



IBRAHIM SAMIR HAMAD

Oil & Gas Company
Qatar

- Corporate Information Security Officer in the oil and gas sector
- Has a 17 years' experience in IT, Telecom, Industrial Systems and Data Protection
- Active contributor in the Cyber Security Community efforts in Middle East
- CISA, CISM , CRISC , CISSP, CSSA, ITILV3 Found/PPO , ISO27001 LA, PRINCE2

@ishamad





50 Shades of Industrial Controls Systems Security Controls

Ibrahim Samir Hamad CISO Oil and Gas

CISA®, CISM®, CRISC®, CISSP®, CSSA®, ITIL®V3 Found/PPO, ISO® 27001 LA, PRINCE2®

Disclaimer ...I represent nobody but me

*This presentation is based on my personal research using the most powerful means of the Knowledge nowadays - Google, Feeds and Twitter.
This material is neither representing my current or previous employers nor their shareholders, and never it shall be.
To reach me, please use my LinkedIn or twitter (@ishamad)*

The Equation !



=



X

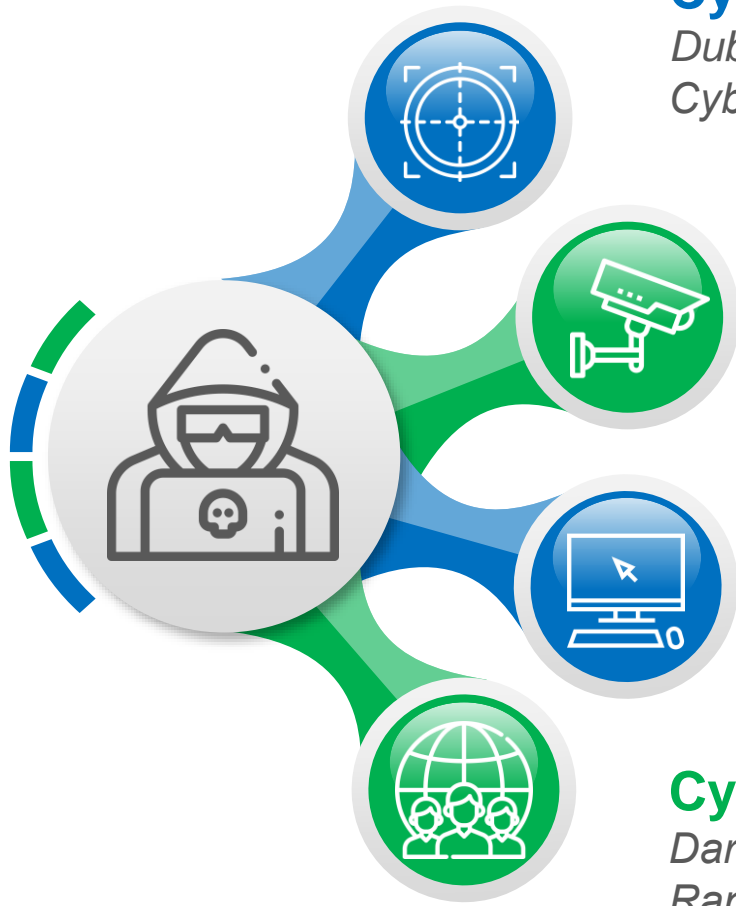


Risk



The State of Global Cyber Threats

Threat



Cyber Weapons

*Dubbed as Cyber War, Cyber Politics , Cold War 2.0 e.g US Elections
Cyber trauma / Sony Hack / French Election, etc...*

Surveillance Tools

*Phineas Fisher – Hacking Team / Shadow Brokers – NSA Leak / Wiki
Leaks – CIA Leak*

IoE

*By 2020 – 26Billion “Things” shall be connected: convergence of the physical
and logical world e.g. Virgin Atlantic, GE , Olympic committees, etc...*

