RADIFLOW & ITS

Industrial Cyber-Security Solutions for Critical Business Operations

Ilan Barda
Radiflow, CEO

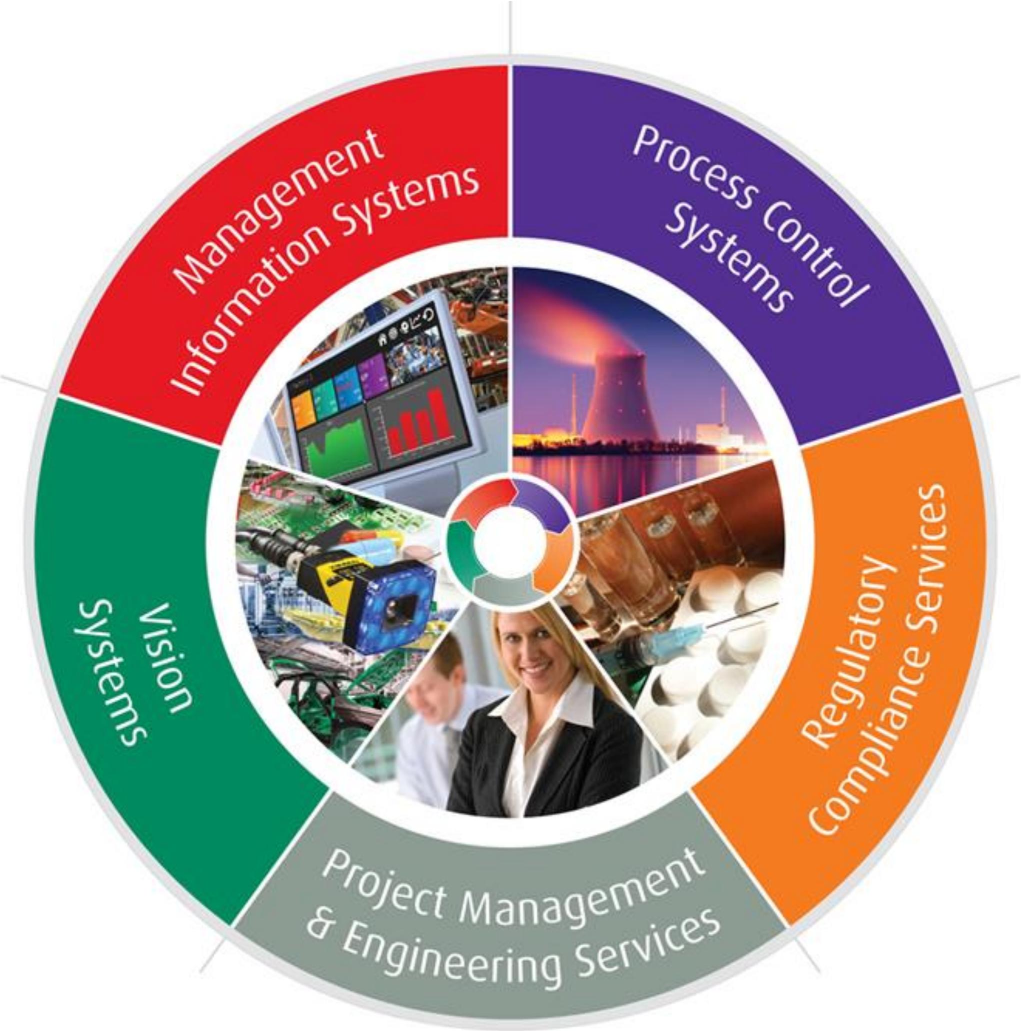
Joanne Rout, MIET
ITS, Sales Account Manager

September 2020

ITS: Introduction

- Established in 1991
- Customer focused, specialist independent systems solution provider
- Strong partnerships with leading systems suppliers
- Extensive experience in design & implementation of automation solutions for the highly regulated industries chemical, pharmaceutical, medical device and nuclear

Complete Service Solution


Management Information Systems
Process Control Systems
Regulatory Compliance Services
Project Management & Engineering Services
Vision Systems

