CYBERSECURITY INDUSTRIALE COME «CICLO DI VITA»

Umberto Cattaneo
PMP, Sec+, ISA99/IEC62443 Specialist
SCHNEIDER ELECTRIC

Organizzato da

Agenda:

L’IEC 62443 come traccia di riferimento per gestire il ciclo di vita Cyber

Il modello proposto:

- Assessment
- Implementazione
- Manutenzione
- Operation
- Gli accessi remoti

FEDERAZIONE NAZIONALE IMPRESE ELETTROTECNICHE ED ELETTRONICHE

CONFINDUSTRIA

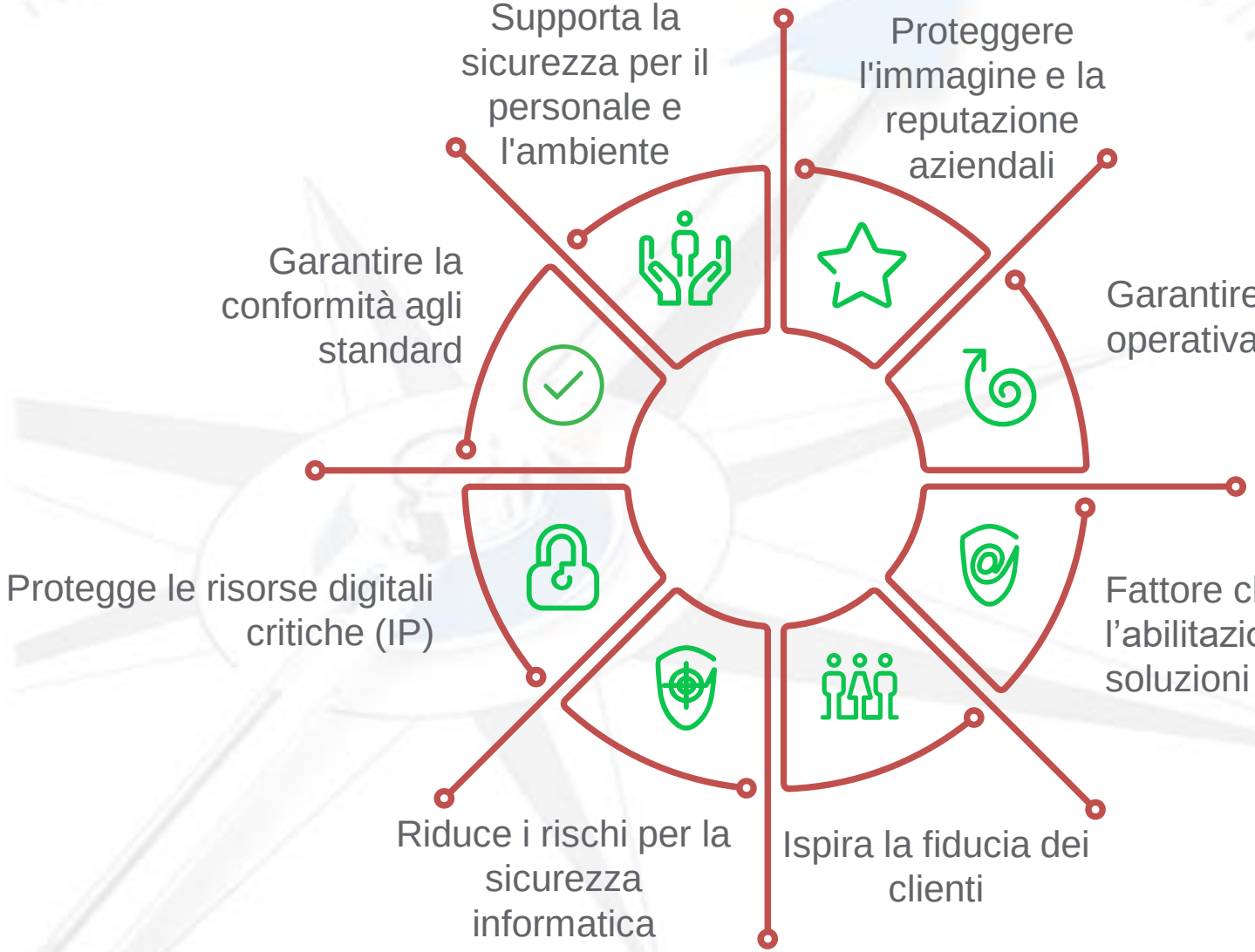
ANIE SERVIZI INTEGRATI

Top 10 Threats 2020* (before Covid-19 crisis)

Rank		Trend	2019
1	Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)	↑	2
2	Business interruption (incl. supply chain disruption)	↓	1
3	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	↑	4
4	Natural catastrophes (e.g. storm, flood, earthquake)1	↓	3
5	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	=	5
6	Fire, explosion	=	6
7	Climate change/increasing volatility of weather	↑	8
8	Loss of reputation or brand value	↑	9
9	New technologies (e.g. impact of artificial intelligence, autonomous vehicles, 3D printing, Internet of Things, nanotechnology, blockchain)	↓	7
10	Macroeconomic developments (e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)	↑	13

*Source: Allianz Risk barometer 2020

Proposta di valore della cybersecurity



Concetti chiave: Data Privacy e Cybersecurity

Che cos'è la data privacy?

•**Data privacy** si riferisce ai requisiti di protezione stabiliti per la manipolazione, la condivisione e la memorizzazione di informazioni personali (PII).