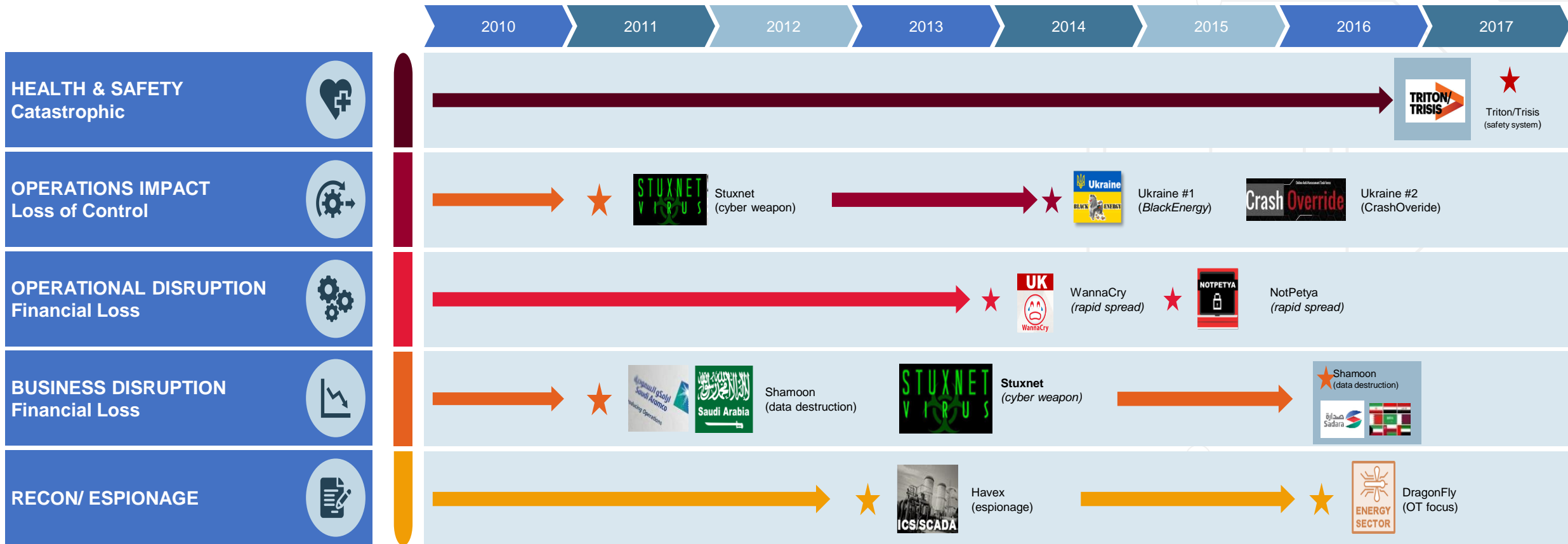
Cyber Underground / Operations

*DarkWeb , Zeronet, TOR...,Cyber Crime as A Service and Shift towards
Ransomware , Fileless malware, etc...*



Malware...

Threat



Disclaimer ...I represent nobody but me

This presentation is based on my personal research using the most powerful of Knowledge nowadays - Google, Feeds and Twitter. This material is neither representing my current or previous employers nor their shareholders, and never it shall be. To reach me, please use my LinkedIn or twitter (@ishamad)



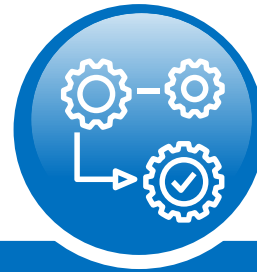
To Begin with ...!

