Applying Detection Engineering Methods to ICS

IoB Working Group

14 June 2022

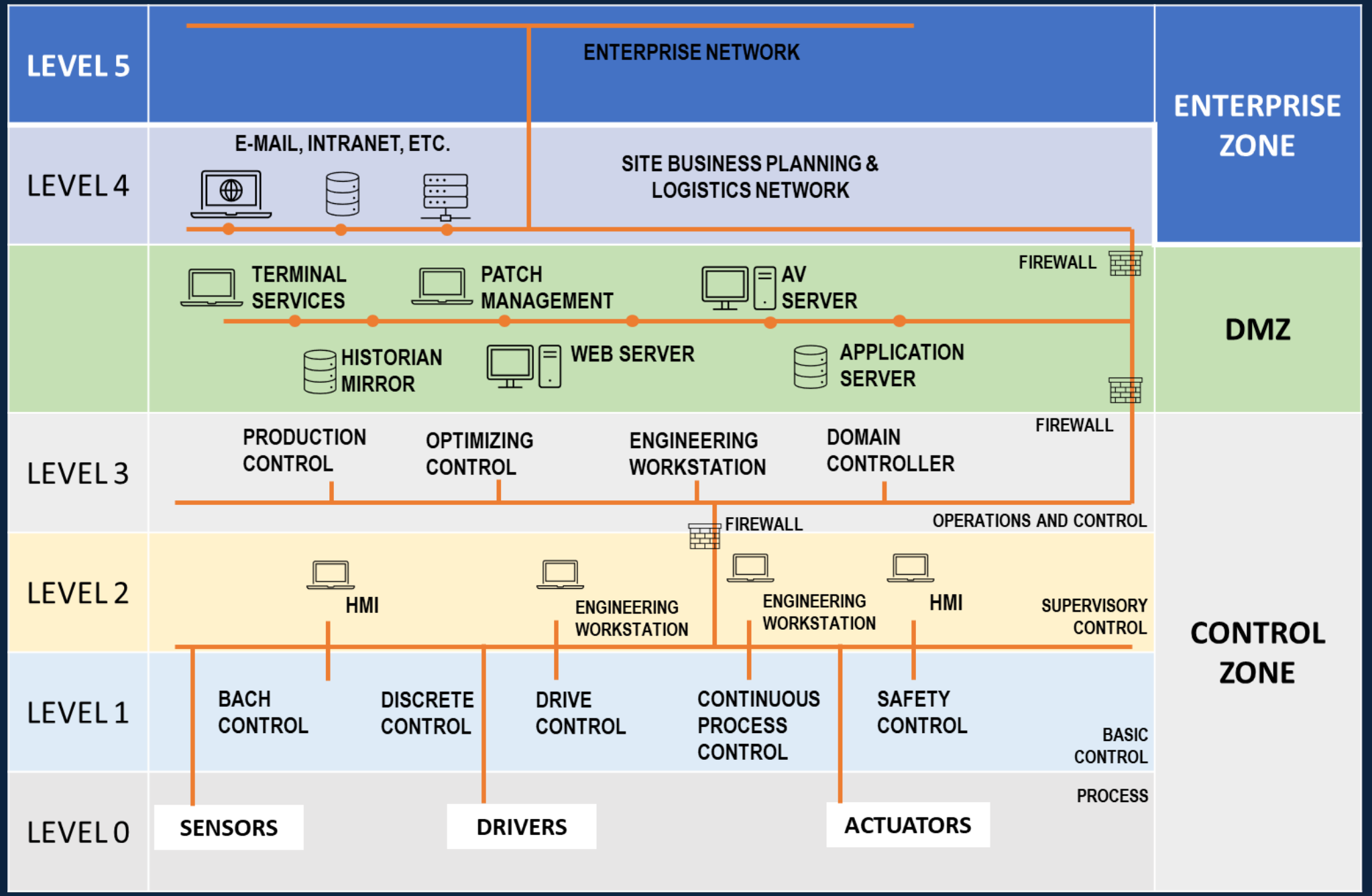
Michael McFail

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

Introduction

- **ICS environments and analytic strategy**
- **Challenges in ICS detection engineering**
- **Overcoming those obstacles**
  - Measuring detection coverage with capability abstractions
  - Use of a detection engineering / threat hunting methodology
  - Effective ICS purple teaming
- **Wrap-up**

Purdue Reference Architecture



ICS Analytic Strategy

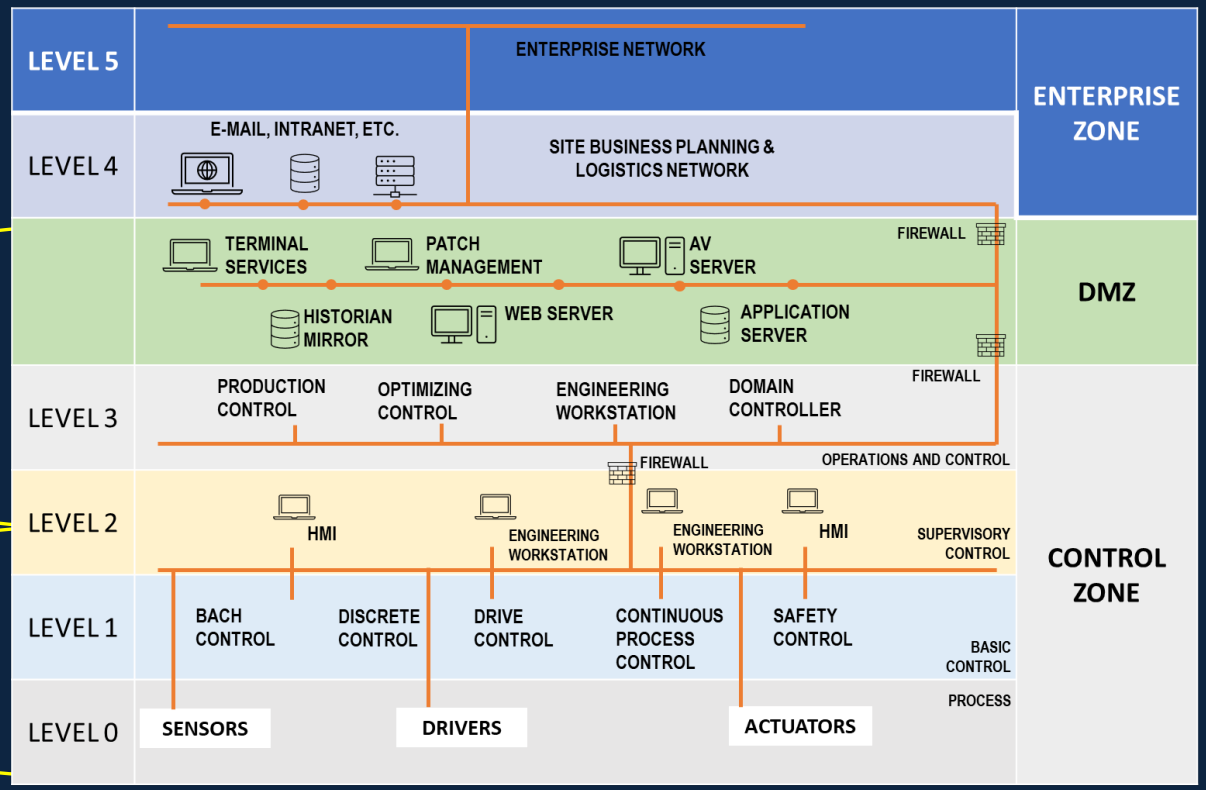
Access to
OT-supporting Devices
"IT/OT Pivot"

Business -> Process
Paradigm Shift

Business Enterprise

"OT Enterprise"

