

Industrial Security

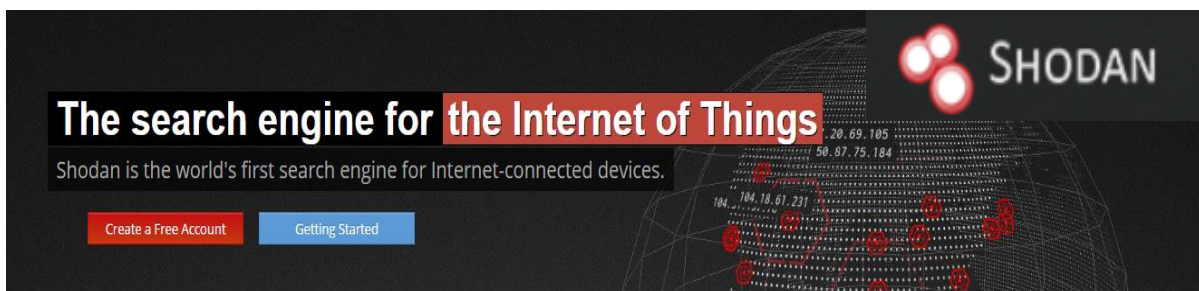
Protecting the productivity | V1

In un mondo sempre più interconnesso
i dispositivi di automazione datati non sono nati per Internet...

SIEMENS
Ingegno per la vita




... quelli recenti (PLC, HMI, SCADA ecc.) invece **SI'**



Shodan è un **motore di ricerca**, chiamato anche il motore di ricerca del mondo dell'**Internet delle cose**, capace di trovare, geolocalizzare e ritornare informazioni (indirizzo IP, **default password** ecc.) relative a qualsiasi dispositivo collegato ad Internet.

