

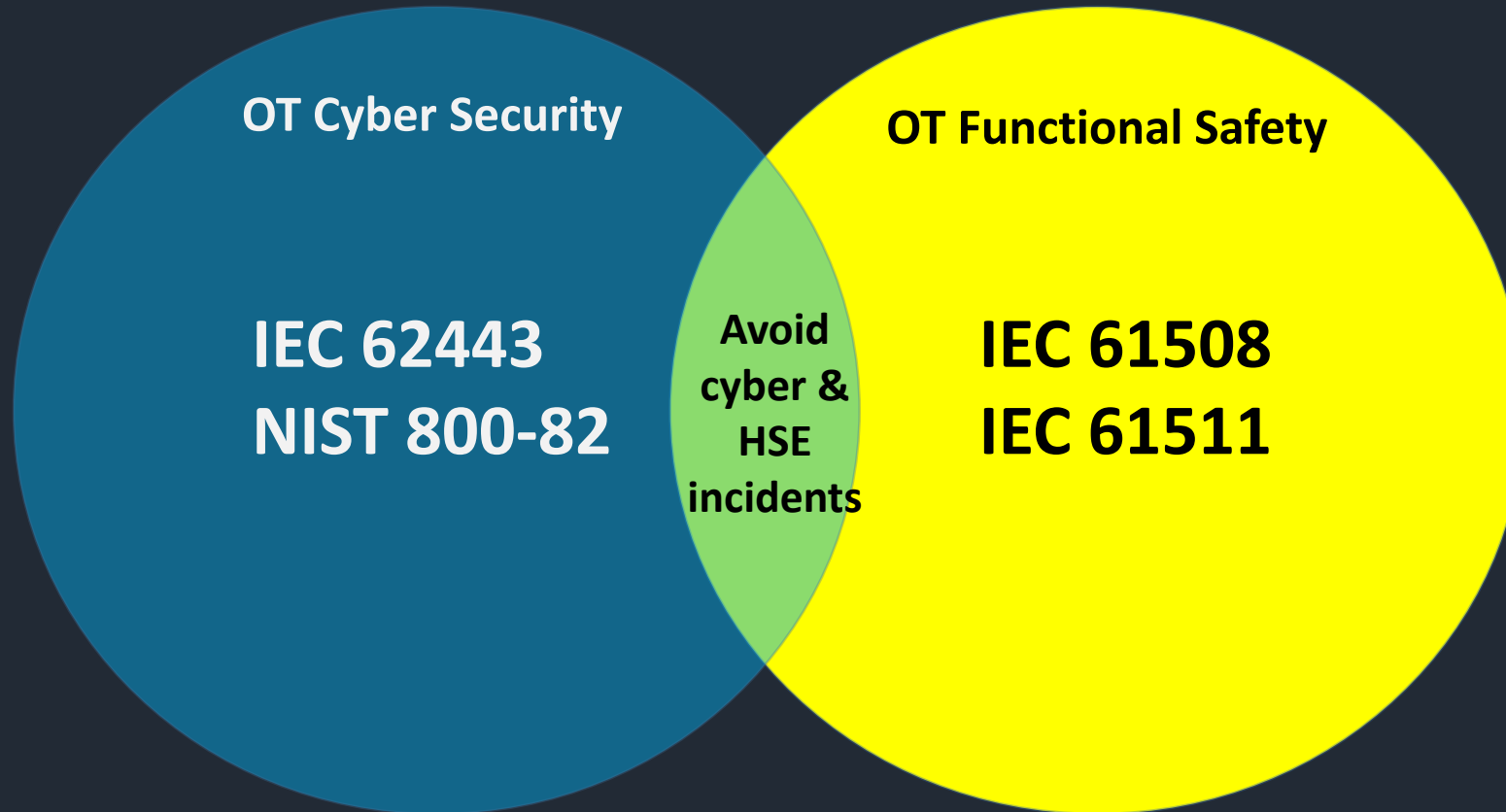


# **Case Study:** Active Defense and Intelligence-driven Cybersecurity in Critical Industries

Martin Fabry, Critical Infrastructure Cybersecurity Consultant  
CISSP, GICSP, CISA, CSSA, IEC 62443

# OT Cybersecurity

**Strong connection between Industrial Cybersecurity and Process Safety**



# Recent (Disturbing) Incidents

Adversaries are getting very sophisticated by using any means

## Indian nuclear power plant's network was hacked, officials confirm

After initial denial, company says report of "malware in system" is correct.

SEAN GALLAGHER - 10/30/2019, 3:25 PM



**Enlarge** / Malware attributed to North Korea's Lazarus group is confirmed to have infected a system on the administrative network of Nuclear Power Corp.'s Kudankulam plant in India.