Process Operations

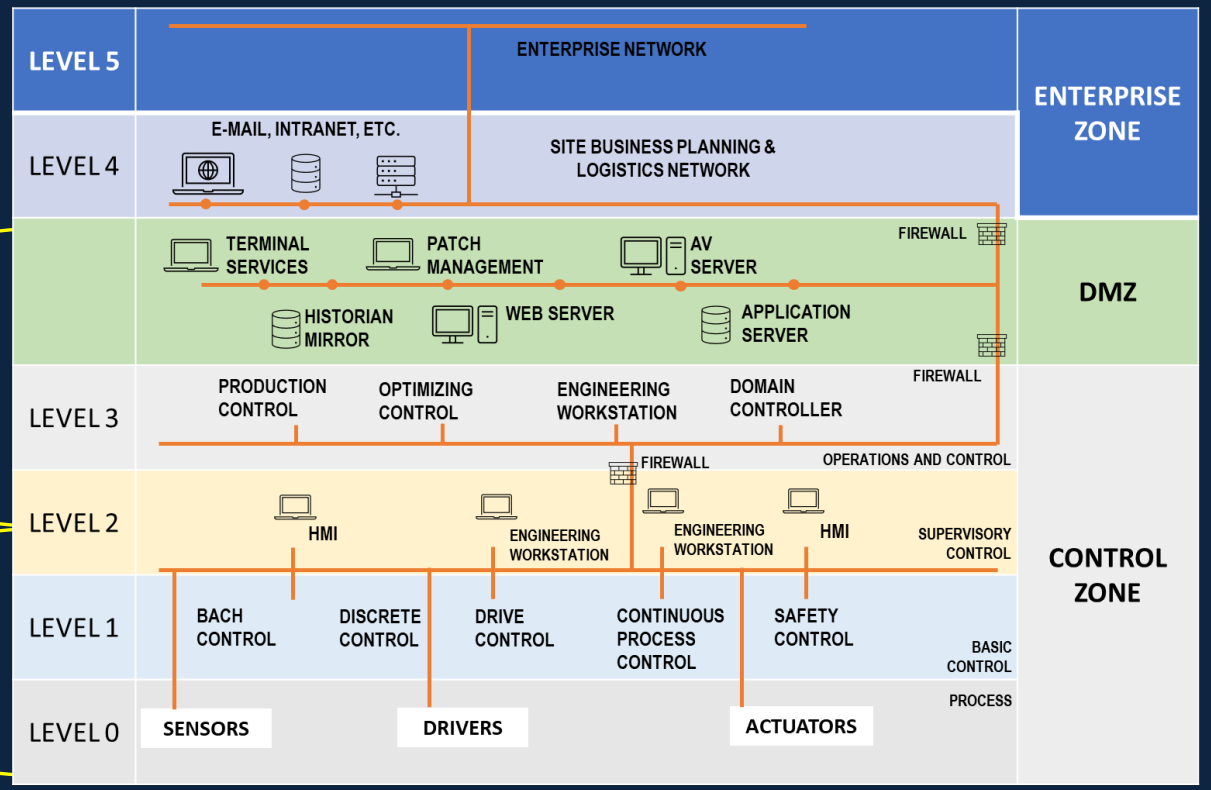


ICS Analytic Strategy

Business Enterprise

“OT Enterprise”

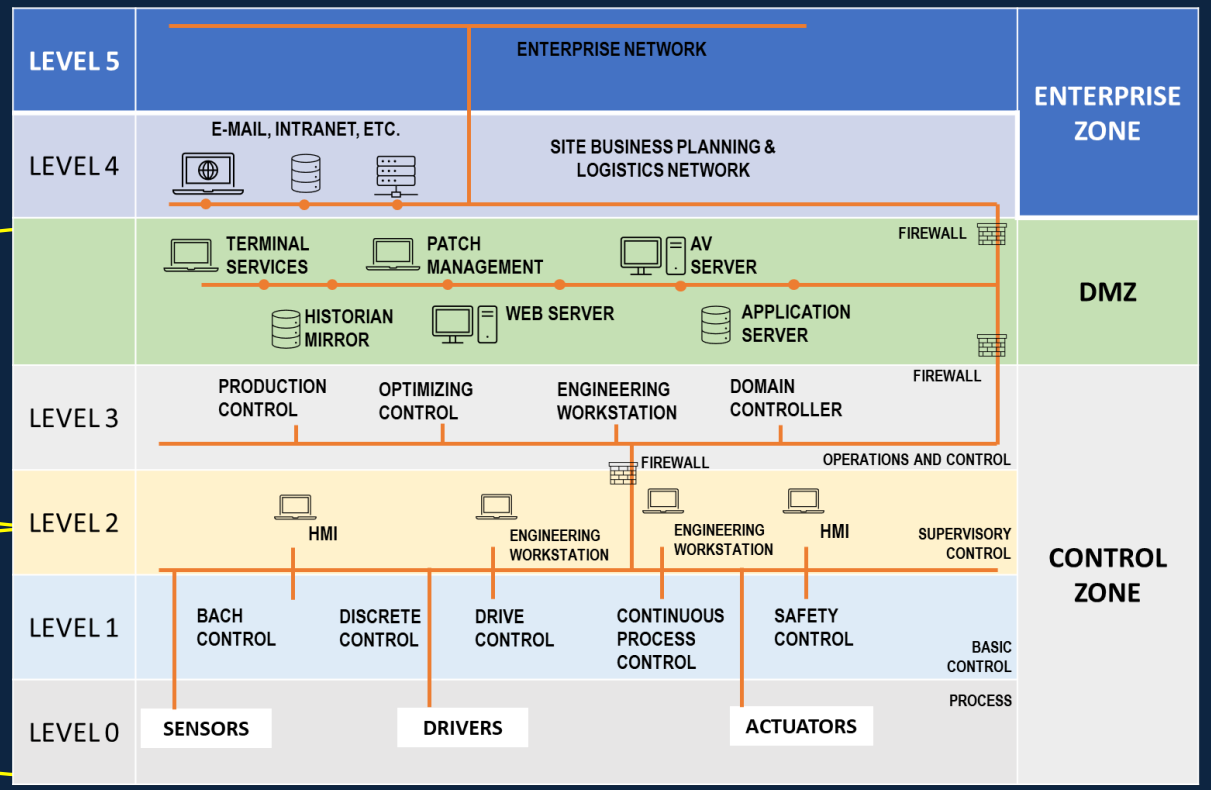
Process Operations



ICS Analytic Strategy

Defenders Should Start Here

- Business Enterprise
- "OT Enterprise"
- Process Operations



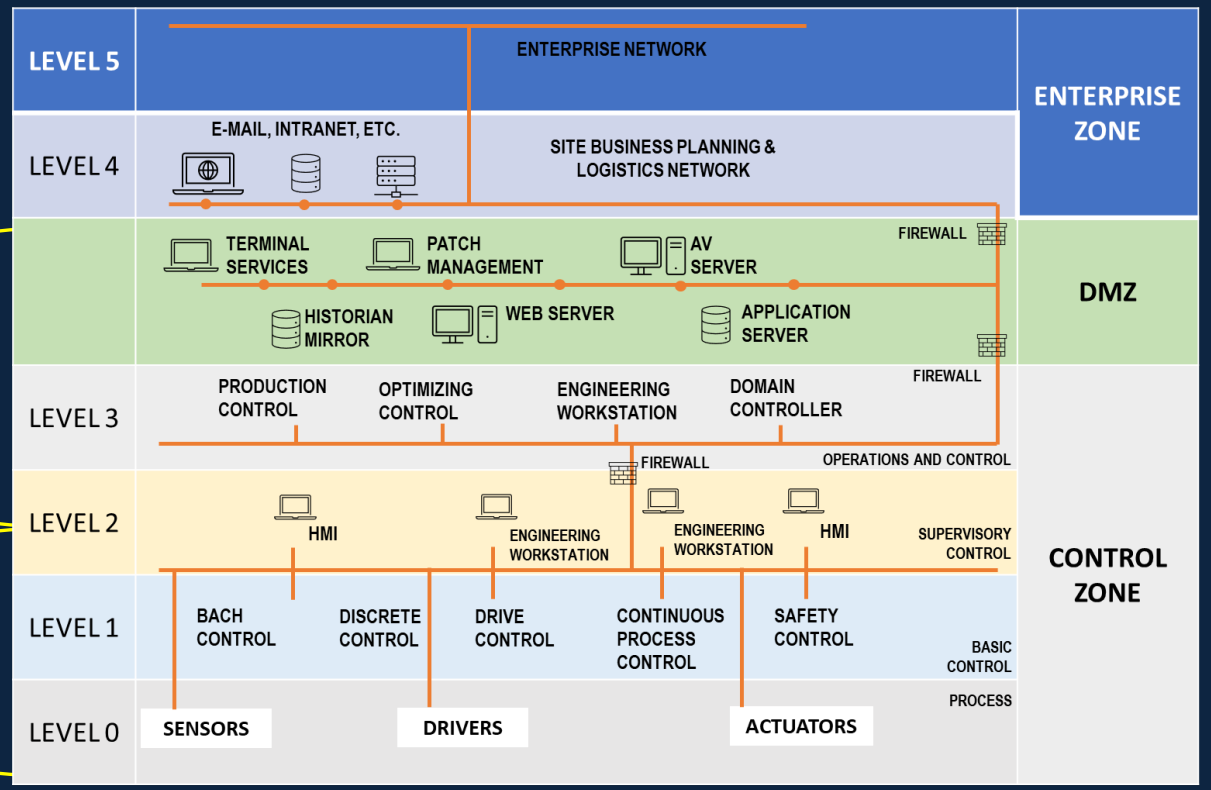
ICS Analytic Strategy

Business Enterprise

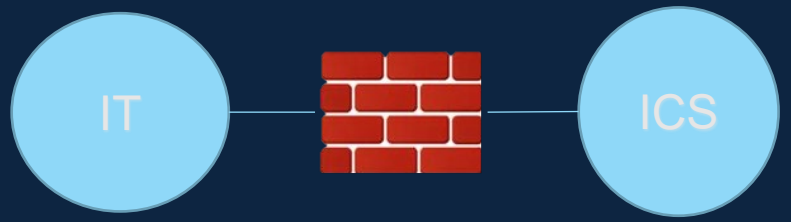
"OT Enterprise"

