



**XIII
JORNADAS
STIC
CCN-CERT**



Catching Mr Mime: Deception in an ICS environment

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



 **Alejandro Scatton Lóndero**

Deloitte.

Infrastructure & Cloud Protection

ascatton@deloitte.es



 **Pedro Tubío Figueira**

Deloitte.

Infrastructure & Cloud Protection

ptubio@deloitte.es

Index

1. Introduction

- Industry 4.0
- Connected Age: OT + IoT
- Industrial Control Systems Role

2. Deception technology

- How it works?
- Deception in an ICS environment

3. It's demo time: 'Catching Mr. Mime'



1

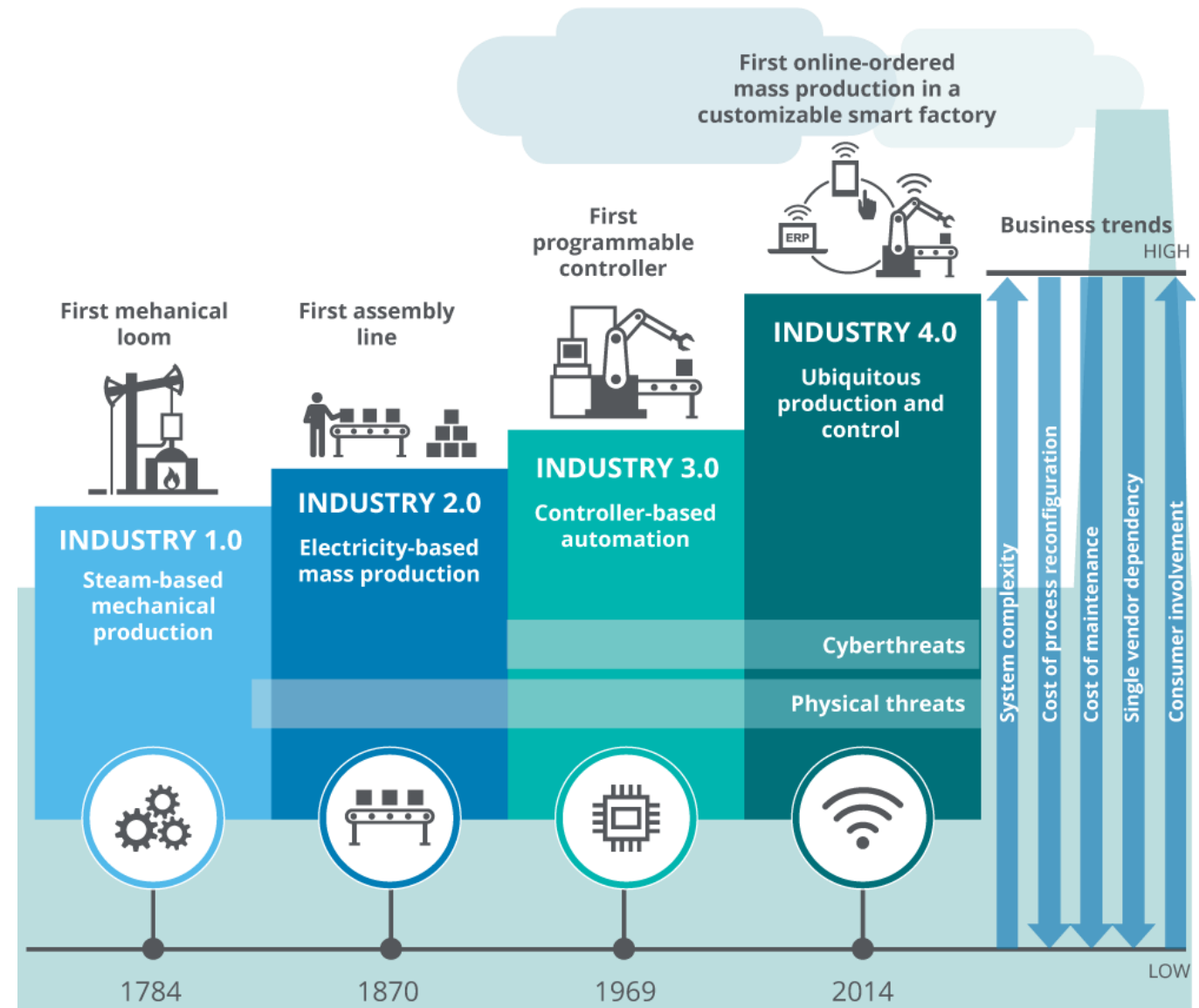
2

3

Introduction

Industry 4.0

- **Evolution:** mechanical, electrical, automation and connectivity.
- **Changes** due to market trends.
- Combination between advanced production techniques and **new technologies**.
- Growth in the number of **communications** between several **devices**, many of which are **not prepared** for that level of exposure.



Source: Deloitte.