Vulnerability



People

- Savvy's
- Obscurity
- Ignorance



Process

- Compliance
- Audit
- Configuration Management
- Outsource
- Access Control



Technology

- Codes
- Applications
- Architecture
- Physical

Economy of Global Cyber Threats

Vulnerability



97% of Phishing emails contained Ransomware

46% of Compromised Systems had no malware on them

23% of phishing recipients opened the attachment

\$3.5 Million average cost of cyber breach

99.9%
Vulnerabilities dated to 1 year or more old

748% increase in Ransomware

\$3 Trillion Impact of lost productivity and business revenue

200+ Days Attackers present on the victim System

80+ Days from detection to recovery

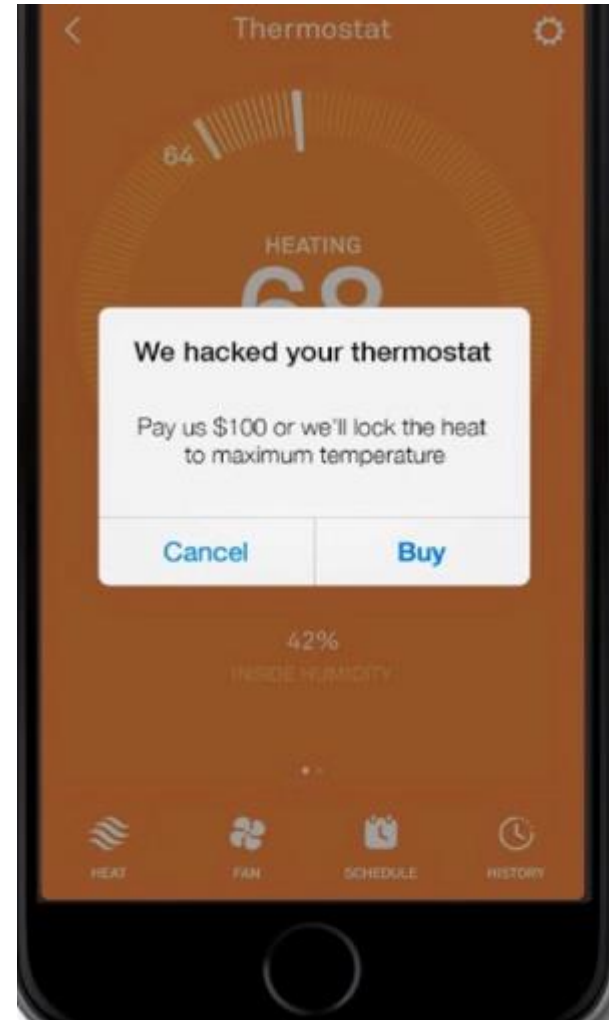
Sample ... Even gets “better” with ICS Savvy's

Vulnerability



Sample IoE ... Make it even more obvious

Vulnerability



rice that lets you control your stove from your smartphone and helps
oved ones from the devastating effects of house fires. Its combination
s enable it to not only detect high levels of smoke, natural gas, and
the kitchen), but also react and turn your stove off to keep you safe.

itor your stove remotely and modulate the burner temperature. With
ve to worry about leaving your stove on again!



Sample Technology Flaws

Vulnerability



Ignition by Inductive Automation is the first SCADA software solution built entirely on Java. Ignition's use of Java makes it totally cross-platform compatible and easily web-deployable, two major reasons for the software's growing community of global Ignition users.



Sample Vendor Flaws

Distribution of ICS Software Update on USBs as secure way of sending updates



Vulnerability



Life Is On | Schneider
Electric

Schneider Electric Security Notification

Security Notification – USB Removable Media Provided With Conext Combox and Conext Battery Monitor

24 August 2018

Overview

Schneider Electric is aware that USB removable media shipped with the Conext Combox and Conext Battery Monitor products may have been exposed to malware during manufacturing at a third-party supplier's facility.

Affected Product(s)




- USB media shipped with Conext Combox (sku 865-1058), all versions
- USB media shipped with Conext Battery Monitor (sku 865-1080-01), all versions