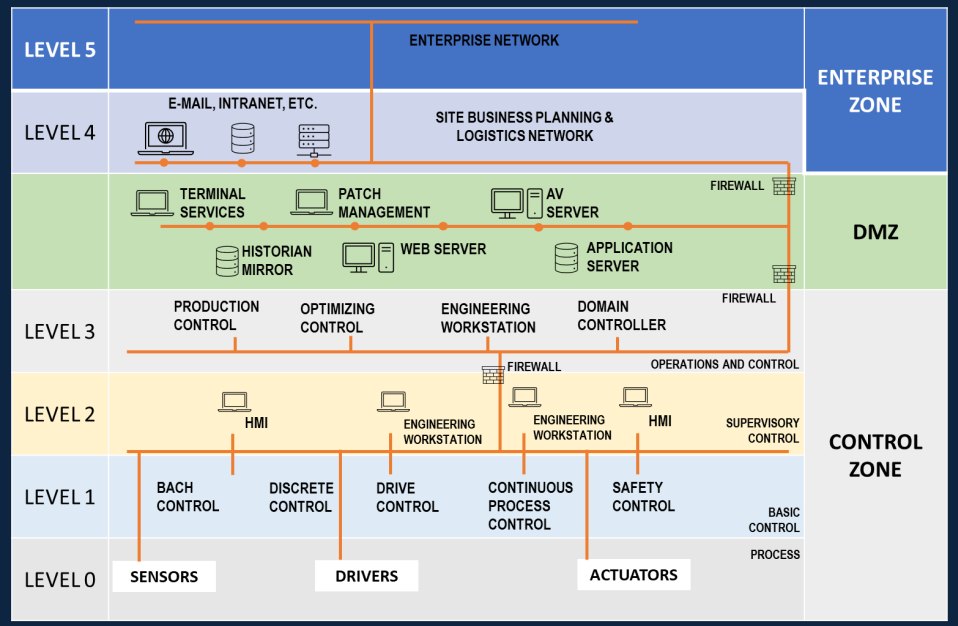
Process Operations

Our Focus

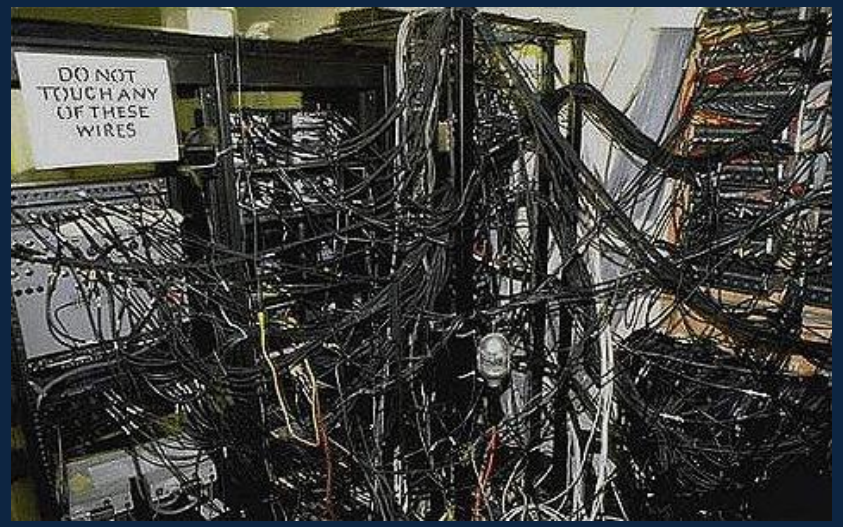


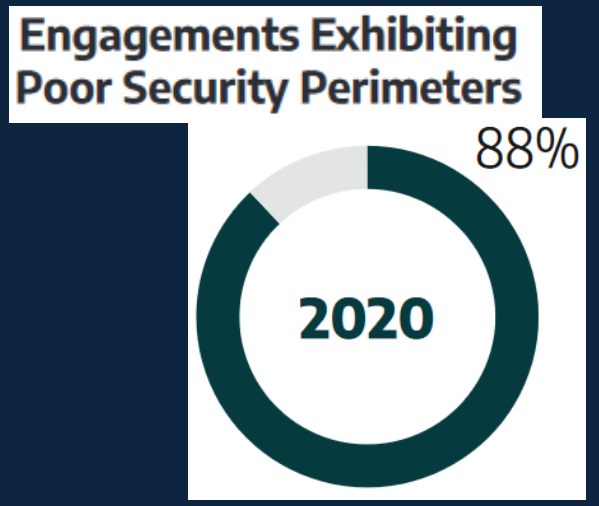
ICS is less like this…





and more like this…





https://www.researchgate.net/figure/Purdue-Enterprise-Reference-Architecture_fig1_336152125
http://faculty.ccbcmd.edu/~smacadof/
https://hub.dragos.com/hubfs/Year-in-Review/Dragos_2020_ICS_Cybersecurity_Year_In_Review.pdf

The Real World is Large and Messy

- **ICS environments are small and static *in some limited cases***
  - Your small-town wastewater treatment plant
  - A single electric substation
  - Certain DoD use cases, e.g, some weapons systems
- **The same thing holds in IT**
  - The Scranton branch of Dunder Mifflin is small and static

The Real World is Large and Messy

- **Small and static is not the environment we need to worry about**
  - Duke Energy handles electric generation, transmission and distribution
  - They have 7.4 million customers across 100k square miles
    - 250k miles of distribution lines
  - They do generation with nuclear, coal, hydro, solar, wind, oil and gas
    - Across ~98 facilities
  - The same scale (or larger!) applies to ICS across gov and private industry
- **That's the level of scale and complexity we need to tackle in the ICS space**
- **This difference in scale becomes a difference in kind**