## BIS ROZBILA SÍŤ RUSKÝCH ZPRAVODAJCŮ SKRYTÝCH ZA POČÍTAČOVOU FIRMOU

Šéf služby Michal Koudelka veřejně potvrdil akci, o které už Respekt letos psal



Šéf BIS Michal Koudelka • Autor: ČTK

# Active Defense & Monitoring in ICS/DCS

# OT Cybersecurity Standards

Recent survey says:







## Top 2019 Initiatives for Increasing OT/Control System and Network Security

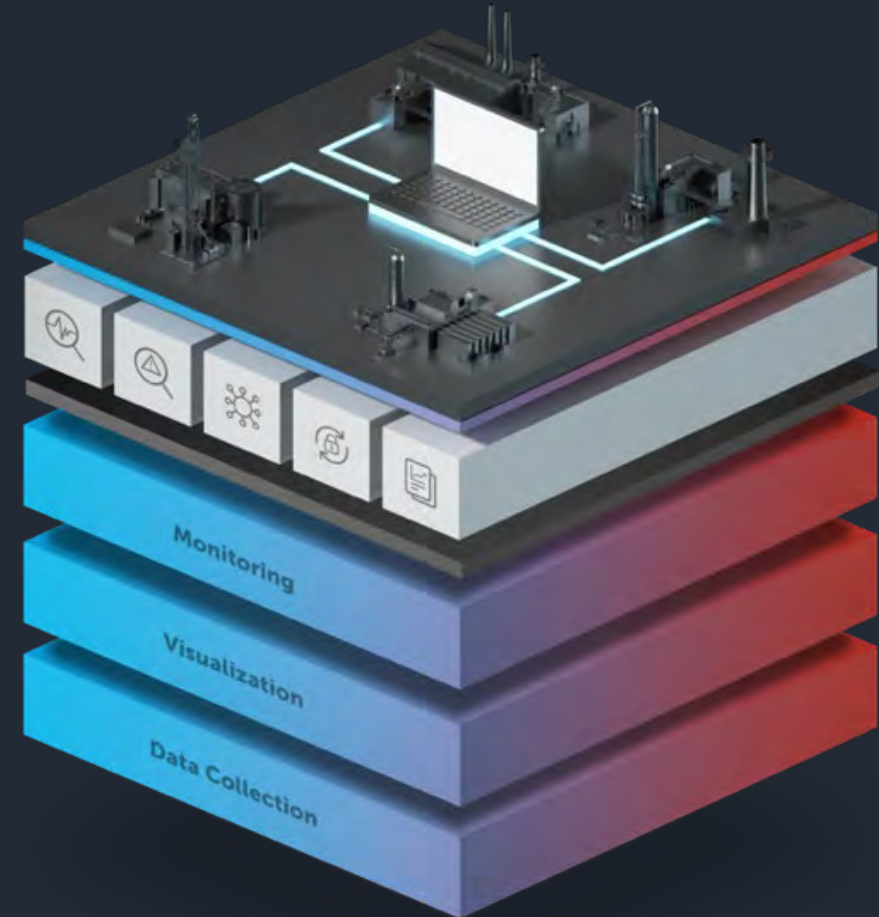
- |   |       |
|---|-------|
| 1. Increase visibility into control system cyber assets and configurations .....                                      | 45.5% |
| 2. Perform security assessment or audit of control systems and control system networks .....                          | 37.3% |
| 3. Invest in general cybersecurity awareness programs for employees including IT, OT and hybrid IT/OT personnel ..... | 29.5% |
| 4. Invest in cybersecurity education and training for IT, OT and hybrid IT/OT personnel .....                         | 29.1% |
| 5. Implement anomaly and intrusion detection tools on control system networks .....                                   | 28.3% |
| 6. Bridge IT and OT initiatives .....   | 26.6% |

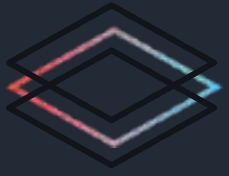


# Mandatory Monitoring Capabilities in Critical Industries

Identify | Protect | Detect | Respond

-  Advanced Threat Detection (DPI) for OT/ IT protocols
-  Continuous Vulnerability Monitoring (passive)
-  Asset Query Monitoring (active queries)
-  Automatic Asset Discovery and Conversation
-  Detection of Functional anomalies and Misconfigurations
-  Ongoing Risk and Compliance Posture





# Active (Query) versus **Passive** monitoring

Extreme Visibility – Enhanced

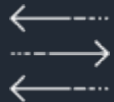
## **Passive**



### **Continuous, Real-time Monitoring of OT Networks**

- Rapidly discover network communications and asset details down to the I/O level
- Field Proven and 100% safe for OT networks