Reality... OT Vs Banking Security



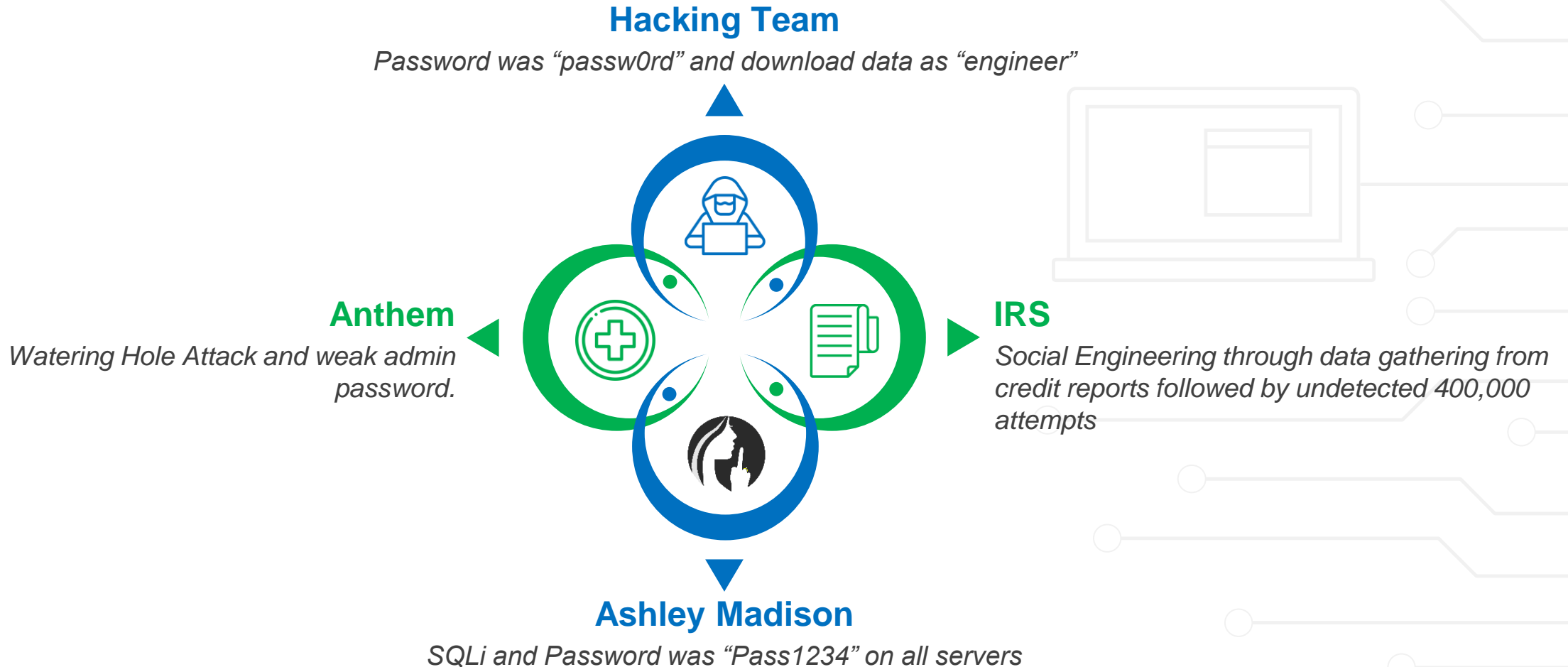
Big Picture



Banking		Industrial
<ul style="list-style-type: none"> • Monetary • Reputation • Privacy 	 Impact	<ul style="list-style-type: none"> • Fatalities • Environment • State Disruption
<ul style="list-style-type: none"> • Fraud • Data Leak 	 Threat	<ul style="list-style-type: none"> • Nation State • Domain 5 • Vendors
<ul style="list-style-type: none"> • Insider • Application • Accessible to ALL 	 Vulnerability	<ul style="list-style-type: none"> • Legacy • Everything

Zoom Out ... Where did IT Controls fail ?