Source: https://en.wikipedia.org/wiki/Duke_Energy

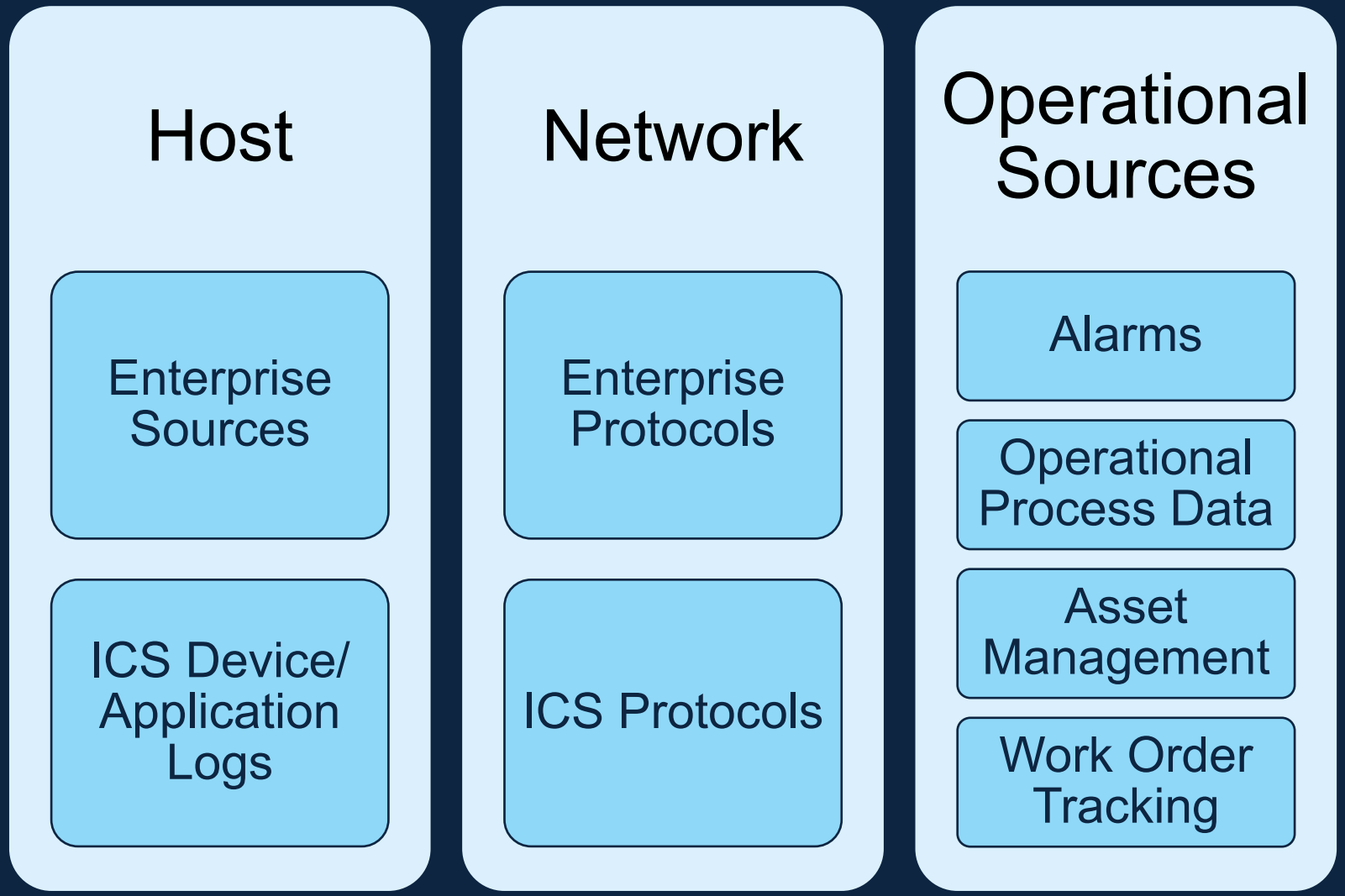
ICS Detection Engineering Challenges

- **ICS is *incredibly diverse***
  - Hardware, software, protocols, and configurations, oh my!
- **Domain knowledge is fragmented and difficult to generalize**
- **Use of legacy hardware, software and protocols**
- **ICS community is catching up to the importance of cyber security**
- **Difficulties with data collection**

ICS Detection Engineering Challenges

- **Extrapolating from a small number of incidents**
  - Even within those, we have gaps in finished intelligence
- **ATT&CK maps high confidence behaviors**
  - Appropriate for a public knowledge base
  - Lower confidence intel assessments may still be a good starting place for detection engineering
- **Generalizing procedures from intel to TTPs/behaviors is challenging**
  - Need context on the environment you're defending
  - Adversary emulation is especially valuable

ICS Data Sources



“Simplified Schema” for Documentation

Protocol

Protocol is the top-level differentiator used in defining requirements

While some vendor implementations will deviate from spec, largely we can find great re-use in building protocol features

e.g. BACnet, OPC-DA

Function

For each protocol, exposing the functions they support creates an explicit definition of protocol capabilities

Modbus → Function Code

BACnet → Service

S7 → Command

OPC-DA → Method

Payload

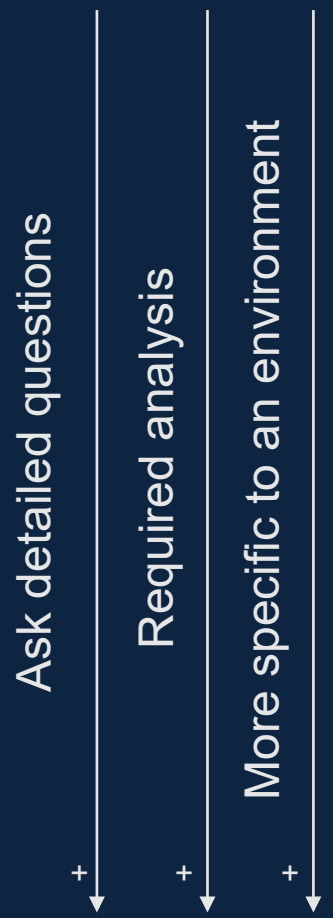
The payload contains the required contents needed to exact the effect intended for the given (protocol, function)

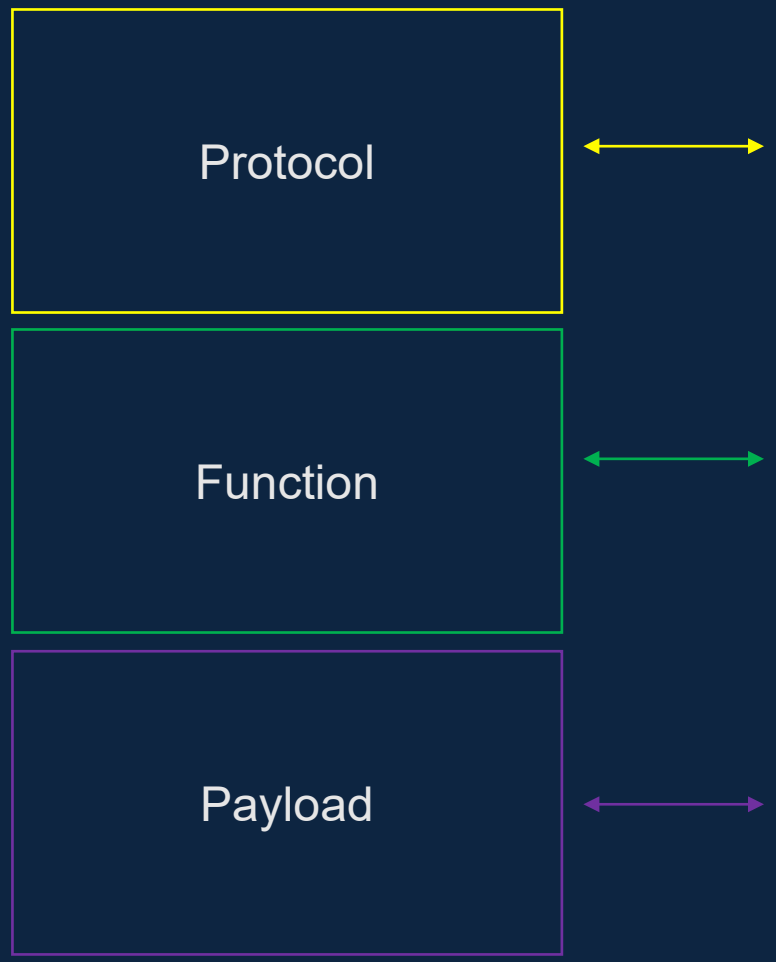
The payload defines a required interface to populate data against.

BACnet ReadProperty →

(device, obj-type, obj-inst, property, [index])

ICS Network Analytic Schema





DNP3 example

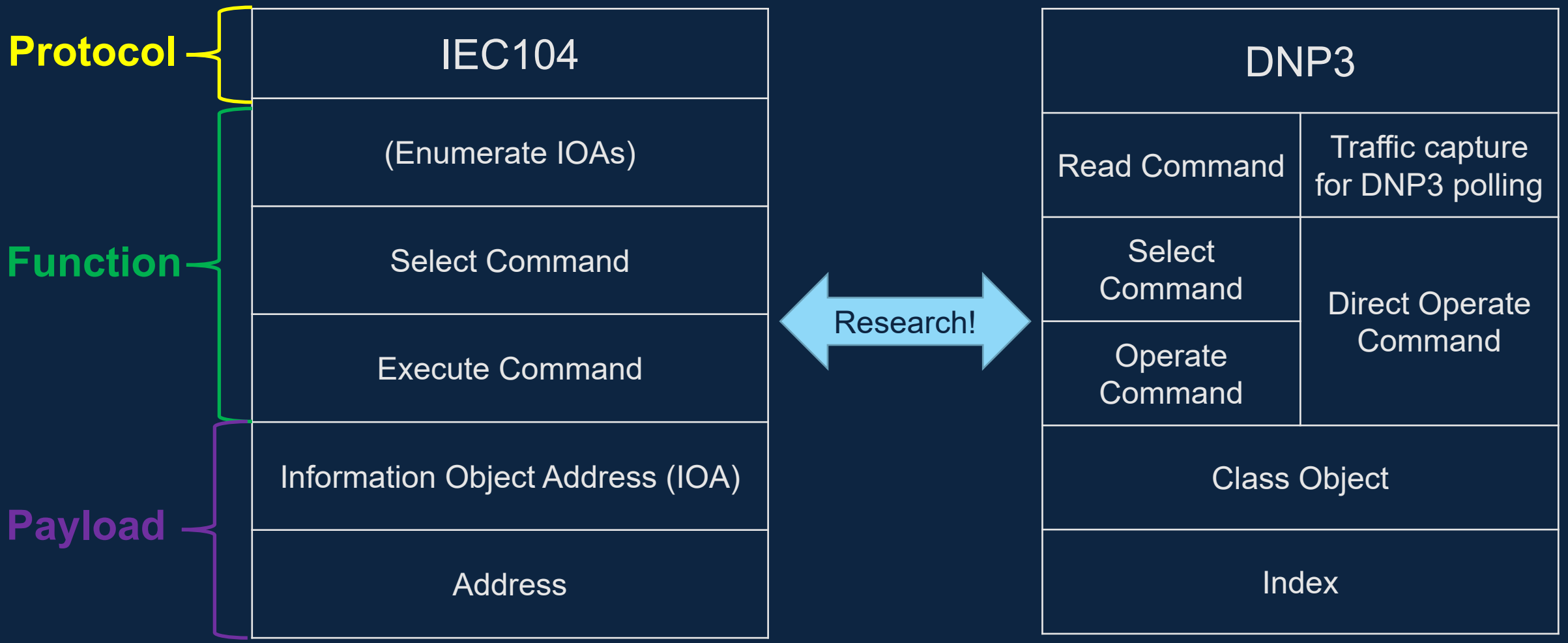
"I want to see when new DNP3 Clients (via IP address) talk to my DNP3 controller at 192.168.1.10."