Deloitte University Press | dupress.deloitte.com

1

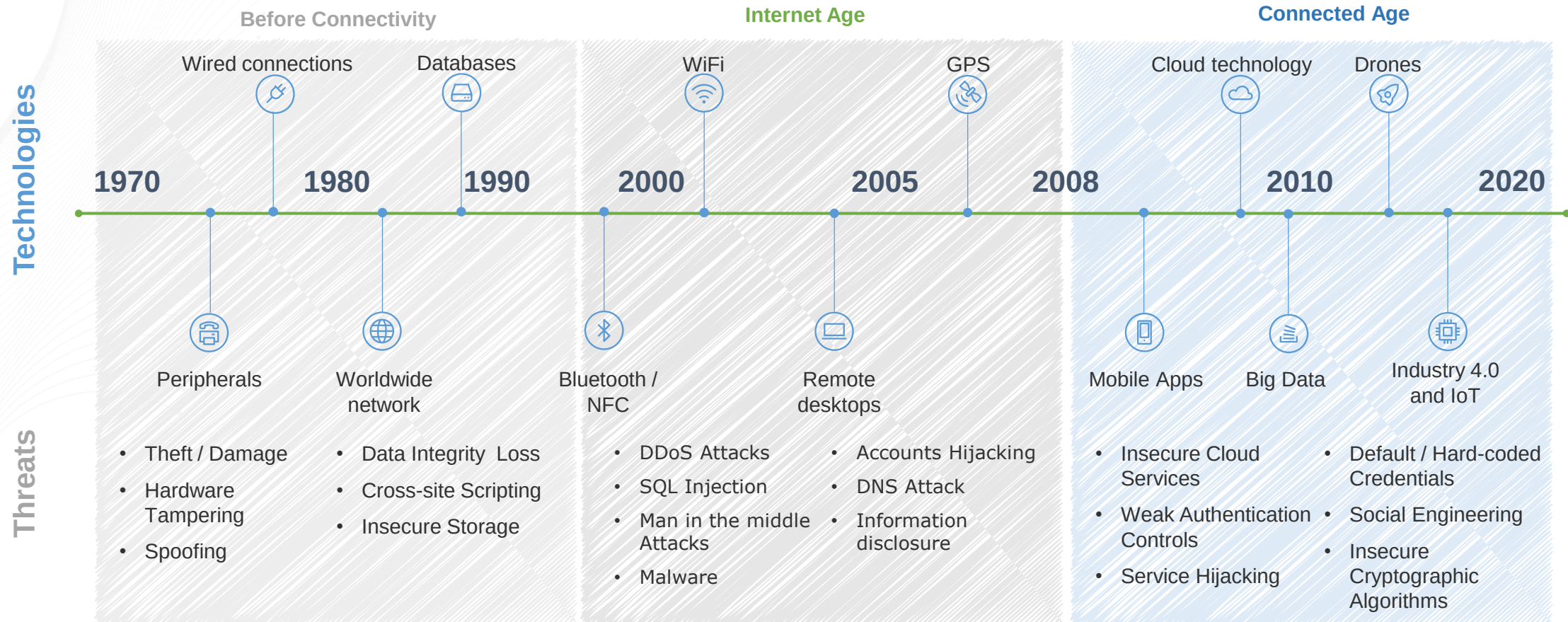
2

3

Introduction

Connected Age: OT + IoT

*"We only have to be **lucky once**. You will have to be **lucky always**."*



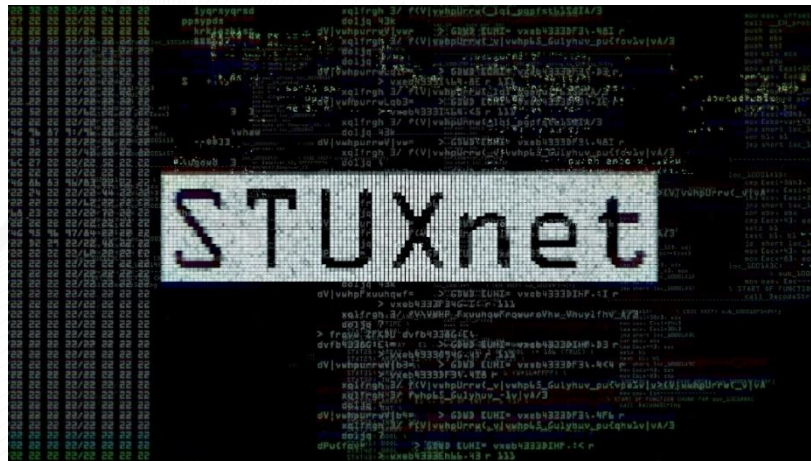
1

2

3

Introduction

Industrial Control Systems Role



Triton is the world's most murderous malware, and it's spreading

Siemens Contractor Pleads Guilty to Planting 'Logic Bomb' in Spreadsheets

Kamerka OSINT tool shows your country's internet-connected critical infrastructure