IT



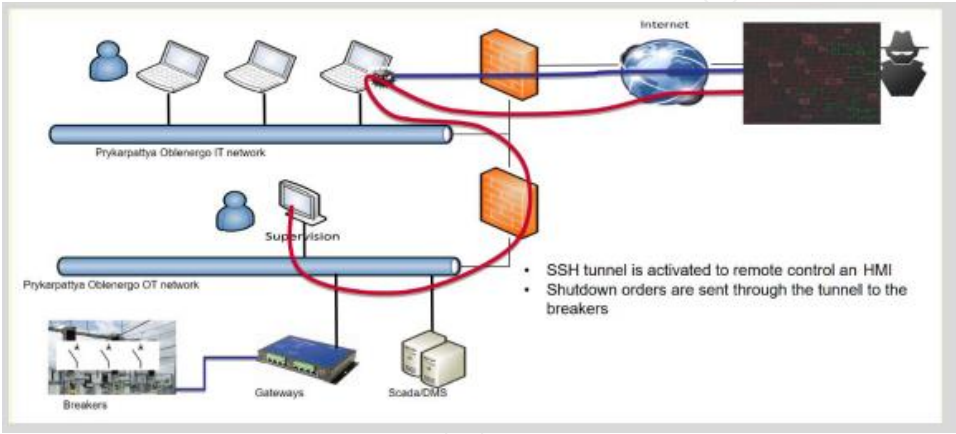
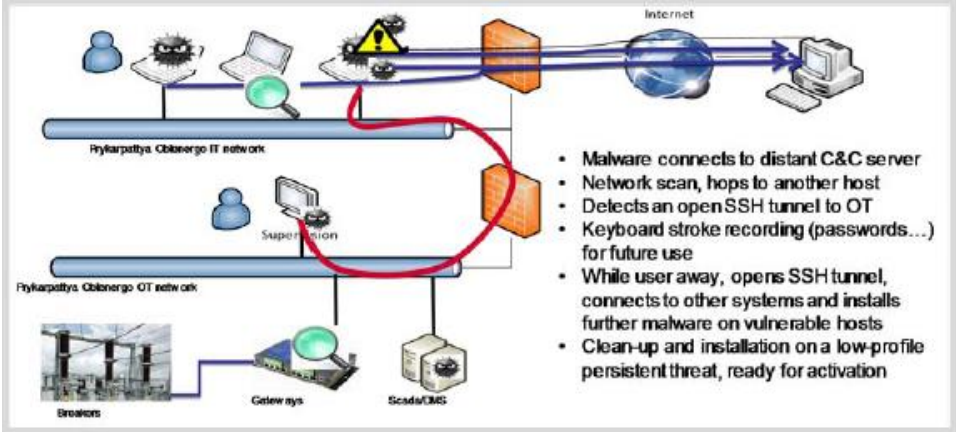
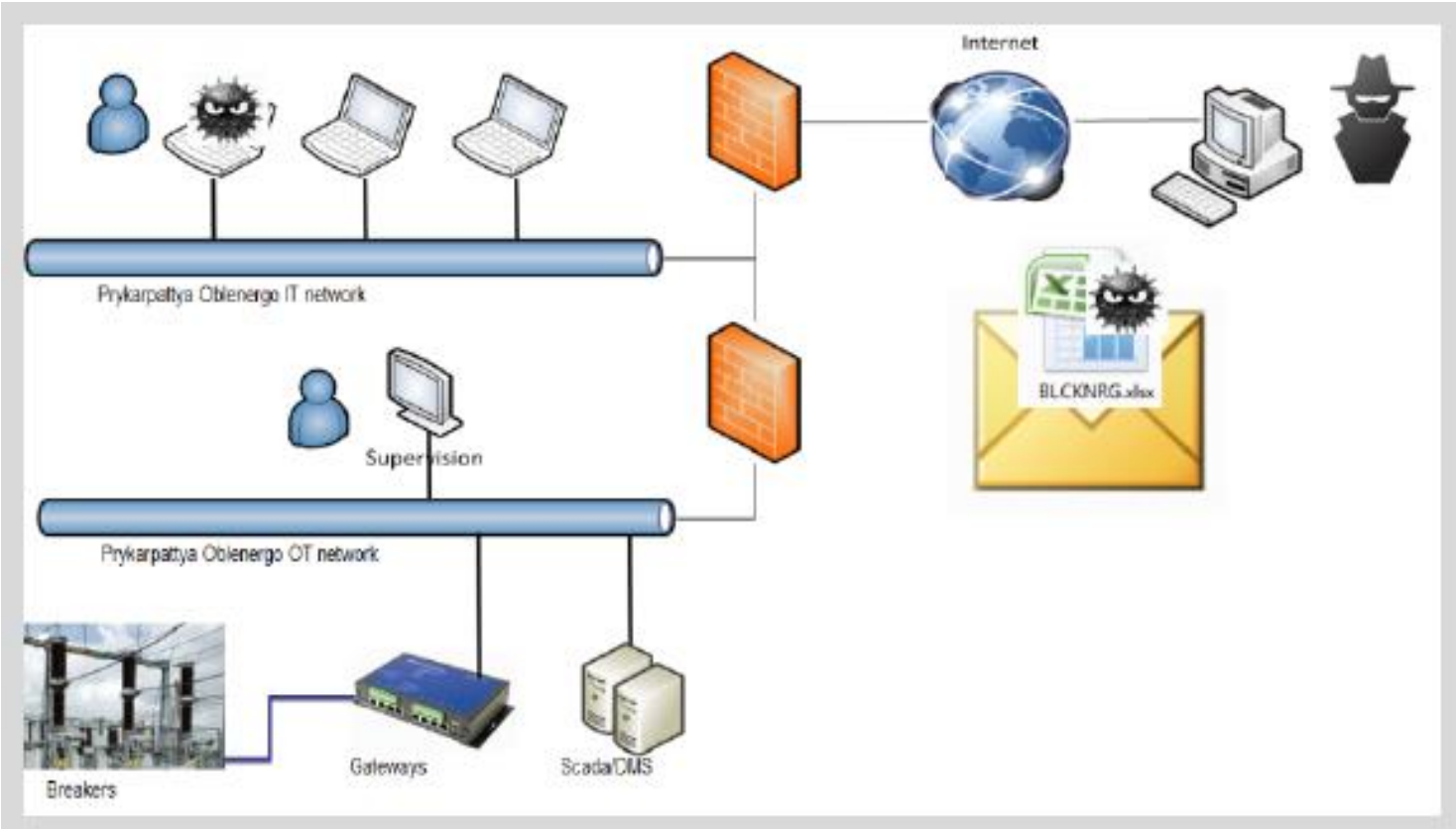
Zoom In....