"I want to be alerted whenever new devices issue DNP3 Read commands."

"I want to know the values of READ responses from my controller's memory to identify values I don't expect."

MITRE

Translating Data Requirements Across Protocols



OT Enterprise: Creating a New Windows Service

Create or Modify System Process: Windows Service (T1543.003)				
Procedure	Direct Service Creation			Sideloading via Registry Key
Tool	sc.exe	psexec.exe	wimic.exe	reg.exe
Windows API	CreateServiceA	RCreateServiceW	Win32_Service::Create	
RPC	SMB named pipe \PIPE\svcctl	SVCCTL	DCOM	
	UUID 367ABB81–9844–35F1-AD32–98F038001003		000001a0-0000-0000-c000-000000000046	
	Service Control Manager (services.exe)			
Artifacts	New/modified registry subkey under HKLM\SYSTEM\CurrentControlSet\Services			

SpecterOps Capability Abstraction concept

- https://posts.specterops.io/capability-abstraction-fbeaeeb26384
- https://abstractionmaps.com/maps/t1050/

OT Enterprise: Creating a New Windows Service

Create or Modify System Process: Windows Service (T1543.003)				
Procedure	Sandworm (Ukraine 2016) Direct Service Creation			Sideloading via Registry Key
Tool	sc.exe	psexec.exe	wimic.exe	reg.exe
Windows API	CreateServiceA	RCreateServiceW	Win32_Service::Create	
RPC	SMB named pipe \PIPE\svcctl	SVCCTL	DCOM	
	UUID 367ABB81–9844–35F1-AD32–98F038001003		000001a0-0000-0000-c000-000000000046	
	Service Control Manager (services.exe)			
Artifacts	New/modified registry subkey under HKLM\SYSTEM\CurrentControlSet\Services			

Event Log 4688
Sysmon 1

Event Log 4697
Event Log 7045

Sysmon 12

RPC Network Traffic

SMB Network Traffic

MITRE

An anecdote on protocol capabilities - BACnet

- bacpypes and sourceforce BACnet project's implementation
  - AtomicWriteFile operations take a filename as the required parameter
  - Taking this, we could hypothesize use of bytes transferred is a good metadata source for detection
  - A 12KB file transfer in short time would help identify any write file

172.20.32.200	47808	172.20.32.105	47808	udp	-	19.200213	170
172.20.32.200	47808	172.20.32.116	47808	udp	-	0.684077	85
172.20.32.200	47808	172.20.32.57	47808	udp	-	301.736106	1700
172.20.32.200	47808	172.20.32.55	47808	udp	-	304.756060	1700
172.20.32.200	47808	172.20.32.53	47808	udp	-	301.611212	1700
172.20.32.200	47808	172.20.32.50	47808	udp	-	307.124768	1700
172.20.32.200	47808	172.20.32.56	47808	udp	-	305.666934	1700
172.20.32.200	47808	172.20.32.52	47808	udp	-	303.296444	1700

Bytes transfered

An anecdote on protocol capabilities - BACnet

But…

- The implementation differs from the specification

Table 14-2. Structure of AtomicWriteFile Service Primitives

Parameter Name	Req	Ind	Rsp
Argument	M	M(=)	
File Identifier	M	M(=)	
Stream Access	S	S(=)	
File Start Position	M	M(=)	
File Data	M	M(=)	

- Byte transfer is an insufficient data source for identifying file writes by itself
- This affects how we can develop and emulate adversary capabilities
- This affects our technical goals and detection development

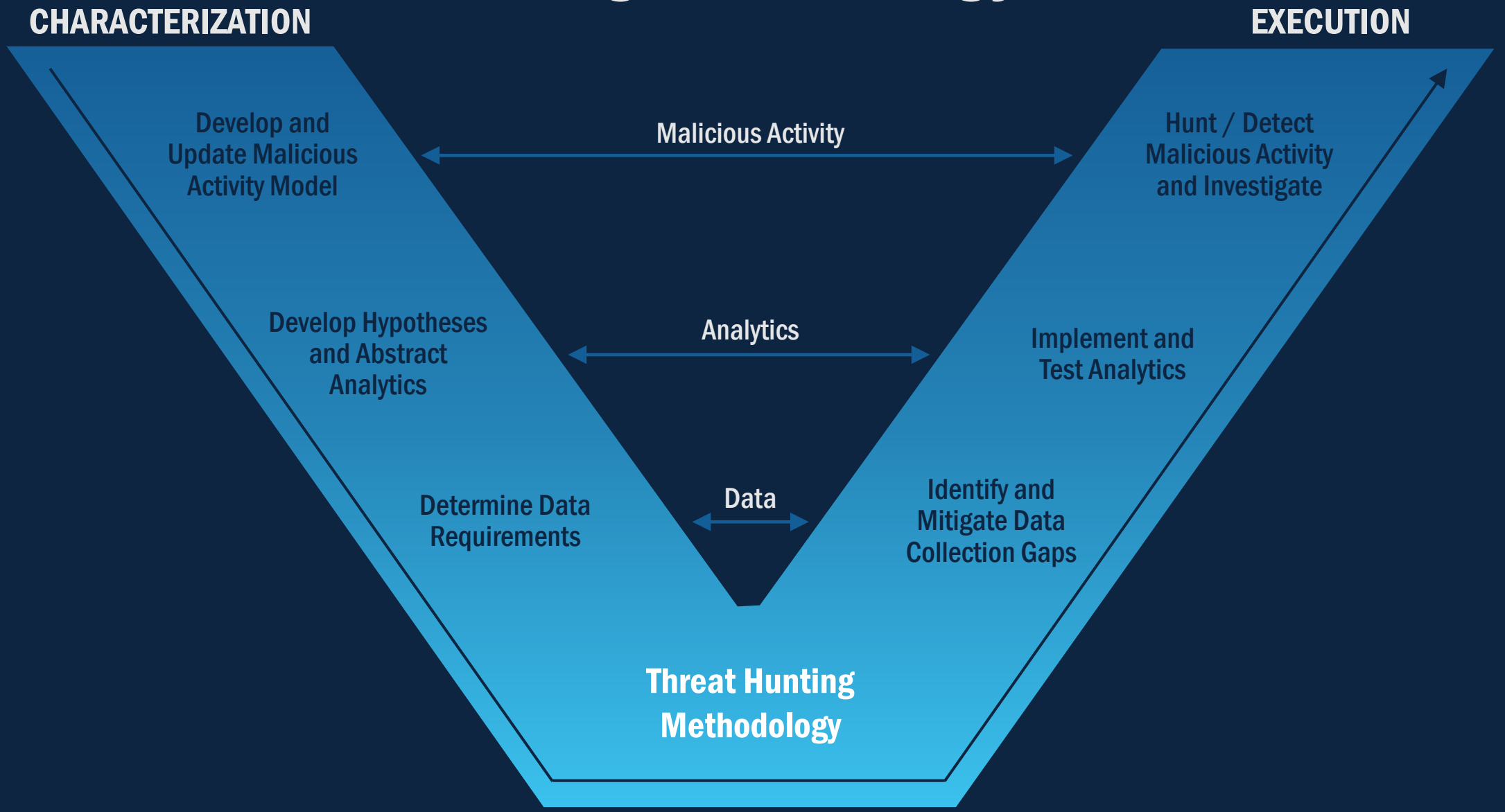
We cannot trust reference implementations blindly