GDPR ISO 27001

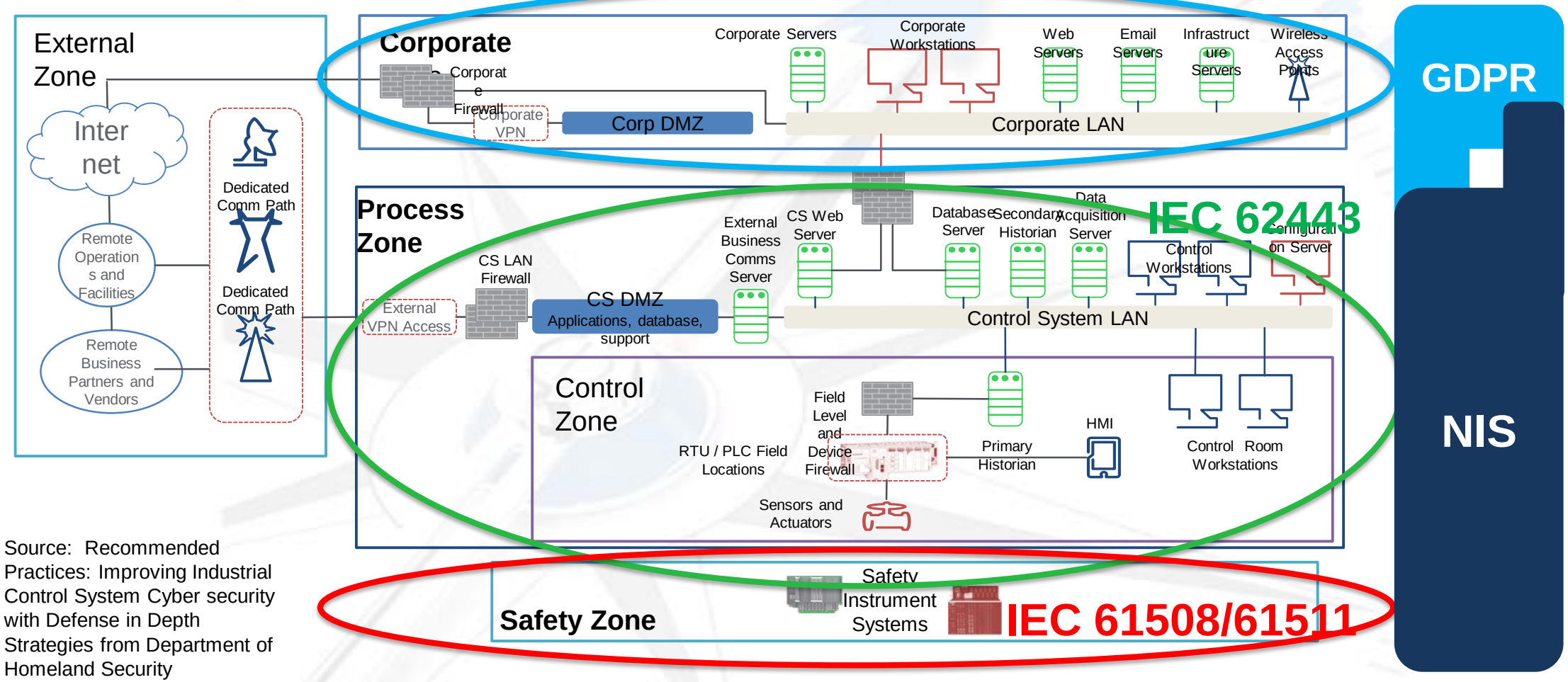
Che cos’è la cybersecurity?

Cybersecurity è l'arte di proteggere in modo sicuro reti, dispositivi, programmi e dati da accessi non autorizzati o uso criminale, garantendo al contempo la riservatezza, l'integrità e la disponibilità di informazioni.

NIS IEC62443, NIST, NERC

Standard aplicabili in IACS

ISO 27001



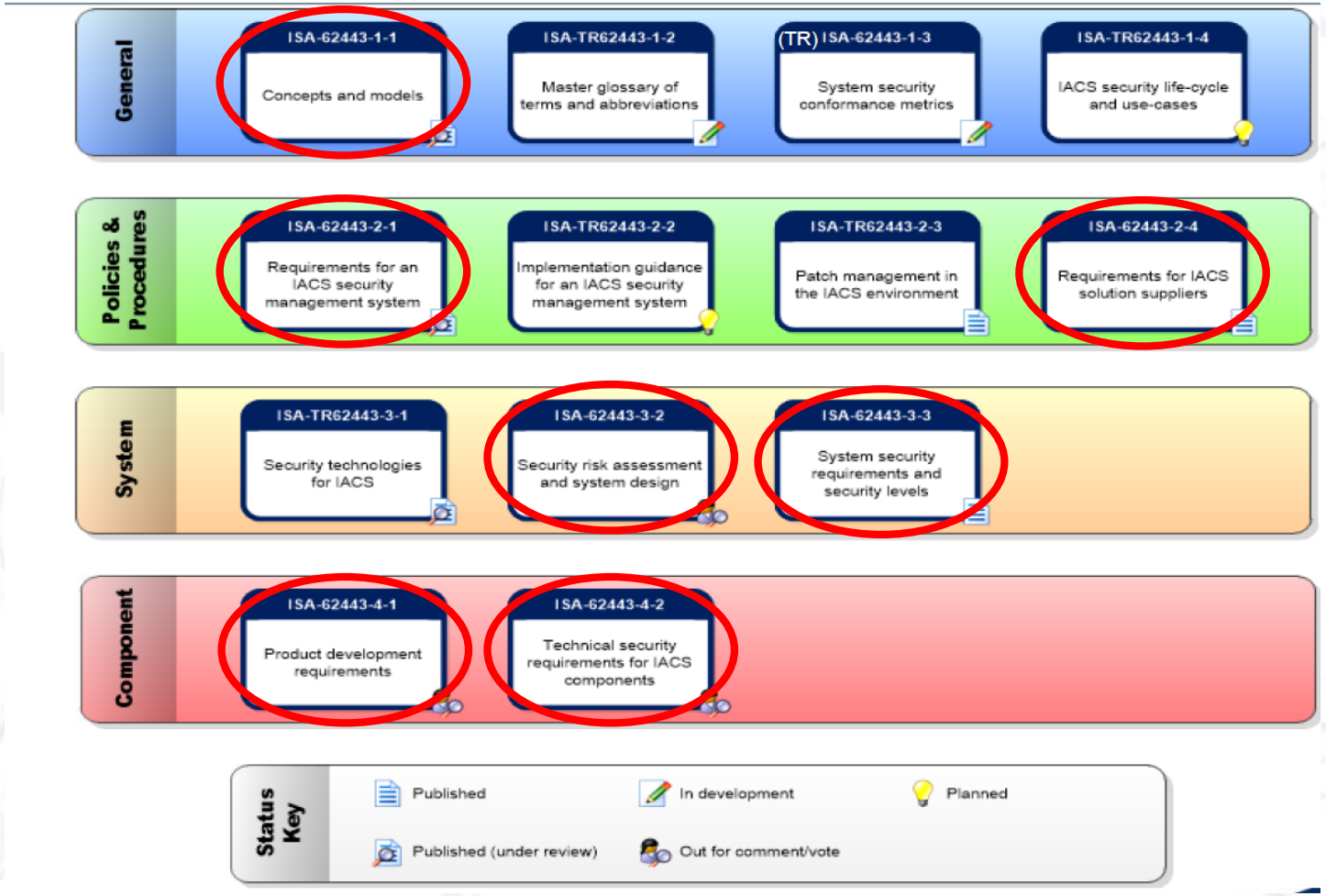
Source: Recommended Practices: Improving Industrial Control System Cyber security with Defense in Depth Strategies from Department of Homeland Security