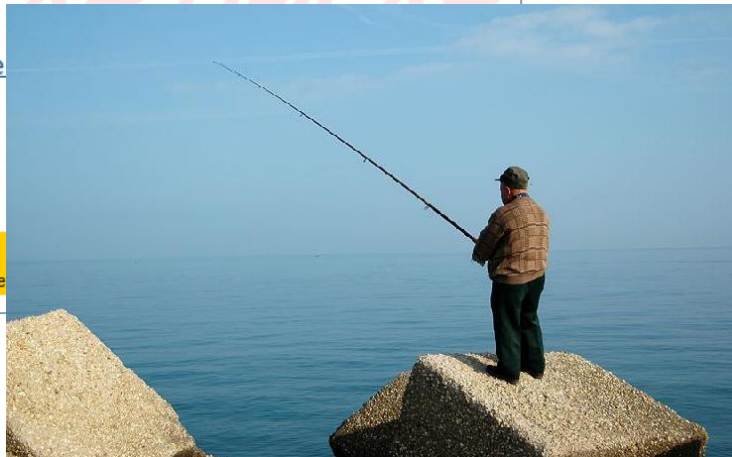
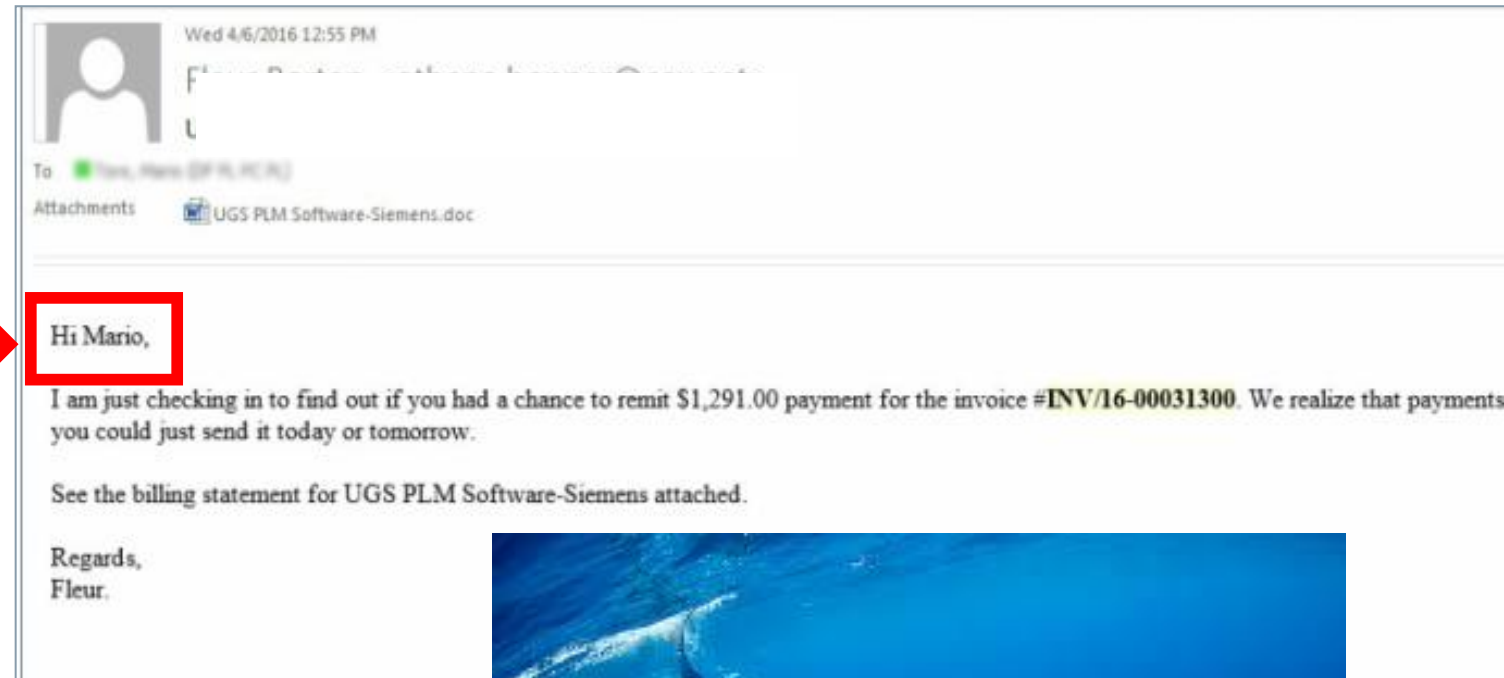
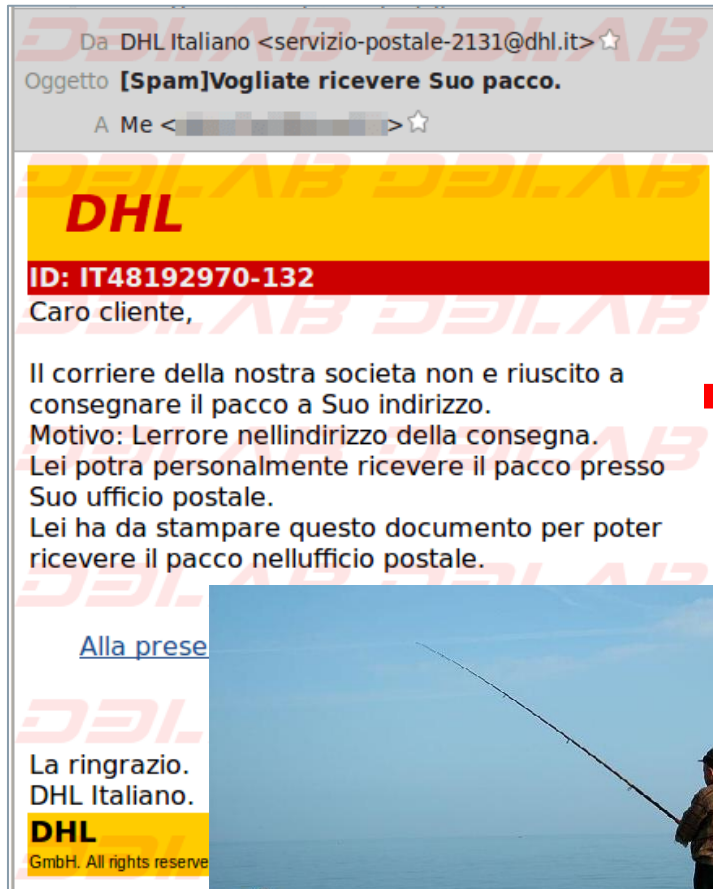
Quel che preoccupa è la **quantità di dispositivi** individuati esposti sul web **senza alcun livello di protezione**.

