Continuous Security Monitoring
Techniques for Energy Delivery Systems

Armin Rahimi, Adam Hahn, Mathew Merrick
Washington State University
Problem

“Continuous security state monitoring of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators”

– DOE Roadmap to Achieve Energy Delivery Systems Cybersecurity Year 2020 Goal

What to monitor?

Unclear what data is available

Unclear how valuable various data is

• Configuration vs Events
• System vs Network
• Granularity
• False negatives
• False positives
• Information overload
## Current Technologies

<table>
<thead>
<tr>
<th></th>
<th>Continuous monitoring/real time detection</th>
<th>Risk assessment</th>
<th>Asset discovery</th>
<th>Use of AI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness Solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CyberX</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Claroty</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Darktrace</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dragos Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indegy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NexDefense</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nozomi Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SecurityMatters</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Utilidata</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integrated Solutions</strong></td>
<td><strong>Generic IT product. Not geared towards PG</strong></td>
<td><strong>Generic IT product. Not geared towards</strong></td>
<td><strong>Generic IT product. Not geared towards</strong></td>
<td><strong>Generic IT product. Not geared towards</strong></td>
</tr>
<tr>
<td>Aperio</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CyberArk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nextnine</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sentryo</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Veracity Industrial Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Cybex: Continuous real time threat monitoring, asset discovery, use of AI
- Claroty: Continuous monitoring, Risk assessment
- Sentryo: Continuous monitoring, asset discovery, vulnerability management, user defined severity
- Veracity Industrial Networks: Continuous monitoring, security zone creation
What to Monitor?

**Approach**

1. Identify feasible system attack paths
2. Determine coverage of attack monitoring capabilities
3. Develop system-level coverage metrics

---

MITRE ATT&CK based Tactic and Techniques

Graph Modes/Algorithms
**What Mechanisms?**

**Questions:**
1) What feature set is important to detect malicious activity?

2) What mechanisms must be deployed to detect those feature?

<table>
<thead>
<tr>
<th>Mechanisms</th>
<th>Network</th>
<th>Process</th>
<th>File/Registry</th>
<th>Authentication</th>
<th>Power Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Flows</td>
<td>Payload</td>
<td>Exec</td>
<td>Read</td>
<td>Write</td>
</tr>
<tr>
<td>Switch/NF</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDS</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Win Logs</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>AV</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>App Logs</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

* Rough estimate
System Model

For each node define attributes based on

Configurations
i) operating system
ii) enabled services

Monitoring capabilities

Mechanisms (NF, IDS, Event Logs, etc) and features

Attacks

MITRE ATT&CK (Tactics and Techniques)
System Model - Monitoring strategy

Define the set of deployed monitoring mechanisms

**Monitoring Strategy**

\[ S : N(G) \rightarrow M \]

\[ M = \{NF, IDS, Event Log, \ldots\} \]

\[ m_i = \{NF, BRO, Snort, Winlog, relay config\} \]

Example

- \( S(fw1) = \{BRO\} \)
- \( S(fw2) = \{BRO\} \)
- \( S(sw1) = \{NF\} \)
- \( S(sw2) = \{NF\} \)
- \( S(hmi) = \{Win Evt\} \)
- \( S(dms) = \{Win Evt\} \)
- \( S(gw) = \{Win Evt\} \)
### Attack Techniques - MITRE ATT&CK...

<table>
<thead>
<tr>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense and Operational Tactic</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Execution</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
<th>Disruption</th>
<th>Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware</td>
<td></td>
<td>Loadable Module</td>
<td>Block Comm Port</td>
<td>Create Account</td>
<td>Control Process</td>
<td>Exploitation of Vulnerability</td>
<td>Alternate Modes of Operation</td>
<td>Data Staged</td>
<td>Data Compressed</td>
<td>Communication Through Removable Media</td>
<td>Block Comm Port</td>
</tr>
<tr>
<td>Interactive Service</td>
<td></td>
<td>Valid Accounts</td>
<td>Block Reporting Message</td>
<td>Credential Dumping</td>
<td>File and Directory Enumeration</td>
<td>External Remote Service</td>
<td>Command-Line Interface</td>
<td>Data from Local System</td>
<td>Data Encoding</td>
<td>Connection Proxy</td>
<td>Block Command Message</td>
</tr>
<tr>
<td>Loadable Module</td>
<td></td>
<td>Web Shell</td>
<td>Code Signing</td>
<td>Credentials in Files</td>
<td>ID/OD Module</td>
<td>Man in the Middle</td>
<td>Exploitation of Vulnerability</td>
<td>Data from Network Service</td>
<td>Data Encrypted</td>
<td>Custom Command and Control Protocol</td>
<td>Block Reporting Message</td>
</tr>
<tr>
<td>Modify Control Logic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module Firmware</td>
<td></td>
<td>Module Firmware</td>
<td>Inhibit Security Tools/Systems</td>
<td>Input Capture</td>
<td>Network Connection Enumeration</td>
<td>Taint Shared Content</td>
<td>Loadable Module</td>
<td>Screen Capture</td>
<td>Exfiltration Over Command and Control Channel</td>
<td>Data Obfuscation</td>
<td>Exploitation of Vulnerability</td>
</tr>
<tr>
<td>Non-Interactive Service</td>
<td></td>
<td>Man in the Middle</td>
<td>Function Multi-Factor Authentication</td>
<td>Network Enumeration</td>
<td>Third-party Software</td>
<td>Minimize System Settings</td>
<td>Non-Interactive Service</td>
<td>Video Capture</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Firmware</td>
<td>Man in the Middle</td>
</tr>
<tr>
<td>Rootkit</td>
<td></td>
<td>Virtual Terminal Services</td>
<td>Password Management</td>
<td>Role Identification</td>
<td>Third-party Software</td>
<td>Virtual Terminal Services</td>
<td>Virtual Terminal Services</td>
<td>Scripting</td>
<td>Multi-Stage Channels</td>
<td>Multi-Stage Channels</td>
<td>Multi-Stage Channels</td>
</tr>
<tr>
<td>Valid Accounts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Shell</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CARS