EN ISA99/IEC62443: A systematic approach to cybersecurity

13 Publications:

7 Standard

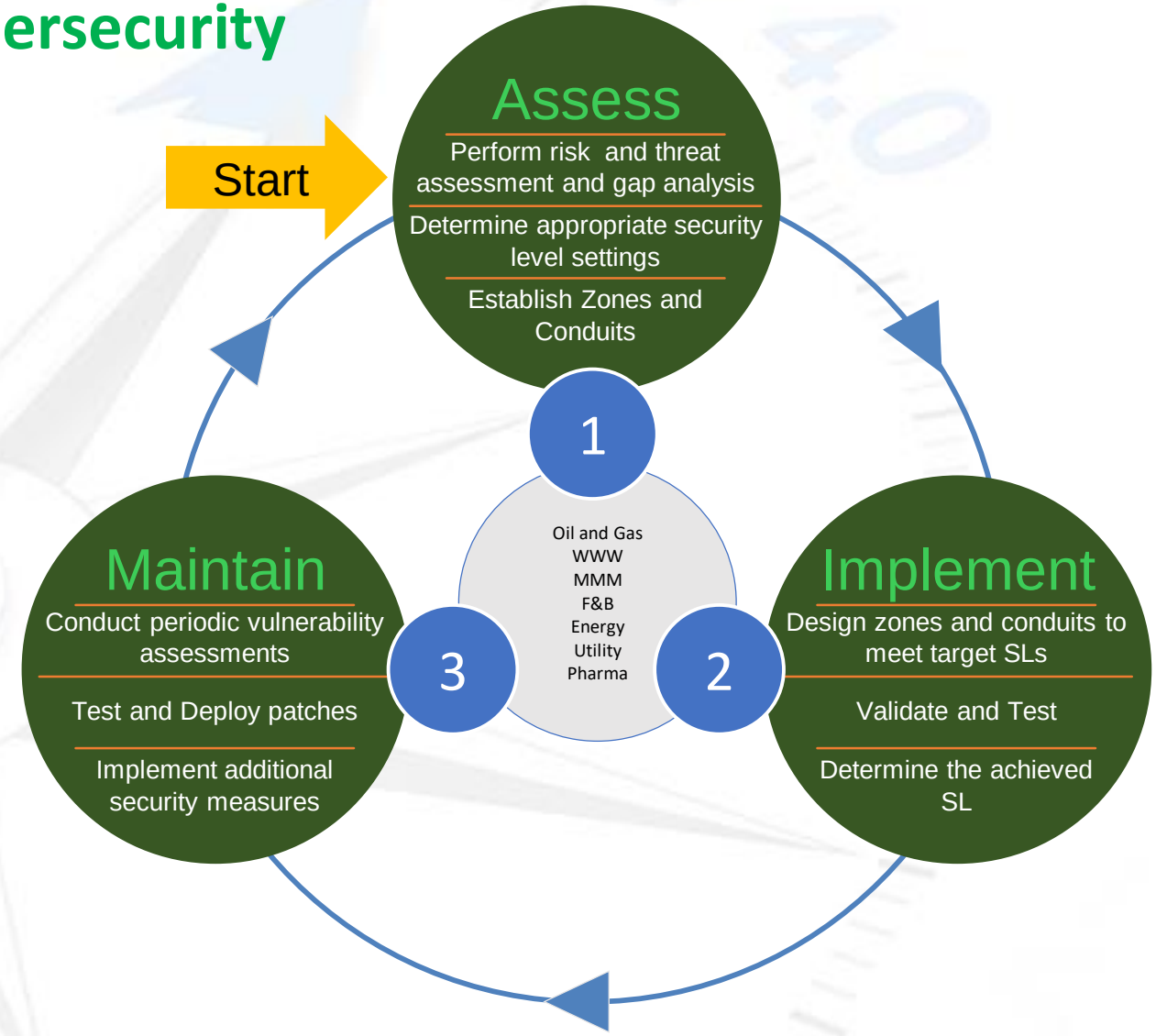
6 Technical Reports



Un approccio sistematico alla cibersecurity

Adattato da IEC62443-1-1

La cybersecurity è un ciclo di vita non un percorso da "A a B”




Assess
I rischi e le
minacce

Cyber Security Risk Assessment

Risk Analysis

1. Definire la metodologia del rischio

2. Identificare gli elementi principali

3. Identificare e valutare le minacce, l'impatto e la probabilità

Prima di proteggere l'ICS dobbiamo sapere con cosa abbiamo a che fare

Risk Reduction

4. Ridurre i rischi progettando adeguate contromisure

5. Documentare i risultati nel registro dei rischi

Sviluppare un piano per affrontare i rischi inaccettabili

Ogni valutazione deve essere specifica per sito

Processo per il Cybersecurity Risk assessment

START

Identificare i sistemi da considerare (SuC)

Condurre un Cybersecurity Risk Assessment di alto livello

Suddividere il SuC in Zone e conduits

Condurre un Cybersecurity Risk Assessment di dettaglio

Documentare i requisiti di sicurezza, le ipotesi e i vincoli

Conoscere il rischio

Risk assessment di alto livello

- Identificare gli assets critici
- Determinare le Minacce reali
- Identificare le Vulnerabilità esistenti
- Capire le Conseguenze di una compromissione
- Valutare l'efficacia della contromisure esistenti

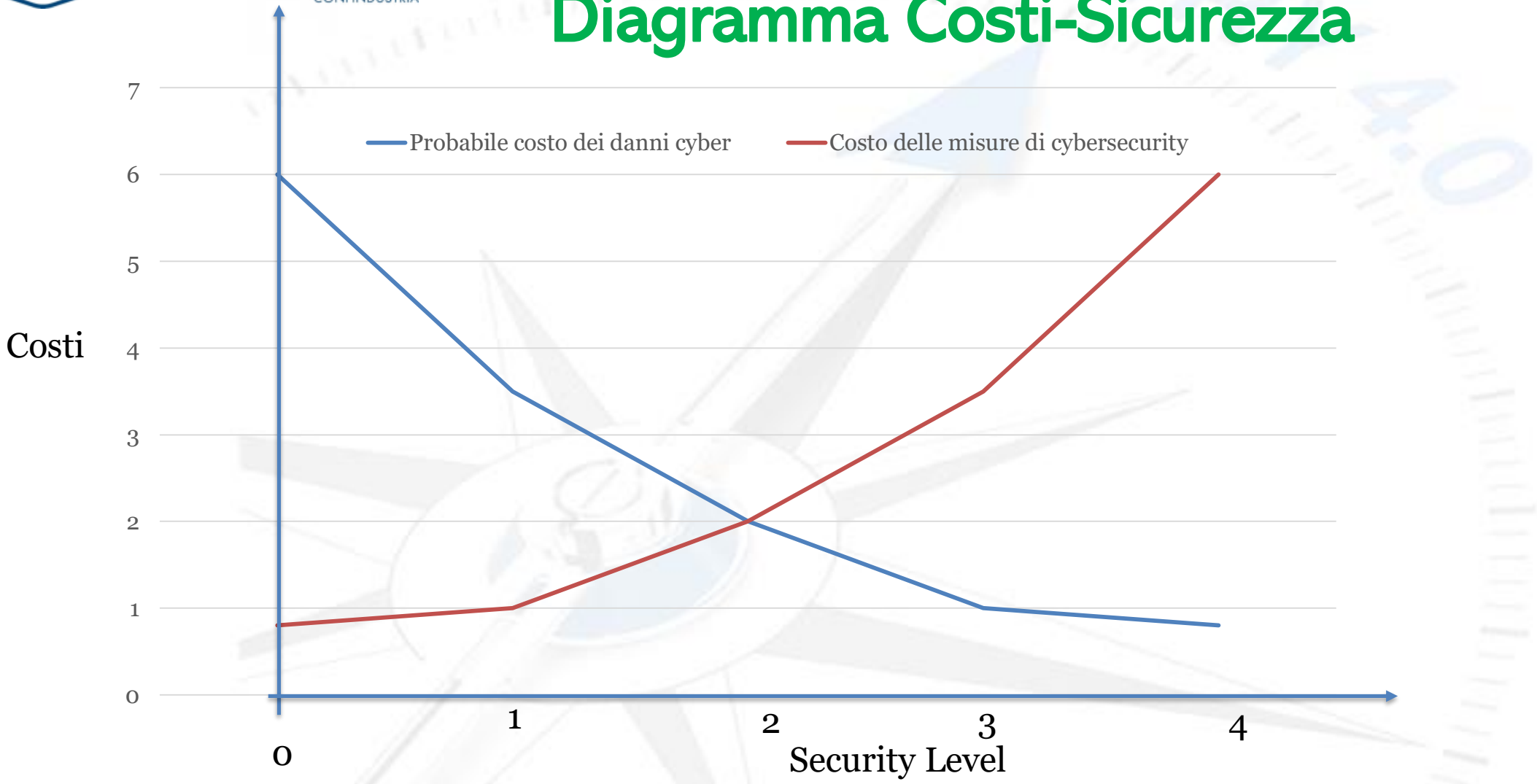
Individuare e definire le politiche di gestione dei rischi:
evitare, mitigare, trasferire, accettare

