Isolation of Malware	Alarm Prioritization Method	Event Trace and Replay	Vendor Support Availability	Process	Latency	ICS Specific Flags	ICS Protocols	Logging Type	Rule Creation	Interface	SIEM	Net Flow or PCAP	% Blocked	% Monitored	Measures	Packets/Second	% Memory Usage	Processes	Backup	Reduncy	Hot Standby	Failover	Resilience Measures
Cisco Systems	*The Cisco Security Technical Alliances (CSTA) program focuses on use-case driven cross-vendor solutions, delivering over 120 engineered security integrations with our technical alliance partners. And among our most prolific integration partners across our portfolio is Splunk. We are pleased to have been named recipient of Splunk's Revolution Award for "technology partner of the year" a few days back. In our latest work together, we are working to address the "kill chain" in a practical fashion. While network security often focuses on threat detection, this joint effort between Splunk and Cisco brings more focus to what happens after detection. Clearly detection is the first step of enforcing security. But that next step… actually taking action on a threat… is still nascent in cybersecurity. Together Cisco and Splunk are bringing together actionable pieces of threat context and mitigation capabilities to form an effective and practical "kill switch" for the kill chain.*	http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/public_cio_special_report_cybersecurity.pdf	CISCO	CISCO Intrusion Prevention System Threat Response Secure network devices Network IDS (SourceFire) Cisco firewall Cisco (base OS for Rockwell industrial switches) Cisco Defense Orchestrator		Security Orchestrator	x	x			x	x	x	x		x									x									x	x	x	x	x	x					x		x					Splunk															
Cyberoam	*Cyberoam Identity-based UTM appliances offer comprehensive protection against existing and emerging Internet threats, including viruses, worms, Trojans, spyware, phishing, pharming and more. Cyberoam UTM delivers the complete range of security features such as stateful inspection firewall, VPN, gateway anti-virus, gateway anti-malware, gateway anti-spam, intrusion prevention system, content filtering in addition to bandwidth management and multiple link management over a single platform. The Cyberoam solution portfolio includes Cyberoam iView, a logging and reporting appliance solution and Cyberoam Endpoint Data Protection suite to protect data and manage assets over endpoints in organizations. Cyberoam is certified with CheckMark UTM Level 5 Certification, ICSA Labs, and is a member of the Virtual Private Network Consortium. Cyberoam was positioned as a "Visionary" in the Magic Quadrant for Unified Threat Management by Gartner.*	https://www.cyberoam.com/pressrelease_waf.html	Sophos	Cyberoam	Division of Elitecore Technologies			x			x	x	x	x											x									x	x	x	x	x	x				x	x		x		x	x	x																