## **Active**

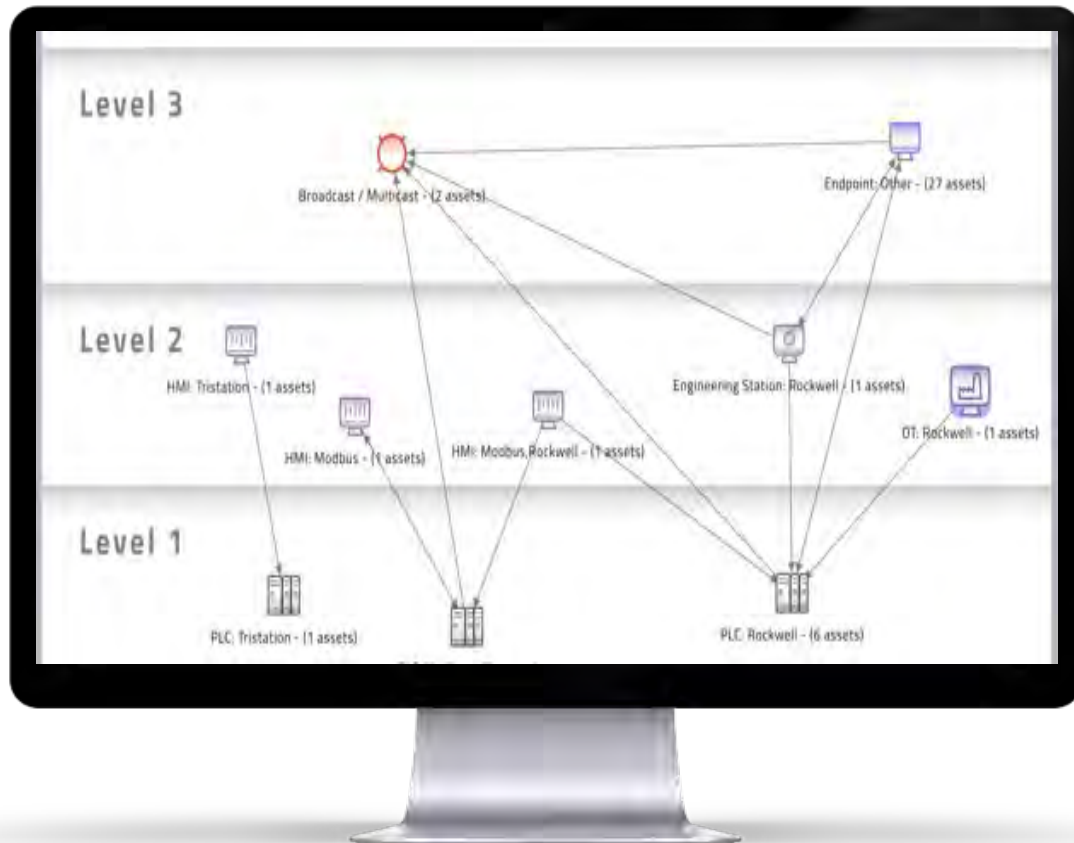


### **Precise, Periodic Queries of OT and IT Assets**

- Safely query ICS and non-ICS assets for enhanced visibility into asset configurations
- Enhanced context for alerts and vulnerabilities

# Asset Discovery & Conversations

We need to know who's talking to whom



## Asset Monitoring:

- ✓ Automatic asset inventory
- ✓ Automatic discovery of new OT assets in ICS / DCS network
- ✓ Rogue or Shadow asset detection
- ✓ Conversation among OT assets is critical to know



# Industrial **Protocols Visibility**

## Example Protocol: Siemens S7

- Siemens **proprietary** TCP protocol – TSAP (port 102)
- PLC <-> PLC – partner devices exchange data
- HMI <-> PLC – request, response
- Engineering Workstation <-> PLC



### S7 Commands are divided into categories

- Data Read / Write from PLC
- Cyclic Data Read/Write
- Directory Info
- System Info
- Blocks Move
- PLC Control - Restart
- Firmware upload/download
- Security
- Programming