Kamerka lets you see what a hacker sees. It plots maps with SCADA equipment, webcams, and printers that have been left exposed on the internet inside any given country.

Industroyer: Biggest malware threat to critical infrastructure since Stuxnet

Cyber attack on India's largest nuclear power plant confirmed

Mexican state oil firm Pemex hit by ransomware attack

Islamic State cyber-attack could 'cripple Britain's water, gas and electricity supplies'

1

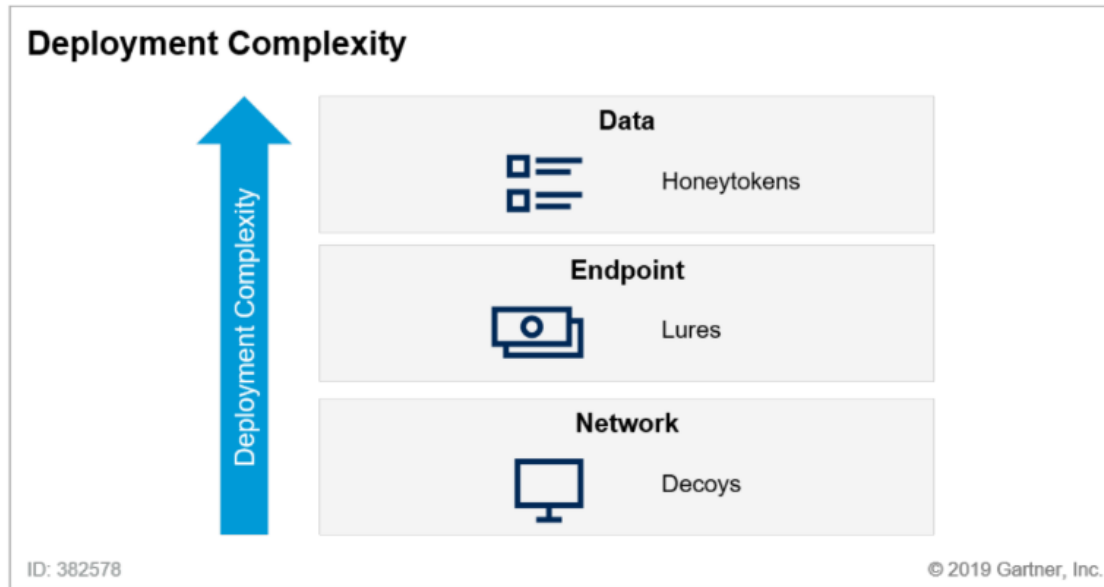
2

3

Deception technology

How it works?