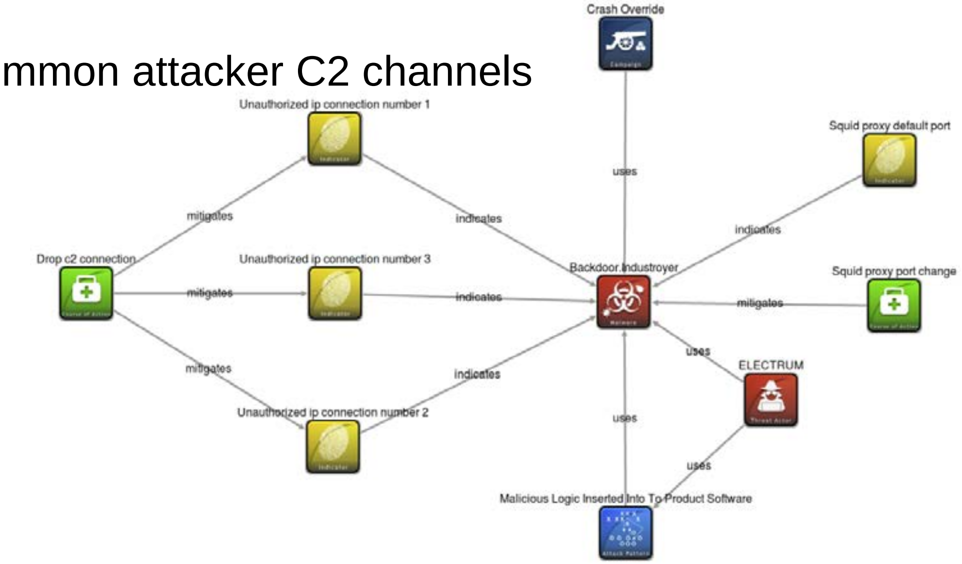
Progress to Date



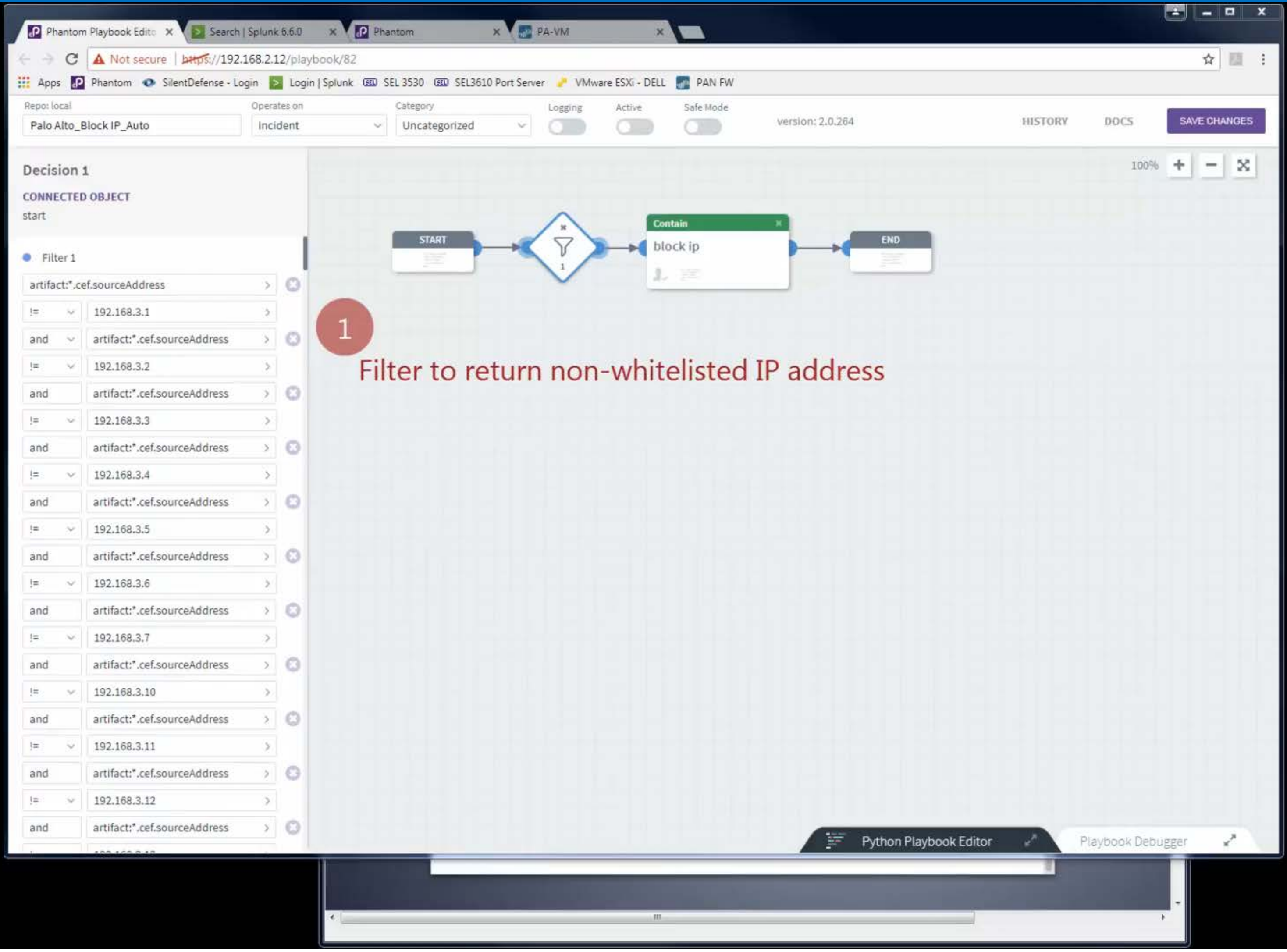
```
"type": "indicator",
"id": "indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f",
"created": "2014-06-29T13:49:37.079Z",
"modified": "2014-06-29T13:49:37.079Z",
"labels": [
  "malicious-activity"
],
"name": "Malicious site hosting downloader",
"pattern": "[url:value = 'http://x4z9arb.cn/4712/']",
"valid_from": "2014-06-29T13:49:37.079000Z"
```