Overview of the top 10 threats 2019

- 
- » Introduzione di Malware tramite **chiavette USB** ed altri dispositivi rimovibili
 - » **Errore Umano** e Sabotaggio
 - » Ingegneria Sociale e **Phishing**
 - » Controllo dei dispositivi di automazione industriale connessi ad internet
 - » Guasti e Cause di Forza Maggiore
- Malware scaricati da Internet o intranet
 - Compromissione di Cloud o reti esterne
 - (Distributed) denial-of-service attacchi ((D)DOS)
 - Intrusione tramite accesso remoto
 - Compromissione di smartphone connessi alla rete di stabilimento

1) Bundesamt für Sicherheit in der Informationstechnik
Federal Office for Information Security
Source: BSI publication regarding cybersecurity 2019

Possibili minacce: Dal Phishing allo Spearphishing (ingegneria sociale)



Tipi di attaccanti e loro obiettivi



Attacchi non sofisticati
“Script Kid”



Attacchi sofisticati
“Hacker”



Spionaggio industriale
“Insider”



Gruppi organizzati
“Advanced Persistent Threats (APT)”

Attaccante tipico per impianti industriali

IT Security e Industrial Security: sfide simili, ecosistemi diversi



IT Security

Confidentiality

3-5 anni

Frequenti update/migrazioni forzate

Installati ed aggiornati centralmente

Bassa (~2 generazioni, Windows 7 e 10)

Gestiti centralmente (forced patching)



Ciclo di vita Hardware

Ciclo di vita Software

Antivirus & Internet Security

Eterogeneità sistemi operativi

Criteri di protezione

Industrial Security

Availability

20-40 anni

Fintanto che l'HW sarà manutenibile

Non previsti e/o non installabili

Alta (da Windows 95 a Windows 10)

Gestiti caso per caso, sulla base dei rischi

Difesa della Produzione



- Da attacchi **esterni**
- Da **errori/disattenzioni interne**
- Da **nuove minacce**

Valorizzazione degli Investimenti



- Per l'impiego di **Personale Qualificato**
- Per l'adozione di **Tecnologie di Security**
- **Benefici > Costi**

Conformità a Standard & Legislazione

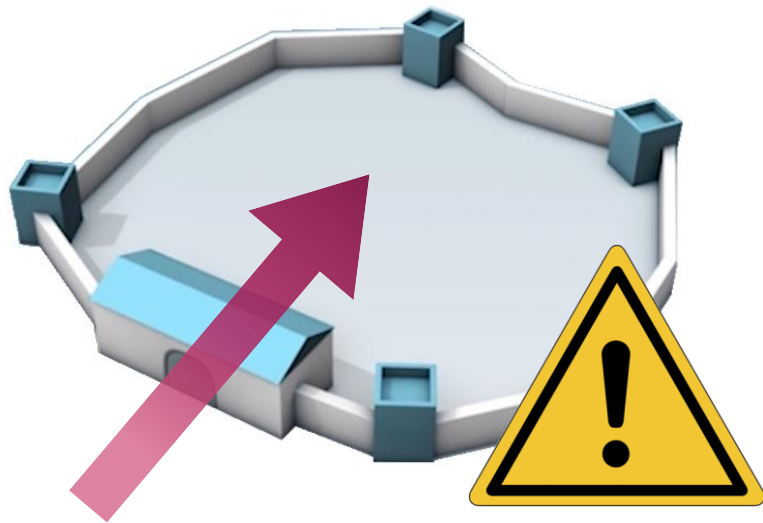


- Requisiti contrattuali Clienti
- **IEC 62443**
- Know-how della Security

Quale struttura difensiva va adottata?

IEC 62443

Singola Barriera



- Singolo livello di protezione
- Singolo punto di attacco
- Muro **“apparentemente”** impenetrabile