- **Deception**: the act of deceiving someone by making them believe something that is not true.
- Deception vs Honeypot



1

2

3

Deception technology

How it works?



Campaigns

A set of elements that implement a particular aspect of the company's cybersecurity counterintelligence strategy. It defines the objective of the campaign, to whom it is addressed, the story to be followed, the environment to be implemented and the necessary monitoring to later make the analysis of the attacker's actions.



Deception hosts

Systems where the elements that will serve as bait for the attackers will be installed. These systems may contain one or more services configured to record all the actions that the attacker makes within the system.



Deception services

Component designed to increase the attacker's residence time in the bait environment, so that cybersecurity analysts can study their tactics, techniques and procedures.



Breadcrumbs or hints

Elements that are intentionally left inside the systems or deception services so that the attacker can move following the story raised in the campaign.



Rules

The rules are established for each campaign. They define the actions that should be triggered depending on the actions of the attacker or what you want to do with the information gathered.

1

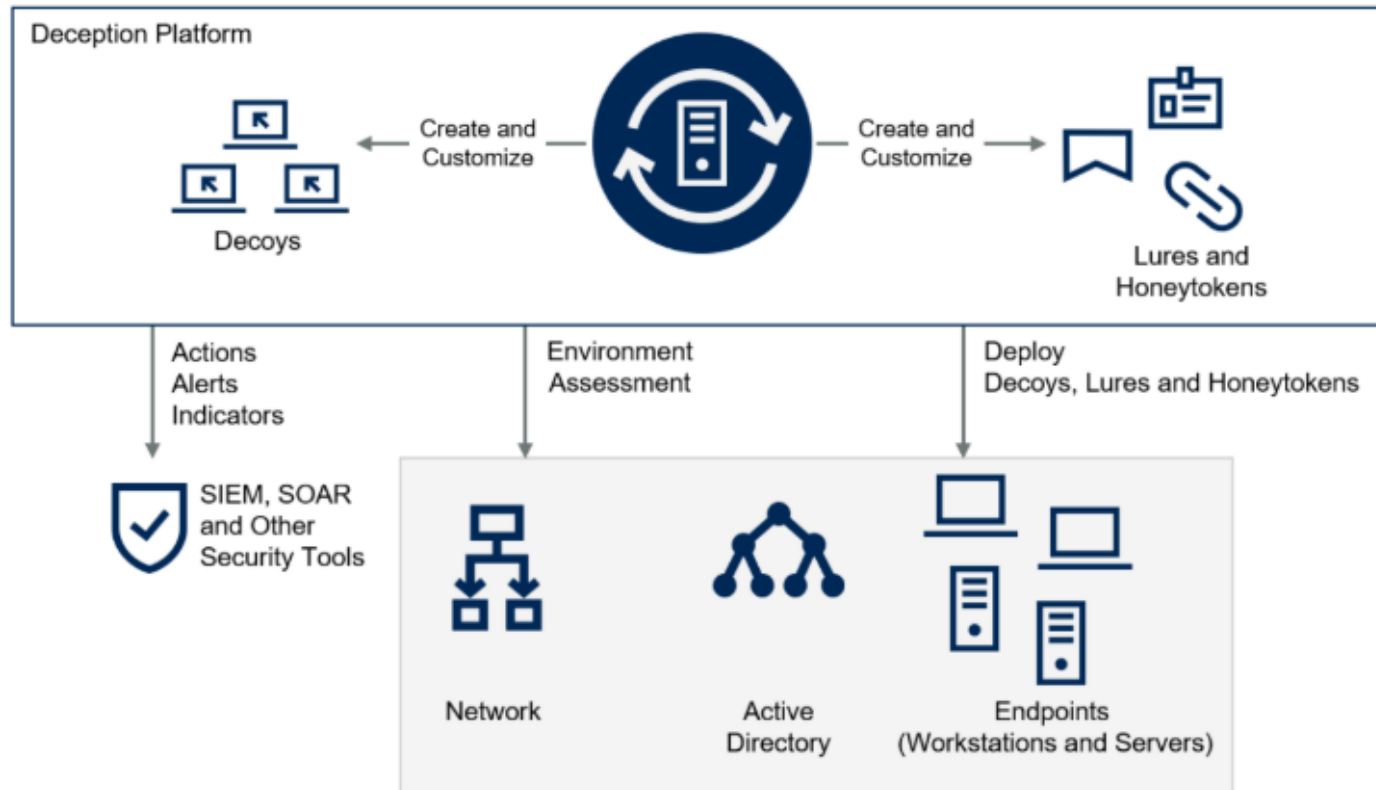
2

3

Deception technology

How it works?

Deception Platform Example



ID: 373461

© 2019 Gartner, Inc.



1 2 3

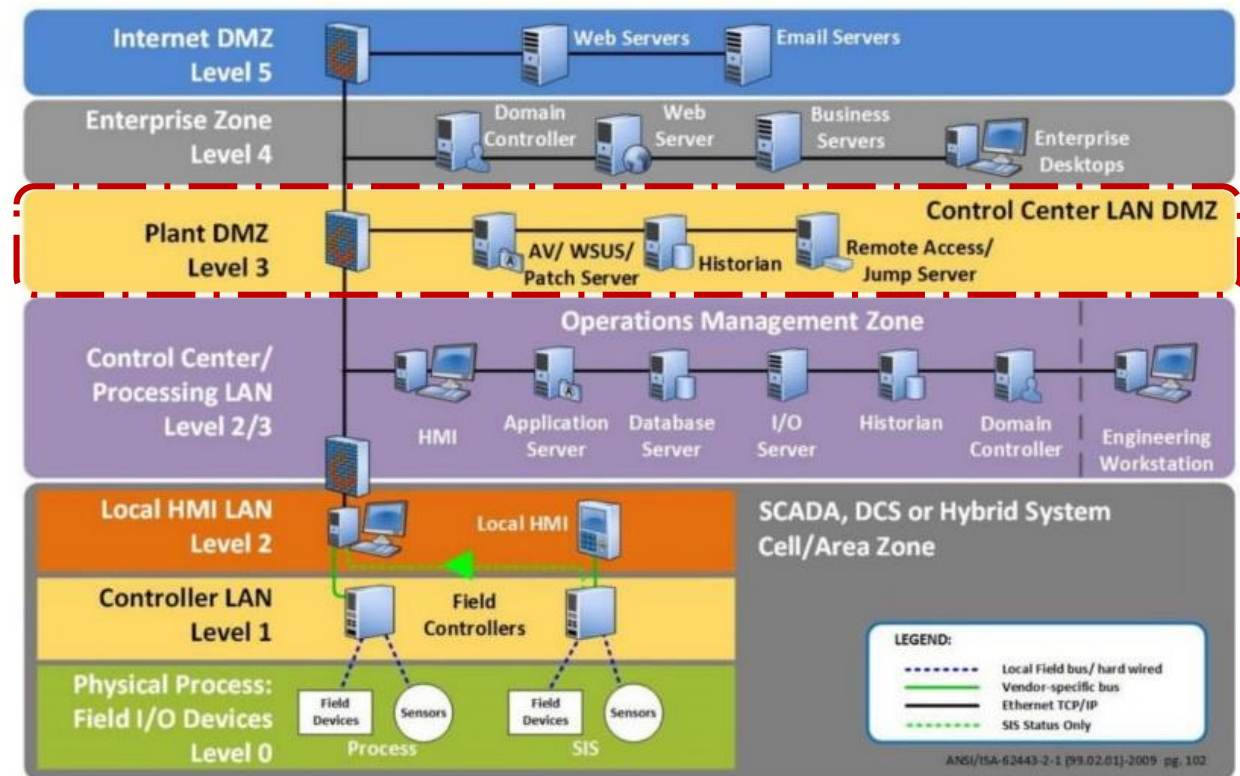
Deception technology

Deception in an ICS environment

Industrial Control Systems characteristics:

- Operation is the priority
- New connections, old devices
- Devices out of date
- Lack of security monitoring
- Low performance
- Reduced fault tolerant
- Physically isolated

Critical infrastructures = targets





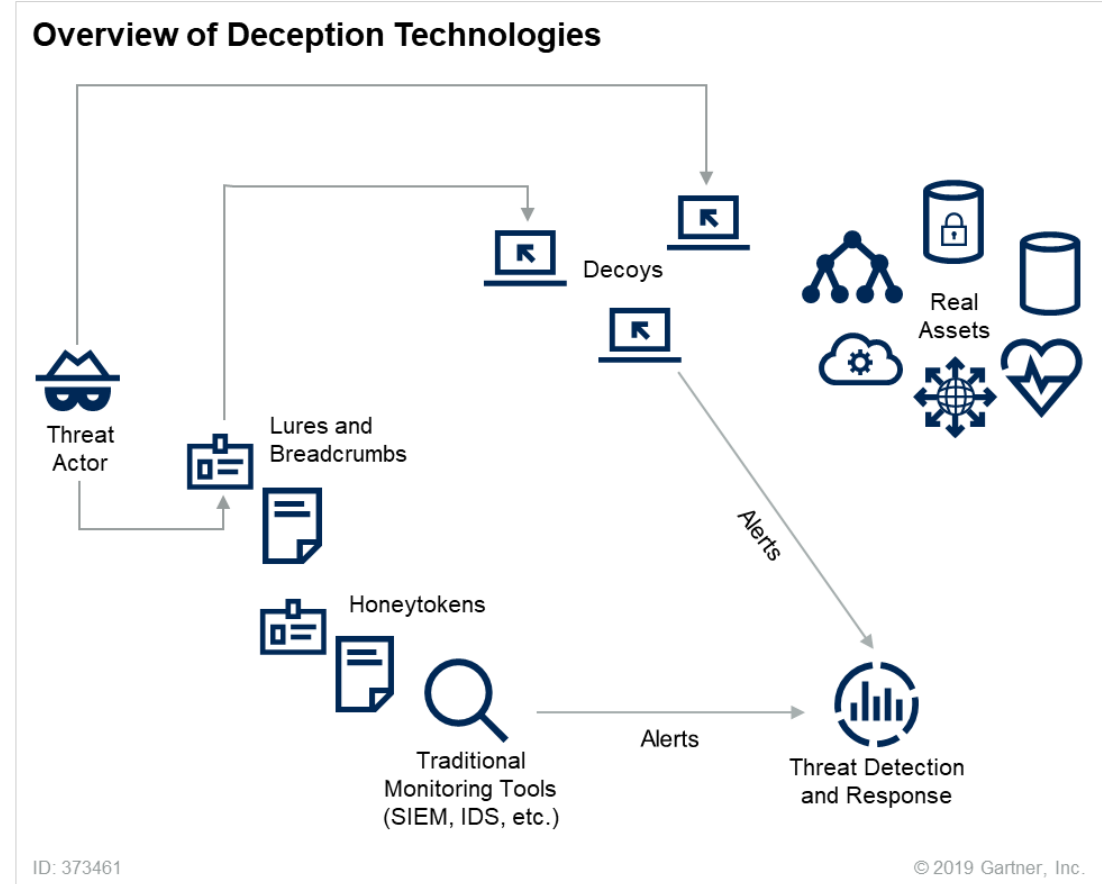
Deception technology

Deception in an ICS environment

- Self contained solution
- Avoid interaction with other devices. Reduce impact on operation.
- Outside of real systems
- Ease of deployment and customization
- Real-time countermeasures
- Security monitoring and rising alerts