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



Repo: local
Palo Alto_Block IP_Auto

Operates on: Incident

Category: Uncategorized

Logging | Active | Safe Mode

version: 2.0.264

Decision 1

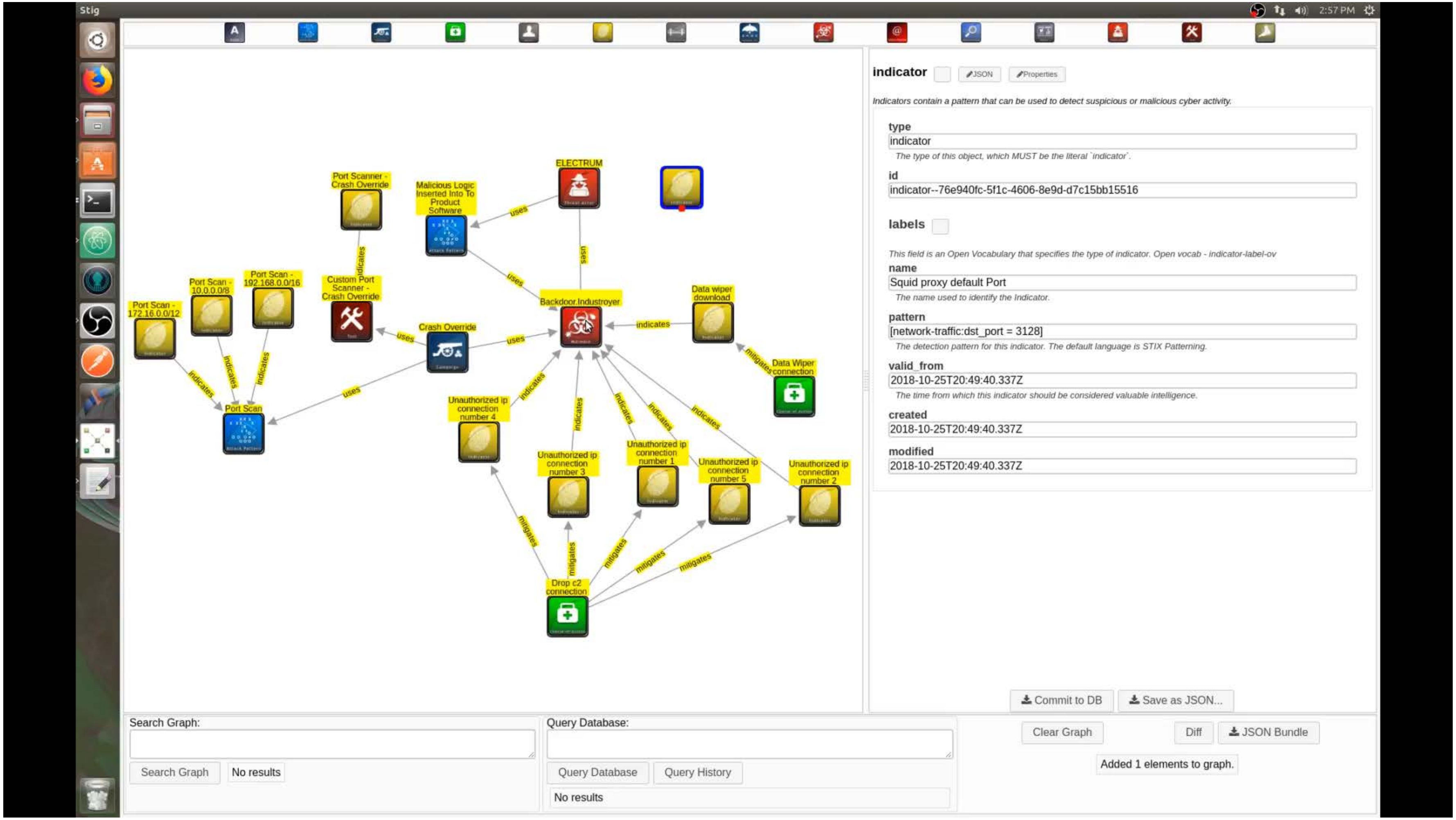
CONNECTED OBJECT
start

Filter 1

artifact:*.cef.sourceAddress
!= 192.168.3.1
and artifact:*.cef.sourceAddress
!= 192.168.3.2
and artifact:*.cef.sourceAddress
!= 192.168.3.3
and artifact:*.cef.sourceAddress
!= 192.168.3.4
and artifact:*.cef.sourceAddress
!= 192.168.3.5
and artifact:*.cef.sourceAddress
!= 192.168.3.6
and artifact:*.cef.sourceAddress
!= 192.168.3.7
and artifact:*.cef.sourceAddress
!= 192.168.3.10
and artifact:*.cef.sourceAddress
!= 192.168.3.11
and artifact:*.cef.sourceAddress
!= 192.168.3.12
and artifact:*.cef.sourceAddress

1 Filter to return non-whitelisted IP address

Structured Threat Intelligence Graph



indicator

Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity.

type
indicator
The type of this object, which MUST be the literal `indicator`.

id
indicator--76e940fc-5f1c-4606-8e9d-d7c15bb15516

labels □

This field is an Open Vocabulary that specifies the type of indicator. Open vocab - indicator-label-ov

name
Squid proxy default Port
The name used to identify the Indicator.

pattern
[network-traffic:dst_port = 3128]
The detection pattern for this indicator. The default language is STIX Patterning.

valid_from
2018-10-25T20:49:40.337Z
The time from which this indicator should be considered valuable intelligence.

created
2018-10-25T20:49:40.337Z

modified
2018-10-25T20:49:40.337Z

Search Graph:

No results

Query Database:

No results

Added 1 elements to graph.

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Multiple pathways for technology transfer
  - o Open source code for multiple asset owners
  - o Technology Provider partnership
  - o Asset Owner partnership
- What are your plans to gain industry acceptance?
  - o 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

Collaboration/Technology Transfer

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