## **Risposta ad attività cybersecurity (e contratto)**

Contenuti

* [Puntualizzazioni su elenco attività](#_9uo0rarh8ald)
* [Domande su gestione attività](#_38fotw1oli2e)
* [Puntualizzazioni su contratto](#_1mpf3j9ritnj)

### **Puntualizzazioni su elenco attività**

Propongo alcuni chiarimenti a livello generale prima dell’esame delle singole attività proposte.

#### 1) SSDL

Il volume 4-1 della IEC 62443 riguarda i processi per lo sviluppo sicuro del software (Secure Software Development Lifecycle, SSDL) in ambito OT/ICS. A differenza del volume 4-2, che definisce i requisiti tecnici dei componenti, il 4-1 si concentra su come organizzare lo sviluppo software, coprendo 8 aree principali (es. gestione dei requisiti di sicurezza, progettazione sicura, verifica), suddivisi in 48 processi e un totale di 160 punti di verifica.

Per garantire un’implementazione efficace, suggerisco di:

1. Trattare l’SSDL come un’area distinta, con una checklist dedicata per i 160 punti di verifica, come previsto dal Task 4 (Documento per l’audit).
2. Sviluppare policy e procedure specifiche per l’SSDL (Task 3), ad esempio sulla gestione delle vulnerabilità o la validazione del codice.
3. Definire l’ambito dell’audit: coprire tutte le 8 aree o iniziare con un’esperienza pilota su alcune aree (es. ‘Security Requirements’ e ‘Vulnerability Management’) per i clienti pilota come Breton o Piovan.

#### 2) Requirements componenti e sistemi IACS (macchine)

Il volume 4.2 della 62443, riguarda invece i requirement che il software dei singoli componenti deve soddisfare.

La 62443-4-2 suddivide i componenti in 4 tipologie:

* embedded device (PLC, DCS e altri),
* network device (Industrial firewall, Managed switch e altri),
* host device (HMI server, Patch management server e altri),
* software applications (SCADA system, Data historian e altri).

Il volume 3.3, riguarda invece i requirements dei componenti assemblati in un sistema IACS, o macchina. Specificano le misure di protezione per flussi di dati e sicurezza del sistema.

Un produttore come Breton ad esempio dovrà utilizzare la 4-2 per verificare che i componenti forniti da Siemens o altri siano conformi al Security Level Capability (SL-C) dichiarato e utilizzerà la 3-3 per verificare flussi di dati e sicurezza di sistema della macchina realizzata.

Dal punto di vista dell’audit l’oggetto può essere una sistema o macchina (un insieme di componenti) o un singolo componente.

L’esecuzione dell’audit richiede un processo articolato in step, guidato dalle caratteristiche della macchina:

1. Identificare i componenti di ogni macchina suddivisi per tipo, i flussi dei dati da componente a componente e i trust boundaries.
2. In base a questi dati e al contesto di utilizzo della macchina o componente debbono essere identificate le minacce (Threat Model).
3. In base alle minacce si devono recuperare i requirements 4.2 e 3.3 per le misure di protezione, la cui implementazione conforme costituisce l’oggetto dell’audit.

I requirement da verificare dipenderanno anche dal security level capability (SL-C) che il produttore vuole supportare per la macchina o componente.

Il produttore deve scegliere se la macchina, o il componente, avrà SL-C 1, 2, 3 o 4. Più alto il livello e maggiori dovranno essere i requirements da soddisfare. I volumi 4.2 e 3.3 fanno da guida per individuare i requirement di ogni livello.

Per le macchine il processo di audit è quindi più articolato e i punti di verifica, lo scope dell’audit, dipendono dalla macchina. Per questo motivo più sotto propongo di attuare un LLM assisted audit process su cui, come avevo anticipato sto lavorando, e che utilizza come primo input le caratteristiche della macchina. Delle attività LLM assisted vorrei parlare il 23 o 24 quando sarai a Reggio.

Per un singolo componente il processo è più semplice, ma comunque dobbiamo sapere il suo SL-C ed eseguire i 3 step.