BACNet File Write Capability Abstraction

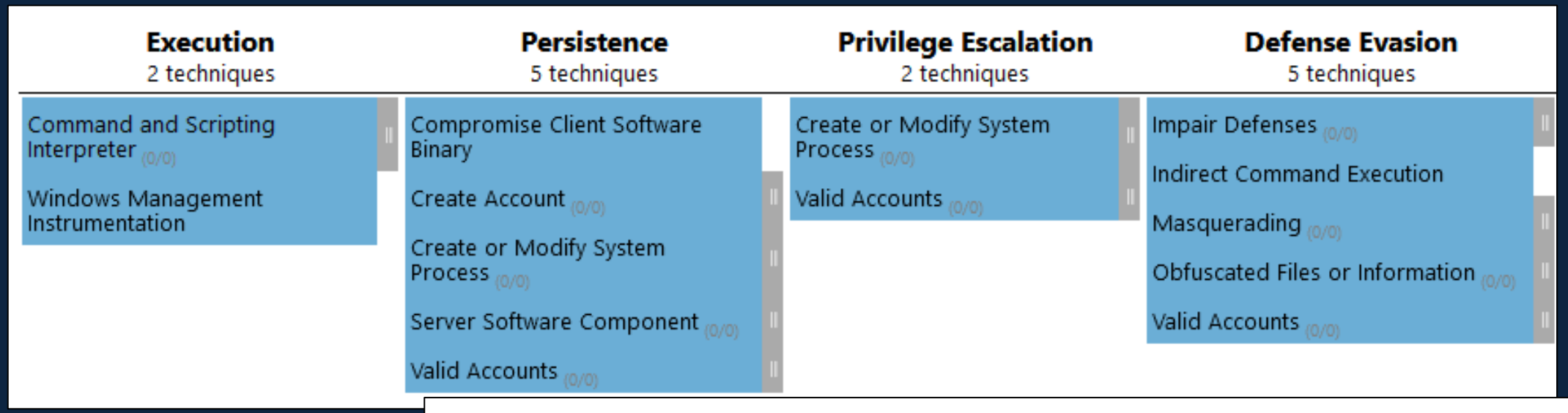
- We must seek to better understand system capabilities > implementations
  - Capability abstraction to the rescue!

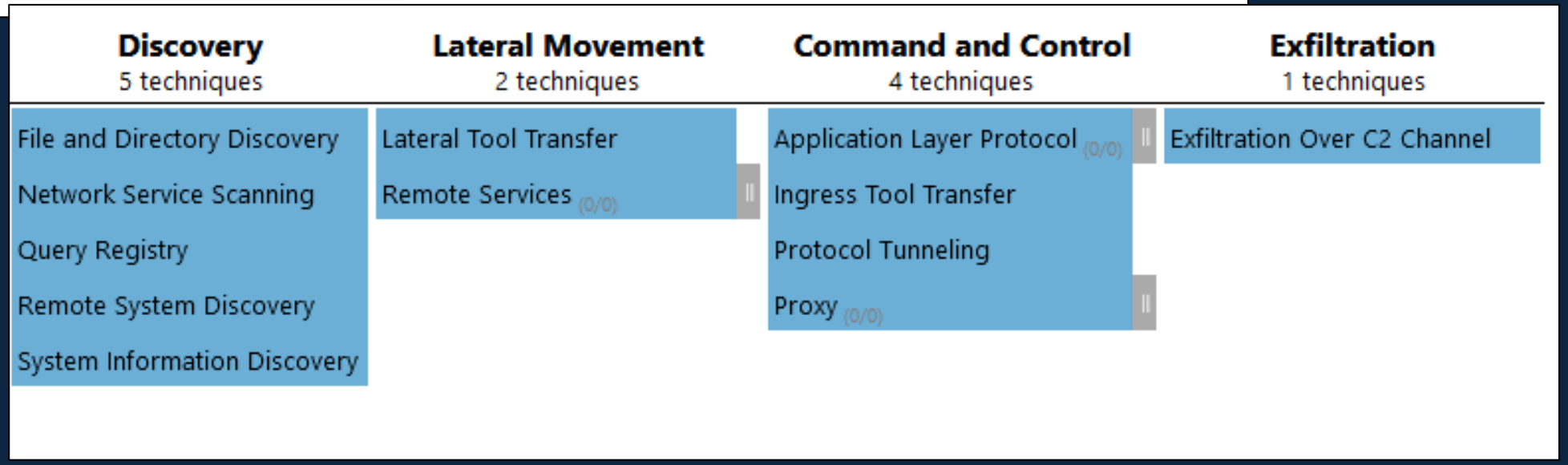
<table>
<tr><th colspan="5">BACNet</th></tr>
<tr><td colspan="5">Program Download / Modify Program / Modify Controller Tasking / System Firmware / Module Firmware / Modify Parameter</td></tr>
<tr><td>Behavior</td><td colspan="4">Use BACNet to write a file</td></tr>
<tr><td>Function</td><td colspan="4">Atomic File Write</td></tr>
<tr><td rowspan="2">Payload</td><td colspan="2">Stream Access</td><td colspan="2">Record Access</td></tr>
<tr><td>Write Entire File</td><td>Write File Chunk at Offset</td><td>Write Entire File</td><td>Write Records at Index</td></tr>
</table>

TCHAMP Threat Hunting Methodology

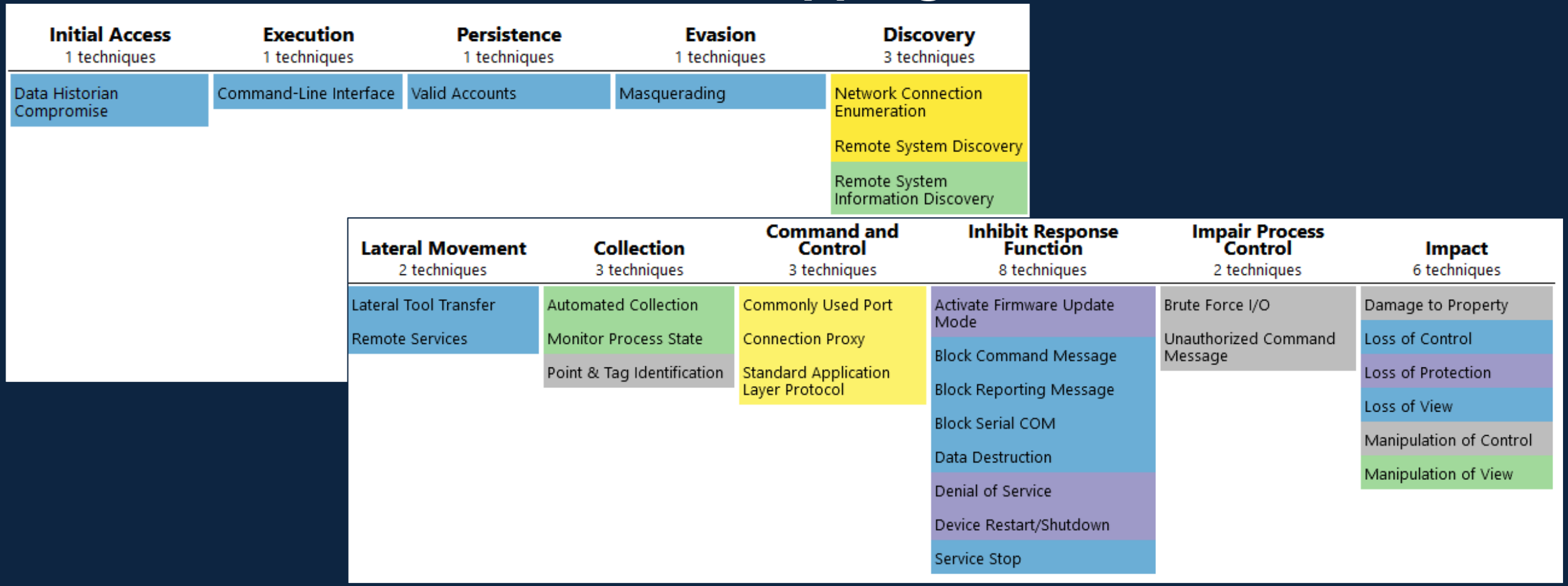


Ukraine 2016 Enterprise ATT&CK Mapping





Ukraine 2016 ICS ATT&CK Mapping



Windows (OT Enterprise)

IT Protocol

SCADA Specific

Env Specific

OT Protocol

MITRE

Ukraine 2016 - Analytics for Electric Distribution

Developing Abstract Attacks and Analytic Hypotheses

- **Creating broadly applicable abstract attacks and detections**
- **List out assumptions and walk-through attack and detection implications**
- **This has been a good exercise in dealing with environmental diversity**
- **OT enterprise (Windows) systems are in scope**
  - Many analytics will be widely reusable across environments
  - Review of open-source analytics (CAR, Sigma, Elastic)

Purple Teaming for Robust Detection Coverage

ATT&CK Mapping	Adversary Procedure	AE Behavior	High Level Analytic Idea	Data Requirements
ICS Matrix Collection Point and Tag Identification	The IEC104 module had the ability to use *Select and Execute* to switch state and confirm whether the IOA belongs to the single command type	Actively inserting DNP3 integrity polling (reads for class 0,1,2,3) from existing Master	Function Code Anomaly Detection (volume, periodicity, etc)	DNP3 function code
			Payload Anomaly Detection (FC anomaly detection with extra features)	DNP3 function code and payload

