Come Endian Secure Digital Platform contribuisce a soddisfare la IEC 62443 compliance

Con l'implementazione e la rapida diffusione della digital transformation nei mercati industriali la necessità di cybersecurity diventa fondamentale. Fortunatamente ci si è resi conto di questo molto presto e sono stati quindi istituiti gli standard di sicurezza IEC 62443 (precedentemente conosciuti come ISA 99) per fornire paradigmi di sicurezza che si adattassero a tutte le applicazioni industriali. Gli standard IEC 62443 consentono agli operatori industriali di individuare e mitigare i rischi di cybersecurity su tutti i processi, dispositivi e reti. Lo standard è articolato in 4 categorie principali, ciascuna con propri componenti rilevanti (Figura 1).

© 2023 Endian SRL. Soggetto a modifica senza preavviso. Endian e Endian UTM sono marchi di Endian SRL. Tutti gli altri marchi e marchi registrati sono di proprietà dei loro rispettivi proprietari.

Figura 1: IEC 62443

Ruoli e responsabilità

Lo Standard IEC 62443 definisce 3 ruoli primari che sono incaricati di progettare, implementare e gestire i sistemi di industriali di controllo e automazione (IACS).

- **Asset Owner:** Responsabile per le operazioni e il mantenimento dei sistemi IACS
- **System Integrator:** Responsabile dell'integrazione e il collaudo di prodotti IACS e componenti
- **Product Supplier (Vendor):** Responsabile per lo sviluppo e i test dei prodotti IACS

Endian come fornitore (Vendor) si occupa di sviluppare e testare la Secure Digital Platform che include lo Switchboard col ruolo di componente centrale, e la serie 4i Edge come device da installare in campo. Ciò significa che Endian Secure Digital Platform è solo una parte di un più vasto sistema di persone, processi e prodotti che ogni azienda deve coinvolgere per soddisfare i requisiti di IEC 62443. In altre parole la soluzione Endian è uno strumento che, quando configurato e utilizzato correttamente, può contribuire al raggiungimento della compliance del IEC 62443, per ciò che riguarda i servizi forniti.

© 2023 Endian SRL. Soggetto a modifica senza preavviso. Endian e Endian UTM sono marchi di Endian SRL. Tutti gli altri marchi e marchi registrati sono di proprietà dei loro rispettivi proprietari.

