OT CYBER DEFENSE

La cybersecurity a protezione dell'Industria 4.0: cosa mettere in sicurezza e come farlo

Giorgio Campiotti
Senior Security Engineer - Director Of Services
giorgio.campiotti@securenetwork.it

19/01/2023

SECURE NETWORK

BV TECH Group
Securing the Future.

2004

Fondazione come start-up del Politecnico di Milano, con cui collaboriamo strettamente ancora oggi

Oltre 350

Partecipazioni a conferenze di stampo tecnico

250+

Clienti in Europa, Stati Uniti e Medio Oriente, per cui abbiamo operato nel campo dell'offensive security

2018

Fusione con il gruppo BVTech, nato nel 2005, ad oggi uno dei principali attori del mercato dell'Information & Communication Technology, con circa 1400 dipendenti e 100mln di fatturato

20+ Security Engineer

Il nostro Red team è composto da più di 20 ingegneri, specializzati in Cyber Security, con esperienza pluriennale nel settore e sempre all'avanguardia grazie alla stretta collaborazione con il Politecnico di Milano

CONFINDUSTRIA VICENZA

securenetwork
Your Protection, Our Mission

CHI SONO

BV TECH Group
Securing the Future.

Giorgio Campiotti

Senior Security Engineer and Director of Service @ Secure Network

Specializzato nello sviluppo di piattaforme e sistemi integrati OT e IOT, ha avuto numerose esperienze professionali nel settore di progettazione elettronica industriale, networking, system integration e system administration. Svolge principalmente attività di fractional CISO, analista di cybersecurity e penetration test per analisi approfondita di sistemi hardware e OT anche nell'ambito di Industria 4.0.

I suoi interessi riguardano dispostivi OT e IOT, sistemi embedded, dispositivi RF anche per attività SIGINT e microcontrollori.

Certified Information Security Manager (**CISM**)

OSSTMM Wireless Security Expert (**OWSE**)

GIAC Penetration Tester (**GPEN**)

Certified Ethical Hacker (**CEH**)

PRINCE2 Foundation Project Management (**CPD**)

Sans Institute **Industrial Control System Security** for Managers

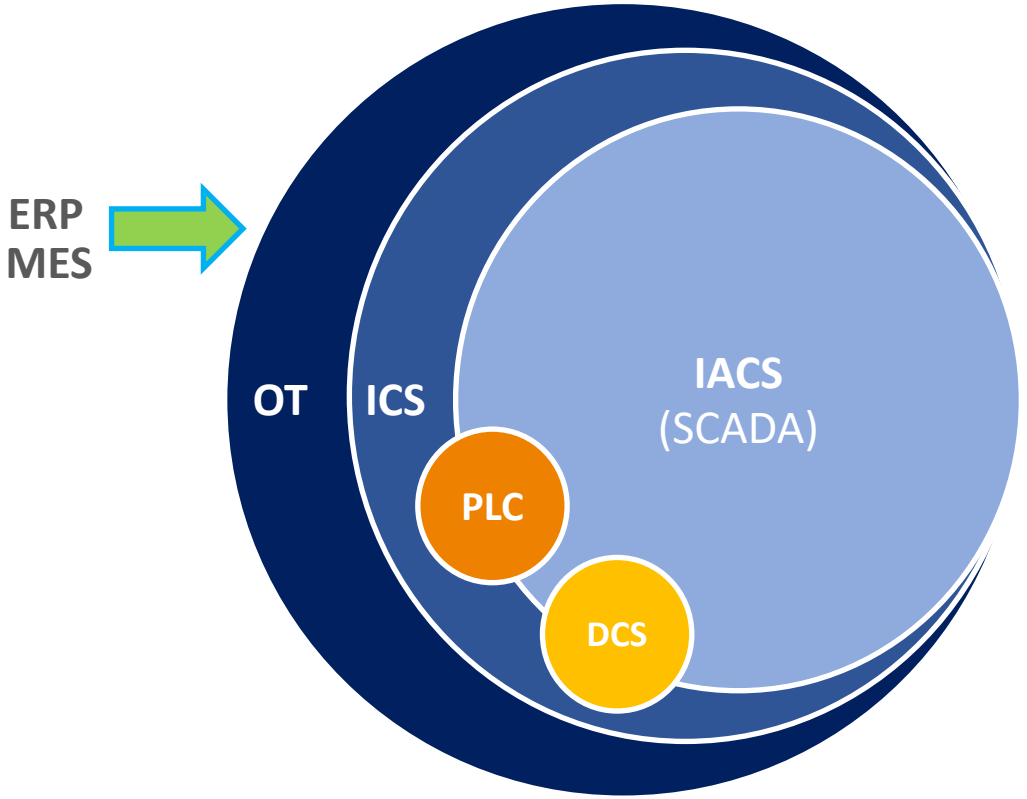
CONFINDUSTRIA VICENZA

securenetwork
Your Protection, Our Mission

COSA SIGNIFICA OT

BV TECH Group
Securing the Future.

- **OT**: Operational Technology
- **ICS**: Industrial Control System
- **IACS**: Industrial Automation Control System
- **PLC**: Programmable Logic Controller
- **DCS**: Distribuited Control System
- ***SCADA****: Supervisory Control and Data Acquisition
- **ERP**: Enterprise Resource Planning
- **MES**: Manufacturing Execution System

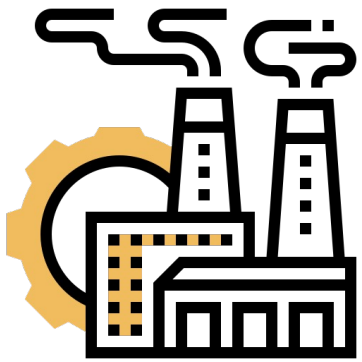


SCADA* è un termine che è stato recentemente deprecato. Nel 2002 l'International Society of Automation (ISA) ha iniziato a lavorare sugli standard di sicurezza per quelli che ha chiamato ***sistemi di automazione e controllo industriale* (IACS), sotto l'egida del suo standard 99. Il SIGC includeva servizi SCADA e rifletteva le infrastrutture industriali sempre più ampie basate su IP e interfacciate con i sistemi IT*

CONFINDUSTRIA VICENZA

securenetwork
Your Protection, Our Mission

OT CYBERSECURITY TREND (USA)



Culture & Governance

Risk Management

Standardization, management through policies and procedures

Awareness – the human factor

Technical security

2005 2010 2015 2020 2022 …

OT CYBER SECURITY

E in italia?

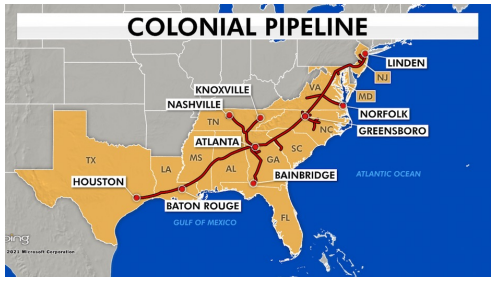
Fonte: https://otcybersecurity.blog/

QUALCHE ESEMPIO

Attacco Stuxnet: Nel 2010, un malware noto come **Stuxnet** è stato scoperto nelle reti di controllo industriale (ICS) in Iran. Il malware è stato progettato specificamente per colpire i sistemi di controllo industriale, in particolare quelli utilizzati per controllare le centrifughe utilizzate nell'arricchimento dell'uranio. L'attacco ha causato danni significativi alle centrifughe e ha rappresentato una delle prime volte che un attacco informatico ha avuto un impatto tangibile sull'infrastruttura fisica.

Attacco ai sistemi di controllo delle centrali elettriche: Nel 2016, un gruppo di hacker noto come "Dragonfly" ha preso di mira i sistemi di controllo delle centrali elettriche negli Stati Uniti e in Europa. L'attacco ha permesso agli hacker di acquisire accesso ai sistemi di controllo delle centrali elettriche e di causare interruzioni del servizio elettrico in alcune aree. Questo attacco ha dimostrato la vulnerabilità degli impianti di produzione e distribuzione di energia alle minacce informatiche.

L'attacco alla Colonial Pipeline: un attacco informatico perpetrato nel maggio 2021 che ha causato la chiusura temporanea della principale pipeline di petrolio degli Stati Uniti, che collega i raffinatori del Golfo del Messico con le aree del Nord-Est degli Stati Uniti. L'attacco, attribuito alla cyber-gang nota come DarkSide, ha causato una carenza di carburante e un aumento dei prezzi in alcune aree degli Stati Uniti. L'amministrazione Biden ha dichiarato che sta lavorando per prevenire futuri attacchi informatici.



securenetwork
Your Protection, Our Mission

COME INTRODURRE LA CYBER-SECURITY?

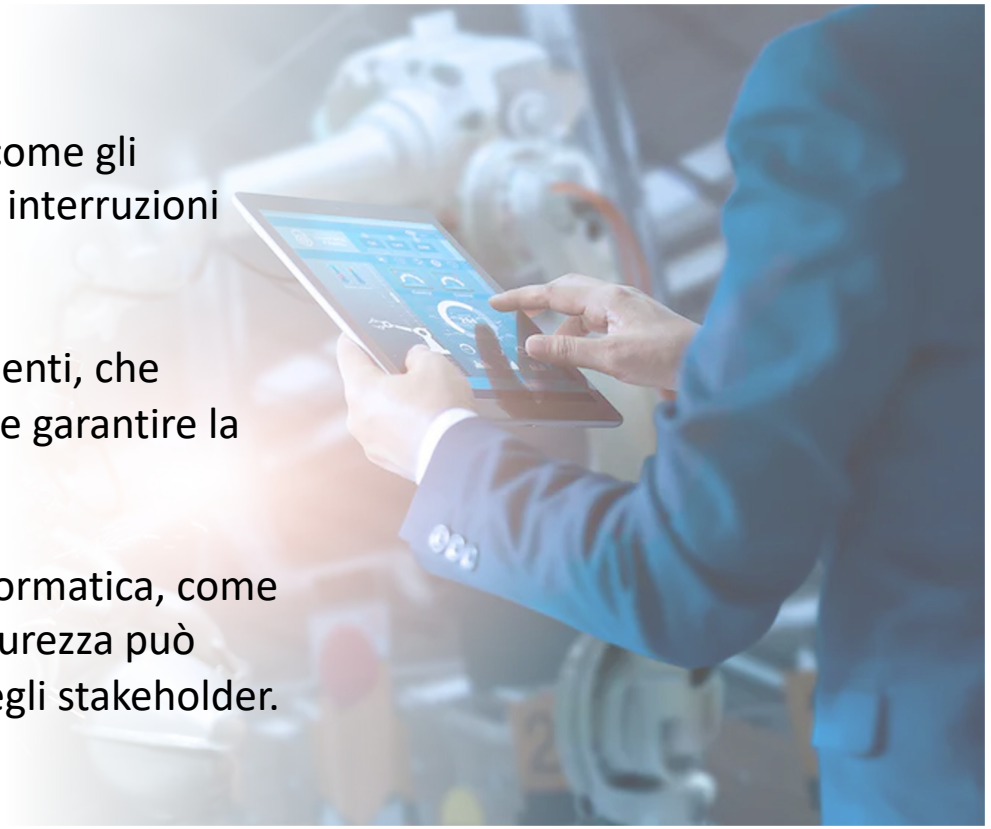
La Cyber Security in ambito industriale è importante per:

• Proteggere i sistemi e le infrastrutture critiche dalle minacce informatiche, come gli attacchi ransomware o gli attacchi di ingegneria sociale, che possono causare interruzioni del servizio, perdite economiche e danni ambientali.

• Garantire la protezione dei dati sensibili, come quelli dei clienti o dei dipendenti, che possono essere utilizzati per attività illecite come il furto d'identità o la frode e garantire la protezione delle proprietà intellettuali.

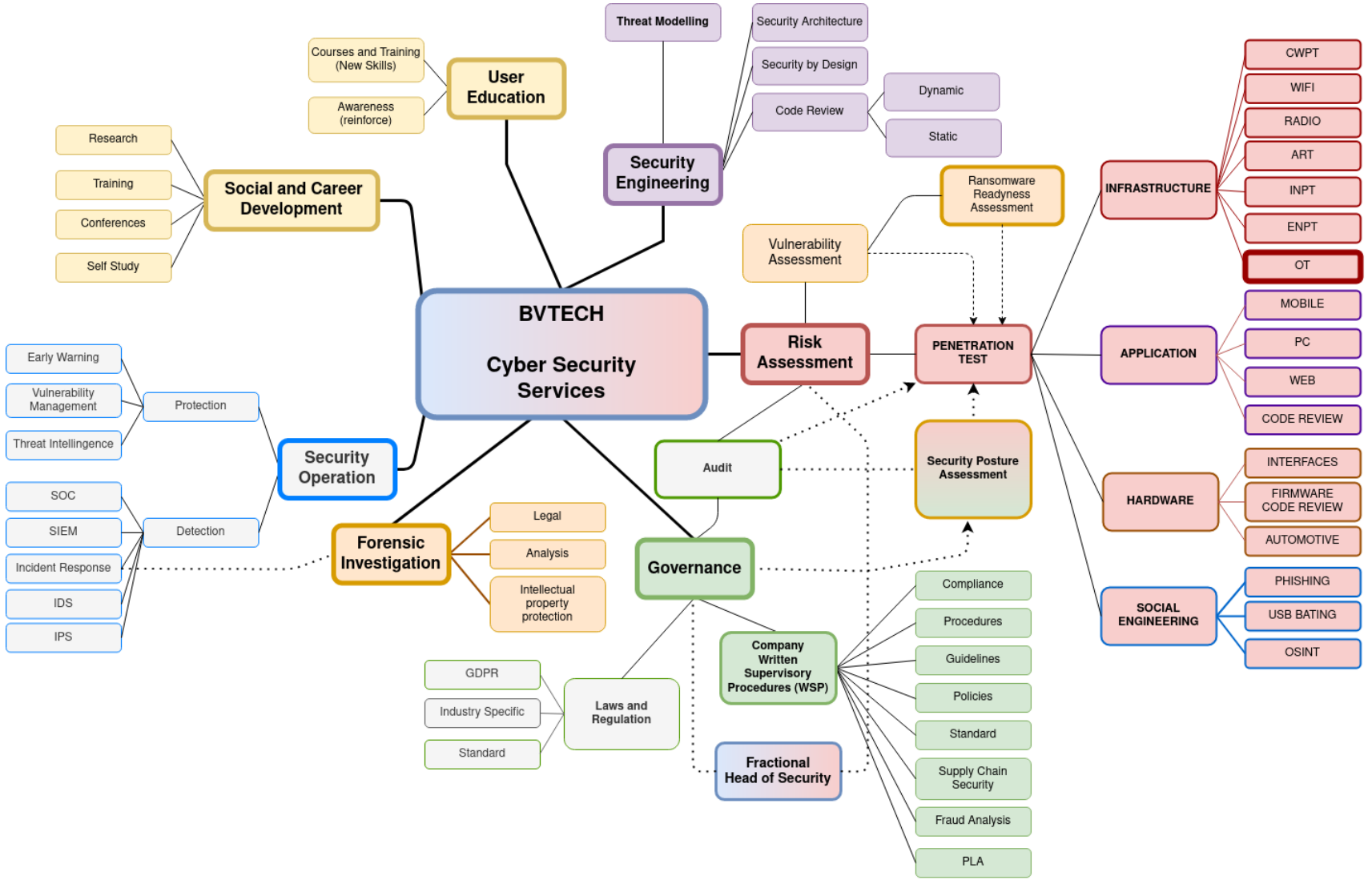
• Garantire la conformità alle normative e alle leggi in materia di sicurezza informatica, come ad esempio il GDPR in Europa. Inoltre la conformità a norme e standard di sicurezza può garantire maggiore qualità, fiducia e trasparenza nei confronti dei clienti e degli stakeholder.

• Saper gestire qualsiasi tipo di (inevitabile) incidente informatico



… Si, ma la Cyber Security che cosa è?

CYBER SECURITY SERVICES

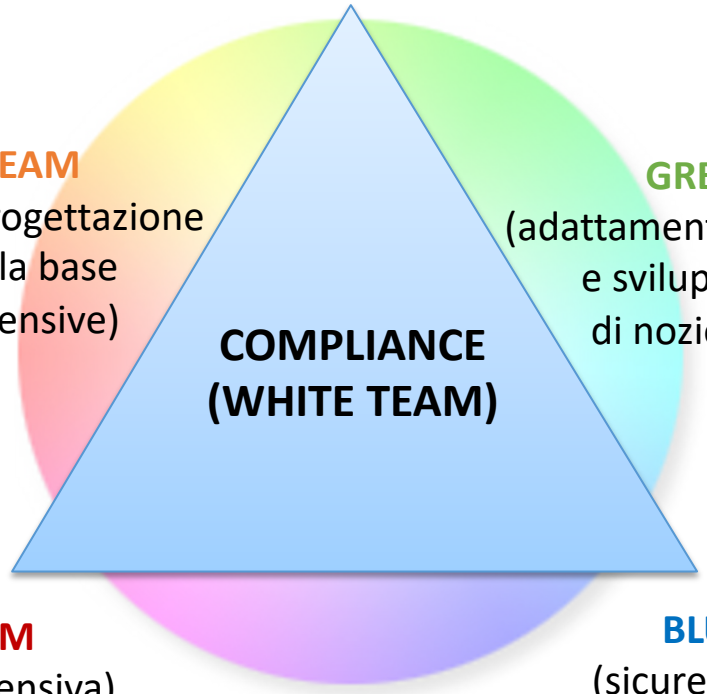


BLUE TEAM — RED TEAM

CONFINDUSTRIA VICENZA

securenetwork
Your Protection, Our Mission

CYBER SECURITY TEAMS

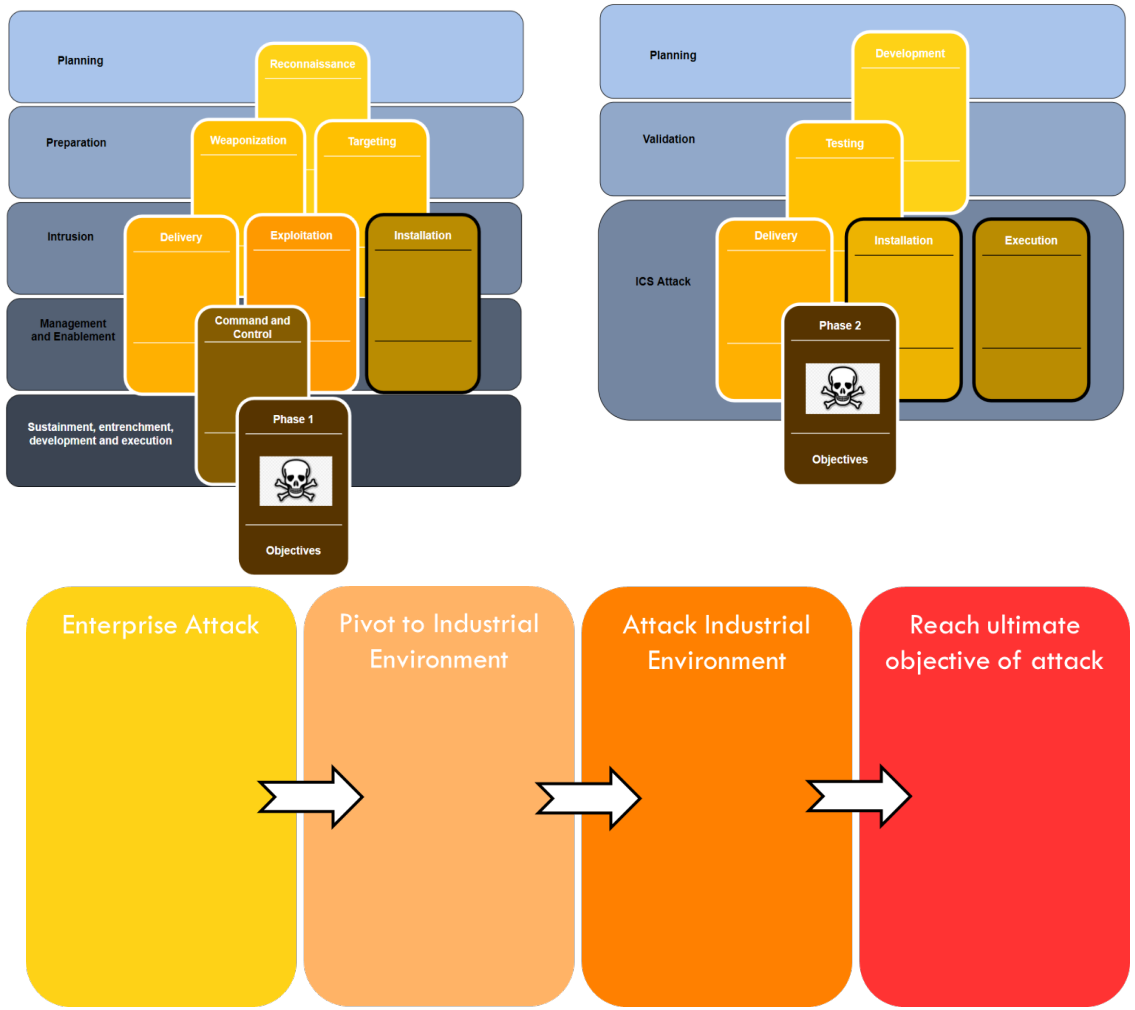


La cybersecurity abbraccia a 360 gradi i processi e le organizzazioni aziendali

- Per un processo di cybersecurity il primo step è la costruzione dei flussi organizzativi abbinata alla progettazione e implementazione dei sistemi (architetture, applicazioni e servizi)
- L'efficacia del processo richiede la sinergia di tre pilastri di competenze
  - Progettazione e sviluppo
  - Sicurezza offensiva
  - Sicurezza difensiva

PRIMO NECESSARIO APPROCCIO DI ANALISI

- Ogni analisi di Cyber Security dovrebbe (deve) iniziare con un **Threat Model** di quel che si sta analizzando
- Il Threat Model deve identificare tutti i possibili aggressori e le risorse temporali ed economiche degli stessi (aggressore esterno, dipendente scontento, fornitori, nazione ostile, etc)
- Questo permette di disegnare degli **scenari di attacco** verosimili e completi



SECURITY POSTURE ASSESSMENT OT

BV TECH Group
Securing the Future.

Un approccio **completo** in ambito cybersecurity OT. Lo scopo è quello di riuscire a catturare una fotografia completa dell'insieme degli aspetti di Cyber Security e sviluppare una roadmap.

- **Threat Model**
- **Governance**
- **Procedure e Processi**
- **Vulnerability Assessment and Management**
- **Penetration Test**
- **Security Advisoring**
- **Formazione**
- **Consulenza continuativa**

CONFINDUSTRIA VICENZA

securenetwork
Your Protection, Our Mission

SECURITY POSTURE ASSESSMENT

BV TECH Group
Securing the Future.

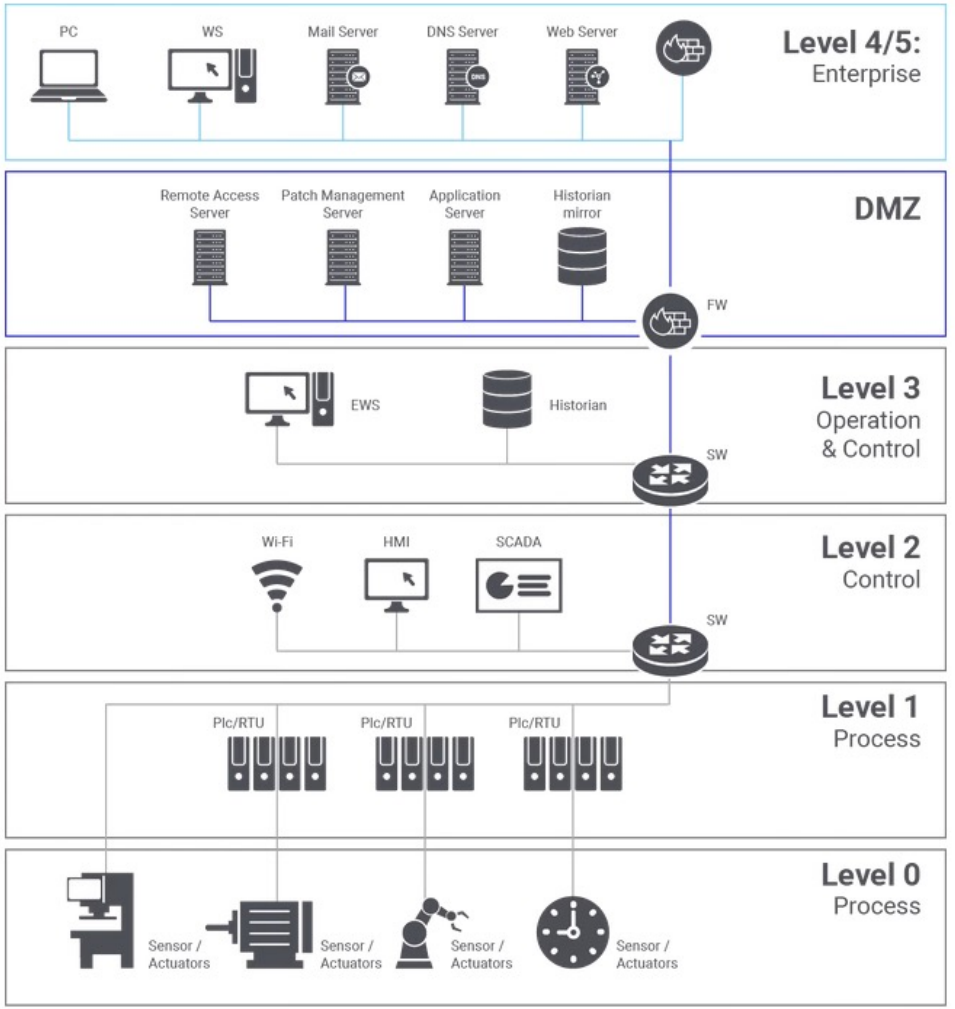
L’analisi deve essere completa e deve tenere in considerazione **tutti** i diversi fattori:

- **Analisi del disegno complessivo dell’infrastruttura, procedure, processi, asset inventory, application inventory**
- **Valutazione tecnica delle vulnerabilità logiche e fisiche**
- **Sicurezza logica**
- **Sicurezza fisica**
- **Preparazione tecnica delle persone sulle tematiche di cybersecurity**
- **Analisi presenza informazioni censite in Internet (Shodan, etc)**
- **Governance OT**

ANALISI INFRASTRUTTURA

Prima analisi:

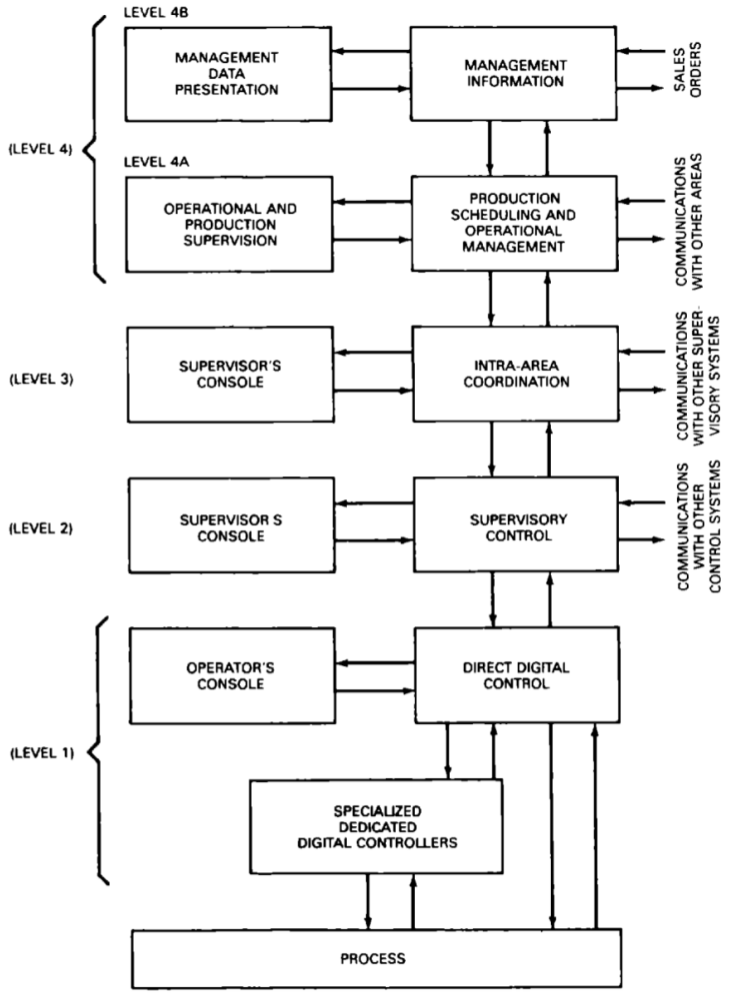
- Analisi degli schemi di rete dell'infrastruttura OT (se presenti)
- Segregazione IT vs OT
- Protocolli radio?
- Aderenza al modello **Purdue**
- Asset Inventory
- Application Inventory



IL MODELLO PURDUE ORIGINALE

BV TECH Group
Securing the Future.

- **Sviluppato alla fine degli anni 80** (…)
- Il modello non ha nulla a che fare con una «vera» rete o con la cyber security. **Non ci sono firewall, non c'è DMZ**.
- C'è una console operatore al livello 1. Negli ultimi anni non è più ammissibile, ma in quegli anni era frequente e normale.
- Il livello 4 è stato suddiviso in un livello 4A e un livello 4B, per segmentare le funzioni che interagiscono direttamente con i livelli di automazione e le funzioni che non richiedono un'interfaccia diretta.
- Non esiste un livello 0, lo strato di processo è un mucchio di tubi, pompe, valvole e alcune cose (poche) intelligenti.



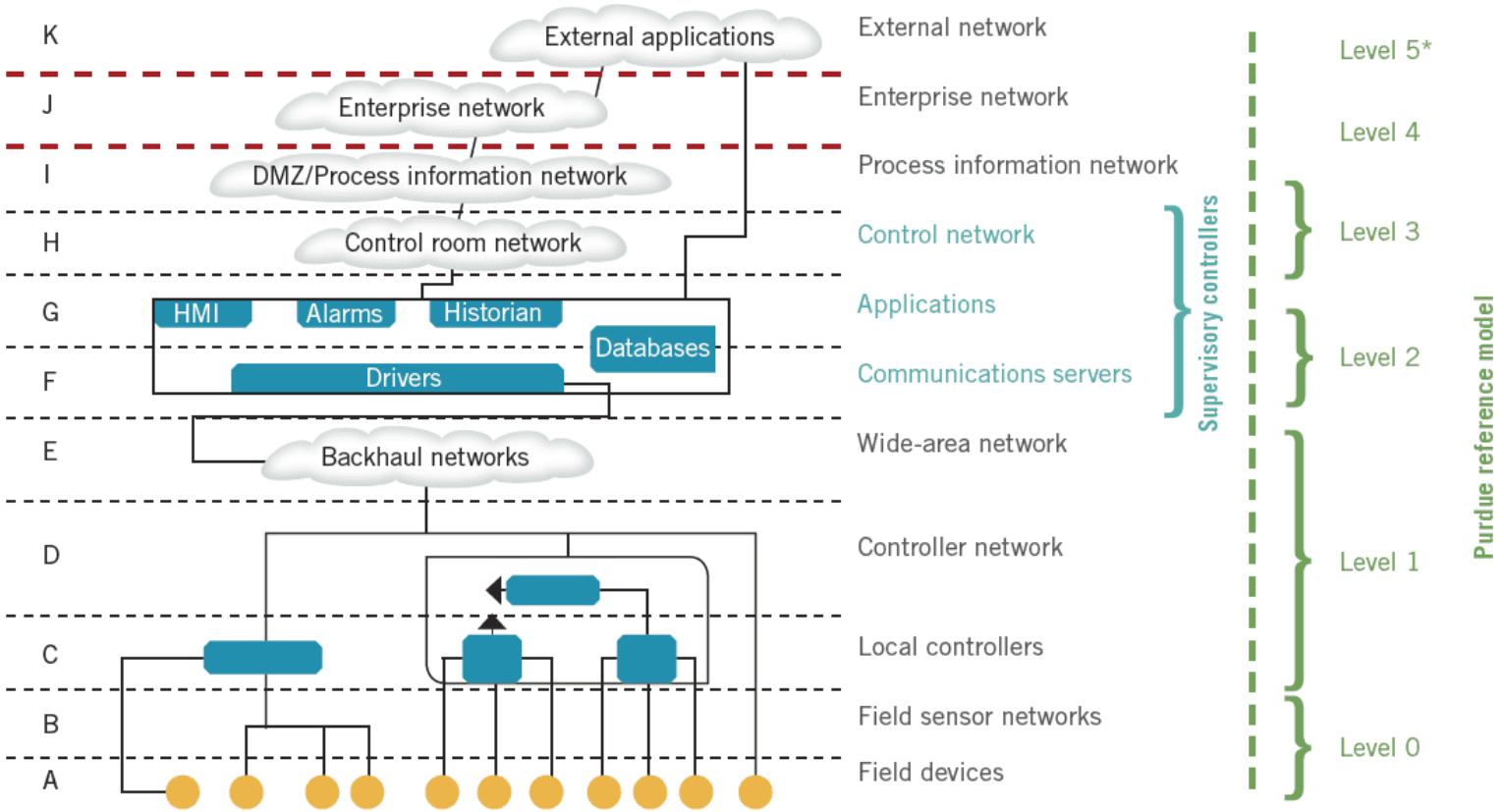
CONFINDUSTRIA VICENZA

securenetwork
Your Protection, Our Mission

ICS NETWORK DEFENSE & SEGMENTATION

BV TECH Group
Securing the Future.

La rete ICS correttamente segmentata seguendo il modello Purdue **ha diversi vantaggi in termini di difesa.** Questa configurazione crea naturalmente punti di convergenza utili per la protezione della rete, la raccolta dei dati per monitoraggio e funge anche da punto di controllo per il contenimento nella risposta agli incidenti:



CONFINDUSTRIA VICENZA

securenetwork
Your Protection, Our Mission

OT IS BUSINESS ORIENTED

- ..Infine c'è il dominio di Business, generalmente non facente parte dell'ICS.
- È il dominio decisionale.
- **In termini di Cyber Security ci interessa? Si! Molto.**

VULNERABILITY ASSESSMENT

BV TECH Group
Securing the Future.

- La produzione OT non può essere impattata, in nessun caso dai test di sicurezza.
- Lo sfruttamento di vulnerabilità potrebbe causare instabilità dei sistemi.
- Alcune recenti normative e compliance però richiedono che tali test vengano fatti.

Quindi, come fare Vulnerability Assessment e Penetration Test in ambito OT?

CONFINDUSTRIA VICENZA

securenetwork
Your Protection, Our Mission

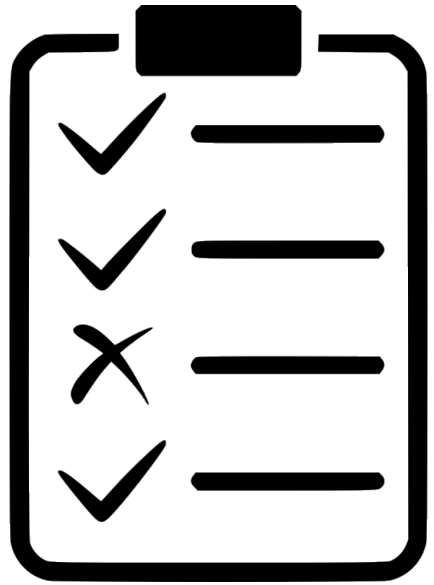
ANALISI VULNERABILITA’

BV TECH Group
Securing the Future.

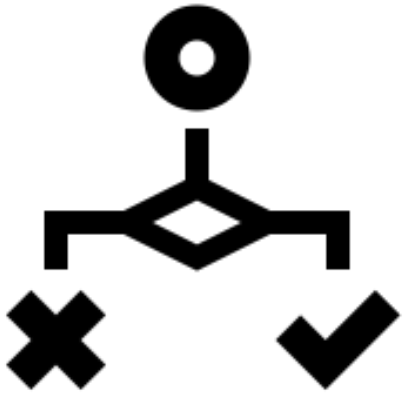
Vulnerability Assessment e Penetration test OT

- **Analisi passiva del traffico di rete** mediante sonde di rete e strumenti proprietari: questa tipologia di analisi è del tutto sicura e non può impattare sulla produzione
  Questa prima fase di analisi permette inoltre già di valutare il livello di monitoraggio che è possibile raggiungere con l’attuale disegno di infrastruttura

- **Penetration Test** mirati tramite negoziazione non invasiva di protocolli che non impattano sulla produzione (es. http, ssh, telnet, etc) e scansioni mirate.



ANALISI SICUREZZA LOGICA

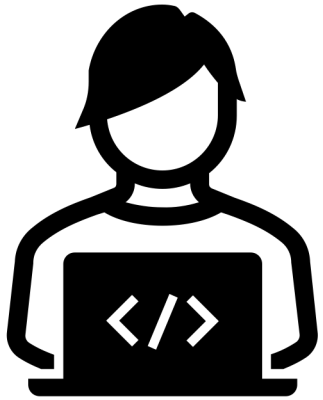


- Sostanzialmente **chi accede a cosa** (e perché)
- Monitoraggio
- I fornitori/manutentori, come accedono alla rete? E ai singoli dispositivi?
- Accesso remoto: Site Access Manager, VPN, 2FA
- Password policy
- Backup
- Permessi Active Directory
- Segmentazione Accessi
- Analisi completa di tutto l'outsourcing ()

SICUREZZA FISICA

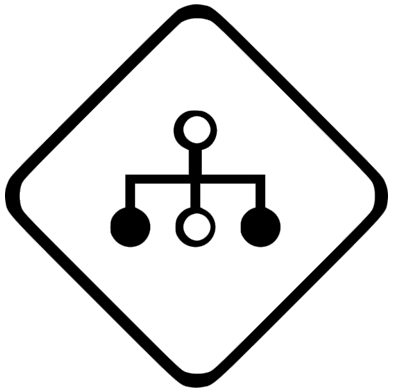
- **La sicurezza fisica è sempre un importante presidio della sicurezza logica**
  - Analisi delle procedure di accesso ai siti produttivi
  - Analisi degli eventuali dispositive RFID di accesso (badge)
  - Analisi dei datacenter, armadi rack, device di rete e console esposte
  - Presenza di telecamere di sorveglianza a presidio degli asset
  - Attività di Red Teaming

SICUREZZA DELLE WORKSTATION AZIENDALI



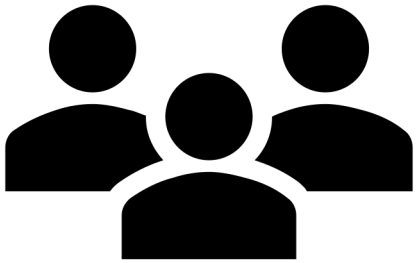
- Analisi di tutti i computer, laptop e postazioni di lavoro utilizzati nei diversi livelli.
- Presenza di dischi cifrati, agent di monitoraggio, antivirus, bios, livello di hardening.
- Analisi delle applicazioni.
- Analisi del livello di patch e update.
- Eventuale analisi dei dispositivi mobile (anche degli operatori)
- Analisi procedure di provisioniong e deprovisioning

SICUREZZA APPLICATIVA



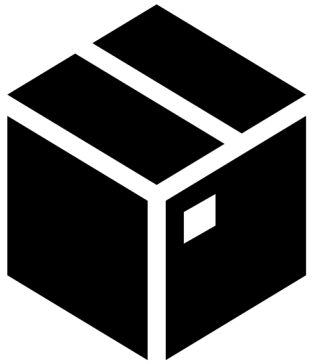
- Presenza di Application Inventory
- Analisi di tutte le applicazioni e middleware utilizzate
- Penetration Test applicativi ed infrastrutturali
- Ricerca di vulnerabilità
- Analisi di contesto dell’esposizione dei singoli asset/endpoint

CYBER SECURITY AWARENESS



- Interviste al personale, soprattutto ai ruoli più importanti
- Analisi del livello di preparazione del personale, a seconda del ruolo, dagli operatori delle control room ai dipendenti amministrativi e di ricerca e sviluppo.
- Campagne di phishing, vhisihing, usb bating
- Social Engineering

DELIVERABLES



- Report Tecnico
- Executive Summary
- Framework di lavoro
- OT Asset Inventory (!)
- Programmazione attività future e assistenza al remediation plan
- Vulnerability management e Risk management

1.2 → Technical·Summary¶

1.2.1 → Security·Posture·Assessment¶

Secure·Network·ha·eseguito·un'attività·di·**Security·Posture·Assessment**·al·fine·di·determinare·lo·stato·in·essere [redacted] rispetto·alle·diverse·tematiche·riguardanti·la·sicurezza·informatica.·L'assessment·ha·preso·principalmente·in·esame·l'infrastruttura [redacted] ¶

Le· attività· di· analisi· ha· portato· alla· luce· una
informatica,·oltre·ad·alcune·inerenti·i·processi·e·
Si·segnala·che·l'intera·infrastruttura·di·rete,·seb
totalmente·di·qualsiasi·livello·di·segregazione,·i
compute [redacted]
amministrative·della·provincia·di [redacted] ·Tale·manc
attacco·informatico,·sia·esso·portato·a·termine·
rete,· che· da· un· malware· o· ransomware.· Le· ne
regionali,· amministrativi,· gestionali· ed· operat
dell'infrastruttura·stessa,·ponendo·ulteriori·vinc
Tale·complessità·è·ulteriormente·confermata·dal

1	5	CRITICAL	Gestione Networking	2.1.1	[redacted]
2	5	CRITICAL	Gestione Networking	2.1.2	
3	3	MEDIUM	Gestione Networking	2.1.3	
4	4	HIGH	Gestione Networking	2.1.4	
5	3	MEDIUM	Gestione Networking	2.1.5	
6	2	LOW	Gestione Networking	2.1.6	
7	4	HIGH	Gestione Networking	2.1.7	
			Gestione		

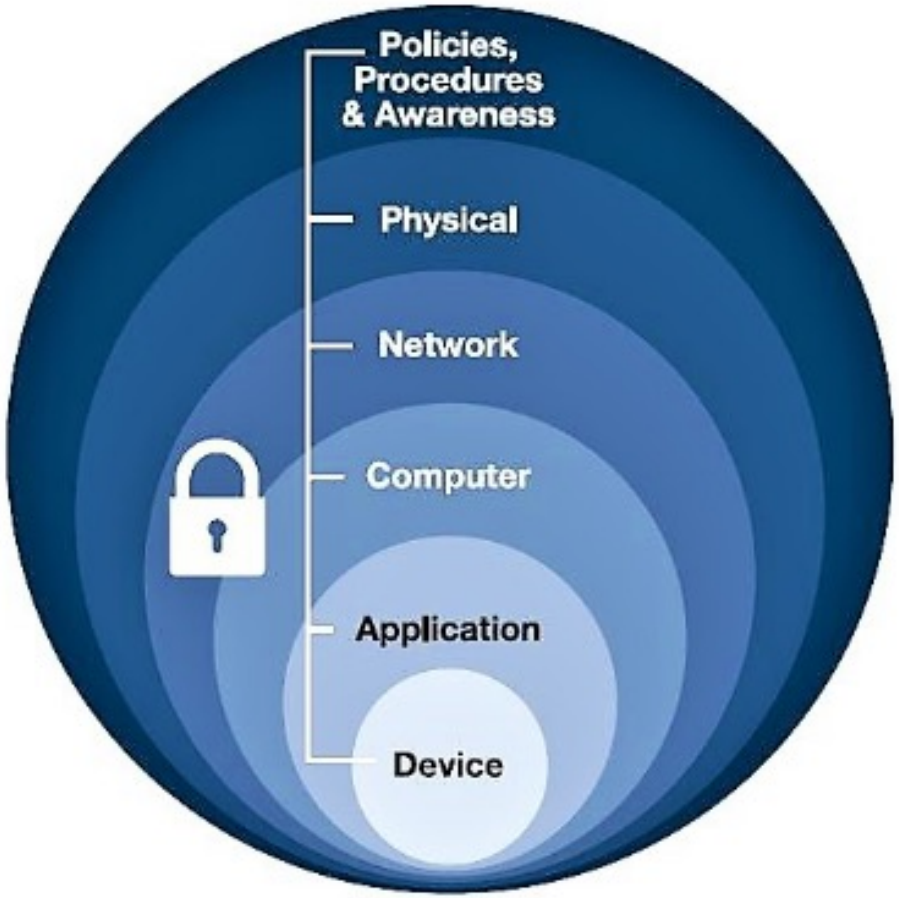
- **Come vanno gestite le vulnerabilità?**
- **Ehm.. Chi le gestisce?**
- **Come?**
- **Quando? (Perché'?)**

INTRODUCING GOVERNANCE OT

BV TECH Group
Securing the Future.

(Where Governance never exist)

- **Vulnerability and Risk Management, patch e update**
- **Certificazioni ISO 9001, 27001, IEC62443, IEC60508**
- **Analisi delle procedure e processi interni**
- **Percorso verso un Security Operation Center (SOC) OT**
- **Incident response e Business Continuity**
- **Protezione e sicurezza perimetrale**
- **CSET tool by CISA**
- **Security Monitoring and Logging**
- **Change, Ticket, Vulnerability Management**



CONFINDUSTRIA VICENZA

securenetwork
Your Protection, Our Mission

DIRETTIVE NIST

BV TECH Group
Securing the Future.

Funzione	Descrizione	Categorie
IDENTIFY	Comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Assessment Strategy • Supply Chain Risk Management
PROTECT	Implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica	• Identity Management and Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology
DETECT	Definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica	• Anomalies and Events • Security Continuous Monitoring • Detection Processes
RESPOND	Definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. Contenere l'impatto determinato da un potenziale incidente di sicurezza informatica.	• Response Planning • Communications • Analysis • Mitigation • Improvements
RECOVER	Definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente. Garantire la resilienza dei sistemi e delle infrastrutture, e supportare il recupero tempestivo delle operazioni.	• Recovery Planning • Improvements • Communications

CONFINDUSTRIA VICENZA

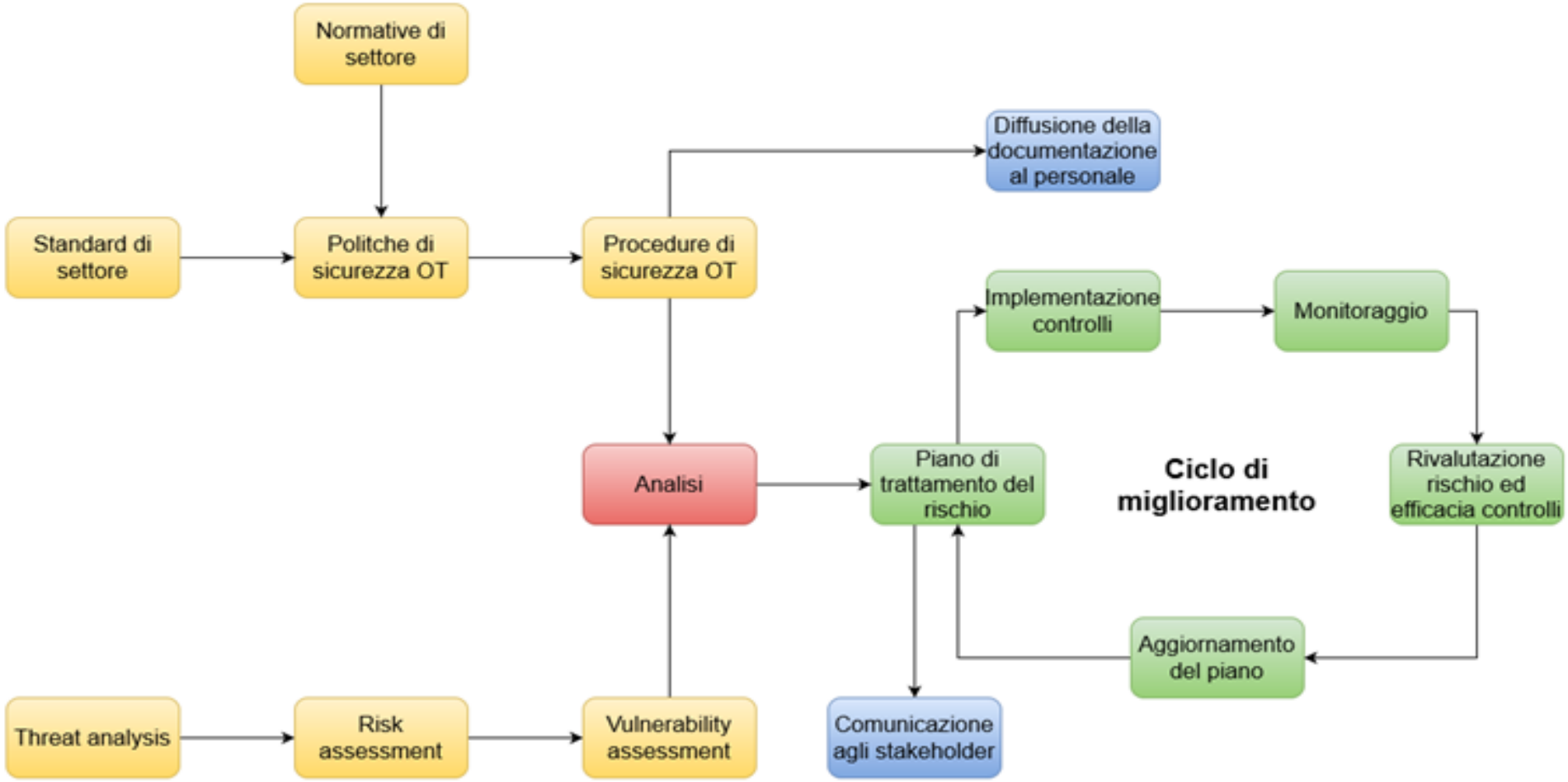
securenetwork
Your Protection, Our Mission

SFIDE DELLA GOVERNANCE OT

- I sistemi OT sono complessi e diversificati, con molti componenti software e hardware. Anche all'interno della stessa azienda, le diverse aree produttive possono utilizzare diverse tecnologie di controllo operativo.
- La mancanza di attenzione alla sicurezza e la necessità di automatizzazione possono portare a una perdita di cognizione delle basi dell'infrastruttura. Inoltre, i sistemi OT spesso sono proprietari, rendendo difficile l'analisi e aumentando la vulnerabilità.

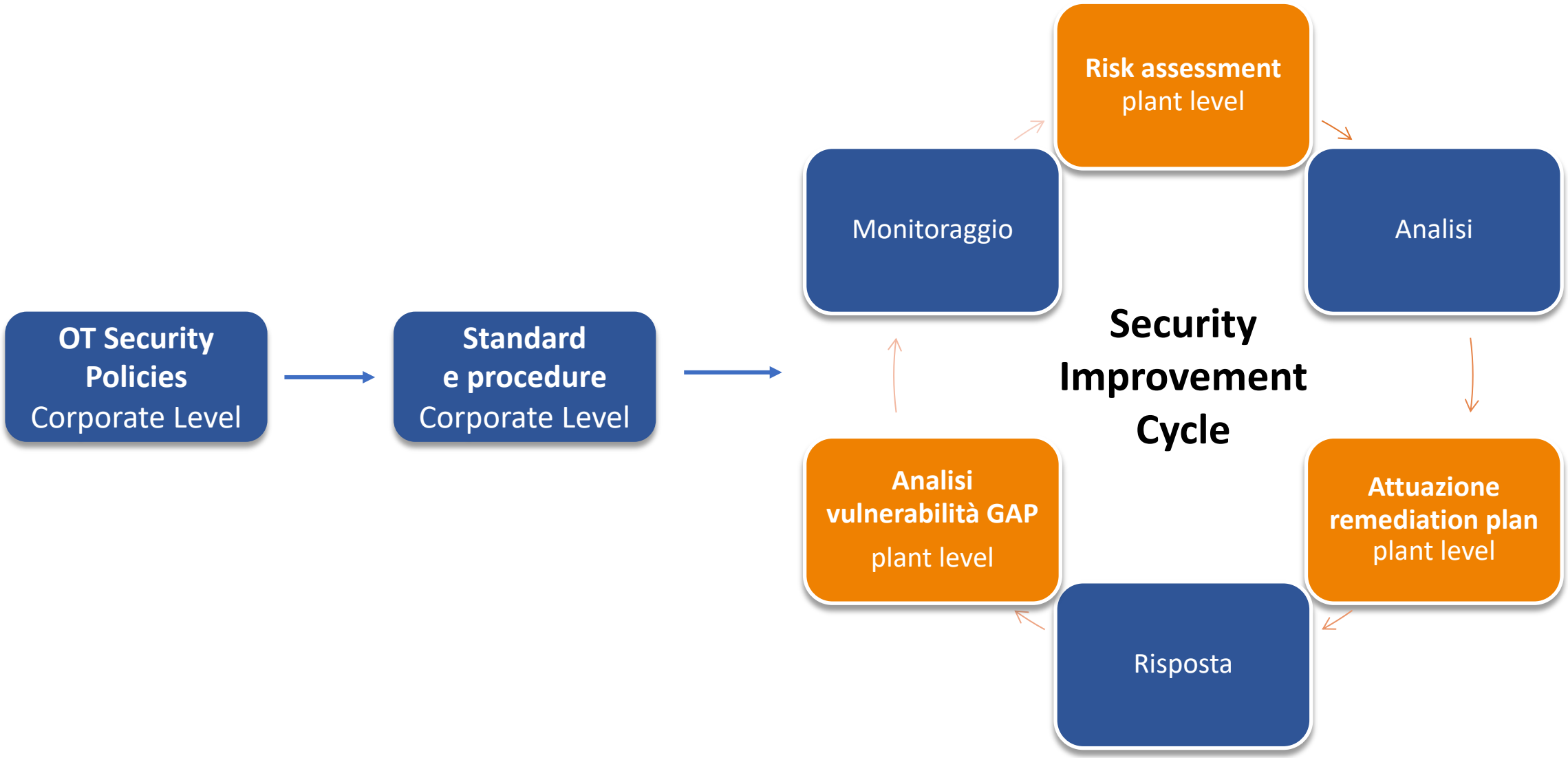
GOVERNANCE OT

La **Governance OT** richiede una gestione globale. Un approccio top-down che semplifichi le variabili attraverso l'analisi dell'organizzazione e dell'infrastruttura OT, fornendo strumenti per gli utenti con un approccio bottom-up.



GOVERNANCE OT: CICLO DI MIGLIORAMENTO

BV TECH Group
Securing the Future.



CONFINDUSTRIA VICENZA

securenetwork
Your Protection, Our Mission

OT GOVERNANCE

Per introdurre ed implementare un corretto sistema di governance OT risulta quindi necessario:

- **Identificare le minacce** attraverso un accurata threat intelligence. Questo permette di contestualizzare e ritagliare il profilo di sicurezza direttamente su misura dell'organizzazione.
- Assicurarsi che le policy aderiscano ai **requisiti normativi e i regolamenti**, compresi quelli in merito alla privacy, siano correttamente compresi e gestiti.
- Assicurarsi che la **gestione del rischio cyber integrata** con la gestione del rischio a livello corporate allineando di fatto tutta l'azienda e collegando il dominio operazionale con quello IT e strategico;
- Assicurarsi che tutto il personale sia pianamente cosciente delle politiche di sicurezza e dei rischi associati alle loro mansioni, al fine di sviluppare una **coscienza della sicurezza aziendale**/ a livello corporate.
- Svolgere regolari analisi complessive di **Vulnerability Assessment e Penetration Test**

DOMANDE?

BV TECH Group
Securing the Future.

Grazie a tutti!

Per contatti:

- giorgio.campiotti@securenetwork.it
- www.securenetwork.it
- www.bv-tech.it
- Twitter: @giorgiofox

CONFINDUSTRIA VICENZA

securenetwork
Your Protection, Our Mission

CONTATTI

giorgio.campiotti@securenetwork.it

+39 02 83994606

+39 335 1778376

www.securenetwork.it

Via dei Valtorta 48,

20127 Milano