# IT monitoring tools **are blind in OT**

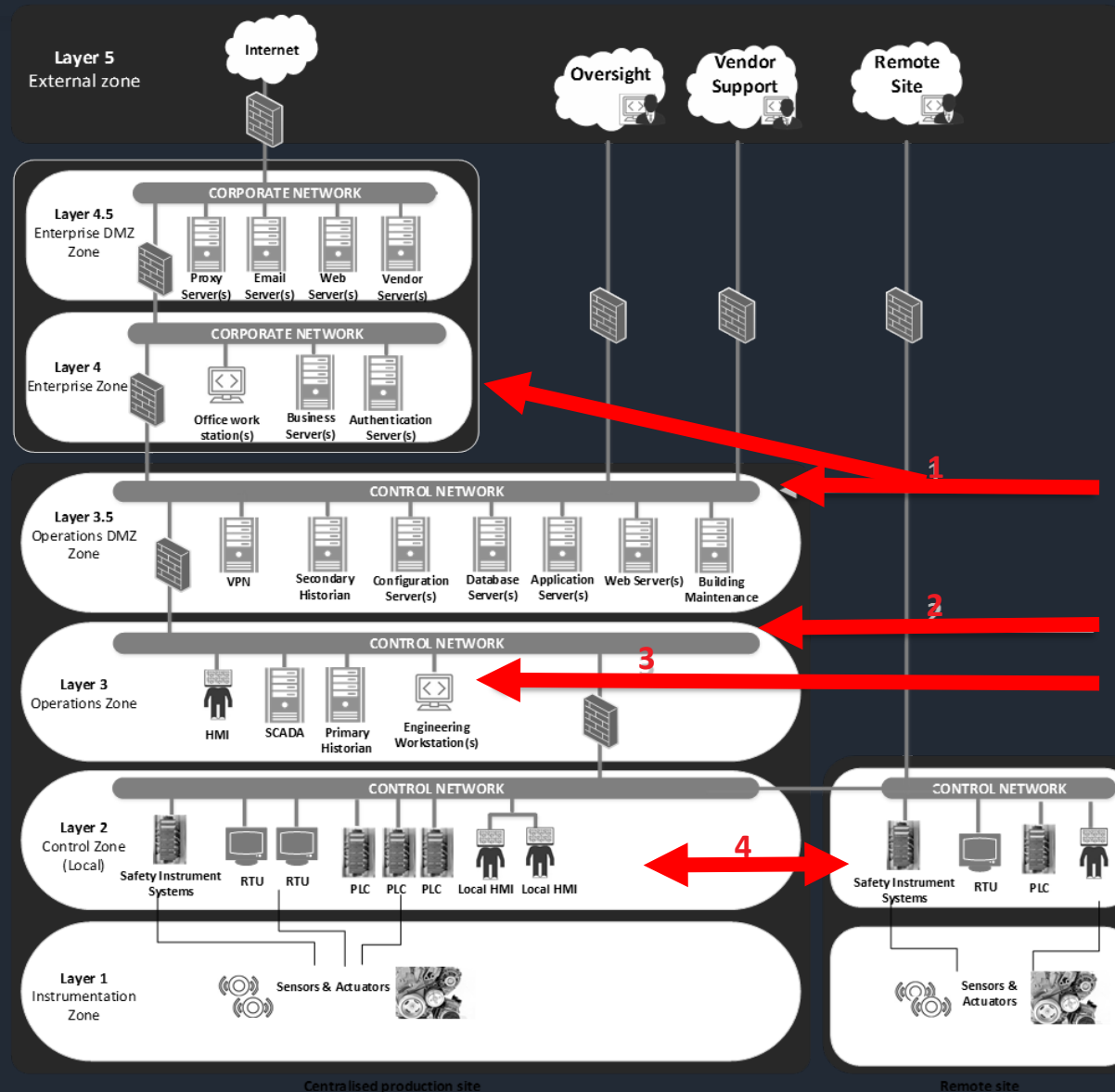
## Example Protocol: Siemens S7

- Siemens **proprietary** TCP protocol – TSAP (port 102)

The screenshot displays a network analysis tool interface. At the top, the 'Metadata Details' tab is active. It shows a session with ID 6613939455810875150 and a size of 246 Bytes, 48 Packets. The sensor is identified as 'DIR'. A diagram illustrates the communication between a Client (172.16.136.142, UNKNOWN) and a Server (172.16.76.60, UNKNOWN). The client's port is 1277, and the server's port is 102. A red oval highlights the connection, labeled 'F.UnknownProtocol\*'. Below the metadata, the 'Decoding Paths' section is expanded, showing two custom decoding paths. The first path, 'CUSTOM0', is for the client and lists attributes: Reason (59% of client data is not printable ASCII, 37% of client data is zero bytes, 56% of server data is not printable ASCII, 37% of server data is zero bytes), MD5 (d55e93158fb92903aa080bc28ffe4ab9), and SHA256 (5752bbc20553e6f89be67ddae14d11e9708080c19498dc01144b106a97c15e8f). The second path, also 'CUSTOM0', is for the server and lists attributes: Reason (59% of client data is not printable ASCII, 37% of client data is zero bytes, 56% of server data is not printable ASCII, 37% of server data is zero bytes), MD5 (6029327fa375619077a0143ae05bde4d), and SHA256 (271ff33fb469167b4e448fee80d4dc6b64c266fc45860275e061027047e872ff).