Gestione dei Rischi non accettabili

Sviluppare un piano per gestire i rischi non accettabili

- Valutare le contromisure esistenti
- Individuare ulteriori contromisure
- Individuare cambiamenti a policy&procedures
- Prioritizzare gli upgrade (sulla base dei sui rischi individuati)
- Valutare i costi e le complessità vs efficacia

Diagramma Costi-Sicurezza



Come gestire un Assessment

Analisi del rischio di dettaglio

Sviluppare un piano per gestire i rischi non accettabili

- Valutare le contromisure esistenti
- Individuare ulteriori contromisure
- Individuare cambiamenti a policy&procedures
- Prioritizzare gli upgrade (sulla base dei sui rischi individuati)
- Valutare i costi e le complessità vs efficacia

Zones and Conduits - Esempio

Food and Beverage

Zones applied as result of risk and threat assessment

Quali sono i differenti tipi di Vulnerability Assessment?

Tipi di Vulnerability Assessment

Assessment di “alto livello” (GAP Analysis)

Assessment di tipo “ATTIVO”

Assessment di tipo “PASSIVO”

Penetration Test

Quali sono le differenze tra Assessment Passivi ed Attivi?

Assessment passivi:

I devices e hosts di rete OT vengono individuati e descritti utilizzando Sistemi di lettura e mappatura del traffico, in grado di rilevare i devices e le eventuali vulnerabilità, senza interferire con il traffico di rete. L'assessment si completa con la raccolta documentale

Assessment attivi:

vengono utilizzati tools di scanning, introducendo traffico sulla rete per interrogare i devices e ricavare la mappa della rete, dei suoi componenenti ed eventuali vulnerabilità.

Quali le differenze tra Vulnerability Assessment e Penetration test?

Vulnerability assessment

- Definiscono, identificano e classificano le vulnerabilità
- Identificano punti di debolezza
- Producono un report su quanto scoperto

Penetration Test

- Sfruttano le vulnerabilità
- Tentano di ottenere l'accesso(non autorizzato) a reti e sistemi
- Usano tools aggressivi e tecniche di attacco per penetrare nel Sistema.

Tecniche passive piu' usate

Packet capturing:

Identifica chi parla con chi

Identifica I protocolli nella rete

Intercetta traffico inatteso o non previsto

Riconosce messaggi con "payload" in chiaro

Consente di definire una "baseline" di traffico lecito

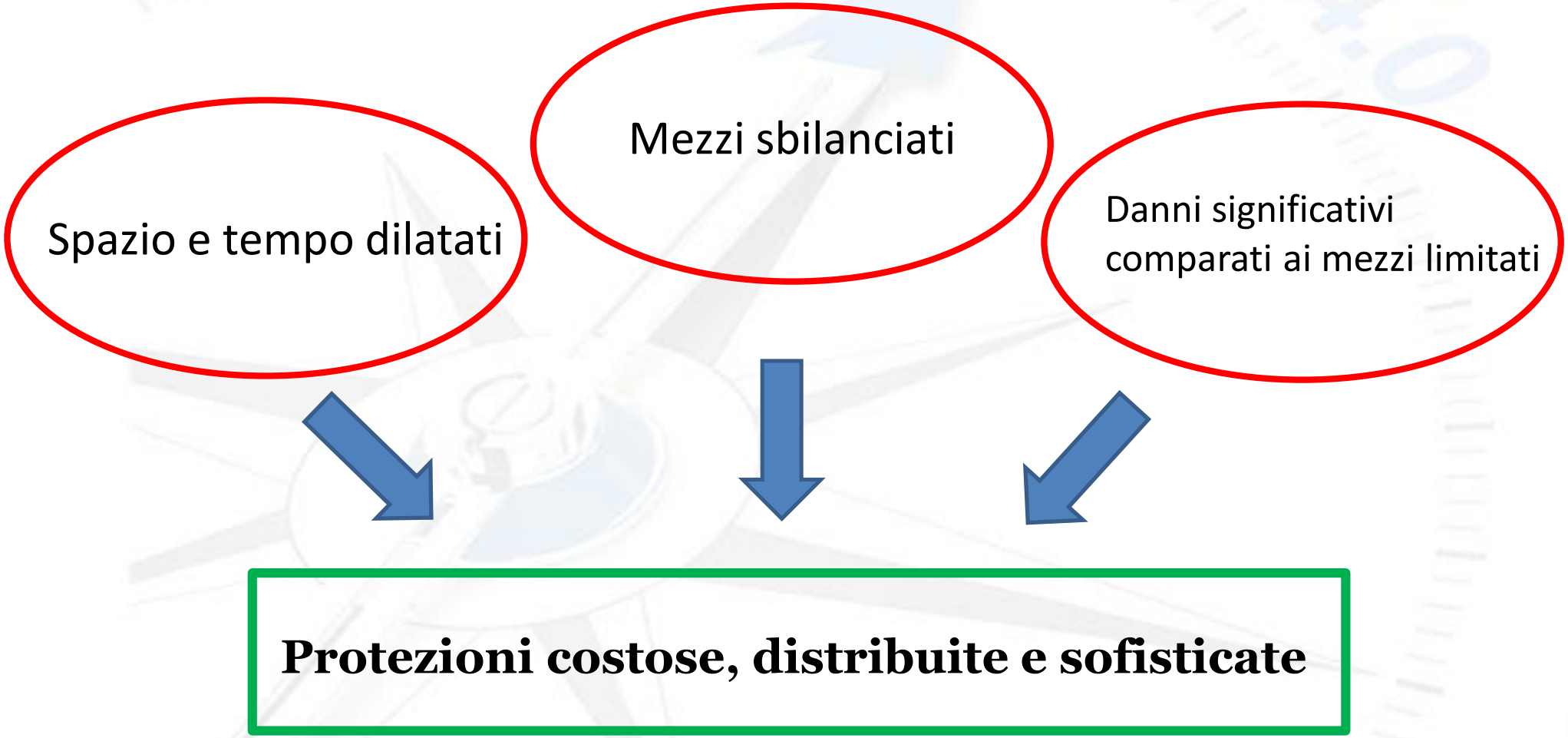
Documentare Requisiti, Assumptions e Vincoli

Deve essere creato un documento CRS (Cybersecurity Requirements Specification) per documentare i requisiti generali di sicurezza.

Un CRS deve includere:

- Descrizione dei SuC
- Vincoli per l'ambiente operativo oltre a criteri e standard aziendali
- Minacce individuate
- Requisiti di sicurezza obbligatori
- Rischio tollerabile e
- Requisiti normativi

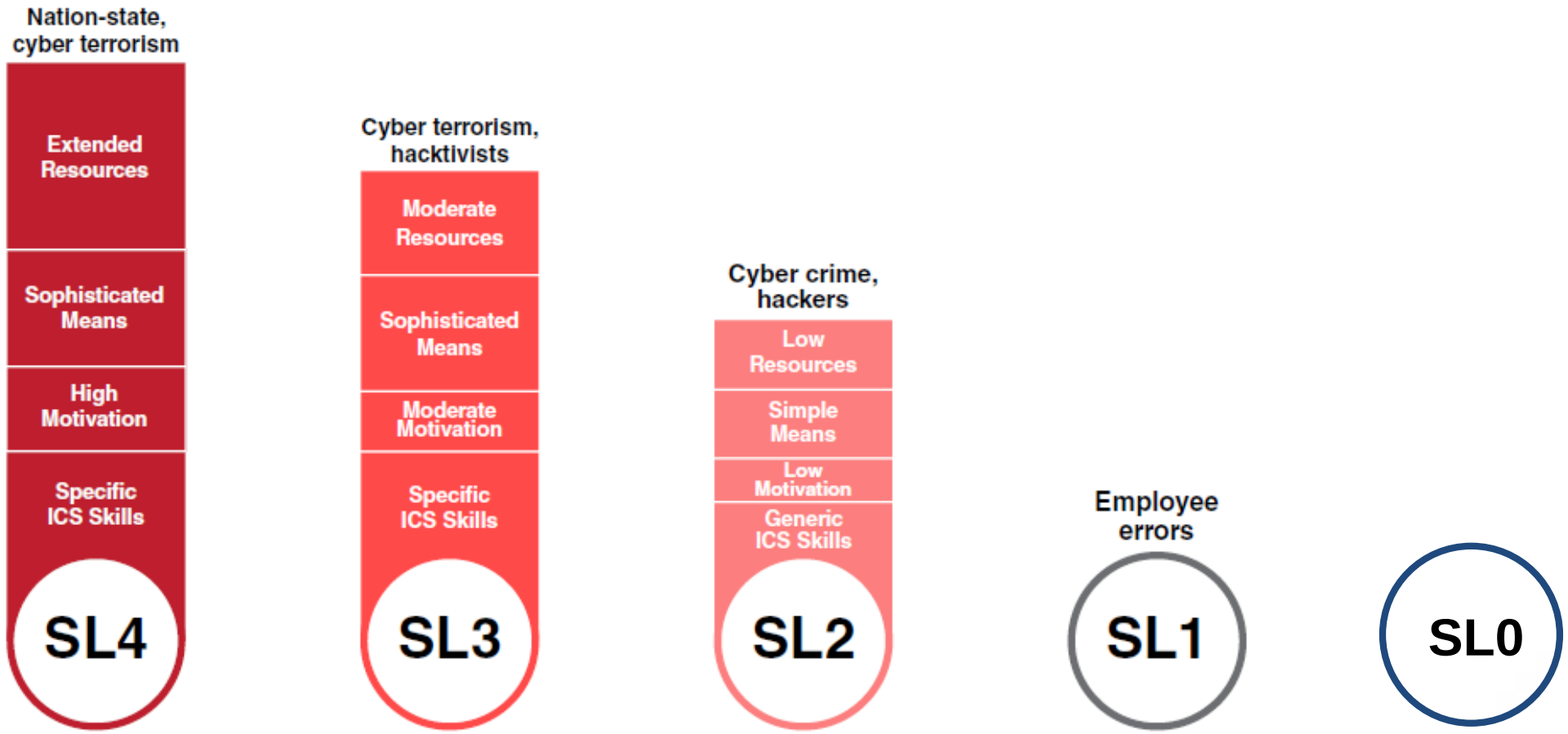
Attacchi Cyber sono basati sui principi di “Guerra asimmetrica”



Chi sono le minacce?

THREATS	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
						
MOTIVATION	Hactivists usano computer e reti per promuovere le loro idee politiche e sociali	Individui e sofisticate organizzazioni criminali rubano informazioni personali e fannno estorsioni per soldi.	Insiders rubano informazioni e per ragioni personali, finanziarie ed ideologiche.	Organizzazioni nemiche conducono intrusioni informatiche per rubare segreti di stato e informazioni proprietarie da società private	Gruppi terroristici sabotano i sistemi informatici che gestiscono le nostre infrastrutture critiche come la rete elettrica.	Organizzazioni nemiche sabotano i sistemi di infrastrutture militari e critici per ottenere un vantaggio in caso di conflitto.

IEC 62443.3.3 Security Level (SL)



Foundational Requirements

ISA99/IEC62443 3-3 Security Levels (SL)

SL-T Target - desiderato

SL-A Achieved - esistente

SL-C Capability - componenti

IAC: Identification and Authentication Control (**13** sys. requirements)

UC: Use Control (**12** system requirements)

DI: Data Integrity (**9** system requirements)

DC: Data Confidentiality (**3** system requirements)

RDF: Restrict Data Flow (**2** system requirements)

TRE: Timely Response to Event (**2** system requirements)

RA: Resource availability (**8** system requirements)

49 SR

Soluzioni Cybersecurity – Level 3 (SL-3)

Identify

- Authentication, Authorization, Accounting
- Multi-Factor Authentication
- Network Segmentation
- Secure Remote Access
- Physical Security

Protect

- Endpoint protection anti-virus, anti-malware,
- DLP, HIPS, whitelisting
- Central Device Control
- CPU/PID Protection
- Patch Management

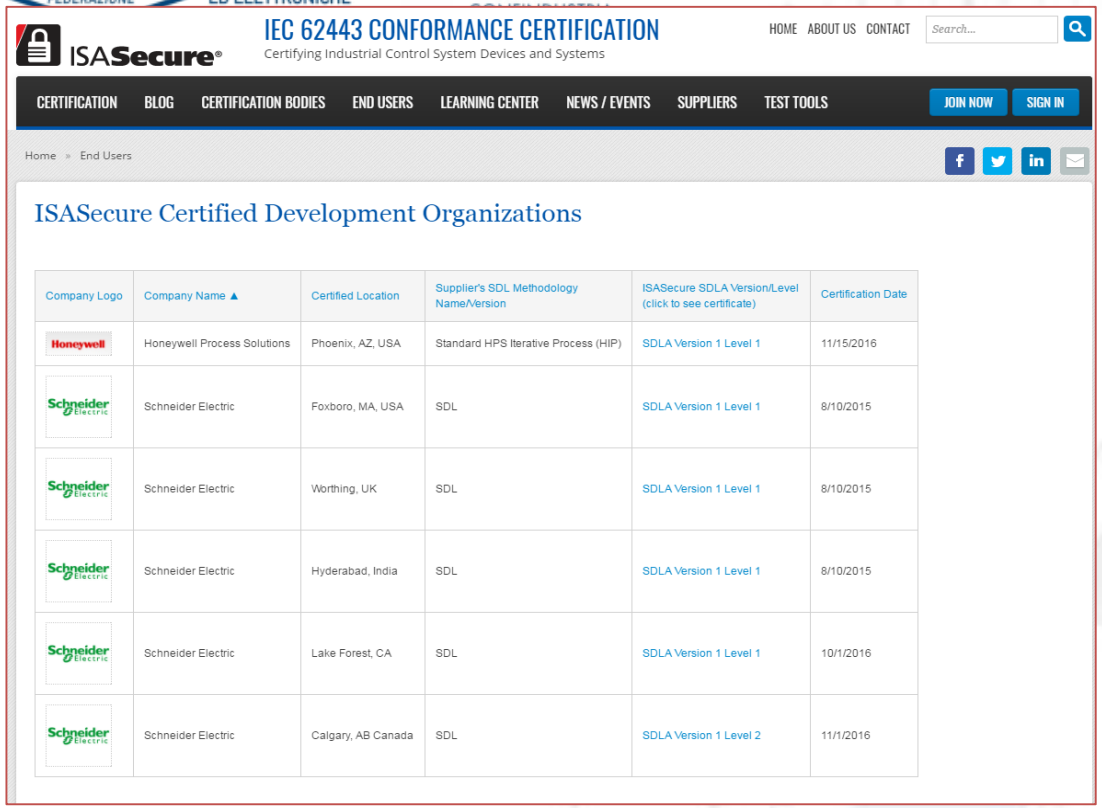
Detect

- Security Information & Event Management (SIEM)
- Network performance monitoring
- Anomaly Detection
- Intrusion Detection (NIPS)
- SOC / NOC

Respond

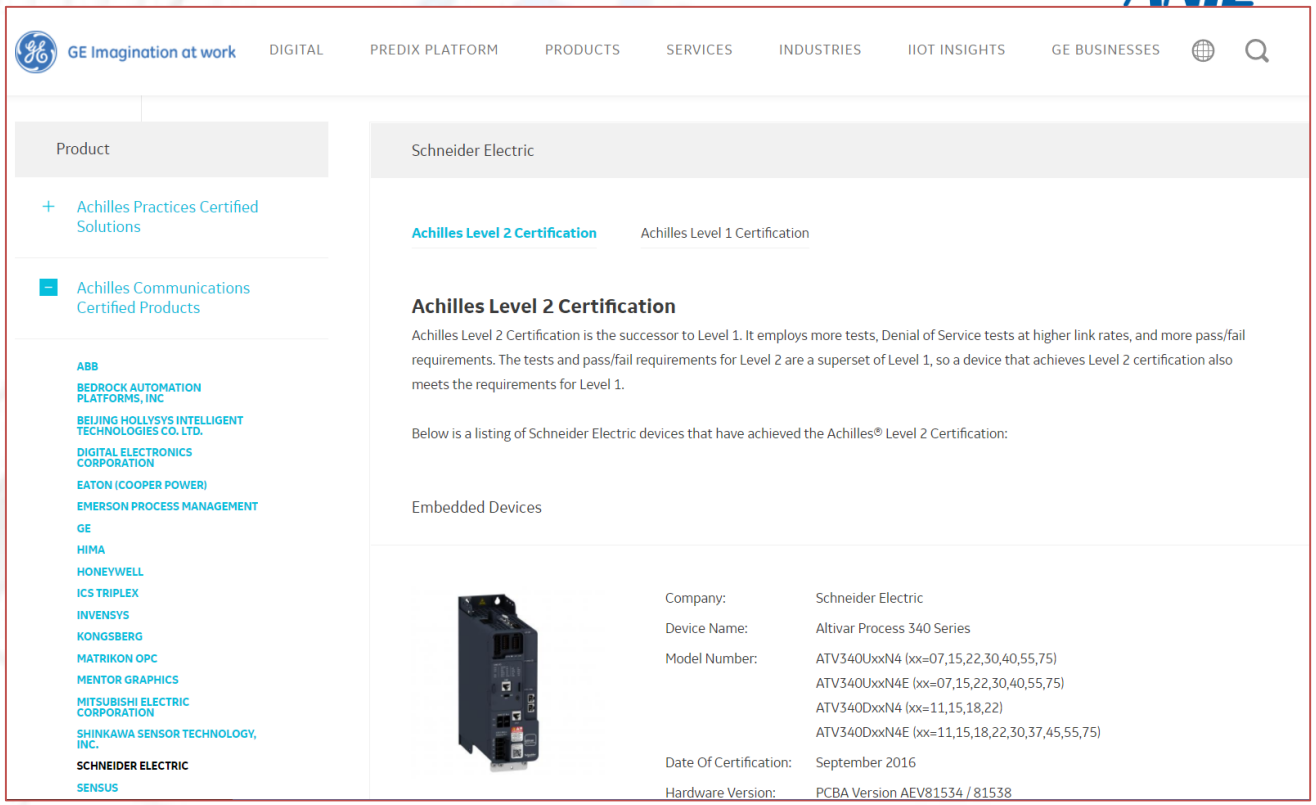
- Backup / Disaster Recovery

Componenti certificati EDSA / SDLA



Company Logo	Company Name ▲	Certified Location	Supplier's SDL Methodology Name/Version	ISASecure SDLA Version/Level (click to see certificate)	Certification Date
Honeywell	Honeywell Process Solutions	Phoenix, AZ, USA	Standard HPS Iterative Process (HIP)	SDLA Version 1 Level 1	11/15/2016
Schneider Electric	Schneider Electric	Foxboro, MA, USA	SDL	SDLA Version 1 Level 1	8/10/2015
Schneider Electric	Schneider Electric	Worthing, UK	SDL	SDLA Version 1 Level 1	8/10/2015
Schneider Electric	Schneider Electric	Hyderabad, India	SDL	SDLA Version 1 Level 1	8/10/2015
Schneider Electric	Schneider Electric	Lake Forest, CA	SDL	SDLA Version 1 Level 1	10/1/2016
Schneider Electric	Schneider Electric	Calgary, AB Canada	SDL	SDLA Version 1 Level 2	11/1/2016

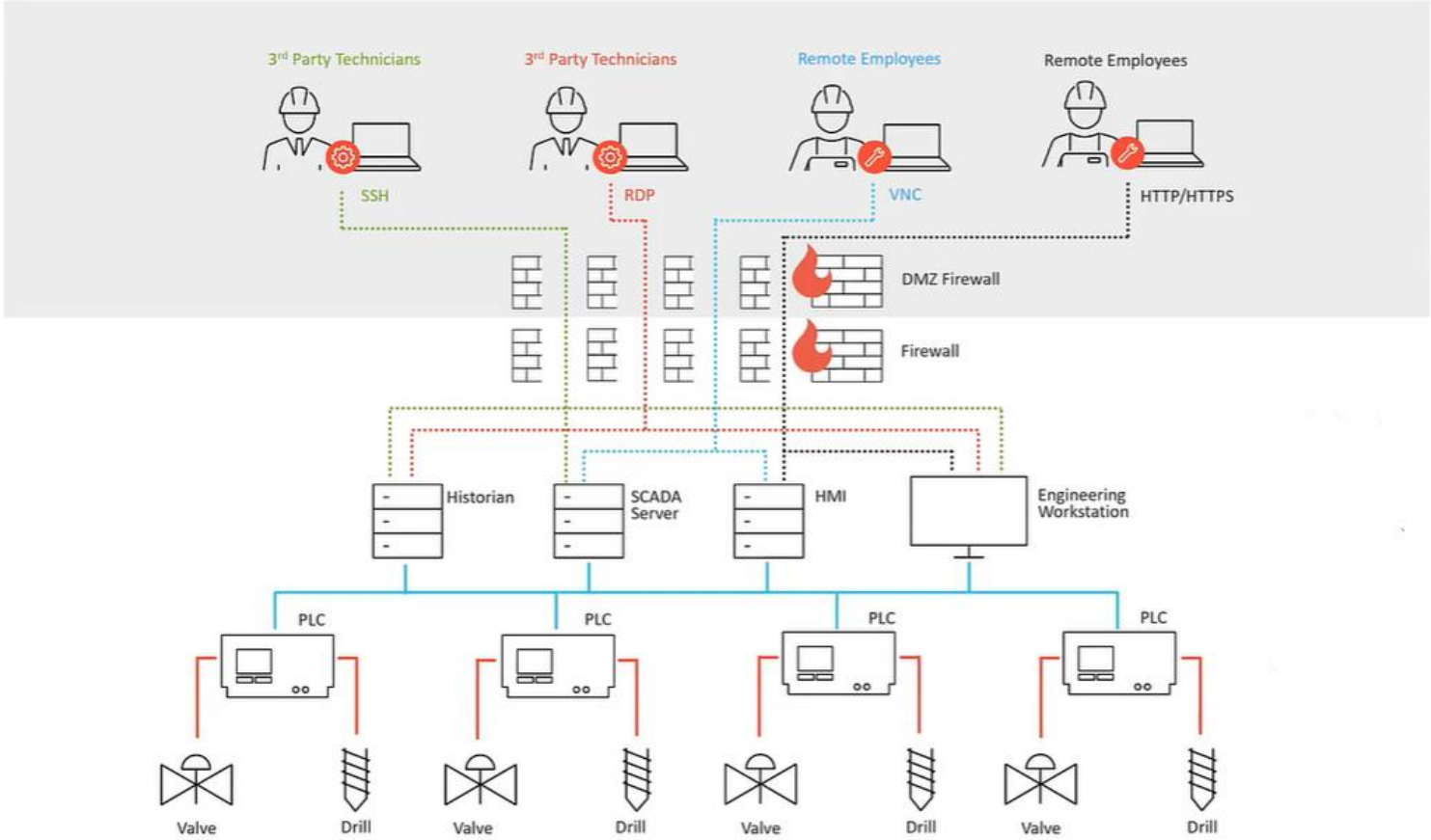
http://isasecure.org/en-US/End-Users/ISASecure-Certified-Development-Organizations



https://www.ge.com/digital/services/certifications/achilles-communications-certified-products/schneider-electric-certified-products