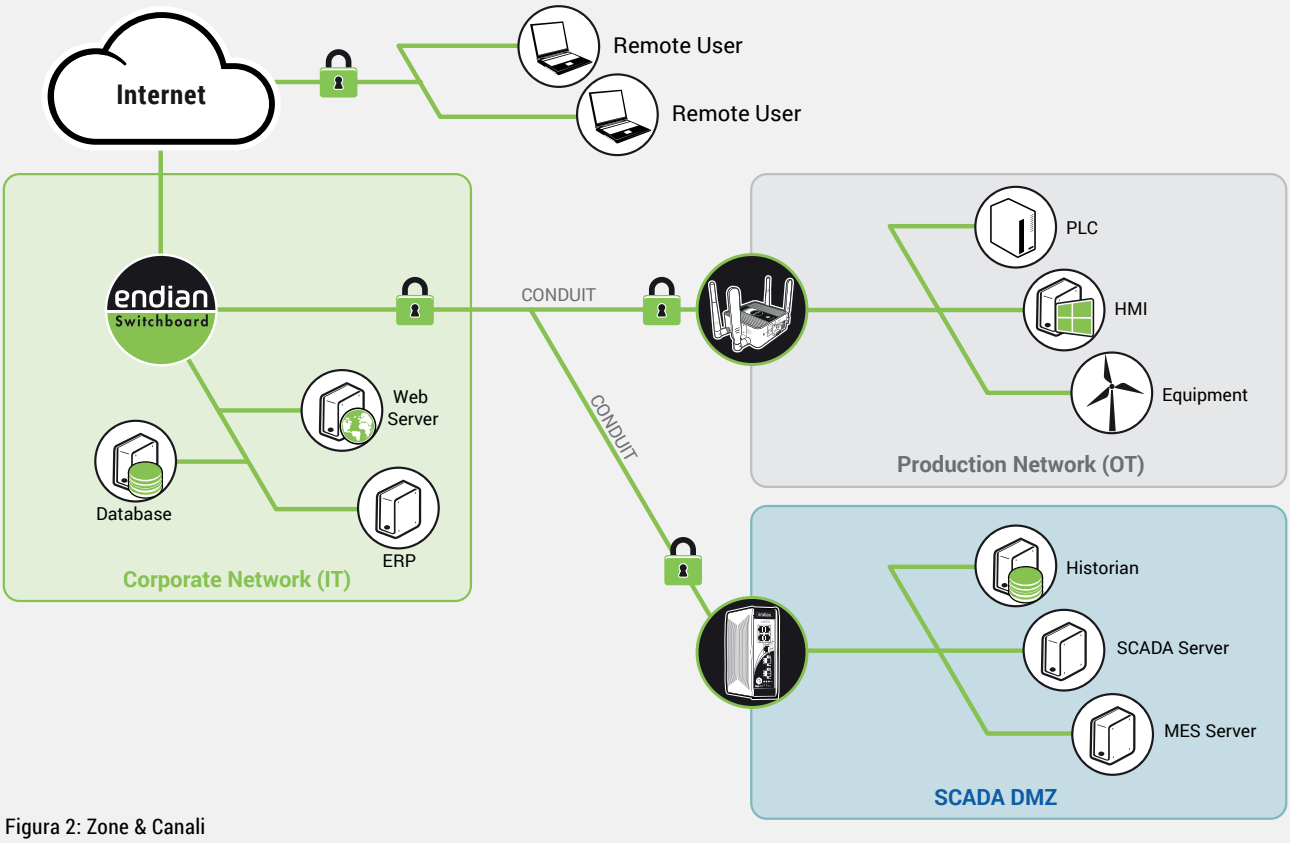

Figura 2: Zone & Canali

Zone e Canali

Lo Standard IEC 62443 descrive una tecnica di separazione della rete conosciuta come “zones and conduits” (zone e canali). In pratica, utilizzando questo metodo si suddividono gli asset industriali in gruppi logici che hanno lo stesso protocollo di comunicazione o gli stessi pattern all’interno delle zone, ed essi vengono quindi interconnessi gli uni con gli altri attraverso tunnel sicuri, utilizzando il firewall, dove il traffico tra le zone è strettamente controllato e monitorato. (Figura 2). Grazie a questa best practice un’azienda può isolare i device per tipo e limitare la diffusione di un eventuale danno su tutti gli altri asset. Inoltre, viene minimizzato il rischio di accesso accidentale o non autorizzato tra le zone. I prodotti Endian 4i Edge permettono proprio l’esecuzione di questi condotti con segmentazione della rete e sicurezza avanzata, includendo controlli firewall (in tutte le direzioni) potenti ma facili da usare, e tecnologia deep-packet inspection con intrusion detection/prevention.

Standard di sicurezza

Lo standard IEC 62443 nelle sezioni 3-3 e 4-2 identifica una lista di requisiti raggruppati in categorie logiche. Questi requisiti specificano i processi e la tecnologia che un prodotto e un sistema devono contenere per corrispondere ai diversi livelli di sicurezza previsti dallo standard. Qui di seguito individuiamo le principali funzionalità di Endian Secure Digital Platform che possono contribuire all’adeguamento ai parametri del IEC 62443 (parti 3-3 e 4-2). E’ importante notare che questa lista non è esaustiva e che alcuni requisiti dello standard 62443 non si applicano per varie ragioni.

© 2023 Endian SRL. Soggetto a modifica senza preavviso. Endian e Endian UTM sono marchi di Endian SRL. Tutti gli altri marchi e marchi registrati sono di proprietà dei loro rispettivi proprietari.

FR 1/ CR 1: Identificazione e Authentication Control

- User/Group account e gestione permessi
- Supporto Active Directory / LDAP
- Supporto Two-factor authentication
- Supporto PKI con certificato X.509
- Opzioni self-service per reset della password
- Richiesta di cambio password o invio email per creazione password iniziale
- Brute force account lockout
- Timeout dell'utente per inattività

FR 2 / CR 2: Identificazione e Authentication Control

- User/Group account e gestione permessi
- Supporto Active Directory / LDAP
- Permessi definiti possono essere aggiunti/rimossi dall'account utente
- Timeout per termine sessione
- Brute force account lockout
- Timeout dell'utente per inattività
- Audit completo dei log abilitato di default
- Tutti gli eventi dell'utente sono loggati all'audit log

FR 3 / CR 3: Integrità del sistem

- Strong VPN encryption utilizzata per tutte le comunicazioni
- I protocolli standard rafforzano i comuni controlli di integrità
- Audit logs archiviati in modo sicuro
- Software updates e upgrades regolari
- Endian fornisce release note con change log per ciascun update/upgrade

FR 4 / CR 4: Confidenzialità dei dati

- Strong VPN encryption utilizzata per tutte le comunicazioni
- La piattaforma supporta esclusivamente algoritmi e chiavi crittografiche avanzate
- Il factory reset elimina tutte le informazioni sensibili
- La soluzione garantisce un'elevata confidenzialità delle informazioni

© 2023 Endian SRL. Soggetto a modifica senza preavviso. Endian e Endian UTM sono marchi di Endian SRL. Tutti gli altri marchi e marchi registrati sono di proprietà dei loro rispettivi proprietari.

FR 5 / CR 5: Trasmissione dei dati riservati

- Tutti i prodotti supportano la segmentazione della rete con zone multiple
- La sicurezza del firewall protegge le zone interne di default
- Il content-filtering rafforza le policy di sicurezza
- Stateful firewall protegge e monitora il traffico in tutte le direzioni
- La tecnologia deep-packet inspection controlla e impedisce attacchi avanzati

FR 6 / CR 6: Reazione tempestiva agli eventi

- Accesso in sola lettura all'audit dei log
- I meccanismi di sicurezza assicurano il monitoraggio continuo

FR 7 / CR 7: Disponibilità delle risorse

- La piattaforma utilizza potenti meccanismi di DoS (Denial of Service)
- Impostazioni di back-up one-time o schedulati assicurano un veloce ripristino del sistema
- Opzioni di elevata scalabilità impediscono colli di bottiglia su utenti o device
- I prodotti prevedono una configurazione sicura di default

Conclusioni

Grazie a quanto descritto sopra, Endian Secure Digital Platform può rappresentare un elemento cruciale nel raggiungimento della compliance dello standard IEC 62443, specialmente per ciò che riguarda l'accesso remoto, la network security (canali e zone) e il monitoraggio della rete. Per scoprire di più sui vantaggi delle soluzioni Endian o per metterti in contatto con un nostro consulente commerciale, visita il nostro sito www.endian.com.

© 2023 Endian SRL. Soggetto a modifica senza preavviso. Endian e Endian UTM sono marchi di Endian SRL. Tutti gli altri marchi e marchi registrati sono di proprietà dei loro rispettivi proprietari.