#### 3) Policies e procedures

Ritengo si debba fare chiarezza sui concetti di policies e procedures e di linee guida per i consulenti.

Policies e procedures debbono essere redatte dal cliente, decidendo quali regole darsi per implementare il CHE COSA richiesto da standard e norme. Noi potremo fornirgli dei templates che lui deve personalizzare, la produzione deve essere sua responsabilità.

Alla pag. 6 di Proposta Cyber Security\_BRETON Spa.pptx.pdf vi è un esempio corretto di policy.

Per i consulenti, invece, parlerei di “linee guida”, come diciamo nel Task 3, cioè indicazioni pratiche per aiutarli a lavorare coi clienti senza perdersi nelle normative. Non le chiamerei policy o procedure, per non fare confusione.

Poi, credo sia meglio definire un ambito (Scope) limitato di definizione delle policy: magari una regola per lo sviluppo software (una practice area del 4-1, tipo gestione delle vulnerabilità) e qualche requisito per le macchine (dal 3-3 e 4-2).

L’importante per il cliente è iniziare col piede giusto impostando correttamente il lavoro, la produzione completa delle policy e delle procedures non credo sia fattibile in breve tempo.

Vi sarebbero poi le policy di alto livello, quelle legate a Security Program e Governance, vedi il seguente punto 4).

#### 4) Security Program e Governance

Abbiamo detto che, in questi primi interventi, il discorso instaurazione Security Program e Governance, per ragioni pratiche, non è affrontabile in termini ufficiali.

Data però la natura di fondamento che questi aspetti hanno per tutte le fasi dei processi di cybersecurity (design, implementazione e revisione continua), dovremo darci nel corso degli interventi alcune regole per il rispetto dei principi di governance, facendo tutto il possibile perché anche il nostro committente si adegui, anche se non è stato (ancora) investito ufficialmente dell’incarico di Project Manager del Security Program dell'intera azienda.

Fare questo è di importanza fondamentale per

* **La correttezza formale del nostro intervento**. Se oggi non vi è consapevolezza diffusa dell’aspetto Governance, in futuro può emergere o alcuni potenziali clienti possono già averla. Potremmo essere giudicati negativamente se la trascuriamo.
* **Beneficio per il cliente**. In una attività di controllo quale la cybersecurity solo la Governance può garantire la giusta intensità operativa e il rispetto di policy e procedures. Nel controllo ‘manca’ un ‘prodotto’ da consegnare al cliente entro tempi prestabiliti che stimoli l’intensità quotidiana dell’impegno.
* **Beneficio per l’intervento di consulenza**. Un intervento di consulenza e audit che copra lo spettro completo di standard e normative non è fattibile se non in tempi lunghissimi. Definire con il cliente ambito (scope) dell’intervento è essenziale. Solo l’autorità di Governance di cui è investito il Project Manager del Security Program può decidere Scope e Priorità. Questo richiede una puntualizzazione anche del concetto di Maturity Level, vedi il seguente punto 5). E’ importante che sia il cliente e non il consulente a prendersi responsabilità su cosa è prioritario affrontare. Questo renderà più facile condividere senza obiezioni il report finale.

Propongo che queste regole per il rispetto dei principi di governance siano inserite nella parte introduttiva delle linee guida per i consulenti.

Per quanto riguarda le policies e procedures di alto livello ricorrerò agli LLM e a risorse open source (ad es. SANS institute) per proporre al cliente un set di template da personalizzare, dal quale egli dovrà scegliere, diciamo circa 10, policies da definire nel corso dell’intervento.

Naturalmente lavoreremo nell’ipotesi che le policies di alto livello siano “aziendali” e non di reparto o servizio. Abbiamo detto che il nostro committente è (è come fosse) il Program Manager del Security Program dell’intera azienda.

Anche su questo sto sperimentando un processo LLM assisted perché sarebbe un ‘plus’ produrre template di policy personalizzati in base a dati raccolti presso il cliente (interviste e documenti).

#### 5) Maturity Level

Ritengo che l’aspetto del Maturity Level del Security Program del produttore debba essere necessariamente affrontato nell’intervento di consulenza. Unitamente al Security Level della macchina o del componente il Maturity Level è parte delle garanzie che il produttore offre al cliente sulla affidabilità del proprio prodotto.