*“Now **you** have to be **lucky always** and **we** only have to be **lucky once**.”*

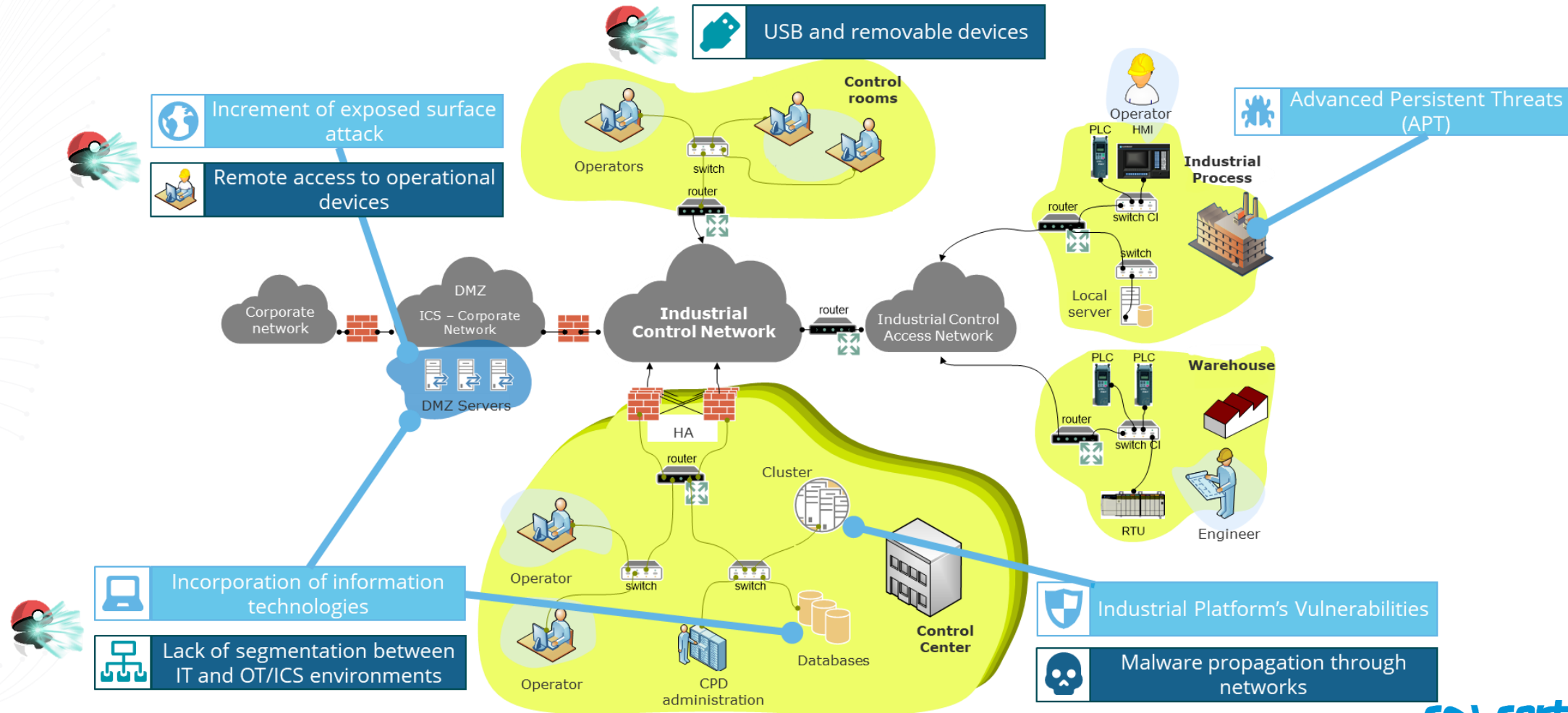
That's what we say now to Mr Mime



1 2 3

Deception technology

Deception in an ICS environment



1

2

3

It's demo time: 'Catching Mr. Mime'



Catching Mr. Mime: Deception in an ICS environment

Conclusions

- Self contained: no interaction with real systems.
- Automated, accurate and correlated.
- Detect threats related with:
 - Exposure of ICS environments.
 - IoT deployments and lateral movements.
 - OT Network segmentation.
 - Lack of hardening and patching.
 - Zero-days.
- Learn of attackers and apply countermeasures.