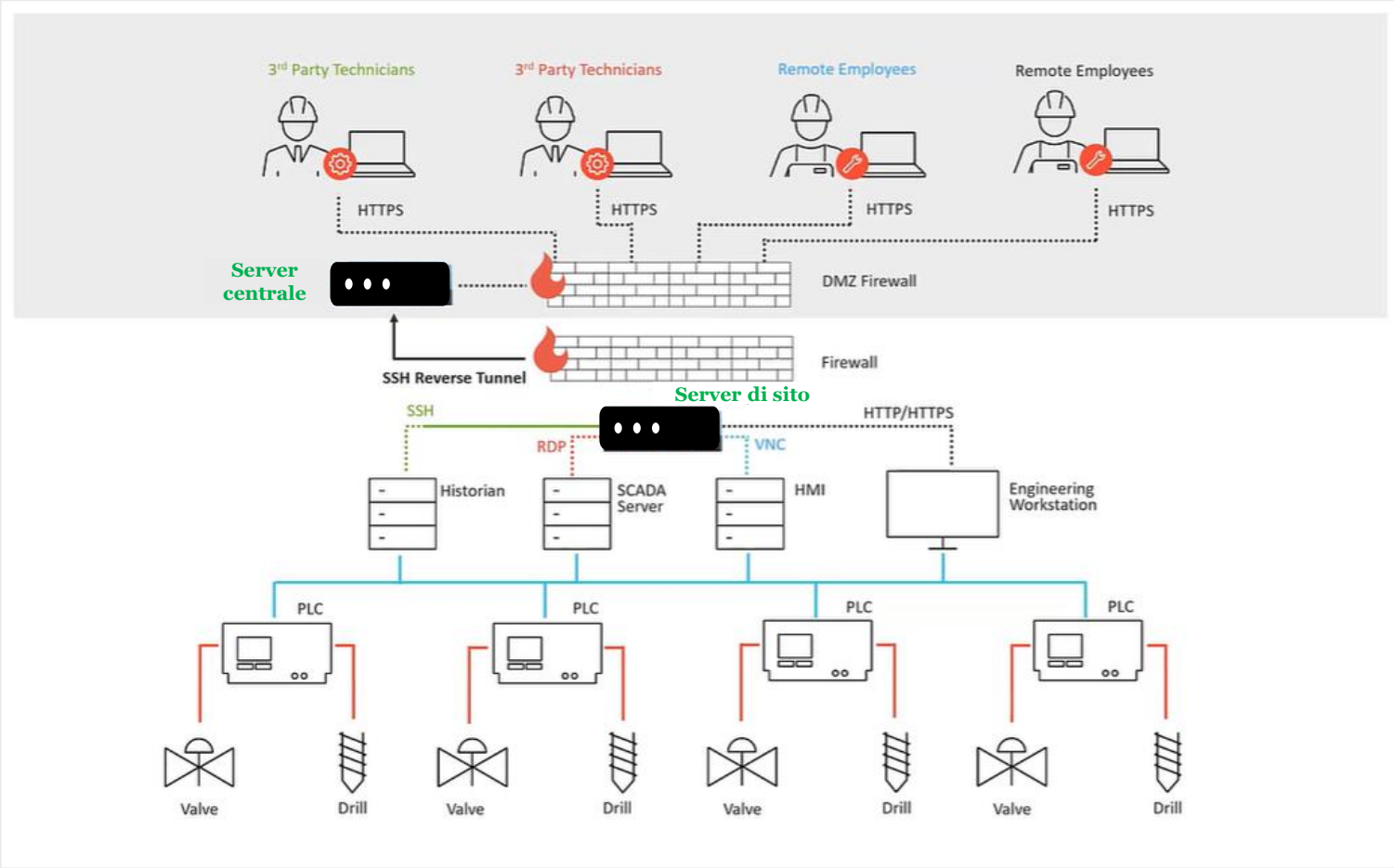
Use the certifying bodies website over vendor material

Gestire gli accessi remoti



Situazione piu' diffusa

Gestire gli accessi remoti



Funzioni base

Control

- Rule based access control (IAC)
- Vault Passwords (DC)
- Manually approve remote connections (UC)
- Segregated and securest access control (RDF)

Monitor

- Session recording (UC)
- ”Red Button” for immediate session termination (UC)

Audit

- Integrated audio/video recording (UC)

Situazione in sicurezza


Mantenere
I più alti livelli di
protezione cyber

MANUTENZIONE: non risparmiare

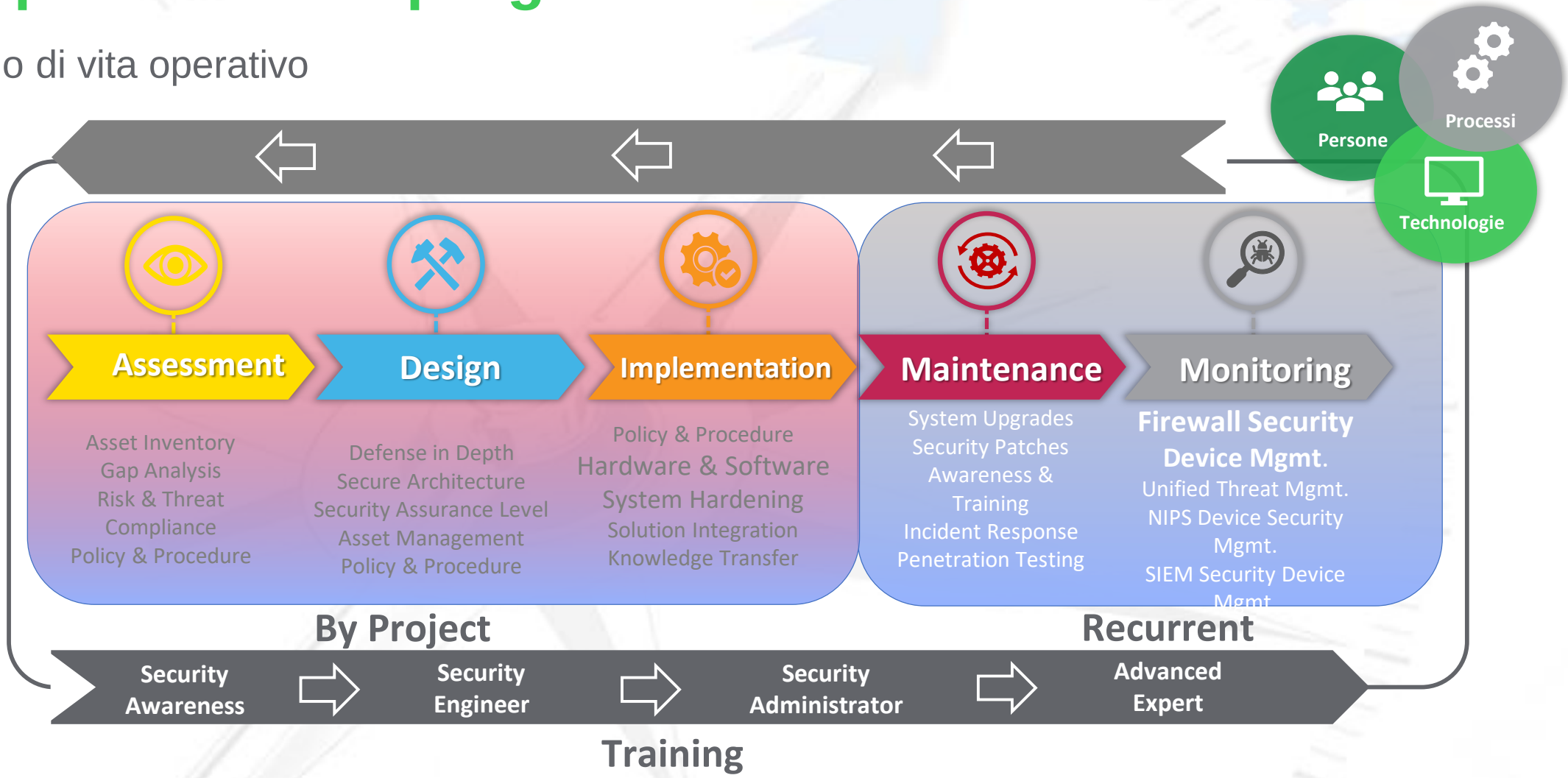
Gold

Silver

Bronze

Approccio a un progetto di sicurezza informatica

Ciclo di vita operativo



GRAZIE PER L'ATTENZIONE

Umberto Cattaneo
PMP, Sec+, ISA99/IEC62443 Specialist

Umberto.Cattaneo@se.com

Mobile:+39 3355821626