Il Maturity Level riflette il grado di maturità dei processi di sicurezza di un’organizzazione (es. in base a standard come IEC 62443-2-1 o ISO 27001), mentre il Security Level definisce i requisiti tecnici (IEC 62443-3-3 e 4-2). Insieme, forniscono un quadro completo dell’affidabilità del prodotto e del sistema di gestione della sicurezza.

Dovrò sottolineare questo aspetto nel corso di formazione e dovremo in qualche modo inserire un commento/valutazione nel report.

Sottolineare il Maturity Level nella consulenza e nella formazione dimostra un approccio olistico, che non si limita ai requisiti tecnici ma considera anche la capacità organizzativa del cliente, oltre ad essere un elemento chiave della 62443.

Ipotizzo che il quadro sinottico come alla pag. 7 di Proposta Cyber Security\_BRETON Spa.pptx.pdf, ricavabile dalla matrice di analisi, possa fornire gli elementi per una valutazione del Maturity Level. Di fatto lo spirito di quella sintesi è quello di una valutazione del Maturity Level.

Sottolineare questo aspetto con il cliente, sin dalla formazione e dai colloqui con il responsabile e i suoi collaboratori, si collega all’aspetto Governance+Scope+Priorità. Non si può fare tutto subito, si deve partire da ciò che è più urgente e ha più valore. Il Maturity Level più alto si raggiunge col tempo.

Questo:

* Rinforza l’importanza della Governance, vedi 4), poiché il Maturity Level dipende da come l’organizzazione gestisce la sicurezza.
* Sostiene l’idea che “non si può fare tutto subito”, promuovendo un percorso graduale verso un Maturity Level più alto.
* Coinvolge il cliente nella definizione delle priorità, rendendo il report finale più accettabile, vedi 4).

| **1. Matrice di Analisi (Excel)** ● Descrizione: Realizzazione di un file Excel contenente una matrice completa di tutti i punti da analizzare durante le consulenze.  ● Specifiche:  ○ La matrice deve fare riferimento alle normative IEC 62443-3-3, 4.1 e 4.2.  ○ Deve includere collegamenti ad altre normative pertinenti, come la ISO 27001 e la NIS 2.  ○ Per il mercato europeo, oltre alla NIS 2, si devono considerare normative specifiche del settore come la Direttiva Macchine (MD) e la Cyber Resilience Act (CRA).  ○ Per il mercato nordamericano, si dovranno includere riferimenti alle normative NIST (National Institute of Standards and Technology) e alle linee guida di agenzie come la CISA (Cybersecurity and Infrastructure Security Agency).  ● Tempo di consegna: bozza entro metà settembre, definitivo entro fine settembre  ● Premio: json per future implementazioni che metta in relazione tutti i requirements, i riferimenti alle altra normativa 62443 e le altre normative considerate, le bozze di policy, le bozze di procedure, i riferimenti ai manuali dei prodotti prodotti Siemens (lista prodotti  TBD), Intouch (lista prodotti TBD) e txone (lista prodotti TBD) per l’implementazione  -> consegna dicembre | Mi sembra di capire che la matrice di analisi ha gli stessi contenuti delle check list al punto 4. Audit.  Se ciò che interessa è fornire una visione sinottica come alla pag. 7 di Proposta Cyber Security\_BRETON Spa.pptx.pdf, si tratta di una view sugli stessi dati.  Come espresso al punto “Premio”, il valore di questo obiettivo è nella struttura dei dati, di processi (4.1) e requirements (3-3 e 4-2) della 62443 e di controlli di altre norme e standard.  Come struttura dell’Excel, da utilizzarsi anche per l’Audit, propongo di prendere spunto da quella del NIST CSF 2 <https://docs.google.com/spreadsheets/d/1uVPq_9z-9X2sBg-bOxweE2-4LKJmzhsZ/edit?gid=493799187#gid=493799187> oltre che da quella di Carel [https://docs.google.com/spreadsheets/d/1Jn\_EDLxROhF9gZpswxpj6nhjR3LsB4TDFTyWk4pBDVM/edit?gid=851105920#gid=851105920.](https://docs.google.com/spreadsheets/d/1Jn_EDLxROhF9gZpswxpj6nhjR3LsB4TDFTyWk4pBDVM/edit?gid=851105920#gid=851105920)  Una macro potrebbe produrre i dati per il quadro sinottico per il report. |
| --- | --- |
| **2. Materiali per la Formazione dei Clienti** ● Descrizione: Creazione di un set di slide per i corsi di formazione destinati ai clienti.  ● Specifiche:  ○ Deve includere una parte introduttiva generale sulla normativa 62443 (struttura generale, dettagli delle sezioni dedicate a end users, system integrators, components suppliers, aspetti legati alla governance) e sulle altre normative citate nell' excel (NIS 2, ISO 27001...).  ○ Deve contenere sezioni specifiche per la 62443-3-3 (per system integrator e produttori di macchine) e per la 62443-4.1 e 4.2 (per lo sviluppo software in ambito ICS).  ● Tempo di consegna: bozza entro fine agosto, definitivo entro metà settembre  ● Premio: erogazione corsi di formazione a interni e clienti -> consegna secondo scaletta | E’ importante una stima dei tempi delle lezioni, è difficile sintetizzare e dilatare ad hoc i tempi su argomenti complessi. |
| **3. Bozza di Policy e Procedure** ● Descrizione: Redazione di bozze e template per le policy e le procedure che i consulenti applicheranno presso i clienti.  ● Specifiche:  ○ Le linee guida devono essere sufficientemente dettagliate per essere adattate a casi specifici, come la gestione delle password... (es. complessità, frequenza di cambio).  ○ Il materiale servirà come traccia per chi si interfaccerà con il cliente, conoscendo l'automazione ma non necessariamente la normativa in dettaglio.  ● Tempo di consegna: bozza entro fine settembre, definitivo entro metà ottobre  ● Premio: bozze policy e procedure per prodotti Siemens (lista prodotti TBD), Intouch (lista prodotti TBD) e txone (lista prodotti TBD) -> consegna fine novembre | Policies e procedures debbono essere redatte dal cliente decidendo le regole su COME implementare il CHE COSA chiesto dai requirements di standard e norme. Noi potremo fornirgli dei templates che lui deve personalizzare, la produzione deve essere sua responsabilità.  Vedi sopra puntualizzazione 3). |
| **4. Documento per l'Audit** ● Descrizione: Preparazione di un documento con le domande puntuali da porre ai clienti durante l'audit.  ● Specifiche:  ○ Le domande dovranno essere specifiche per le sezioni 4.1 e 4.2, e ci sarà anche un documento a parte per la 3.3.  ● Tempo di consegna: bozza entro fine settembre, definitivo entro metà ottobre  ● Premio: audit su cliente pilota Breton (assieme a esperto automazione)  -> consegna secondo scaletta | Parliamo di audit   1. del processo di sviluppo del software (SSDL), volume 4.1 della 62443? 2. della impostazione delle misure di protezione della macchina, volumi 3-3 e 4-2?   Io sarei favorevole a fare entrambi. Vi sono elementi di complessità ma credo sia necessario affrontarli.  Il punto 1) può essere un documento con domande puntuali.  Il punto 2) deve essere una procedura più complessa che consista nei seguenti step:   1. raccolta dettagliata dei dati della macchina: componenti, flussi di dati e trust boundaries; 2. esecuzione con l’aiuto della IA e del cliente del Threat Model e produzione dell’elenco minacce; 3. recupero con l’aiuto della IA dei component requirements 4.2 e 3.3 in base alle minacce rilevate; 4. audit (o gap analysis) della implementazione delle contromisure.   Sto lavorando per impostare un LLM assisted Audit della macchina. Una procedure rieseguibile il cui input iniziale sono i dati della macchina.  Vedi sopra puntualizzazione 2). |
| **5. Schema per il Report Finale** ● Descrizione: Creazione di uno schema o una traccia per il report finale da consegnare al cliente.  ● Specifiche:  ○ Il report dovrà integrare i contenuti dell'analisi (come la matrice Excel) e le bozze di policy e procedure.  ○ Dovrà essere strutturato in modo da poter accogliere anche i risultati dell'analisi della rete condotta dall'Università di Padova.  ● Tempo di consegna: bozza entro metà ottobre, definitivo entro fine ottobre  ● Premio: redazione report finale su cliente pilota Breton (assieme a esperto automazione)  -> consegna secondo scaletta | Ok.  Difficile fare ipotesi ora prima di avere delineato i componenti che, riassumendo, sono:   1. matrice Excel, solo quadro sinottico o dettaglio? 2. bozze policy e procedures, direi in allegato 1? 3. data Università di padova, in allegato 2? Da rieditare? 4. analisi del software ??? |
| 6. **Master Deck Promozionale** ● Descrizione: Sviluppo di una presentazione completa per la promozione dei servizi.  ● Specifiche:  ○ Il documento deve includere tutti gli aspetti delle soluzioni offerte, come la consulenza e la formazione, con esempi e usecase sviluppati sui due clienti pilota Piovan e Breton.  ○ Servirà come base per estrarre contenuti per brochure, cataloghi, post su LinkedIn, articoli e presentazioni per i venditori.  ○ Il materiale promozionale deve essere conforme allo spirito delle norme e degli standard.  ● Tempo di consegna: bozza entro metà settembre, definitivo entro fine settembre  ● Premio: includere anche gli strumenti offerti da logbot nel master deck. Le specifiche degli strumenti saranno definite con il supporto del team tecnico di logbot. | Gli usecase sviluppati sui due clienti pilota Piovan e Breton mi sembrano incompatibili con i tempi di consegna.  Gli spunti sono già tanti, ma qui mi manca un esempio, un punto di partenza. Qualche esempio, anche di altre aziende o di scuola? O anche qui mi affido agli LLM? |
| **7. Articoli Tecnici** ● Descrizione: Scrittura di 5 articoli tecnici specifici per la pubblicazione su riviste, sul sito web o per altre occasioni promozionali.  ● Specifiche: Gli articoli dovranno trattare argomenti tecnici e riflettere l'approccio dell'azienda alla governance.  ● Tempo di consegna: uno al mese per ogni mese da agosto a settembre  ● Premio: whitepaper ed articolo per il sole 24 ore -> consegna secondo scaletta | Titoli proposti  **Avviare con l’AI un Security Program secondo IEC 62443 e normative macchine per Produttori e Integratori di Sistema** Spiega come iniziare un programma di sicurezza conforme a 62443 e altre normative macchine; definire policies di alto livello; definire policies per sviluppo software, sviluppo componenti e integrazione macchine; produrre check list di audit. Il tutto personalizzato in base al contesto aziendale e ai sistemi utilizzati, con tempi e costi ridotti grazie all’aiuto dell’AI.  **Governare la Cybersecurity per potenziare digital-core e crescita di mercato per Produttori e Integratori di Sistema** Focalizzato sulla Governance, per mostrare come l’adeguamento agli standard di sicurezza è sinergico alla reinvenzione dei processi aziendali in ottica di digitalizzazione e crescita produttiva.  **Sviluppare Componenti e Sistemi IACS con un orientamento al Cliente** Security Level e Maturity Level sono il segno esteriore più evidente di una serie di reinvenzioni del processo di produzione di componenti e sistemi che mirano a soddisfare tutte le esigenze del cliente, funzionali, produttive e di sicurezza. Imparare ad inserire nei propri processi un orientamento al cliente significa attivare canali formali e informali di comunicazione con lui e le sue esigenze che lo rassicurano e lo fidelizzano.  **Audit di Sicurezza Sistemi IACS con Supporto AI per Produttori e Integratori di Sistema** Mostra come usare l’AI per predisporre più velocemente audit più efficaci, mirati al contesto tecnologico del produttore o integratore di sistema.  **Strategia di Cybersecurity Logbot per OEM** Promozionale, con focus su come Logbot mette a punto strumenti tecnologici e servizi di formazione e consulenza per ridurre al minimo i costi per le aziende nel pieno rispetto di standard e norme. Grazie alla familiarità delle procedure organizzative e delle pratiche operative in contesto OT/ICS, grazie alla conoscenza delle macchine e grazie al supporto di AI ed LLM per generare soluzioni ritagliate sui requisiti dei clienti. |
| **Timeline attività già previste:** - Inizio settembre: ingaggio agenzie per attività di promozione  - Inizio settembre: corso interno a collaboratori che faranno gli interventi dai clienti (nuovo assunto Siemens, Emanuele...)  - Fine settembre: corso breton  - Inizio ottobre: webinar factory software  - Metà ottobre: audit breton  - Metà ottobre: fiera A&T  - Metà ottobre: corso Starpool  - Fine ottobre: relazione Piovan  - Novembre: 2o corso fenice  - Novembre: corso factory | Per eventuali trasferte dovrai darmi 100 euro di rimborso spese oltre al compenso complessivo pattuito.  Io viaggerò in treno + mezzi pubblici + taxi.  Perchè relazione Piovan e audit Breton?  Fiera A&T: quanti giorni? |
| **Modalità e compensi:** ● Totale attività 10k€ liquidato mensilmente da agosto a dicembre  ● Premio 2.5k€ liquidato a fine anno  ● Report mensile attività (consegna deliverables) per eventuale rendicontazione bandi (concordare con adm)  ● ATECO consulenza (verificare con adm)  ● CV firmato per eventuale rendicontazione bandi (verificare con adm)  Da definire ASAP contratto e aspetti tecnici ingaggio | 1. **Report mensile**: può andare un ‘rendicontazione.md’ in una cartella ‘Pianificazione attività’, del package ‘cybersecurity-kit’, in un formato concordato con adm? 2. **ATECO e CV**:    * Per l’ATECO, pensavo a 70.22.09 per la consulenza in cybersecurity. Verifico con adm.    * Per il CV firmato, serve in formato Europass o basta un PDF con le mie esperienze? Verifico con adm. 3. **Contratto**:    * Redazione a cura di adm? |