Where Do ICS Controls Promise to Fail

OT



When IT & ICS Risks Converge..... German Steel Factory



ISA FLASH N°62 – Décembre 2016



Controls ...

“Typical IT Modern” High Level Controls



Digital Ready Security

Data centric security

Cloud security

Supply Chain Security

IT & IoE security convergence



Mature Security

Threat Management

Mobile device security

Identity governance

Data Ecosystem

Business resilience strategy



Foundational Security

Organization Governance Compliance

Inventory, Identification and Classification

End point hardening & Perimeter Security

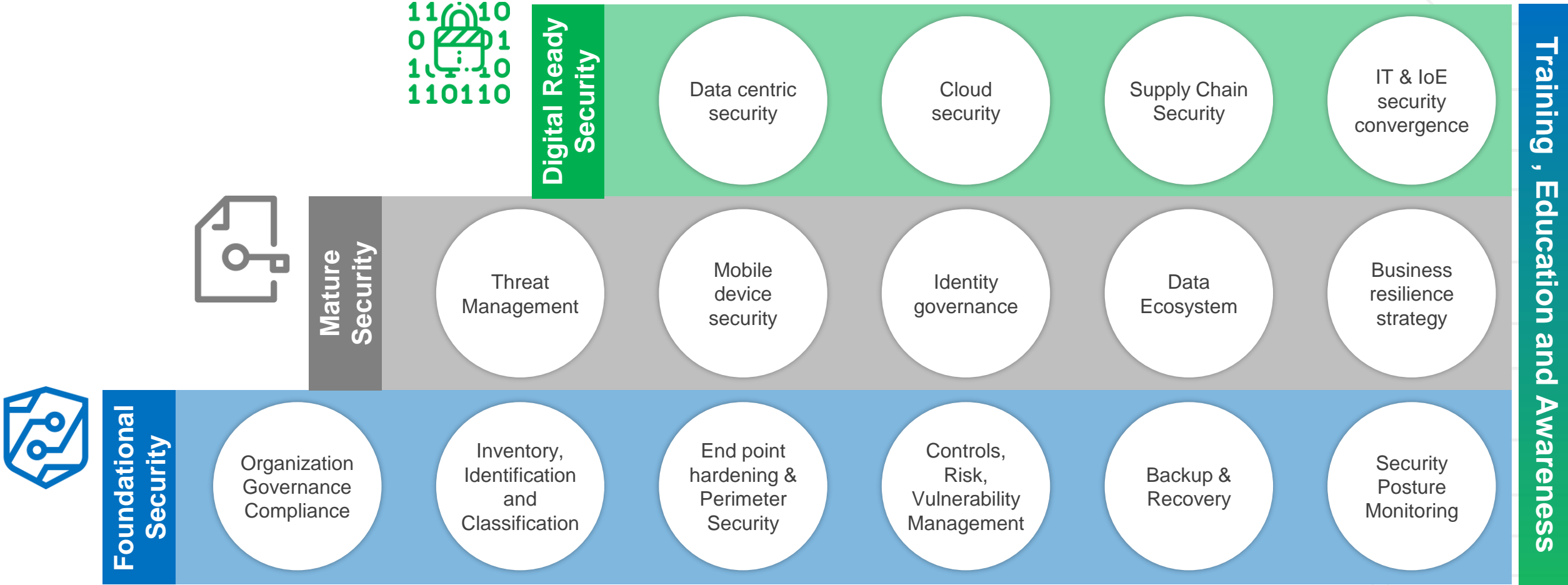
Controls, Risk, Vulnerability Management