Is not a stand-alone strategy: additional layer.



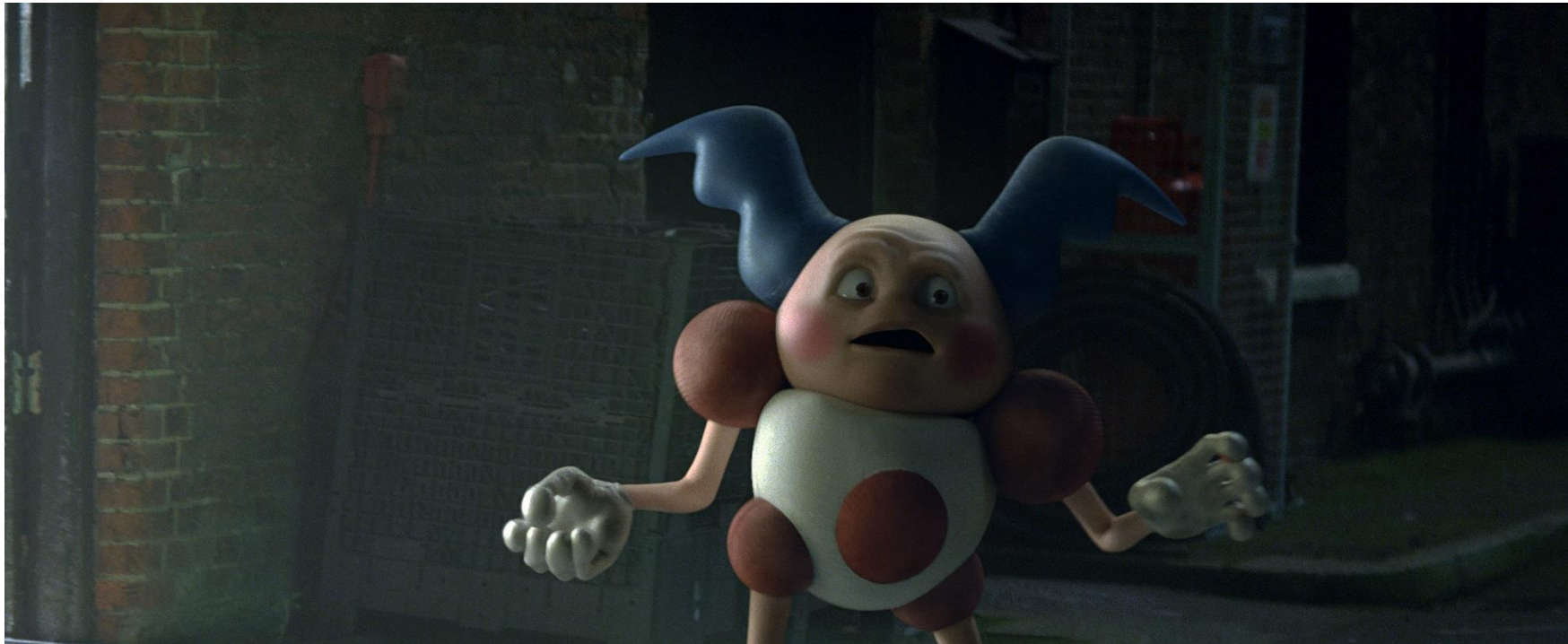
1

2

3

Catching Mr. Mime: Deception in an ICS environment

Questions, comments...?



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional