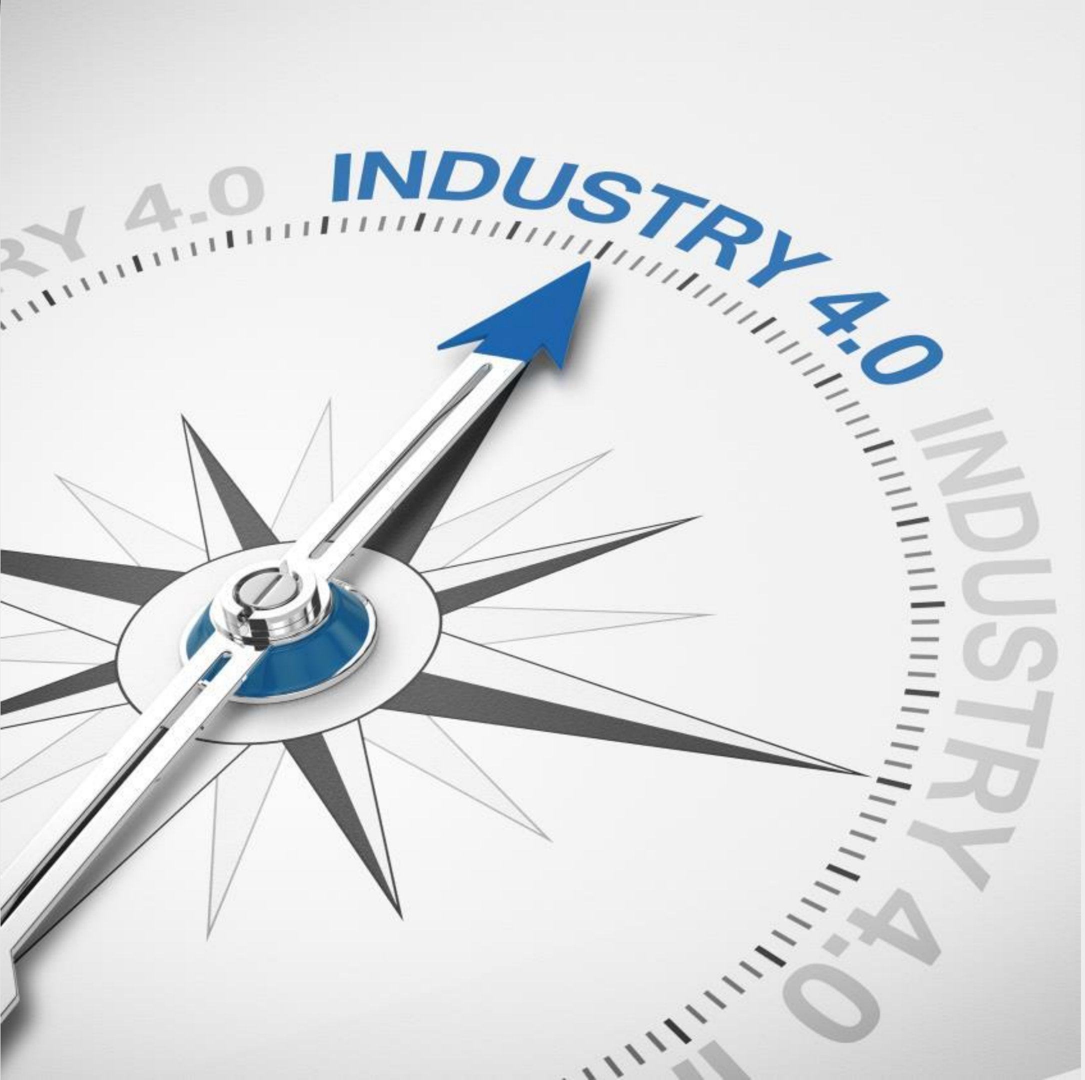


# Sicurezza IT: un nuovo modello per il mondo digitale

Fabio Panada
Consulting Security Engineer

Organizzato da

# Today’s risk reality

## More interconnected than ever

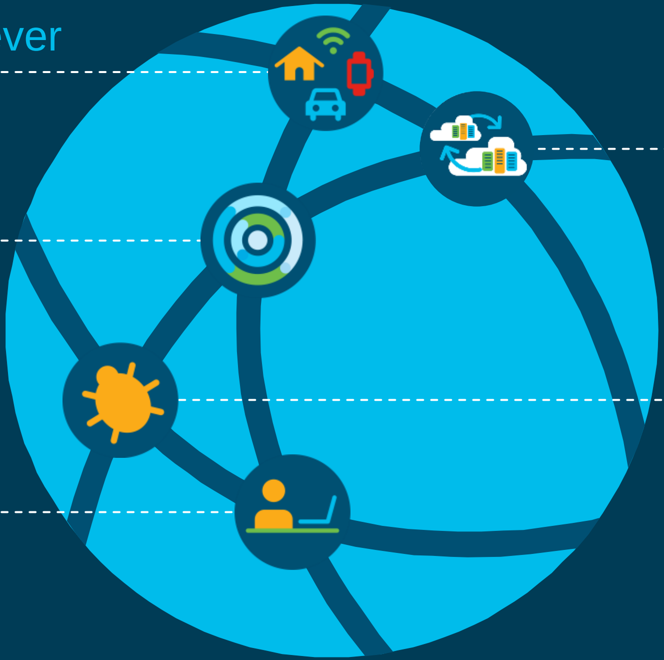
Expanded attack surface

## Continuous operations

Must keep business running

## Workers connecting everywhere

Loss of control



## Multi-cloud reality

A software-defined world

## Automated and sophisticated threats

High likelihood of a breach

# Attack landscape constantly evolving

Advanced Persistent Threats

Unpatched Software

Spyware/Malware

Wiper Attacks

Phishing

Man in the Middle

DDoS

Cryptomining

Supply chain attacks

Ransomware

Data/IP Theft

Malvertising

Drive by Downloads

Rogue Software

Botnets

Credential compromise

# The Italian cybersecurity situation

**2018**

has been the **worst year to date** in terms of the **evolution of «cyber» threats**

**Phishing** and social engineering have increased by **57%**

In the past two years, **growth in the number of serious attacks** has increased **tenfold** compared to the previous two-year period (+37.7% compared to the previous year).

The main purposes of the cyber attacks suffered by companies in the current scenario are **frauds,** such as phishing and business email compromise (83%), **extortion** (78%), **intrusion for the purpose of spying** (46%) and **interruption of service** (36%).

***Sources***:

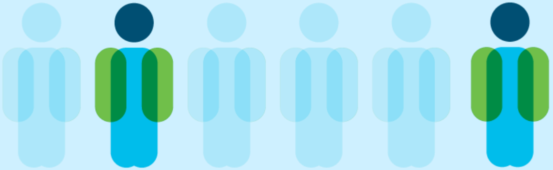
- Clusit Report 2019 on ICT security in Italy
- Information & Security Privacy Observatory 2019 - Politecnico di Milano

# Financial damage following an attack

**62%**

of attacks in Italy in 2018 caused **damage greater than € 80,000**.

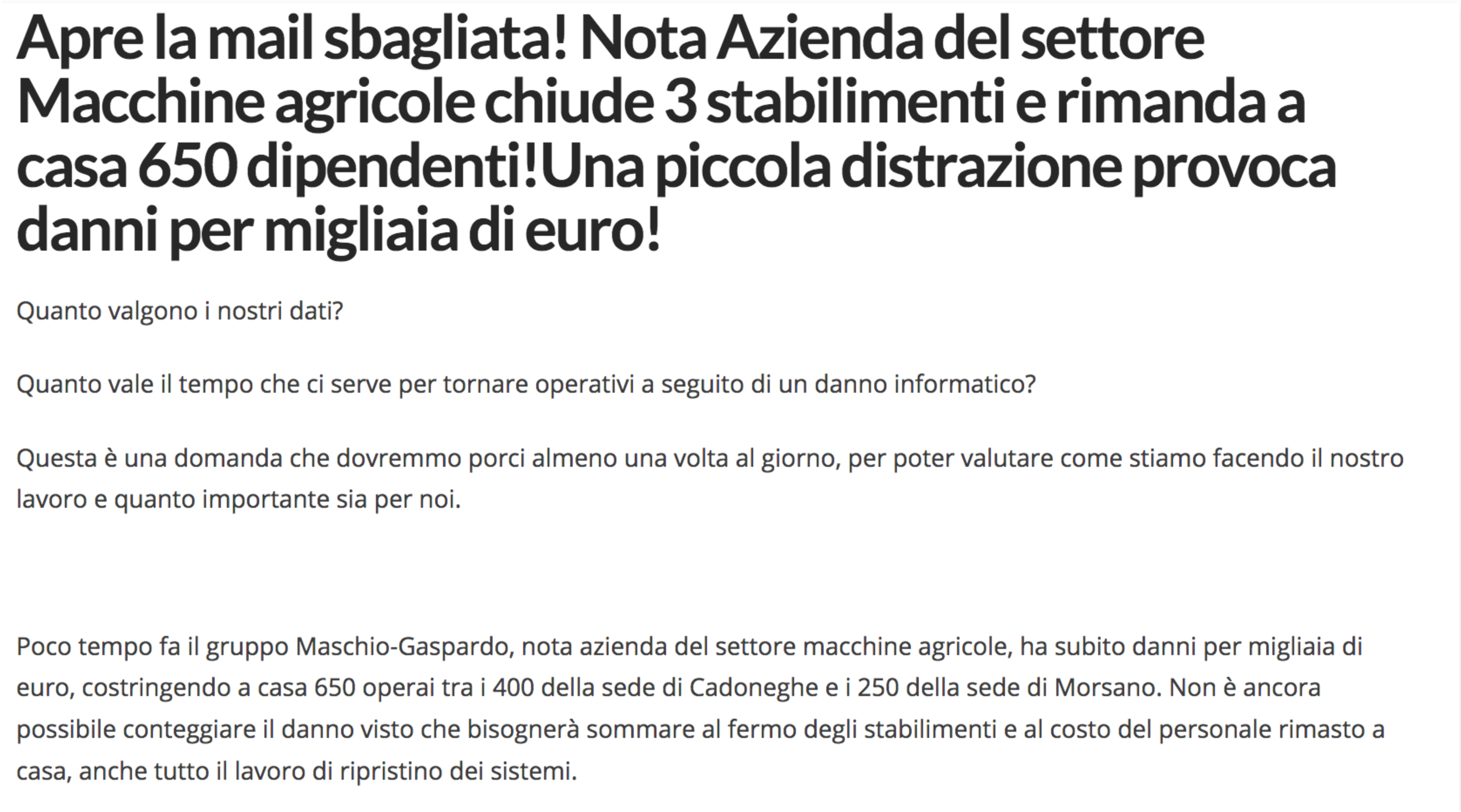
for **18%** of companies, that damage results in **loss of clients.**



**In 2018, the violations in Italy** caused damage to **more than half of company systems**. Why? Many Italian companies still struggle to integrate legacy systems into their infrastructure and adequately protect them.

***Source:***

**- Security Capabilities Benchmark Study 2018 by Cisco**



# Apre la mail sbagliata! Nota Azienda del settore Macchine agricole chiude 3 stabilimenti e rimanda a casa 650 dipendenti!Una piccola distrazione provoca danni per migliaia di euro!

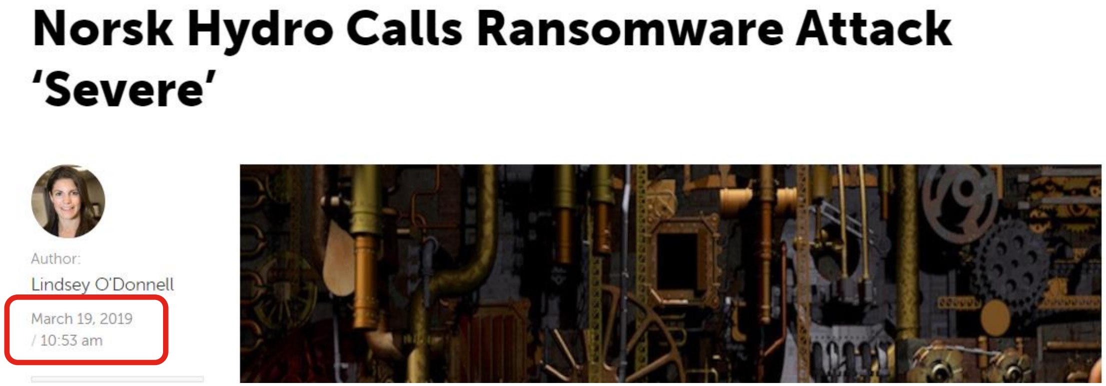
Quanto valgono i nostri dati?

Quanto vale il tempo che ci serve per tornare operativi a seguito di un danno informatico?

Questa è una domanda che dovremmo porci almeno una volta al giorno, per poter valutare come stiamo facendo il nostro lavoro e quanto importante sia per noi.

Poco tempo fa il gruppo Maschio-Gaspardo, nota azienda del settore macchine agricole, ha subito danni per migliaia di euro, costringendo a casa 650 operai tra i 400 della sede di Cadoneghe e i 250 della sede di Morsano. Non è ancora possibile conteggiare il danno visto che bisognerà sommare al fermo degli stabilimenti e al costo del personale rimasto a casa, anche tutto il lavoro di ripristino dei sistemi.

# Industrial Attack of the Month – Hydro Norsk



**Norsk Hydro Calls Ransomware Attack 'Severe'**

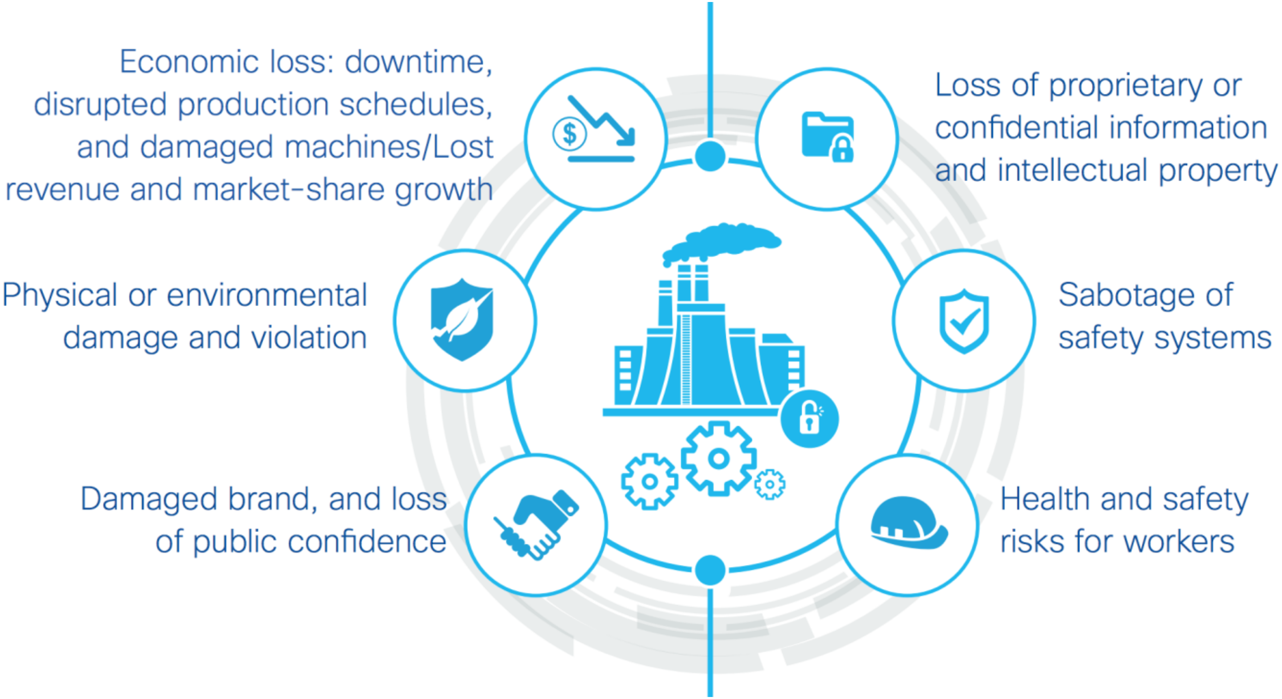
Author:
Lindsey O'Donnell

March 19, 2019
/ 10:53 am

## Enterprise and Plants impacted

- Some plants (smelters)shut down by infection.
- Others being manually operated.
- Others purposely being shut down for safety.

# The Effect of a Threat - Impact



Economic loss: downtime, disrupted production schedules, and damaged machines/Lost revenue and market-share growth

Loss of proprietary or confidential information and intellectual property

Physical or environmental damage and violation

Sabotage of safety systems

Damaged brand, and loss of public confidence

Health and safety risks for workers

# A Multi-Layered Defense Strategy

- Threat intelligence – Knowledge of existing Ransomware and communication vectors
- E-mail security – Block Ransomware attachments and links
- Web Security – Block web communication to infected sites and files
- DNS Security - Break the Command & Control call back

- Client Security – Inspect files for Ransomware and Virus's, quarantine and remove
- Segment infrastructure – Authenticate access, separate traffic based on role and policy
- Intrusion Prevention - Block attacks, exploitation and intelligence gathering
- Monitor Infrastructure communications – Identify and alert on abnormal traffic flows

# A Multi-Layered Defense Strategy

## Prevent:

Back up all of your critical data

Protect users on any device, anywhere, anytime

Consistent and comprehensive patch management

## Detect and Contain:

Continuously monitor your networks

Identify malware exploit kits and prevent malware code form executing

Block malicious command and control traffic, malicious files and malicious URLs in email

## Reduce Risk of Infection:

Develop a proactive security plan that leverages a multi-layer defense

Use predictive intelligence to understand where attacks are staged on the internet

Continuously improve network hygiene and evaluate your security posture

# Security challenges in the IoT

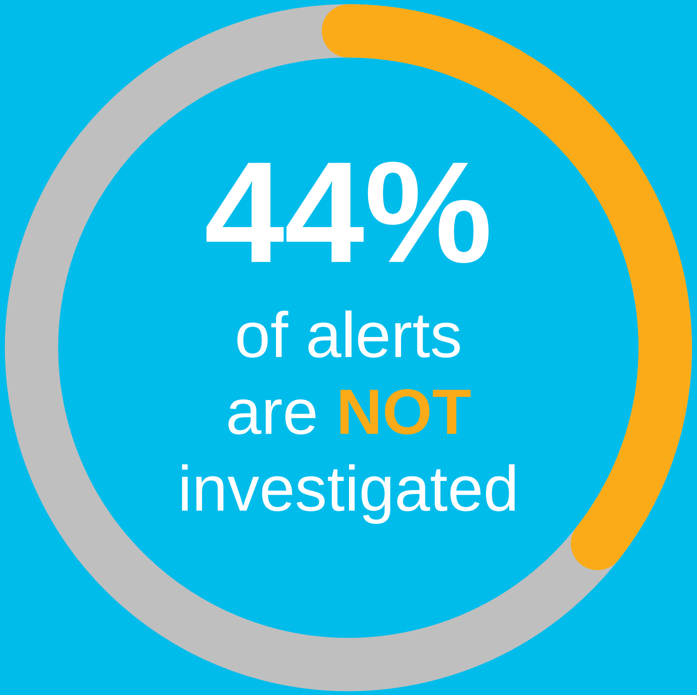
New to cybersecurity

Insufficient resources

Market pressures

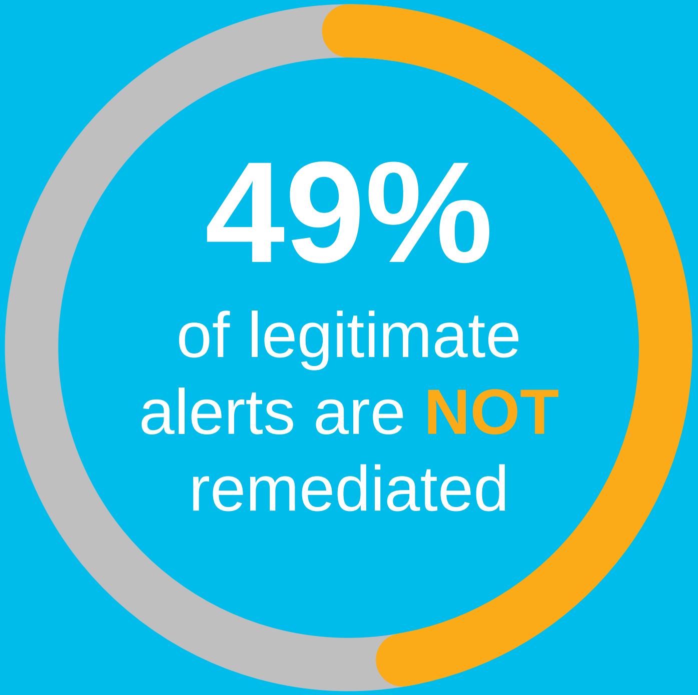
Cyberattacks against IoT devices where up by 310% in 2018 with 90% of attacks being against IoT devices*

*Source: Cisco



**44%**

of alerts are **NOT** investigated



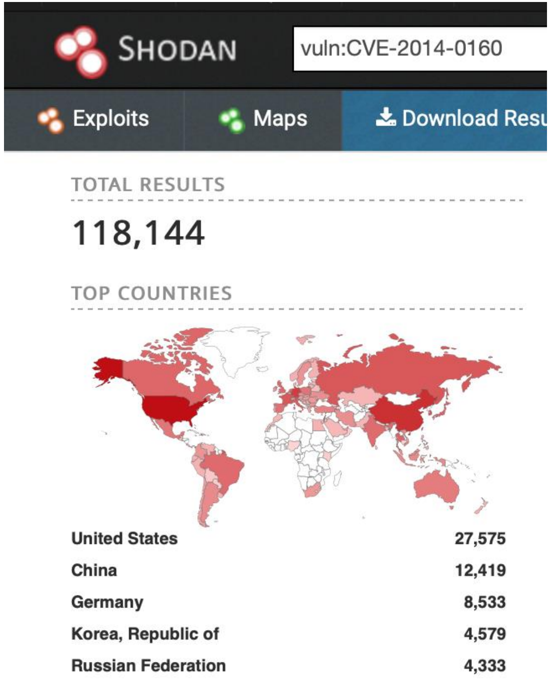
**49%**

of legitimate alerts are **NOT** remediated

Source: Annual Cisco Cybersecurity Report

# We Can Always Patch

- Right?

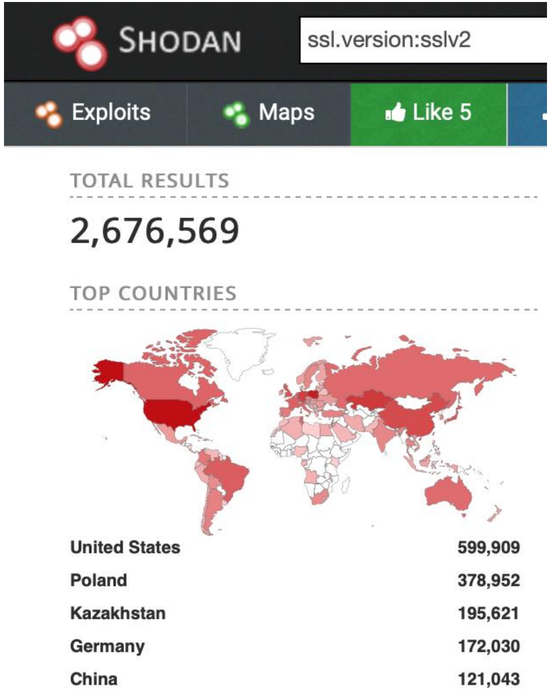


TOTAL RESULTS

118,144

TOP COUNTRIES

| | |
|---|---|
| United States | 27,575 |
| China | 12,419 |
| Germany | 8,533 |
| Korea, Republic of | 4,579 |
| Russian Federation | 4,333 |

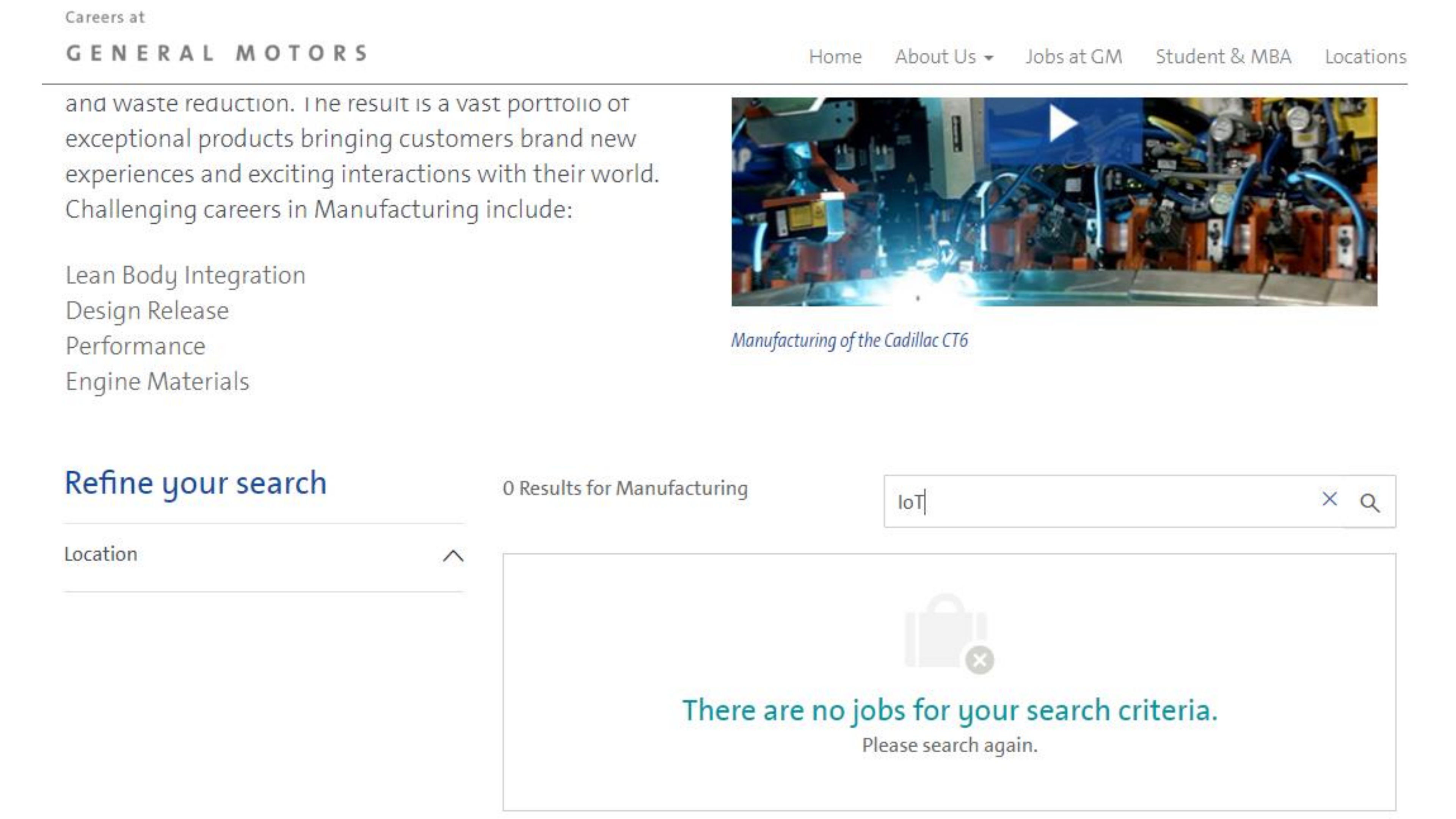


TOTAL RESULTS

2,676,569

TOP COUNTRIES

| | |
|---|---|
| United States | 599,909 |
| Poland | 378,952 |
| Kazakhstan | 195,621 |
| Germany | 172,030 |
| China | 121,043 |



and waste reduction. The result is a vast portfolio of exceptional products bringing customers brand new experiences and exciting interactions with their world. Challenging careers in Manufacturing include:

Lean Body Integration
Design Release
Performance
Engine Materials

*Manufacturing of the Cadillac CT6*

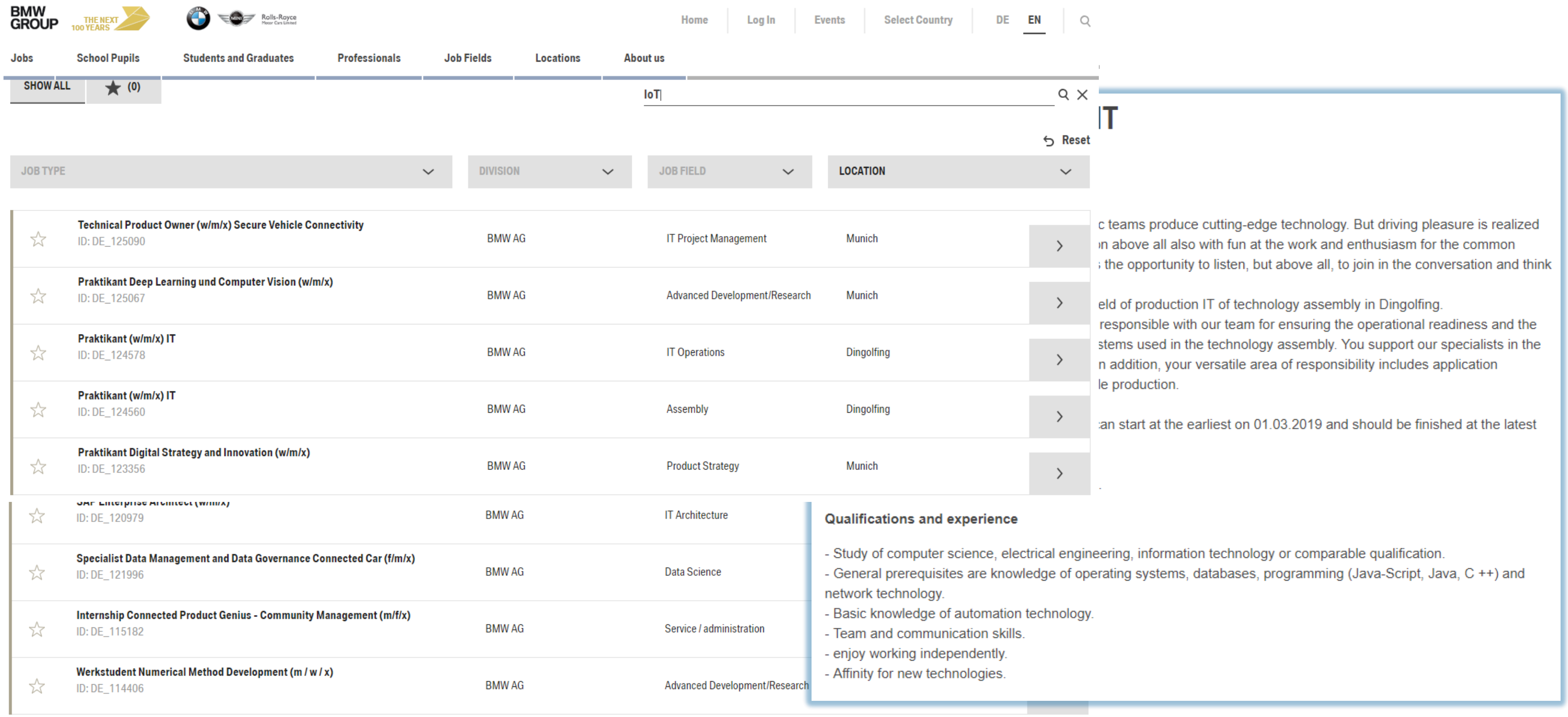
Refine your search

0 Results for Manufacturing

IoT

There are no jobs for your search criteria.

Please search again.



| | | | |
|---|---|---|---|
| Technical Product Owner (w/m/x) Secure Vehicle Connectivity<br>ID: DE_125090 | BMW AG | IT Project Management | Munich |
| Praktikant Deep Learning und Computer Vision (w/m/x)<br>ID: DE_125067 | BMW AG | Advanced Development/Research | Munich |
| Praktikant (w/m/x) IT<br>ID: DE_124578 | BMW AG | IT Operations | Dingolfing |
| Praktikant (w/m/x) IT<br>ID: DE_124560 | BMW AG | Assembly | Dingolfing |
| Praktikant Digital Strategy and Innovation (w/m/x)<br>ID: DE_123356 | BMW AG | Product Strategy | Munich |
| SAP Enterprise Architect (w/m/x)<br>ID: DE_120979 | BMW AG | IT Architecture | |
| Specialist Data Management and Data Governance Connected Car (f/m/x)<br>ID: DE_121996 | BMW AG | Data Science | |
| Internship Connected Product Genius - Community Management (m/f/x)<br>ID: DE_115182 | BMW AG | Service / administration | |
| Werkstudent Numerical Method Development (m / w / x)<br>ID: DE_114406 | BMW AG | Advanced Development/Research | |

IT

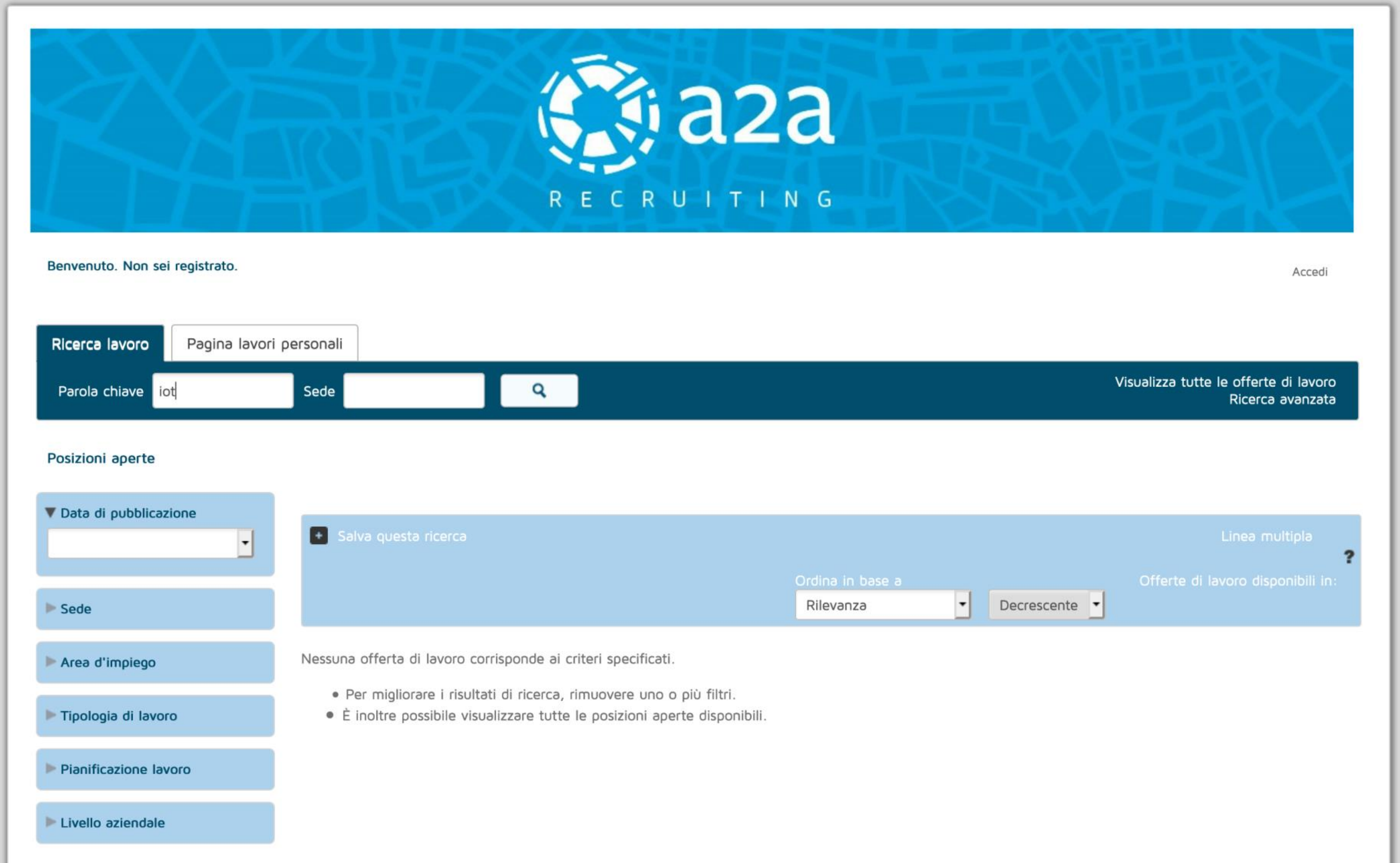
c teams produce cutting-edge technology. But driving pleasure is realized
n above all also with fun at the work and enthusiasm for the common
; the opportunity to listen, but above all, to join in the conversation and think

eld of production IT of technology assembly in Dingolfing.
responsible with our team for ensuring the operational readiness and the
stems used in the technology assembly. You support our specialists in the
n addition, your versatile area of responsibility includes application
le production.

an start at the earliest on 01.03.2019 and should be finished at the latest

**Qualifications and experience**

- Study of computer science, electrical engineering, information technology or comparable qualification.
- General prerequisites are knowledge of operating systems, databases, programming (Java-Script, Java, C ++) and network technology.
- Basic knowledge of automation technology.
- Team and communication skills.
- enjoy working independently.
- Affinity for new technologies.



Benvenuto. Non sei registrato.

Parola chiave: iot

Sede:

Posizioni aperte

Ordina in base a: Rilevanza, Decrescente

Offerte di lavoro disponibili in:

Nessuna offerta di lavoro corrisponde ai criteri specificati.

- Per migliorare i risultati di ricerca, rimuovere uno o più filtri.
- È inoltre possibile visualizzare tutte le posizioni aperte disponibili.

# Intersection of IT & OT – Fusion or Parallel Universe?

| IT Network | | OT Network |
|---|---|---|
| **Protecting Intellectual Property and Company Assets** | **Focus** | **24/7 Operations, High OEE, Safety, and Ease of Use** |
| Confidentiality, Integrity, Availability | Priority | Availability, Integrity, Confidentiality |
| Converged Network of Data, Voice and Video (Hierarchical) | Types of Data Traffic | Converged Network of Data, Control Protocols, Information, Safety and Motion (P2P & Hierarchical) |
| Strict Network Authentication and Access Policies | Access Control | Strict Physical Access and<br>Simple Network Device Access |
| Continues to Operate | Implications of Device Failure | Could Stop Processes, Impact Markets, Physical Harm |
| Shut Down Access to Detected Threat and Remediate | Threat Protection | Potentially Keep Operating with a Detected Threat |
| ASAP, during uptime | Upgrades & Patch Management | Scheduled, during downtime |

# Two Paths to Implementation

## Brown Field

- Legacy Infrastructure
- Incremental changes
- Understand risks
- Outline long term architecture
- Migrate when possible

## Green Field

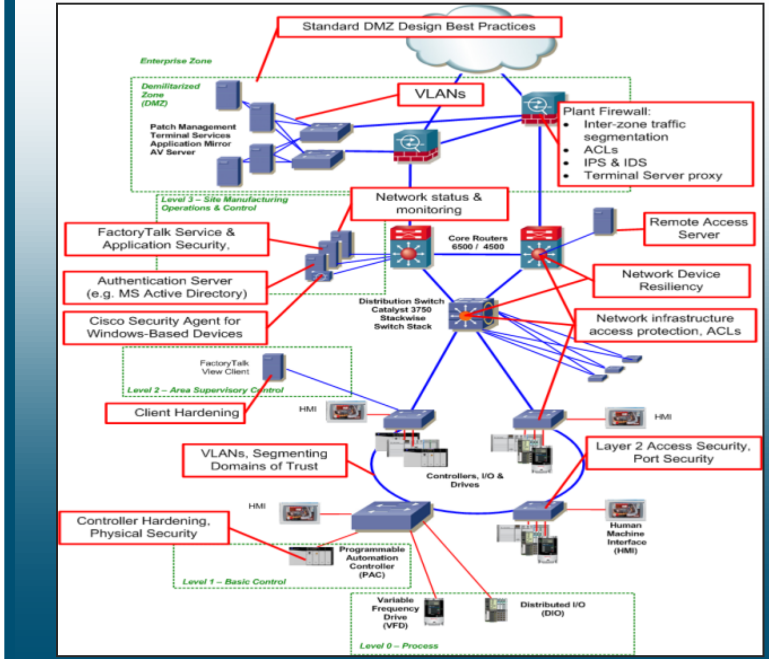
- New technologies
  - Open protocols
  - Distributed workflows
  - Fog Computing
  - Machine learning
- Industry Mindshare Forums
- Transformational IoT

# How do we Implement Industrial Cyber Security?

**Follow ISA99 / IEC 62443 Security Guidelines**

Recommends:

- Documented Controls Security Policy
- Network Demilitarised Zone (DMZ)
- Defending the Industrial edge (IPS, ISE)
- Protect the Interior (ACLs, Port Security, StormControl)
- Remote Access Policy (VPN)
- Endpoint and Network Hardening
- Physical Security


Standard DMZ Design Best Practices
Enterprise Zone
Demilitarized Zone (DMZ)
Patch Management
Terminal Services
Application Mirror
AV Server
VLANs
Plant Firewall:
• Inter-zone traffic segmentation
• ACLs
• IPS & IDS
• Terminal Server proxy
Level 3 – Site Manufacturing Operations & Control
Network status & monitoring
FactoryTalk Service & Application Security,
Core Routers 6500 / 4500
Remote Access Server
Authentication Server (e.g. MS Active Directory)
Network Device Resiliency
Distribution Switch Catalyst 3750 Stackwise Switch Stack
Cisco Security Agent for Windows-Based Devices
Network infrastructure access protection, ACLs
FactoryTalk View Client
Level 2 – Area Supervisory Control
Client Hardening
HMI
HMI
VLANs, Segmenting Domains of Trust
Controllers, I/O & Drives
Layer 2 Access Security, Port Security
HMI
Controller Hardening, Physical Security
Programmable Automation Controller (PAC)
Human Machine Interface (HMI)
Level 1 – Basic Control
Variable Frequency Drive (VFD)
Distributed I/O (DIO)
Level 0 – Process

http://isa99.isa.org

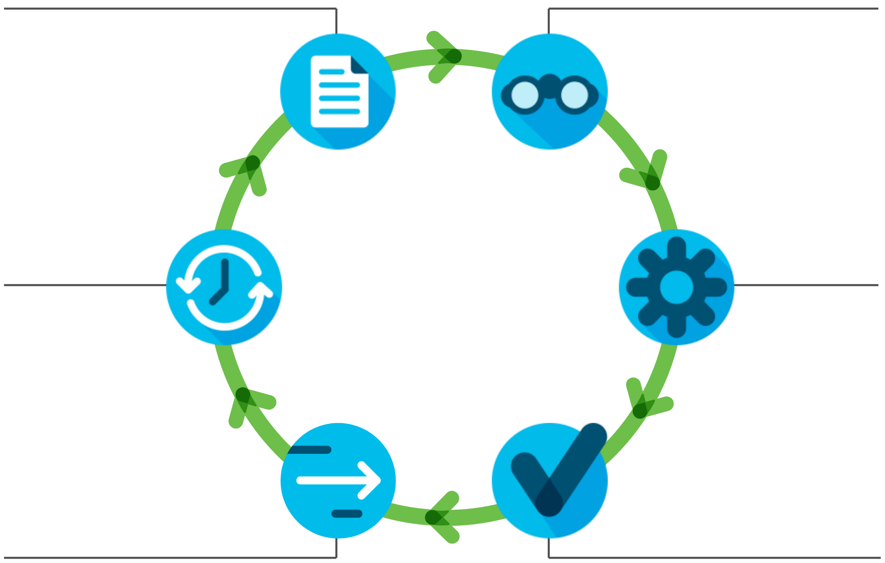
*Setting the Standard for Automation™*

The International Society of Automation is a nonprofit organization that helps its 30,000 worldwide members and other automation professionals solve difficult technical problems, while enhancing their leadership and personal career capabilities.

# Capabilities in Industrial Security

| | |
|---|---|
| Visibility | Recognition of zones, conduits, and their control networks. |
| Control | Ability to react to and isolate problems. Ensure stability of infrastructure. |
| Compliance | Having the audit trail |
| Segmentation | Fault domain isolation. Differentiated Services. Security zones |
| Threat Detection | Continuously updated detection engines from world-class security researchers. Available endpoint to core. |
| Secure Access | Secure and manage partner and vendor plant floor access |

# Segmentation is THE process



Visibility

See what is on the network

Cluster analysis and segment definition

Classify

Validation

Author (push polices)

Segmentation enforcement

Active enforcement

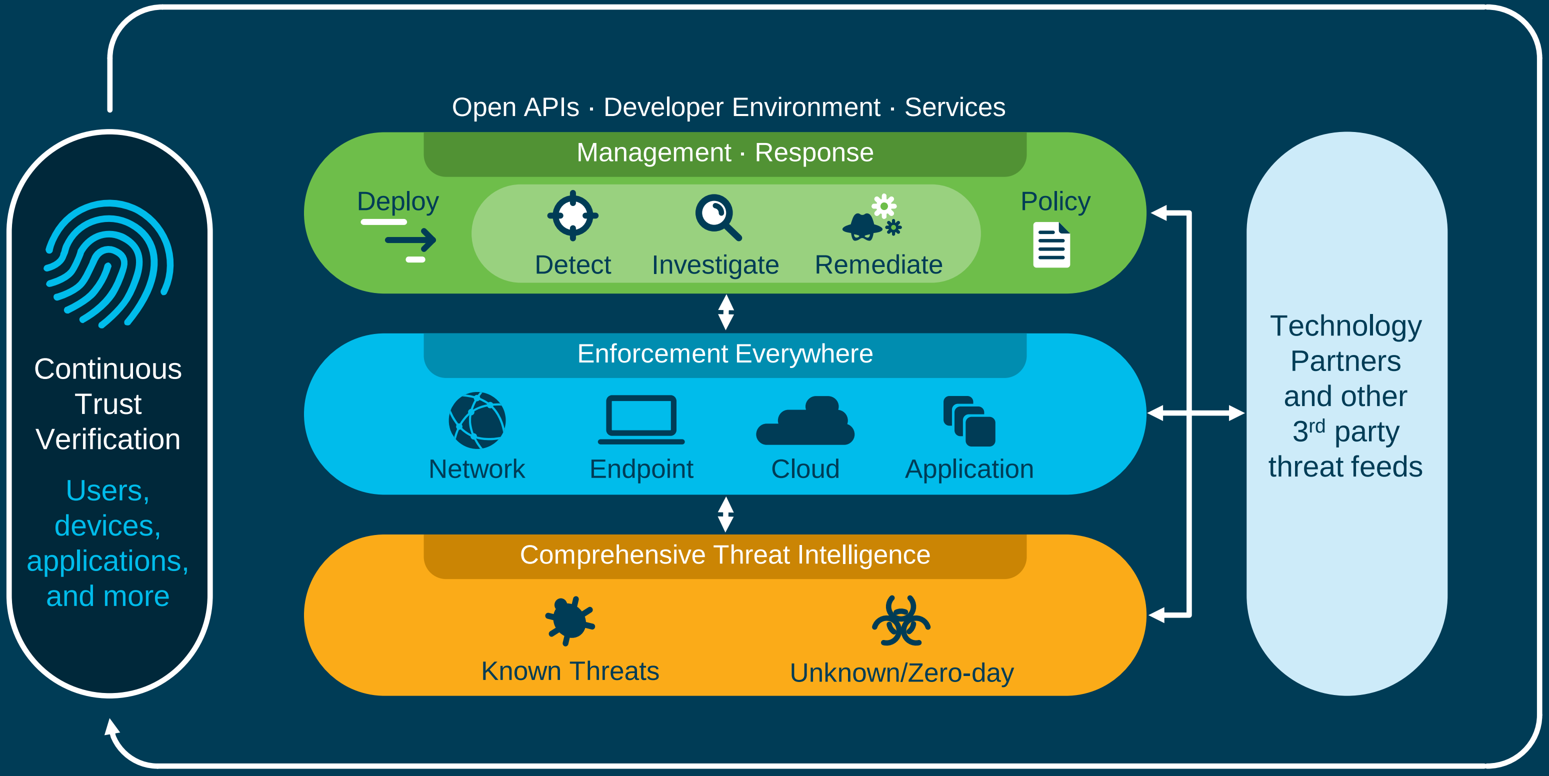
Compliance and audit

Ongoing monitoring and validation

Design, review, and policy management

Refine policy

# Modern Security Architecture



Open APIs · Developer Environment · Services

Management · Response

Deploy

Detect

Investigate

Remediate

Policy

Enforcement Everywhere

Network

Endpoint

Cloud

Application

Comprehensive Threat Intelligence

Known Threats

Unknown/Zero-day

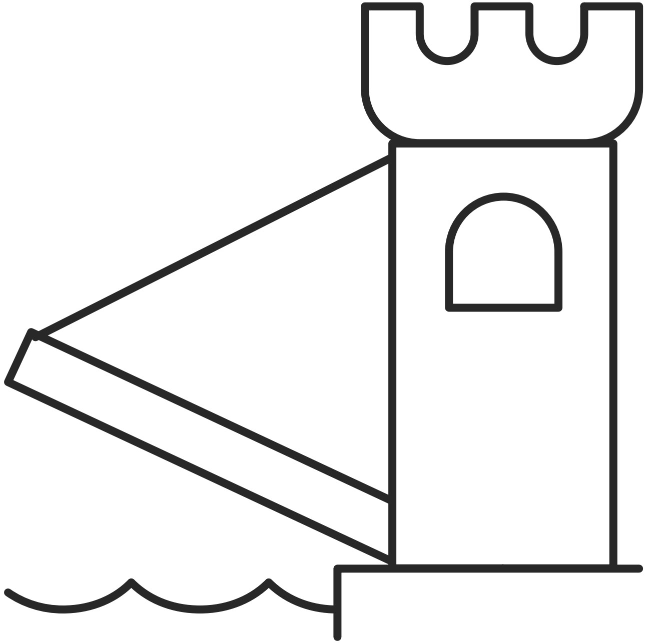
Continuous Trust Verification

Users, devices, applications, and more

Technology Partners and other 3rd party threat feeds

# ZERO Trust Model

# The traditional security model



Perimeter-based defense

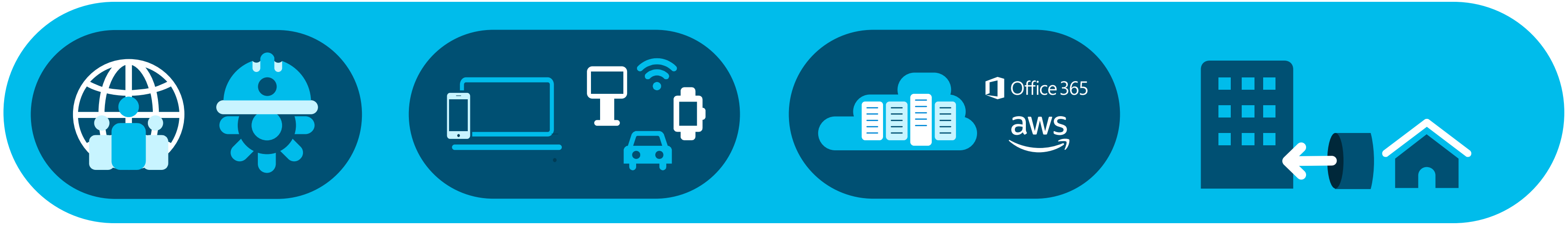
# **Zero Trust** changes the paradigm

What Zero Trust really means is "*Least-Privilege Access*"
(i.e. grant access, but make it specific!)

- ✓ Focuses on **data protection**, not on attacks
- ✓ Assumes **all environments are hostile** and breached
- ✓ **No access** until **user + device** is proven **"trusted"**
- ✓ Authorize and encrypt **all transactions and flows**

# Trusted Access

Using a phased Zero Trust approach to security



## Any User

- ✓ Employee
- ✓ Contractor
- ✓ Partner

## Any Device

- ✓ Corporate-Issued
- ✓ Bring-Your-Own
- ✓ IoT

## Any App

- ✓ Data Center
- ✓ Multi-Cloud
- ✓ SaaS

## In Any Location

- ✓ On-Premises
- ✓ On-VPN
- ✓ Off-Network

# Recommendations

Invest in upgrading OT networks

Get to know your OT network

Map out accountability

Acknowledge the lack of visibility

Segmentation IT and OT

Security is a continuous exercise

Education

Prepare & Response

# Have a plan

cisco