Some of Our Customers

inovyn
سابك
sabic
Lilly
Lucite
International
Going further
CalaChem
FINE CHEMICALS
AstraZeneca
Piramal
Newcastle International
Your Airport
px
YOUR LONDON AIRPORT
Gatwick
gsk
GlaxoSmithKline
AkerSolutions
glanbia

ITS & Radiflow Partnership

- ITS, in partnership with Radiflow, offers trusted Industrial Cyber Security Solutions for the chemical process industry sector
- Introduction to Ilan Barda, CEO of Radiflow

About Radiflow

Radiflow provides OT-dedicated Cyber-Security Solutions for Critical Business Operations

- Solutions & Services for the complete security life cycle
- Ecosystem with both IT & OT tools
- Compliance enabler for all int'l standards (e.g. IEC62443)

STRONG BACKING

Zohar Zisapel
Co-Founder, RAD Group

RADBynetGroup

ST Engineering

TECHNICAL EXPERTISE

Cybersecurity	OT
BeyondTrust cisco Cyber Israel National Cyber Directorate DELL EMC	BELDEN GE MEKOROT ISRAEL NATIONAL WATER CO. RUGGEDCOM INDUSTRIAL STRENGTH NETWORKS SIEMENS

Radiflow Install Base: Stats & Verticals

4187

Protected Sites

Power Generation

Power T&D

Renewable Energy

Oil & Gas

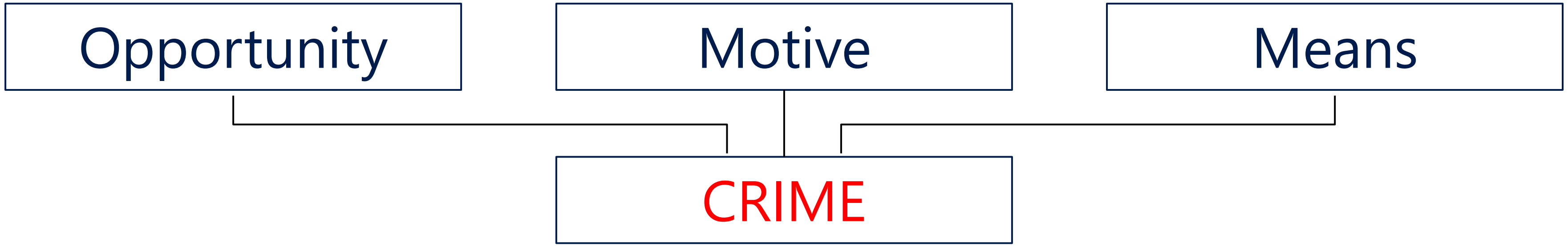
Transportation

Water & Wastewater

BMS

Process Manufacturing

Industrial Cyber Attacks: Imminent Danger



Industry 4.0
digital transformation
increases cyber exposure

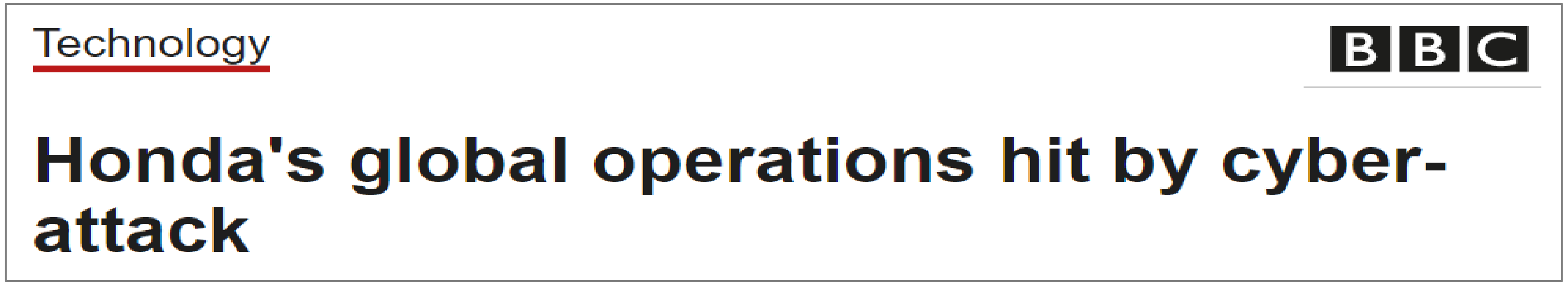
Global IT attacks damaged
industrial enterprises
(e.g. Notpetya in Merck)