Backup & Recovery

Security Posture Monitoring

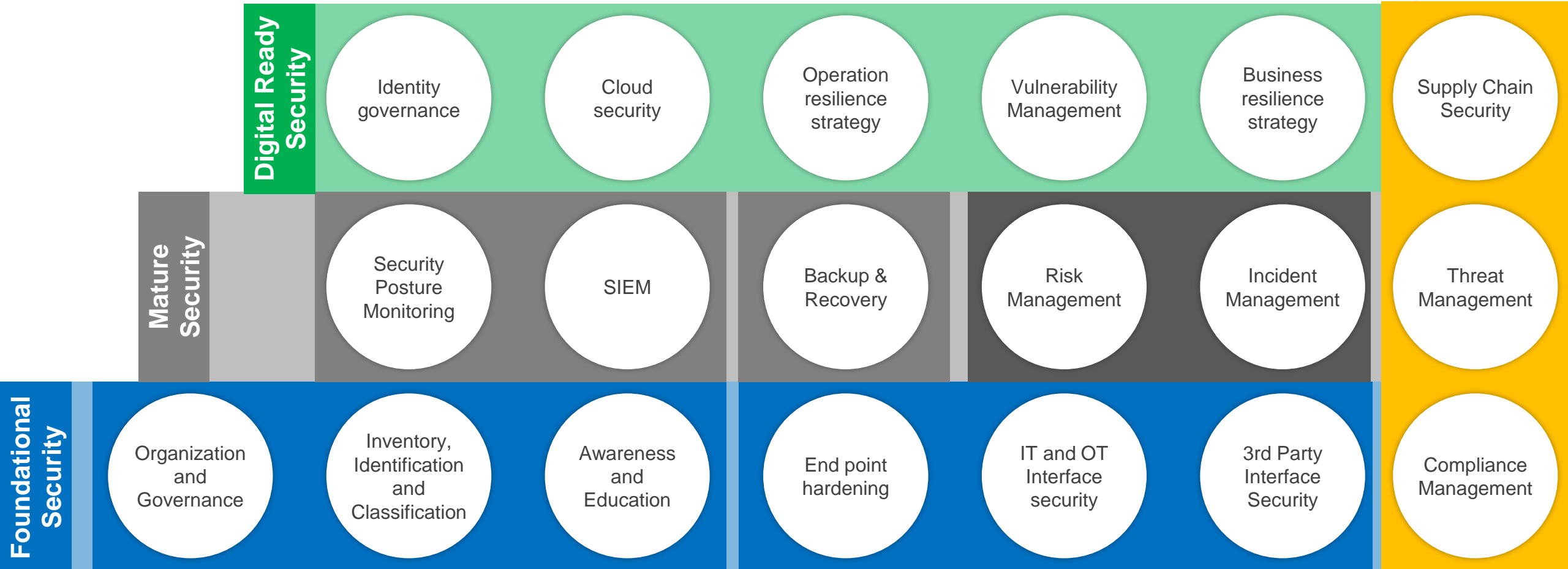
Training , Education and Awareness

Controls ... ICS “Typical” Controls



Controls ... OT “Modern Enough” Controls

Countermeasure



OT Security Monitoring is Key

The Approach



ICS Environment

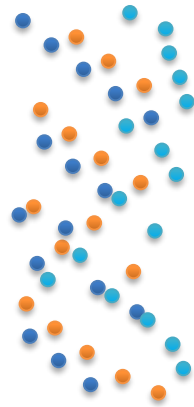
Internal

External

Governance

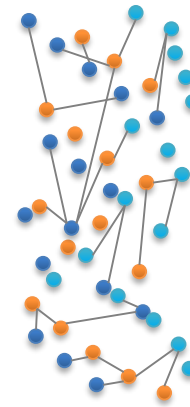
Collection

Gathering of relevant ICS/OT **Events** and **Process Data**



Processing

Correlation of data with **operational base lines** and **posture**

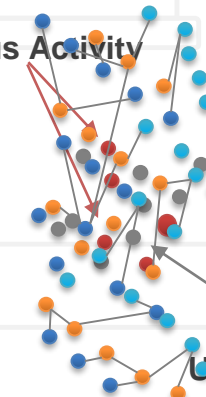


Analysis

Pin point known bads or **Unknowns** outside the baseline

Malicious Activity

Unintentional Activity



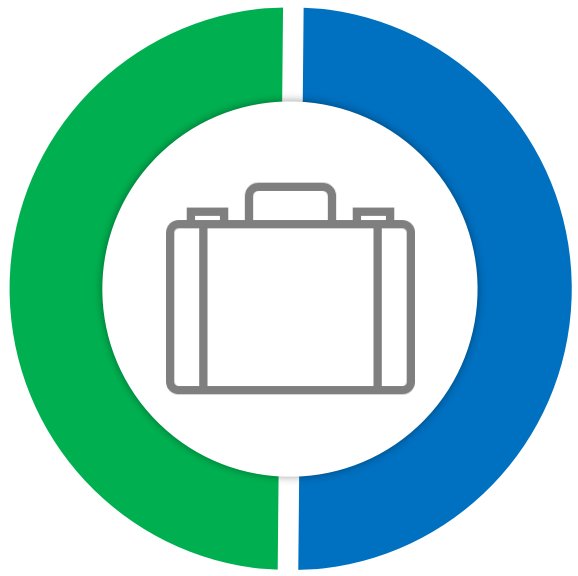
Capability ???

Baseline

- Traffic (North-to-South, East-to-West)
- Asset Behavior
- Commands on the wire (Modbus commands, DNP3...etc)
- Protocol baseline for desired process operations (shutdown, Production, maintenance ...etc)
- Monitor most prevalent vulnerabilities

ICS-CERT Annual Assessment Report

Area of Weakness	Rank	Risk
Boundary Protection	1	<ul style="list-style-type: none"> • Undetected unauthorized activity in critical systems • Weaker boundaries between ICS and enterprise networks
Least Functionality	2	<ul style="list-style-type: none"> • Increased vectors for malicious party access to critical systems • Rogue internal access established
Identification and Authentication	3	<ul style="list-style-type: none"> • Lack of accountability and traceability for user actions if an account is compromised • Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access