# Threat Intelligence & Threat Modeling in ICS/DCS

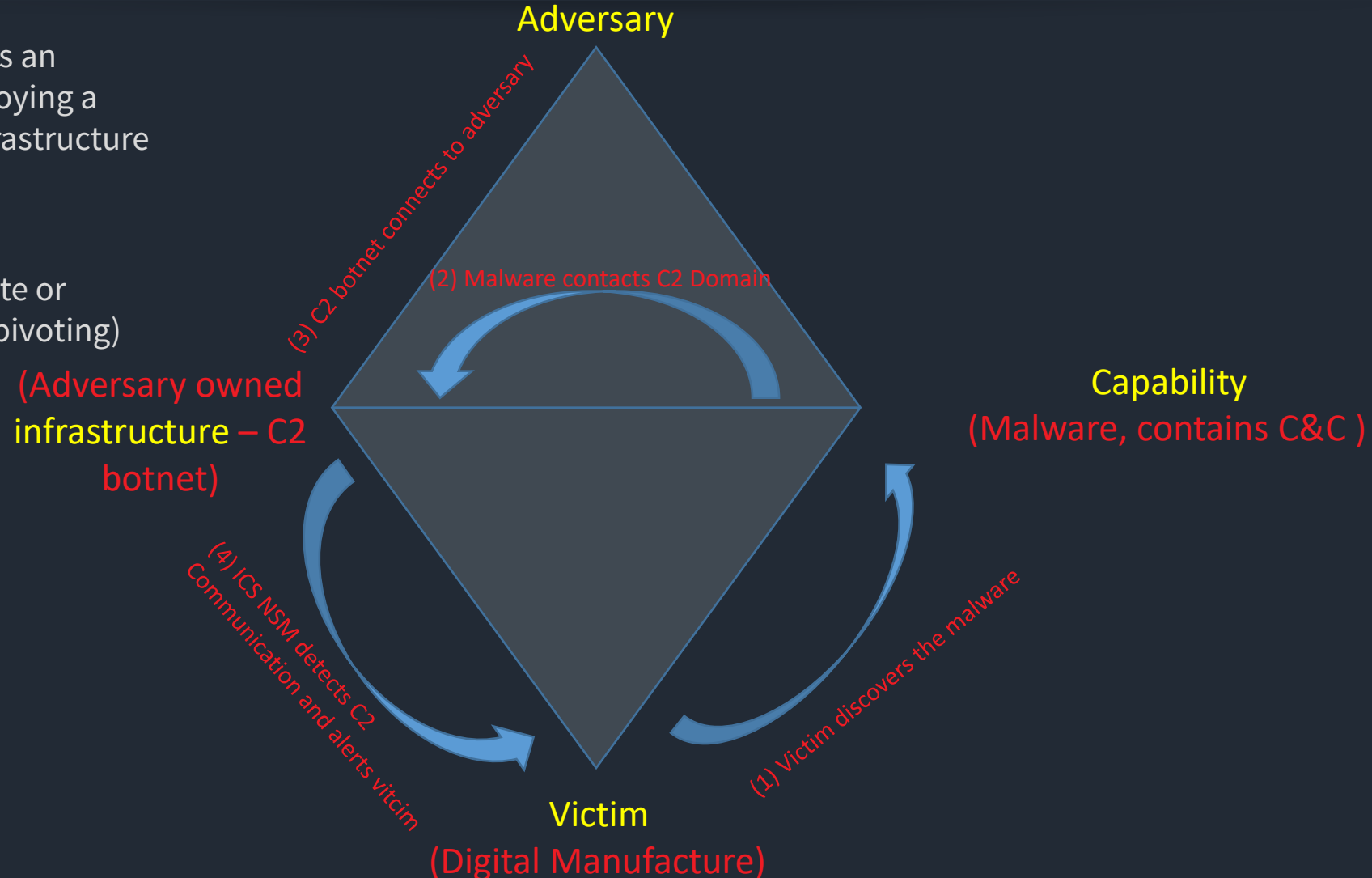
# Vulnerability Assessments helps to identify threats



# Diamond Model – ICS Kill Chain (lite)

Diamond model works in conjunction with ICS Kill Chain process

- Diamond model shows an adversary that is deploying a capability over his infrastructure against a victim.
- Can be used to simulate or analyze an intrusion (pivoting)



source: Dragos and Mandiant

# Common ICS/DCS Threats

These are routine findings

- No antivirus installed in entire OT zone
- Operating Systems such as WinXP SP3 and Embedded still up and running
- Free use of USB media
- Unauthorized 4G modems with industrial VPN concentrator used by integrators (SHODAN loves them!)
- Never heard about patching
- IT/OT Firewall misconfiguration and bypasses
- No OT DMZ
- No security policies, procedures
- No lifecycle management (security-by-design, security-by-default)



# Internal (Operator )Threats

Never underestimate SCADA Operators !!!

- ... Operator Jail Breaks

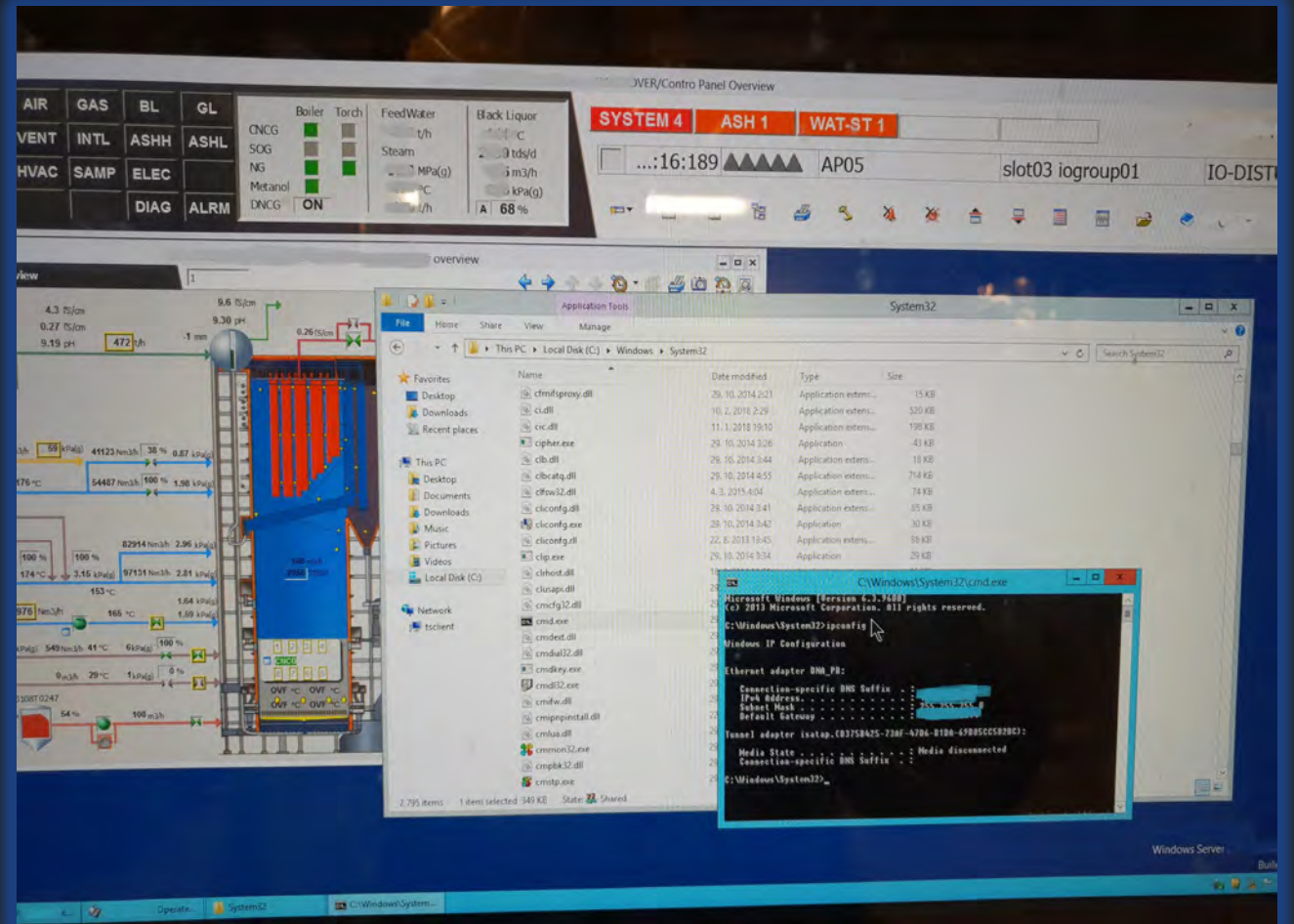


# Internal (Operator) Threats

Never underestimate SCADA Operators !!!

- Operator Jail Break (escape from Windows Kiosk mode)

- Via the help windows and search cmd.exe
- Windows Sticky keys CTRL+O, CTRL+S
- Windows combo keys Windows key and:
  - + E => explorer
  - + R => run
  - + U / + I => (display) settings
  - + Q => search
  - + D => show desktop
  - + A => show notifications sidebar
  - + X => right click start menu

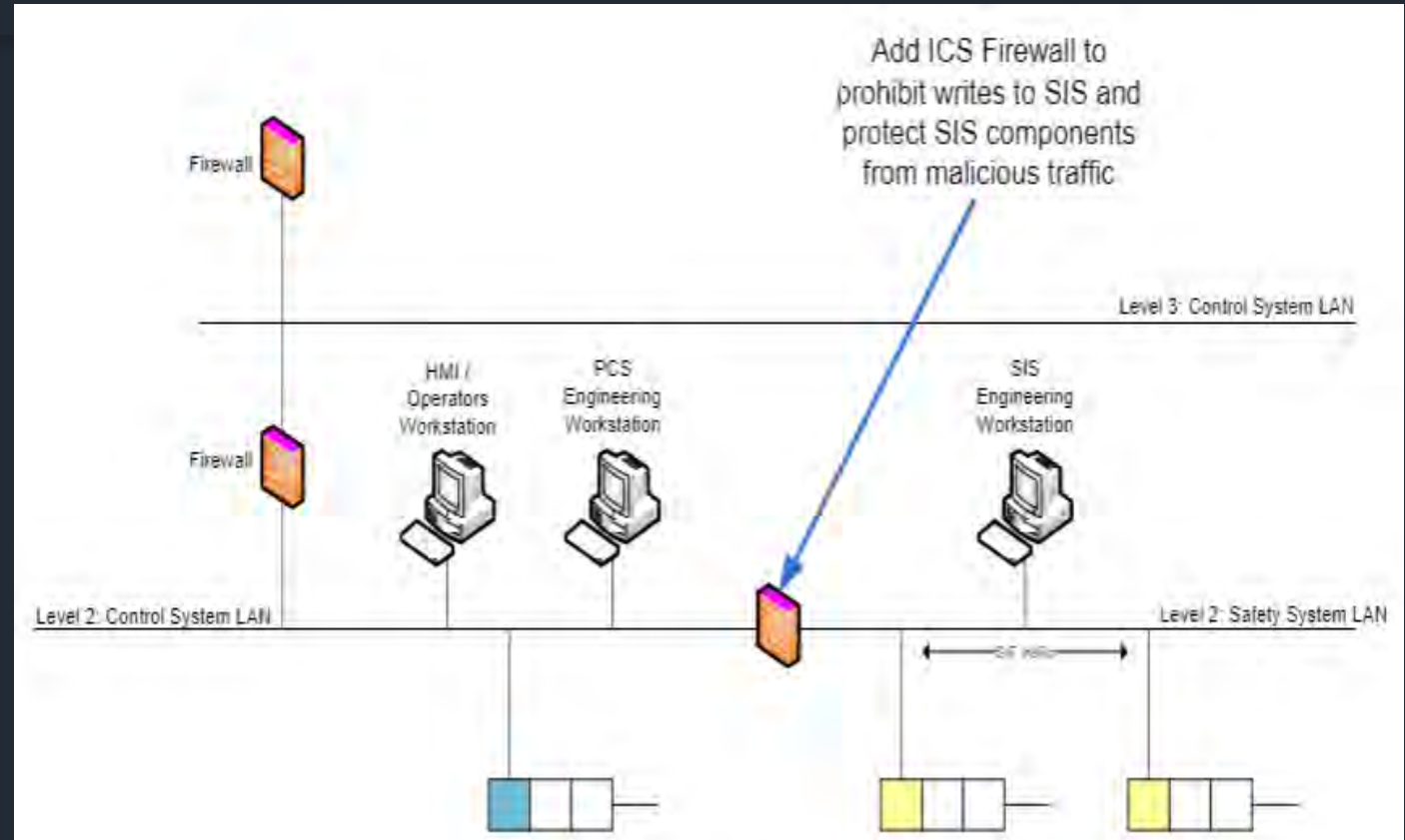


# Not Funny Threats..

These are not funny things out there



- Remote (unapproved) access to SIS/ESD
- Wifi access point connected to SIS/ESD (pilot leftover)
- SIS/ESD fully integrated with BPCS over Ethernet without any firewall
- Operator WS can directly ping SIS/ESD!
- Insecure external communication channels to SIS COM port
- Insecure SIS EWS (USB, Hardening, Windows OS etc.)





# Industrial Threat Intelligence

Proactive Insight and Visibility into APT groups

- Threat intelligence provides deep, context-rich insight, illuminating the malicious actors and activity targeting industrial control networks
- It forms Indicators of Compromise (IOCs) – data + context of adversary activity
- This knowledge enables ICS defenders to make both tactical decisions and strategic recommendations
- Regular threat intelligence content includes:
  - ❑ ICS-themed malware identification and analysis
  - ❑ ICS vulnerability disclosures and analysis
  - ❑ ICS adversary behavior trends
  - ❑ ICS threat/incident media report analysis and commentary



**ELECTRUM** currently focuses on electric utilities and mostly targets entities in Ukraine. It is responsible for the disruptive CRASHOVERRIDE event in 2016.<sup>12</sup> Due to the overlap of vendor technologies and relationships in the supply chain with electric utilities, the potential for collateral impact in an electric-targeting event is a risk to oil and gas. Several ICS entities experienced this consequence in the 2017 NotPetya supply chain compromise that impacted companies worldwide. Intelligence firms determined the SANDWORM group was responsible for the NotPetya event, and Dragos assesses ELECTRUM is an offshoot of SANDWORM.<sup>13</sup>

Associated Group: SANDWORM<sup>14</sup>



**RASPITE** targets electric utilities in the US and government entities located in the Middle East. Dragos also identified additional victims in Saudi Arabia, Japan, and Western Europe, but has not identified new RASPITE activity since mid-2018. Although Dragos has not observed direct targeting of oil and gas firms, such entities experienced collateral impact from this group's watering hole activity, thus RASPITE remains a risk to oil and gas.<sup>15</sup>

Associated Group: Leafminer<sup>16</sup>



**ALLANITE** targets business and ICS networks in the US and UK electric utility sectors. The group maintains access to victims to understand the operational environment and to stage for potential disruptive events. There is no indication ALLANITE has a disruptive or damaging capability or intent at this time.<sup>17</sup>

Associated Groups: PALMETTO FUSION,<sup>18</sup> Dragonfly 2.0, Berserk Bear




**COVELLITE** compromised networks associated with electric energy, primarily in Europe, East Asia, and North America. The group lacks an ICS-specific capability at this time. While technical activity linked to COVELLITE behaviors exist in the wild, there has been no evidence or indications this group remains active from an ICS-targeting perspective.<sup>19</sup>

Associated Group: Lazarus Group<sup>20</sup>

# Industrial Threat Intelligence

## Threat Platform Example













**Adversary**  
**COVELLITE**

**First Seen**  
Sep 2, 2017

**Description**  
The group executes IT compromise with hardened anti-analysis malware against industrial orgs using encoded binaries in documents, evasion techniques. It targets electric utilities in the US, Europe, and East Asia. It is linked to Lazarus, Hidden Cobra.

**Full Report**  
[Activity Group Covellite](#)

You can download IOCs

| Serial   | Released    | Title                                  | TLP   | Threat  | Report  | IOCs  |
|--|-------------|--|---|---|---|---|
| <br>TR-2017-21  | Mar 2, 2018 | COVELLITE Continuing Analysis          |    |    |    |    |
| <p>Dragos initially disclosed COVELLITE activity targeting US electric grid operators in late September 2017 through both WorldView updates and TR-2017-17. Since the initial discovery, Dragos identified additional malware samples that appear linked to COVELLITE, but also indicate a connection to the LAZARUS</p> <div><div>COVELLITE</div><div>Lazarus</div><div>Phishing</div><div>Backdoor</div><div>Electric Generation</div><div>Electric Distribution</div></div> |             |  |   |   |   |   |
| <br>TR-2018-01  | Mar 2, 2018 | New COVELLITE-Related Dropper Document |  |  |  |  |
| <p>COVELLITE is an ICS-targeting activity group with significant technical overlap with the LAZARUS advanced persistent threat. Dragos monitors LAZARUS activity as a means to identify potential changes in tactics, techniques, and procedures (TTPS) that may be reflected in future COVELLITE operations</p> <div><div>COVELLITE</div><div>Lazarus</div><div>Malicious Document</div></div>  |             |  |   |   |   |   |

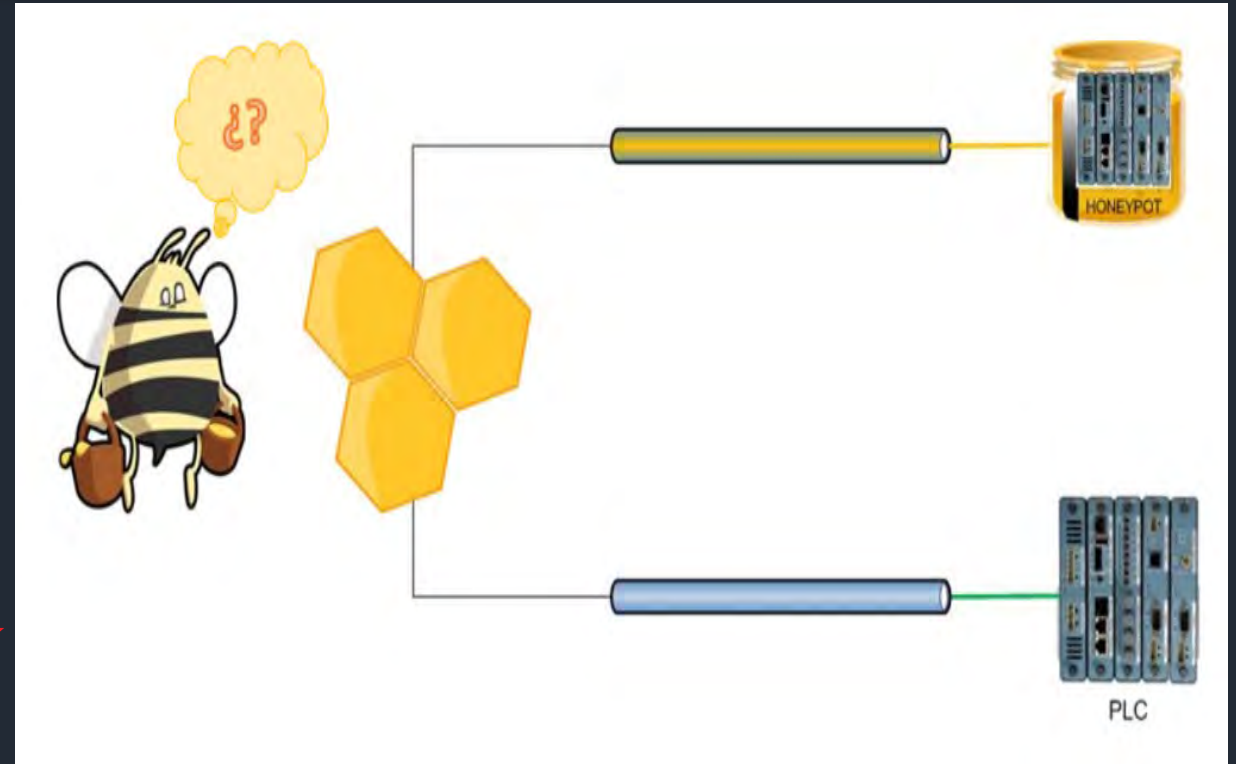
source: Dragos

# Industrial Honeynets/Honeypots

Let's go Honey Bunny!

- ICS Honeypots, can be physical and virtual, usually created with vulnerabilities to attract attackers
- Honeynets can be usefull for:
  - ❑ Detect attacks to ICS
  - ❑ Reveal TTPs (Tactics, Techniques & Procedures)
  - ❑ Mislead the attackers
  - ❑ Offensive security “hack back”
  - ❑ Analyze industrial malware
  - ❑ Analyze APTs

Check  
this  
out



## SCADA HoneyNet Project: Building Honeypots for Industrial Networks

[Venkat Pothamsetty](#) and [Matthew Franz](#)  
[Critical Infrastructure Assurance Group\(CIAG\)](#)  
Cisco Systems, Inc.

source: INCIBE-CERT





**Thank** You and Stay Safe

Questions?