Advanced attack tools used
for Cyber-Physical attacks
(e.g. Triton in Saudi-Arabia)

OT Attacks: Greatest Hits

- 2010 Iran Uranium Enrichment – Stuxnet
- 2015 Ukraine Power Grid – BlackEnergy
- 2017 Shipping sector – NotPetya
- 2018 Saudi Arabia Petrochemical – Triton
- 2019 Norsk-Hydro – LockerGoga
- 2020 Iran attack on Israeli water facilities – Remote Access vulnerabilities

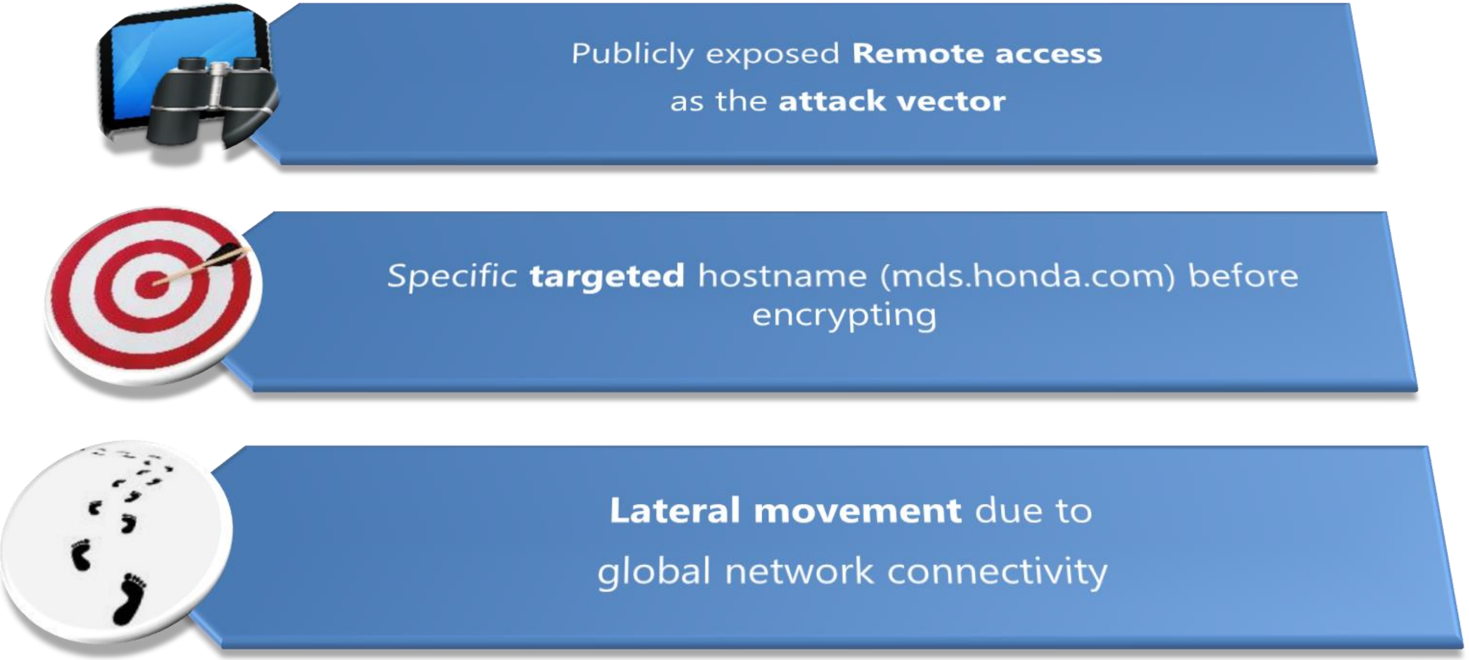
Recent Example:
Honda Ransomware Attack



Technology

BBC

Honda's global operations hit by cyber-attack



Publicly exposed **Remote access** as the **attack vector**

Specific **targeted** hostname (mds.honda.com) before encrypting

Lateral movement due to global network connectivity

The Rise in OT Ransomware Attacks: Insights

***post-compromise** ransomware attacks ("2nd stage ransomwares") tailored to industrial enterprises*

Process kill list tailored to critical OT systems and executables

exfiltrate large quantities of data **prior to its encryption** in the final stage of the attack

Source: Fireeye

Supply Chain Attacks: Insights

Phishing emails targeting industrial industries

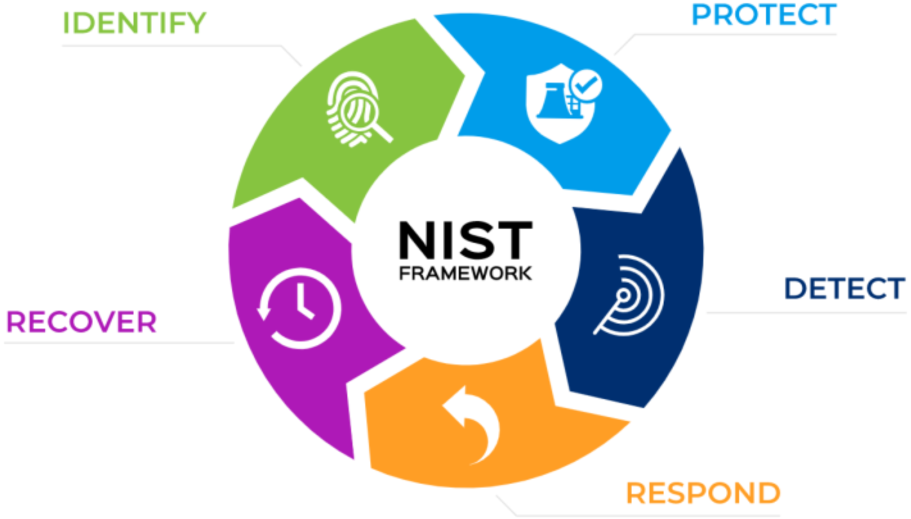
malicious payload was **hidden** in sent **images**

Using **legitimate, public image hosting services** in order to **evade detection**

Source: Kaspersky

Cybersecurity Life Cycle

- Identify Phase – Asset Mapping
- Protect – Enforce Access Policies
- Detect Phase – Anomaly Detection
- Respond Phase - Sync OT & SOC teams
- Recover Phase - Advise OPs on affected assets



Radiflow OT Cyber Portfolio

Detection & Monitoring

iCEN: Central Monitoring

iSID: Industrial Threat Detection

iSAP: Smart Collector

Policy Enforcement

iSIM: Service Manager

iSEG: Secure Gateway

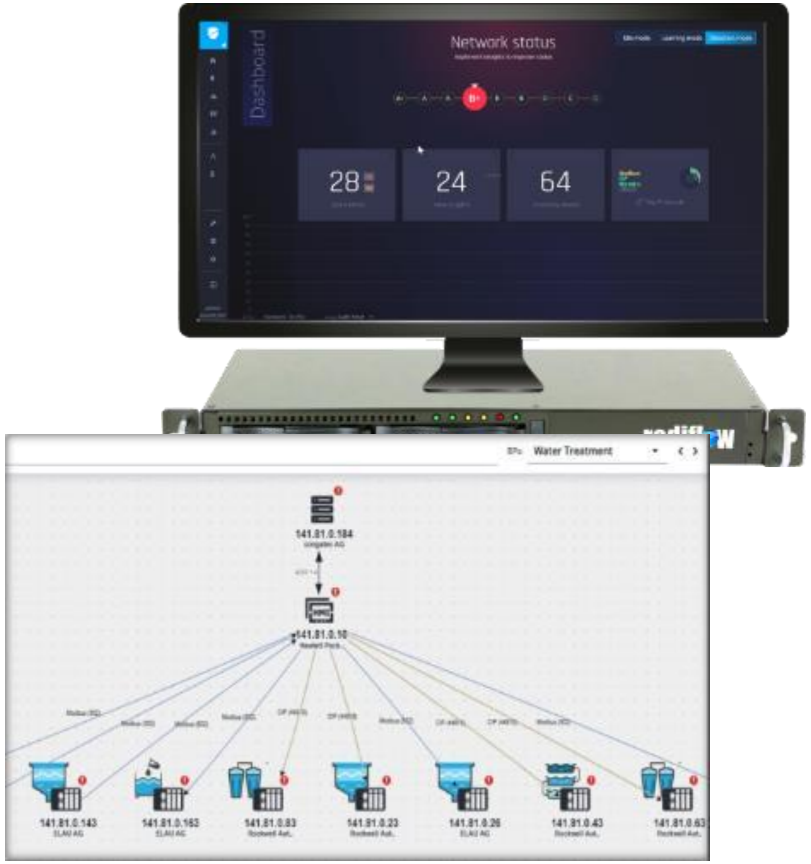
Analytics

CIARA: Risk Analytics

iSOC: MSSP Framework

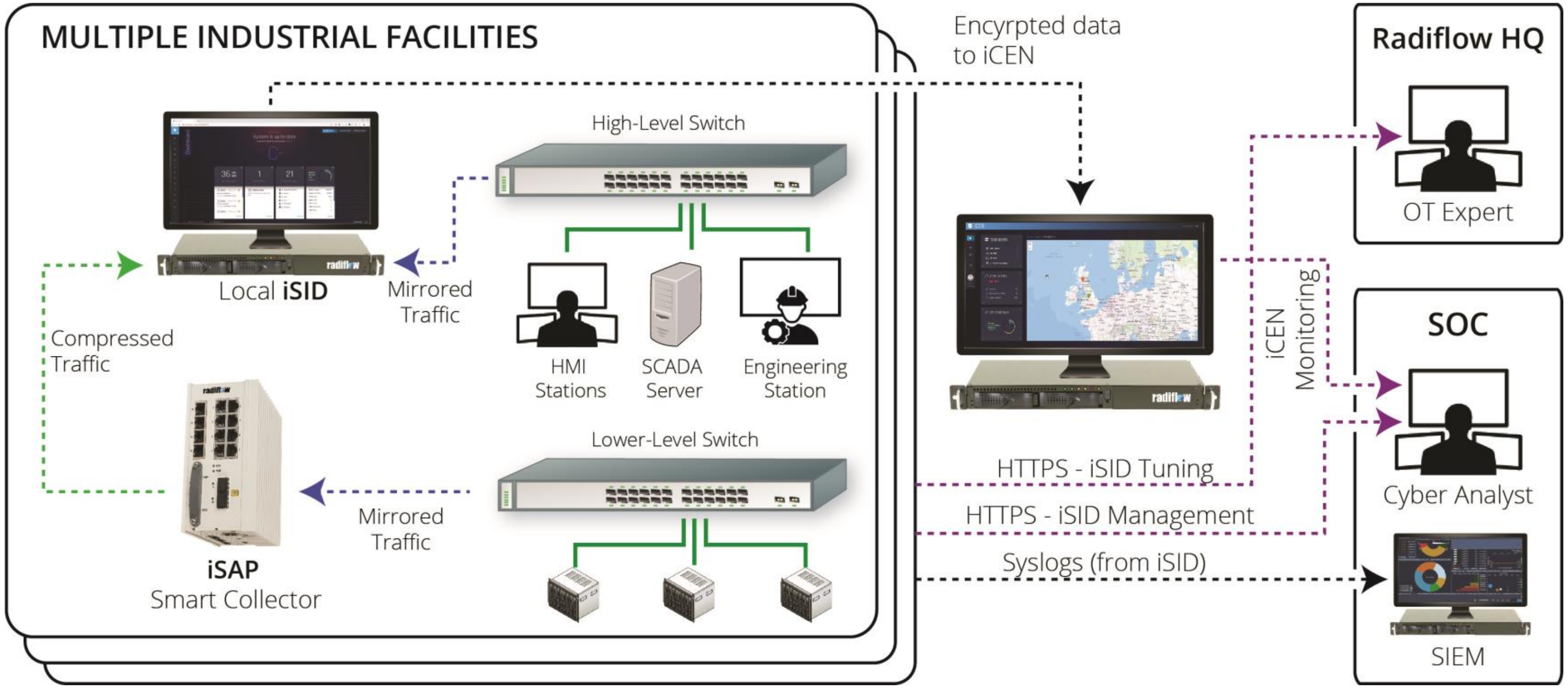
Industrial Threat Detection

- Auto-Mapping
  - Assets & Links
  - Vulnerabilities per Asset
  - Business Processes for Impact analysis
- Anomaly Detection inside the perimeter
- Change management tracking



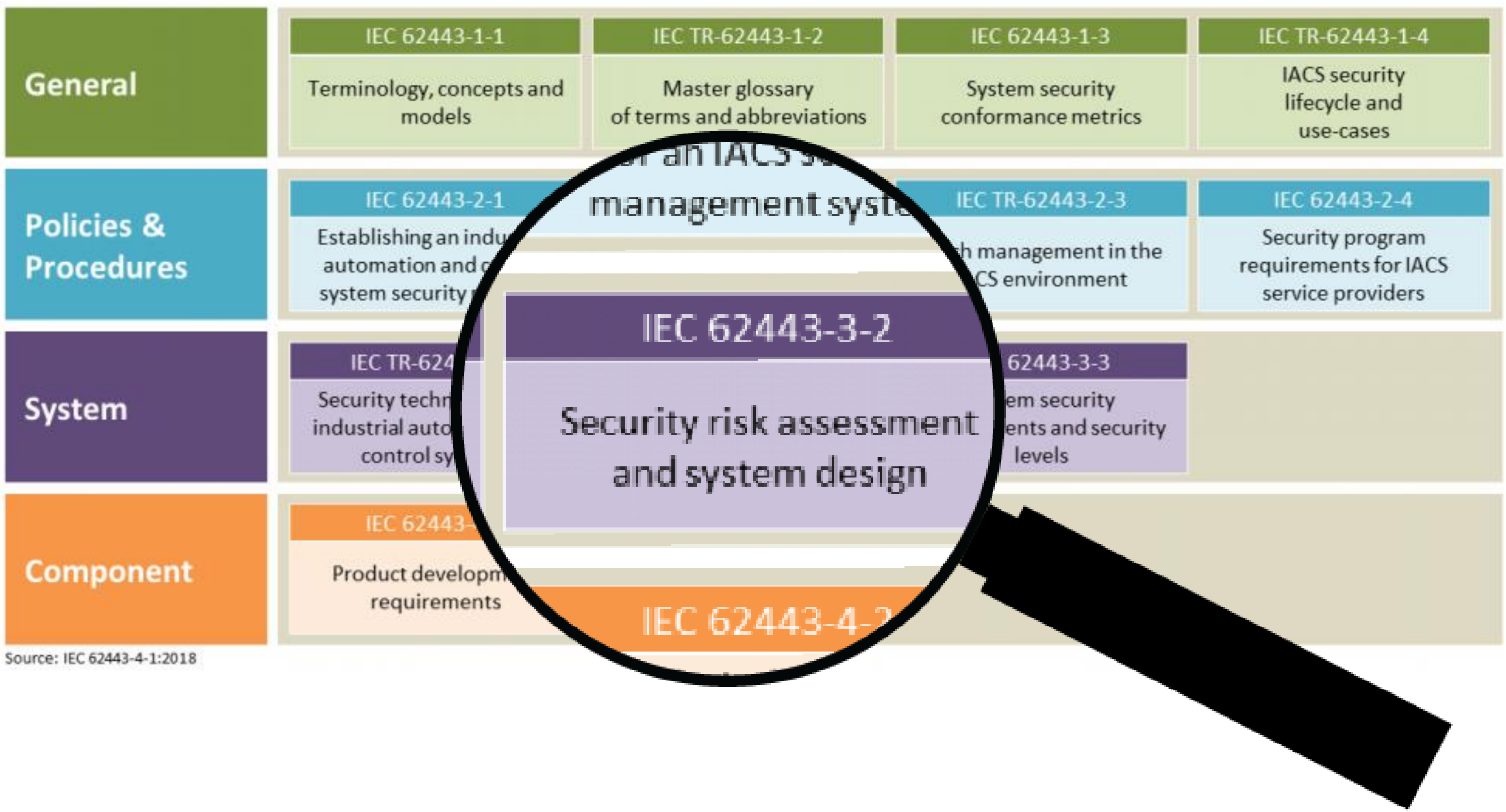
Case Study: Global Chemicals Mfr.

- Local iSID at each plant
- iSAP collectors at each assembly line
- HQ supervision of multiple iSIDs
- Integration with external SOC with OT playbook



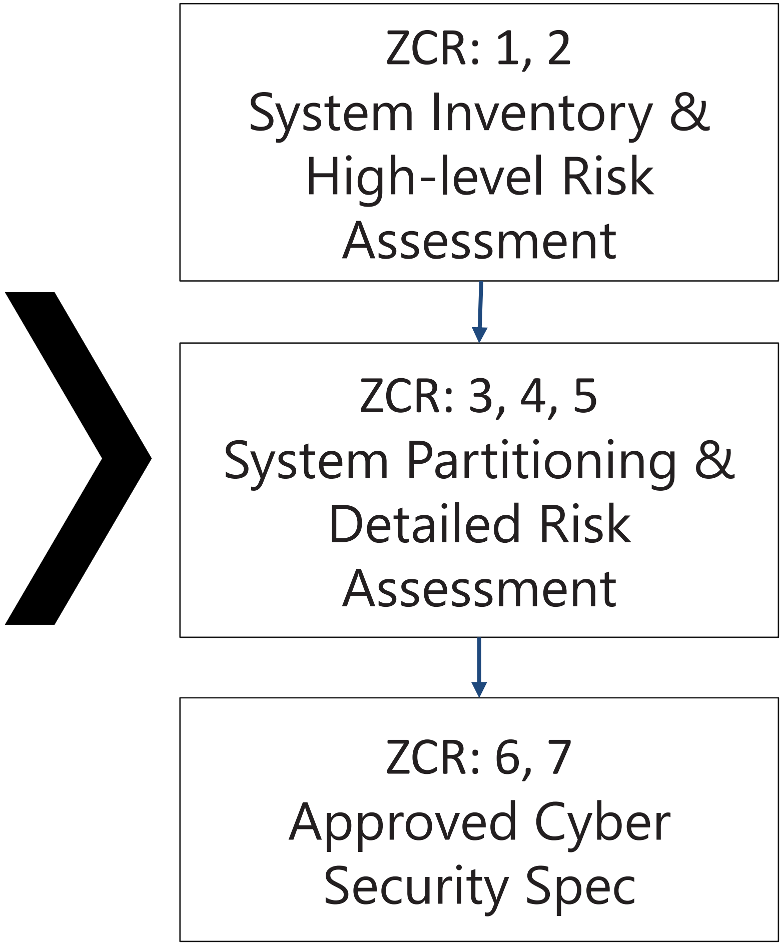
IEC-62443 Guidance

IEC-62443 Directives and corresponding ZCRs
(Zone & Conduit Requirements)



General	IEC 62443-1-1 Terminology, concepts and models	IEC TR-62443-1-2 Master glossary of terms and abbreviations	IEC 62443-1-3 System security conformance metrics	IEC TR-62443-1-4 IACS security lifecycle and use-cases
Policies & Procedures	IEC 62443-2-1 Establishing an indu… automation and c… system security …	…r an IACS s… management syst…	IEC TR-62443-2-3 …h management in the …CS environment	IEC 62443-2-4 Security program requirements for IACS service providers
System	IEC TR-624… Security techn… industrial auto… control sy…	IEC 62443-3-2 Security risk assessment and system design	…62443-3-3 …em security …ents and security levels	
Component	IEC 62443-… Product developm… requirements	IEC 62443-4-2		

Source: IEC 62443-4-1:2018



ZCR: 1, 2
System Inventory & High-level Risk Assessment

ZCR: 3, 4, 5
System Partitioning & Detailed Risk Assessment

ZCR: 6, 7
Approved Cyber Security Spec

CIARA: Industrial Risk Analysis

- OT Cyber Risk Posture
  - Risk scoring per component based on impact
- Risk Reduction Planning
  - Security controls roadmap planning
- Compliance
  - IEC 62443 Workflow & Reports
- Automated Data-Driven Analysis
  - Scenario based Simulations on digital image

Radiflow CIARA - Dashboard

Contact:

Joanne Rout, MIET

ITS Sales Account Manager

E: j-rout@its-ltd.co.uk

T: 07798 900103

its radiflow

THANK YOU

its radiflow