Purple Teaming for Robust Detection Coverage

Adversary Procedure	AE Behavior	High Level Analytic Idea	Data Requirements	Abstract Analytics	Detailed Data Requirements
Use IEC104 *Select and Execute* to confirm whether the IOA type	Actively inserting DNP3 integrity polling from existing Master	Function Code Anomaly Detection	DNP3 function code	High volume of reads	Read command statistics
				Change in read periodicity	Individual read commands
		Payload Anomaly Detection	DNP3 function code and payload	Read for a new data group	Group and Variation fields
				Read for a new class of data	Group and Variation fields

Purple Teaming for Robust Detection Coverage

Abstract Analytic	Detailed Data Requirements	Detailed Analytics
High volume of reads	DNP3 function code read command statistics	Reads from a new device
		Number of reads for a single device above threshold
		Number of reads for a single device below threshold
		Number of reads across multiple devices above threshold
		Number of reads across multiple devices below threshold

OT Protocol Analytic Example: Excessive Reads

- **Analytic: Excessive Read commands (asset enumeration)**
  - Determine if Read commands between two assets exceeds baseline threshold
- **ICS ATT&CK: *Collection: Point and Tag Identification***
  - Tied to technique and procedure – not just blindly throwing ML at the problem
- **Lots of ways to implement: Elastic/Splunk ML, vendors may have detections**
  - Provides requirements we can use to evaluate solutions
- **Data requirements:**
  - DNP3 function code parsing
  - What was being read? Need parsing to down to payload level to enable triage

OT Protocol Analytic Example: Analyst Context

- **Situational awareness context (dashboards)**
  - What is the normal rate of Read commands?
  - Which Objects are being read? Is that within the baseline?
    - Are any of them indicative of Collection?
      - Group 0 – Variation 250: product name and model; Variation 255: list all attributes; etc.
  - What user was logged into the Master?
- **Other analytics (potentially lower severity) – pull the thread on the Tactics lifecycle**
  - What asset normally talks to the outstation? Is this a **Rogue Master**?
  - Any indication of Discovery for the outstation? E.g., scanning, who-is queries (not DNP3)
  - Noisier analytics related to Persistence? New processes/services on the Master?
  - Noisier analytics related to Lat Movement/C2? Remote interactive sessions to Master?

Oh wow, more requirements!

Conclusion

- **Detection engineering needs to draw on**
  - Intelligence reports and models of adversary behavior
  - Adversary emulation
  - Domain knowledge on systems, architecture, protocols, environment
- **Need people in both red and blue hats to enable purple teaming**
- **Provide analyst context beyond ‘simply’ making analytics fire**
- **Detection eng. requirements inform collection and retention strategies**
  - Don’t pull a parser off the shelf and start writing analytics based on it

https://commons.wikimedia.org/wiki/File:Thats_all_folks.svg

Backup

OT Protocol Data Requirements

Determine Data Requirements

- **Decompose TTPs to the protocol, function and payload level**
- **In the attack the Industroyer IEC104 module could use Select and Execute to**
  - Enumerate Information Object Address (IOAs) [Point and Tag Identification]
  - Rapidly flip state on the IOA range of interest [Brute Force I/O]
- **In the target environment DNP3 can be used to**
  - Issue a Read command to enumerate Class 0,1,2,3 Objects
  - Issue Select with an index and operation type to reserve the resource
  - Issue an Operate command with the index and operation type to tell the device to performs the requested operation
- **This provides a framework for defining analytic requirements**
  - Data sources, parsing, sensor visibility, analytic logic operators, etc.

DNP3 Read Response

Default Zeek Parser


```
{
    "ts": 1583869914.742999,
    "uid": "COBIWOlui3Pwb5vlE5",
    "id.orig_h": "10.10.20.5",
    "id.orig_p": 20000,
    "id.resp_h": "10.10.20.8",
    "id.resp_p": 20000,
    "fc_request": "READ",
    "fc_reply": "RESPONSE",
    "iin": 0
}
```


	Time	Source	Destination	Protocol	Length
3	1583869914.742999	10.10.20.8	10.10.20.5	DNP 3.0	122

```
    [Reassembled DNP length: 298]
Application Layer: (FIR, FIN, Sequence 3, Response)
  > Application Control: 0xc3, First, Final(FIR, FIN, Sequence 3)
    Function Code: Response (0x81)
  > Internal Indications: 0x0000
  v RESPONSE Data Objects
    > Object(s): Binary Input With Status (Obj:01, Var:02) (0x0102), 120 points
    > Object(s): Binary Output Status (Obj:10, Var:02) (0x0a02), 34 points
    v Object(s): 16-Bit Analog Input (Obj:30, Var:02) (0x1e02), 20 points
      > Qualifier Field, Prefix: None, Range: 8-bit Start and Stop Indices
      > [Number of Items: 20]
      > Point Number 0 (Quality: Offline), Value: 960
      > Point Number 1 (Quality: Offline), Value: 1247
      > Point Number 2 (Quality: Offline), Value: 1235
      > Point Number 3 (Quality: Offline), Value: 1255
      > Point Number 4 (Quality: Offline), Value: 880
      > Point Number 5 (Quality: Offline), Value: 1350
      > Point Number 6 (Quality: Offline), Value: 870
      > Point Number 7 (Quality: Offline), Value: 0
      > Point Number 8 (Quality: Offline), Value: 0
      > Point Number 9 (Quality: Offline), Value: 0
      > Point Number 10 (Quality: Offline), Value: 0
      > Point Number 11 (Quality: Offline), Value: 0
      > Point Number 12 (Quality: Offline), Value: 0
      > Point Number 13 (Quality: Offline), Value: 0
      > Point Number 14 (Quality: Offline), Value: 0
      > Point Number 15 (Quality: Offline), Value: 0
      > Point Number 16 (Quality: Offline), Value: 0
      > Point Number 17 (Quality: Offline), Value: 0
      > Point Number 18 (Quality: Offline), Value: 0
      > Point Number 19 (Quality: Offline), Value: 0
    v Object(s): 16-Bit Analog Output Status (Obj:40, Var:02) (0x2802), 20 points
      > Qualifier Field, Prefix: None, Range: 8-bit Start and Stop Indices
      > [Number of Items: 20]
      > Point Number 0 (Quality: Offline), Value: 0
      > Point Number 1 (Quality: Offline), Value: 0
```

https://github.com/cisagov/icsnpp-dnp3/blob/master/examples/dnp3_example.pcap

MITRE

DNP3 Read Response

ICSNPP Parser


```
{
    "ts": 1583869914.739725,
    "uid": "COBIWOlui3Pwb5vlE5",
    "id.orig_h": "10.10.20.5",
    "id.orig_p": 20000,
    "id.resp_h": "10.10.20.8",
    "id.resp_p": 20000,
    "function_code": "READ",
    "object_type": "Class 0 Data"
}{
    "ts": 1583869914.742999,
    "uid": "COBIWOlui3Pwb5vlE5",
    "id.orig_h": "10.10.20.5",
    "id.orig_p": 20000,
    "id.resp_h": "10.10.20.8",
    "id.resp_p": 20000,
    "function_code": "RESPONSE",
    "object_type": "16-Bit Analog Input",
    "object_count": 20,
    "range_low": 0,
    "range_high": 19
}{
    "ts": 1583869914.742999,
    "uid": "COBIWOlui3Pwb5vlE5",
    "id.orig_h": "10.10.20.5",
    "id.orig_p": 20000,
    "id.resp_h": "10.10.20.8",
    "id.resp_p": 20000,
    "function_code": "RESPONSE",
    "object_type": "16-Bit Analog Output Status",
    "object_count": 20,
    "range_low": 0,
    "range_high": 19
}
```


	Time	Source	Destination	Protocol	Length
3	1583869914.742999	10.10.20.8	10.10.20.5	DNP 3.0	122

```
[Reassembled DNP length: 298]
Application Layer: (FIR, FIN, Sequence 3, Response)
> Application Control: 0xc3, First, Final(FIR, FIN, Sequence 3)
  Function Code: Response (0x81)
> Internal Indications: 0x0000
v RESPONSE Data Objects
  > Object(s): Binary Input With Status (Obj:01, Var:02) (0x0102), 120 points
  > Object(s): Binary Output Status (Obj:10, Var:02) (0x0a02), 34 points
  v Object(s): 16-Bit Analog Input (Obj:30, Var:02) (0x1e02), 20 points
    > Qualifier Field, Prefix: None, Range: 8-bit Start and Stop Indices
    > [Number of Items: 20]
    > Point Number 0 (Quality: Offline), Value: 960
    > Point Number 1 (Quality: Offline), Value: 1247
    > Point Number 2 (Quality: Offline), Value: 1235
    > Point Number 3 (Quality: Offline), Value: 1255
    > Point Number 4 (Quality: Offline), Value: 880
    > Point Number 5 (Quality: Offline), Value: 1350
    > Point Number 6 (Quality: Offline), Value: 870
    > Point Number 7 (Quality: Offline), Value: 0
    > Point Number 8 (Quality: Offline), Value: 0
    > Point Number 9 (Quality: Offline), Value: 0
    > Point Number 10 (Quality: Offline), Value: 0
    > Point Number 11 (Quality: Offline), Value: 0
    > Point Number 12 (Quality: Offline), Value: 0
    > Point Number 13 (Quality: Offline), Value: 0
    > Point Number 14 (Quality: Offline), Value: 0
    > Point Number 15 (Quality: Offline), Value: 0
    > Point Number 16 (Quality: Offline), Value: 0
    > Point Number 17 (Quality: Offline), Value: 0
    > Point Number 18 (Quality: Offline), Value: 0
    > Point Number 19 (Quality: Offline), Value: 0
  v Object(s): 16-Bit Analog Output Status (Obj:40, Var:02) (0x2802), 20 points
    > Qualifier Field, Prefix: None, Range: 8-bit Start and Stop Indices
    > [Number of Items: 20]
    > Point Number 0 (Quality: Offline), Value: 0
    > Point Number 1 (Quality: Offline), Value: 0
```

https://github.com/cisagov/icsnpp-dnp3/blob/master/examples/dnp3_example.pcap

DNP3 Read Response

ICSNPP Parser


```
{
    "ts": 1583869914.739725,
    "uid": "COBIWOlui3Pwb5vlE5",
    "id.orig_h": "10.10.20.5",
    "id.orig_p": 20000,
    "id.resp_h": "10.10.20.8",
    "id.resp_p": 20000,
    "function_code": "READ",
    "object_type": "Class 0 Data"
}{
    "ts": 1583869914.742999,
    "uid": "COBIWOlui3Pwb5vlE5",
    "id.orig_h": "10.10.20.5",
    "id.orig_p": 20000,
    "id.resp_h": "10.10.20.8",
    "id.resp_p": 20000,
    "function_code": "RESPONSE",
    "object_type": "16-Bit Analog Input",
    "object_count": 20,
    "range_low": 0,
    "range_high": 19
}{
    "ts": 1583869914.742999,
    "uid": "COBIWOlui3Pwb5vlE5",
    "id.orig_h": "10.10.20.5",
    "id.orig_p": 20000,
    "id.resp_h": "10.10.20.8",
    "id.resp_p": 20000,
    "function_code": "RESPONSE",
    "object_type": "16-Bit Analog Output Status",
    "object_count": 20,
    "range_low": 0,
    "range_high": 19
}
```


	Time	Source	Destination	Protocol	Length
3	1583869914.742999	10.10.20.8	10.10.20.5	DNP 3.0	122

```
[Reassembled DNP length: 298]
Application Layer: (FIR, FIN, Sequence 3, Response)
> Application Control: 0xc3, First, Final(FIR, FIN, Sequence 3)
  Function Code: Response (0x81)
> Internal Indications: 0x0000
v RESPONSE Data Objects
  > Object(s): Binary Input With Status (Obj:01, Var:02) (0x0102), 120 points
  > Object(s): Binary Output Status (Obj:10, Var:02) (0x0a02), 34 points
  v Object(s): 16-Bit Analog Input (Obj:30, Var:02) (0x1e02), 20 points
    > Qualifier Field, Prefix: None, Range: 8-bit Start and Stop Indices
    > [Number of Items: 20]
    > Point Number 0 (Quality: Offline), Value: 960
    > Point Number 1 (Quality: Offline), Value: 1247
    > Point Number 2 (Quality: Offline), Value: 1235
    > Point Number 3 (Quality: Offline), Value: 1255
    > Point Number 4 (Quality: Offline), Value: 880
    > Point Number 5 (Quality: Offline), Value: 1350
    > Point Number 6 (Quality: Offline), Value: 870
    > Point Number 7 (Quality: Offline), Value: 0
    > Point Number 8 (Quality: Offline), Value: 0
    > Point Number 9 (Quality: Offline), Value: 0
    > Point Number 10 (Quality: Offline), Value: 0
    > Point Number 11 (Quality: Offline), Value: 0
    > Point Number 12 (Quality: Offline), Value: 0
    > Point Number 13 (Quality: Offline), Value: 0
    > Point Number 14 (Quality: Offline), Value: 0
    > Point Number 15 (Quality: Offline), Value: 0
    > Point Number 16 (Quality: Offline), Value: 0
    > Point Number 17 (Quality: Offline), Value: 0
    > Point Number 18 (Quality: Offline), Value: 0
    > Point Number 19 (Quality: Offline), Value: 0
  v Object(s): 16-Bit Analog Output Status (Obj:40, Var:02) (0x2802), 20 points
    > Qualifier Field, Prefix: None, Range: 8-bit Start and Stop Indices
    > [Number of Items: 20]
    > Point Number 0 (Quality: Offline), Value: 0
    > Point Number 1 (Quality: Offline), Value: 0
```

https://github.com/cisagov/icsnpp-dnp3/blob/master/examples/dnp3_example.pcap

DNP3 Read Response

ICSNPP Parser


```
{
    "ts": 1583869914.739725,
    "uid": "COBIWOlui3Pwb5vlE5",
    "id.orig_h": "10.10.20.5",
    "id.orig_p": 20000,
    "id.resp_h": "10.10.20.8",
    "id.resp_p": 20000,
    "function_code": "READ",
    "object_type": "Class 0 Data"
}{
    "ts": 1583869914.742999,
    "uid": "COBIWOlui3Pwb5vlE5",
    "id.orig_h": "10.10.20.5",
    "id.orig_p": 20000,
    "id.resp_h": "10.10.20.8",
    "id.resp_p": 20000,
    "function_code": "RESPONSE",
    "object_type": "16-Bit Analog Input",
    "object_count": 20,
    "range_low": 0,
    "range_high": 19
}{
    "ts": 1583869914.742999,
    "uid": "COBIWOlui3Pwb5vlE5",
    "id.orig_h": "10.10.20.5",
    "id.orig_p": 20000,
    "id.resp_h": "10.10.20.8",
    "id.resp_p": 20000,
    "function_code": "RESPONSE",
    "object_type": "16-Bit Analog Output Status",
    "object_count": 20,
    "range_low": 0,
    "range_high": 19
}
```


	Time	Source	Destination	Protocol	Length
3	1583869914.742999	10.10.20.8	10.10.20.5	DNP 3.0	122

```
[Reassembled DNP length: 298]
Application Layer: (FIR, FIN, Sequence 3, Response)
> Application Control: 0xc3, First, Final(FIR, FIN, Sequence 3)
  Function Code: Response (0x81)
> Internal Indications: 0x0000
v RESPONSE Data Objects
  > Object(s): Binary Input With Status (Obj:01, Var:02) (0x0102), 120 points
  > Object(s): Binary Output Status (Obj:10, Var:02) (0x0a02), 34 points
  v Object(s): 16-Bit Analog Input (Obj:30, Var:02) (0x1e02), 20 points
    > Qualifier Field, Prefix: None, Range: 8-bit Start and Stop Indices
    > [Number of Items: 20]
    > Point Number 0 (Quality: Offline), Value: 960
    > Point Number 1 (Quality: Offline), Value: 1247
    > Point Number 2 (Quality: Offline), Value: 1235
    > Point Number 3 (Quality: Offline), Value: 1255
    > Point Number 4 (Quality: Offline), Value: 880
    > Point Number 5 (Quality: Offline), Value: 1350
    > Point Number 6 (Quality: Offline), Value: 870
    > Point Number 7 (Quality: Offline), Value: 0
    > Point Number 8 (Quality: Offline), Value: 0
    > Point Number 9 (Quality: Offline), Value: 0
    > Point Number 10 (Quality: Offline), Value: 0
    > Point Number 11 (Quality: Offline), Value: 0
    > Point Number 12 (Quality: Offline), Value: 0
    > Point Number 13 (Quality: Offline), Value: 0
    > Point Number 14 (Quality: Offline), Value: 0
    > Point Number 15 (Quality: Offline), Value: 0
    > Point Number 16 (Quality: Offline), Value: 0
    > Point Number 17 (Quality: Offline), Value: 0
    > Point Number 18 (Quality: Offline), Value: 0
    > Point Number 19 (Quality: Offline), Value: 0
  v Object(s): 16-Bit Analog Output Status (Obj:40, Var:02) (0x2802), 20 points
    > Qualifier Field, Prefix: None, Range: 8-bit Start and Stop Indices
    > [Number of Items: 20]
    > Point Number 0 (Quality: Offline), Value: 0
    > Point Number 1 (Quality: Offline), Value: 0
```

https://github.com/cisagov/icsnpp-dnp3/blob/master/examples/dnp3_example.pcap