- Used in conjunction with ATT&CK
- ATT&CK describes general monitoring strategy
- CARS provides specific signatures within network packets or log events to look for in order to identify threats
- System logs for Remote Desktop Logon

\[
\text{[EventCode]} == 4624 \text{ and } \\
\text{[AuthenticationPackageName]} == 'Negotiate' \text{ and } \\
\text{[Severity]} == "Information" \text{ and } \\
\text{[LogonType]} == 10
\]
System Model – Attack Techniques

Goal: reduce number of tactics applied for each node...

**Tactics**

1. Persistence
2. Privilege Escalation
3. Defensive and Operator Evasion
4. Credential Access
5. Discovery
6. Lateral Movement
7. Execution
8. Collection
9. Exfiltration
10. Command and Control
11. Disruption
12. Destruction

**FSM of Attack in Phases**

- Privilege Escalation
- Destruct (S/N)
- Discovery (S/N)
- Execution (N)
- Lateral Movement (S/N)
- Disrupt (S/N)

**Simplified Model**

Q: N -> {Discovery, PrivEsc, Execution}
Q: E -> {Discovery, Lateral Movement}

* Focus on initial exploitation steps
Calculate node-based monitoring coverage score

For each node $n \in N$
  For each technique $t \in T$
    if $t.os \neq n.os$
      remove $t$;
    else if $t.service \notin n.services$
      remove $t$;
    else if $t.CAR \in n.f$
      $Tscore(t) = Pr(t.CAR \in \text{test sample})$
    else
      $Tscore(t) = 0$
  MonitoredScore($n$) = $||tscore||_2$

For each node

Techniques, $t$
Monitored features, $f$
Configuration, $c$
$Tscore$ vector = $[s(t_1)...s(t_m)]$
MonitoredScore = 0
How well monitored is this network?

Perform shortest path analysis from outside systems to each node.
Testbed Evaluation

Platform based on ELK Stack
(Elasticsearch, Logstash, Kibana)

Data Collection
- Syslogs
- Win Event Logs
- Bro Reports
- Relay Configs
- Netflows
- Snort

Visualization
- Kibana Dashboards

Analysis
- logstash
  Real-time monitoring, alerts, and metrics plugins

Corporate IT network

Control Center
- Distribution Mgmt System
- SCADA Server
- HMI

Substation
- Gateway
- Switch
- FW
- WAN
- FW
- FW
- FW
- Gateway Switch
- Relays
- Substation
- WAN
- FW
- FW
- FW
- FW
- FW
- FW
Data Samples

• One month period
• All the data is from normal day to day usage. No isolated data collection
• 6,199,109 Data points
• 1,534,160 netflow
• 4,657,519 Bro
  • DNS, FTP, HTTP, SMTP, SSL, conn, known_certs, Application
• 7,430 Winlog
  • System
  • Application
  • Security
  • PowerShell
### Tables

<table>
<thead>
<tr>
<th>Access Token Manipulation</th>
<th>Accessiblity Features</th>
<th>AppInit DLLs</th>
<th>Application Shimming</th>
<th>Bypass User Account Control</th>
<th>DLL Search Order Hijacking</th>
<th>Dylib Hijacking</th>
<th>Exploitation of Vulnerability</th>
<th>File System Permissions Weaknesses</th>
<th>Launch Daemon</th>
<th>New Service</th>
<th>Path Interception</th>
<th>Plist Modification</th>
<th>Schedule d Task</th>
<th>Service Registey Permissions Weaknesses</th>
<th>Setuid and Sigtgid</th>
<th>Startup Items</th>
<th>Sudo</th>
<th>Valid Accounts</th>
<th>Web Shell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacker</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>HMI</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>switch</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Gateway</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Relays</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Lateral Movement

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacker</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>HMI</td>
<td>N/A</td>
<td>25.15</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>88.5</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>switch</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Gateway</td>
<td>N/A</td>
<td>138.14</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Relays</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- N/A represents attack types we can’t currently monitor
- 0 means we can monitor for but it hasn’t happened
- Numbers are 1/probability of that event happening in the given time period of 30 days
## Tables

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacker</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HMI</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>switch</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relays</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Normalized probabilities using L2 normalization

- **HMI:** 102
- **Attacker:** 44.1
- **Switch:** 292.3
- **Gateway:** 138.4
- **Relays:** 0
Graph Results

Shortest path lengths from attacker:
- To gateway: 284.1
- To HMI: 146.1
- To switch 1: 44.1
- To switch 2: 273.4

- This is not strongly monitored
  - No netflow data from switch 1

- Shortest path for attacker to gateway:
  - 'gw': ['att', 'fw1', 'sw1', 'hmi', 'gw']
Future Works

• Further refine the calculations
• Implement more monitoring features in the ATT&CK list
• Look into automating the graph creation
• Account for what happens when a node goes down
• Account for what happens when an attacker has breached the network
Thanks

armin.rahimi@wsu.edu

https://github.com/wsu-smartcity