### **Domande su gestione attività**

[Torna su](#_14qh4d6xv0b)

**Riunioni regolari**: Che ne dici di fare un check veloce, tipo 10-15 minuti ogni 2-3 giorni, per aggiornarci sui task? O preferisci una volta a settimana per mezz’ora? Così teniamo tutto sotto controllo, soprattutto con le scadenze strette di agosto e settembre.

**Collaborazione con Emanuele**: Puoi dirmi di più sul suo ruolo? Può aiutarmi con le macchine? Devo passargli info o formarlo su normative come IEC 62443? Come impostiamo il lavoro insieme!

**Dati sulle macchine**: Per preparare l’LLM assisted Audit della macchina, mi servono al più presto dati sulle macchine Siemens, Intouch e txOne che mi ha preannunciato. Posso averli subito?

**Richieste dati per Breton e Piovan**: possiamo chiedere dati preliminari sulle loro macchine, visto che sono piloti? Per interventi standard, i dati sarà meglio raccoglierli all’inizio dell’intervento, ma essendo piloti, possiamo chiedere a Breton e Piovan un elenco dei componenti (PLC, HMI, ecc.) o schemi di rete ora? Siamo già in contatto con loro? Posso preparare un template di richiesta? O meglio aspettare l’inizio ufficiale, magari a settembre?

## Puntualizzazioni su contratto

[Torna su](#_14qh4d6xv0b)

Ok a quanto proponi, con queste puntualizzazioni:

* per le trasferte devi riconoscermi 100 euro al giorno di rimborso spese. Viaggerò in treno + mezzi pubblici + taxi.
* vi è una concentrazione di attività nel mese di settembre; per ora non modificherei le scadenze ma occorre tenere in conto probabili slittamenti. Emanuele potrà collaborare? Lavoreremo assieme?
* vi sono attività i cui contenuti sono da definire: durata delle lezioni nella formazione, documentazione macchine Siemens, Intouch , txOne, contenuti degli articoli (ho fatto alcune proposte io, vedi sopra)