**Wiit S.p.A. – Industrial Cyber Security (ICS)**

**<u>Si prega di compilare la scheda rispettando il limite massimo di 5000 caratteri, spazi inclusi</u>**

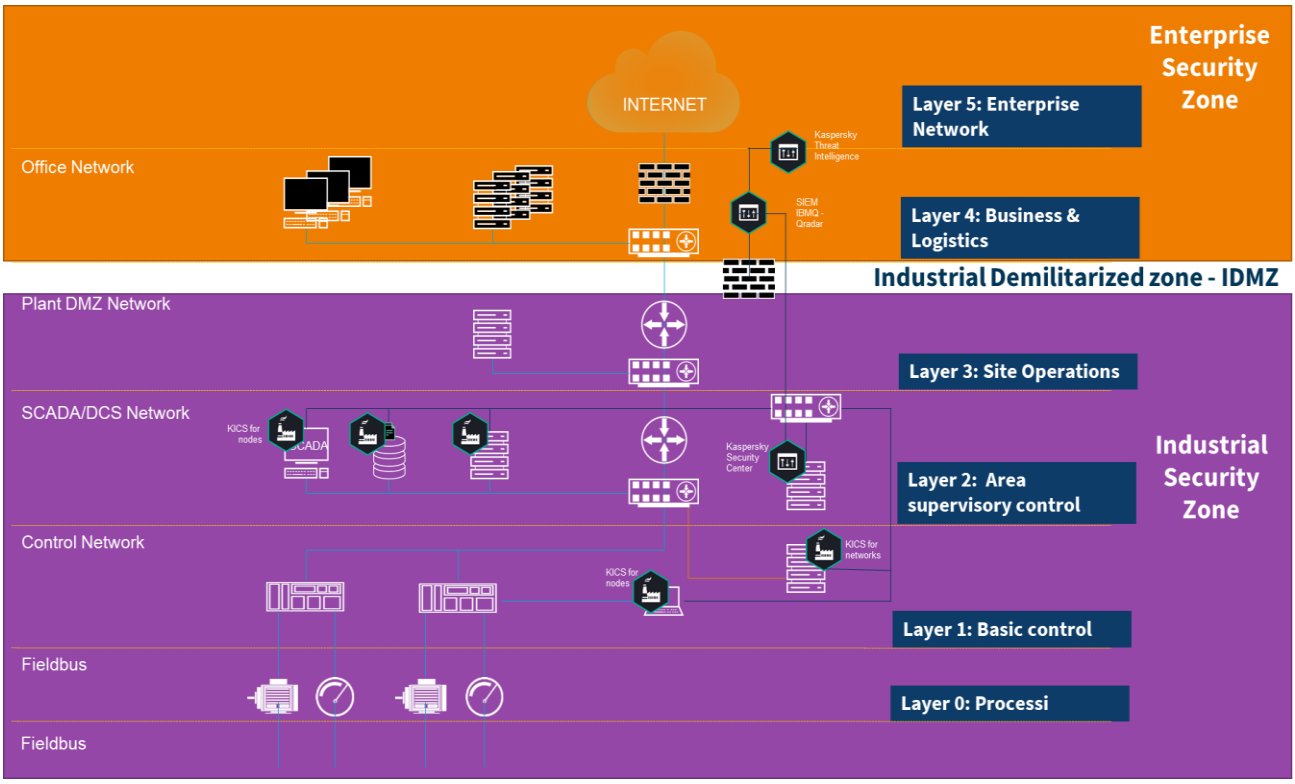
1. Descrizione della problematica o del bisogno nell'azienda o pubblica amministrazione utente.

Azienda Cliente: Arredo3
Il Cliente, uno tra i più grandi produttori di cucine su misura Made in Italy, con circa 60.000 cucine prodotte ogni anno e 8 linee produttive, conta un magazzino automatizzato di 12.242 mq dal quale vengono prelevati 4.000 componenti al giorno ed un impianto automatico che produce 1.000.000 di panelli all'anno. Tale innovativo sistema di produzione risulta all'avanguardia nel panorama Industry 4.0 in quanto i dati sono inseriti nei sistemi IT e di produzione a partire dall'ordine.

Dopo una prima fase di Trasformazione Digitale che ha implementato uno scenario di produzione fortemente automatizzato tramite processi e standard di altissima qualità in cui l'efficienza e la resilienza sono i KPI fondamentali, l'azienda ha sentito il bisogno di estendere i principi di security by design dal perimetro della sicurezza IT agli impianti produttivi OT. Si sentiva infatti la necessità di una soluzione integrata in grado di far dialogare le soluzioni Operational Tecnology della Fabbrica con l'IT e sopperire pertanto alla mancanza di un progetto security by design specifico per l'ambito OT (SCADA).

Le tecnologie OT, infatti, hanno un focus su performance e disponibilità piuttosto che sulla Cyber Security dato che nascono per essere introdotte in reti "air-gapped" (ovvero separate dalle altre reti), le quali con le iniziative Industry 4.0 hanno visto una accelerata adozione dei paradigmi "digital" che necessitano di una comunicazione, sempre crescente, con le infrastrutture IT ed IoT.

## 2. Descrizione della soluzione tecnologica (tecnologie usate, architettura, ecc.).




La soluzione implementata prevede l'implementazione del concetto di "ONE SOC" (Security Operations Center unico) con visibilità integrata sia delle infrastrutture IT sia di quelle OT attraverso le seguenti tecnologie:

- Kaspersky: Threat Intelligence & Industrial CERT – KICS for networks + KICS for nodes
- SIEM Qradar (OT + IT) servizio con perimetro ampliato per monitorare ed analizzare eventi e minacce sulle infrastrutture IT e di produzione

La soluzione permette una visibilità integrata della comunicazione tra tecnologie IT ed OT grazie alla quale è possibile correlare gli eventi di sicurezza (sia dell'IT che dell'OT). Tramite la soluzione WIIT vengono coperti in maniera integrata i livelli del Modello di Purdue dell'Industrial Security dal Livello 0 al Livello 5.

## 3. Descrizione del progetto di implementazione - complessità, tempi, aspetti organizzativi, costi, ecc.

Il perimetro del progetto prevede tutta l'infrastruttura IT e OT dell'azienda Cliente. In particolare l'area produzione è composta da oltre150 PLC e 30 Server di supervisione, dislocati su 8 impianti produttivi a livello worldwide e su un magazzino automatizzato di 12.242 mq su tutti i compartimenti aziendali seguenti:

A - semilavorato
B - magazzino
C - produzione
D - logistica

E - direzionale
F - showroom
G – laccatura

I tempi di implementazione della soluzione sono di circa 3 mesi finalizzati al completamento delle seguenti attività:

- creazione DMZ (Zona Industrial Demilitarized Zone);
- configurazione porte su cui installare "in ascolto" gli apparati di analisi del network(appliance);
- installazione delle soluzioni di sicurezza sugli endpoint;
- configurazione dei comandi ed alert da notificare con riferimento alle macchine degli operatori di produzione.

## 4. Descrizione dei principali benefici raggiunti dall'azienda o pubblica amministrazione utente.

I principali benefici del progetto contemplano l'aumento della resilienza delle infrastrutture di fabbrica fondamentale per implementare i concetti di Business Continuity & Resilience.
Ulteriori benefici sono:

- incremento di livello di Cyber Security sia in ambito IT sia in ambito OT;
- conformità con principali requisiti di settore (NIST SP 800-82);
- possibilità per i clienti di fruire degli incentivi economici "Industria 4.0";
- ROI dell'investimento dimostrato e controllato attraverso un Executive Report con periodicità trimestrale che aumenta il controllo e la supervisione di eventuali misconfiguration e vulnerabilità presenti nel perimetro.

## 5. Descrizione degli elementi distintivi e di reale innovatività/originalità della soluzione, anche con riferimento a soluzioni «concorrenti».

Rispetto alle soluzioni di mercato la soluzione WIIIT permette una visione integrata della Cyber Security negli ambiti IT ed OT su tutti i livelli del Modello di Purdue con la possibilità di gestire minacce provenienti da diversi vettori di attacco.

Per un'azienda che ha implementato processi automatizzati fin dall'arrivo dell'ordine di produzione, è fondamentale che:

- gli impianti ICS/SCADA soggette ai processi di trasformazione digitale vengano messi sotto controllo della soluzione di Industrial Cyber Security e che, pertanto, le proprietà intellettuali della produzione vengano salvaguardate,
- eventuali attacchi mirati vengano scoperti in anticipo grazie al collegamento al Security Operation Center che utilizza strumenti di threat intelligence globali e specifici per rilevare le minacce in ambito Manufacturing.