Defense In Depth

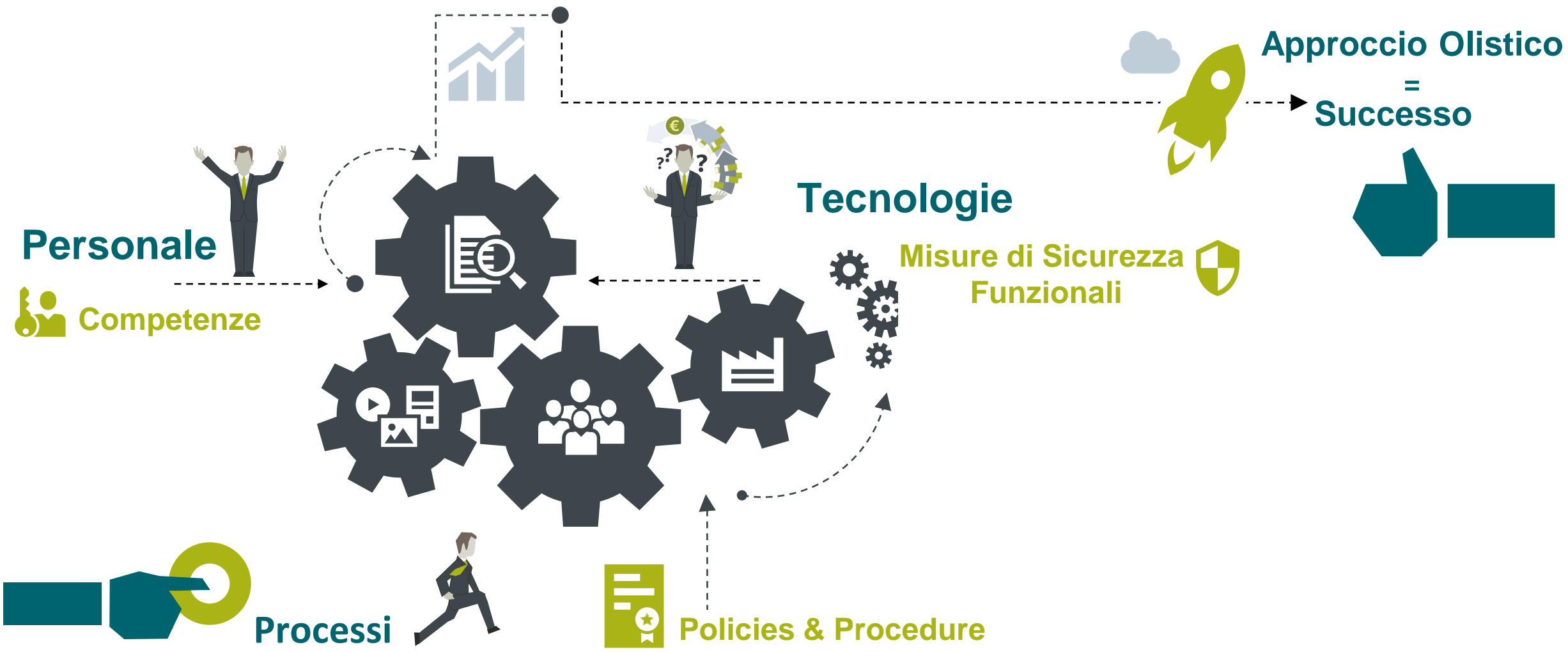


- **Protezione su più livelli**
- Ogni livello protegge i successivi
- Un attaccante deve **spendere tempo ed energie per ogni transizione**

Defence in depth nel tuo Business

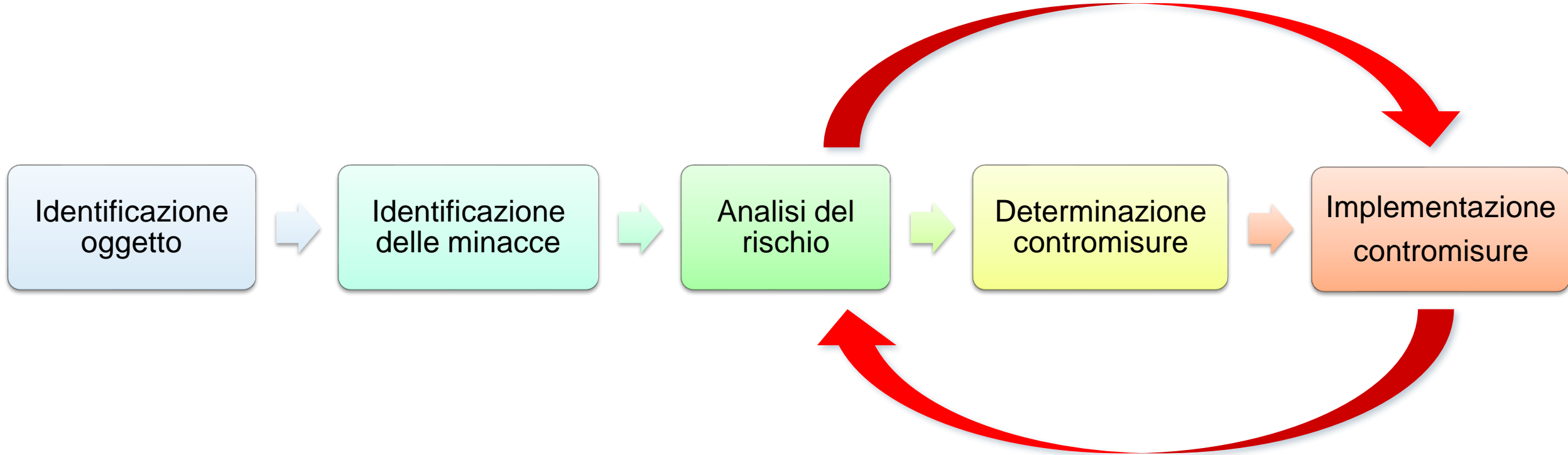
IEC 62443

SIEMENS
Ingegno per la vita



Una volta implementate le difese sono al sicuro? IEC 62443

Il processo parte dall'**identificazione** completa del sistema (**oggetto**) da proteggere e del caso applicativo in cui viene considerato.



Cyber Security è un **Processo Continuo**

Industrial Security

The Charter of Trust



Charter of Trust

SIEMENS

Ingegno per la vita

Alla Munich Security Conference del 2018, Siemens ed altri otto partners del comparto industriale hanno firmato la prima carta congiunta per la cybersecurity. Su iniziativa di Siemens, la Charter of Trust nasce per raccogliere regole e standards con l'obiettivo di promuovere la cybersecurity come fondamento del processo di digitalizzazione delle Aziende. La Charter of Trust conta attualmente 16 partecipanti: oltre a Siemens e Munich Security Conference hanno aderito anche AES, Airbus, Allianz, Atos, Cisco, Daimler, Dell Technologies, Deutsche Telekom, IBM, NXP, SGS, Total e TÜV Süd.

Charter of Trust

on Cybersecurity

charter-of-trust.com | [#Charter of Trust](https://twitter.com/CharterofTrust)

Unrestricted © Siemens 2020

Pagina 11

Industrial Security – Protecting the productivity | V1

Industrial Security

The Charter of Trust

Questi i motivi per cui abbiamo firmato la “Charter of Trust”: i nostri tre importanti obiettivi

1. Protezione dei dati di privati ed Aziende

2. Prevenzione dei danni a persone, Aziende ed infrastrutture

3. Creazione di una fondazione accreditata dove la fiducia in un mondo digitale ed interconnesso può svilupparsi e crescere

SIEMENS
Ingegno per la vita

enel

IBM

Munich Security
Conference **msc**
Münchner Sicherheitskonferenz

NXP

SIEMENS

AES

AIRBUS

Allianz 

Atos

CISCO

DAIMLER

DELL Technologies

SGS

T . .

TOTAL



Industrial Security

I 10 fondamenti della Charter of Trust

01 Ownership di cyber ed IT security

02 Responsabilità attraverso tutta la digital supply chain

03 Security by default

04 Centralità dell'utente

05 Innovazione e co-creazione



Charter of Trust

For a secure digital world

06 Cultura e formazione

07 Certificazione per infrastrutture critiche e soluzioni

08 Garanzia di trasparenza e risposte

09 Definizione di un quadro normativo

10 Nascita di iniziative comuni



Charter of Trust

Siemens Industrial Security Services: la homepage Italia

SIEMENS
Ingegno per la vita

SIEMENS

Prodotti e Servizi > Service > Industrial Security Services

Industrial Security Services

Sicurezza a tutto tondo

In un contesto dove l'esigenza di connessione sempre più estrema al web aumenta in modo esponenziale il rischio di essere oggetto di cyberattacco, l'Industrial Security non può che essere parte essenziale dell'intero processo di digitalizzazione di ogni azienda. I nostri esperti di servizi per la Industrial Security sono i partner sui quali potrai contare per farti accompagnare lungo l'intero cammino di trasformazione digitale a protezione dell'efficienza e disponibilità dei tuoi asset di produzione, perché digitalizzazione e cybersecurity vanno di pari passo.

I nostri esperti sono a tua disposizione

[> Contattaci](#)

<http://www.siemens.it/industrial-security-services>

Industrial Security

protecting the productivity

SIEMENS
Ingegno per la vita



Siemens Industrial Security Services

Siemens SpA, Digital Industries

Via Vipiteno 4
20128 Milano

e-mail: industrialsecurity.rc-it@siemens.com

Con riserva di modifiche e salvo errori. Il presente documento contiene solo descrizioni generali o informazioni su caratteristiche non sempre applicabili, nella forma descritta, al caso concreto o che possono cambiare a seguito di un ulteriore sviluppo dei prodotti. Le caratteristiche desiderate sono vincolanti solo se espressamente concordate all'atto di stipula del contratto.

Tutte le denominazioni dei prodotti possono essere marchi oppure denominazioni di prodotti della Siemens AG o di altre ditte fornitrici, il cui utilizzo da parte di terzi per propri scopi può violare il diritto dei proprietari.

<http://www.siemens.it/industrial-security-services>