Physical Access Control	4	<ul style="list-style-type: none"> • Unauthorized physical access to field equipment and locations provides increased opportunity to <ul style="list-style-type: none"> ◦ Maliciously modify, delete, or copy device programs and firmware ◦ Access the ICS network ◦ Steal or vandalize cyber assets ◦ Add rogue devices to capture and retransmit network traffic
Audit Review, Analysis and Reporting	5	<ul style="list-style-type: none"> • Without formalized review and validation of logs, unauthorized users, applications, or other unauthorized events may operate in the ICS network undetected
Authenticator Management	6	<ul style="list-style-type: none"> • Compromised unsecured password communications. • Password compromise could allow trusted unauthorized access to systems



Identify

- Identify Anomalous behavior by deviation from the Baseline
- Detect new running services and new files , Spot changed files
- Monitor on the wire commands and detect inserted commands (computational), sensor overwrite value (false data injection) and traffic reroute.
- Monitor firmware upload to serial-to-ethernet devices
- Some specific indicators e.g.
 - Discover anomalous DNS requests
 - Identify any network connections using the Windows SMB1 protocol
 - port scan Automatically to create a baseline of network devices,
 - network communication patterns (e.g. machines communicating using BE3 and Killdisk)

CISO perspective... OT Security Monitoring is Key

Ecosystem



THANKYOU
