TECHNICAL CYBERSECURITY ASSESSMENT

CRA Technical Evidence Pack

Evidenze tecniche, gap analysis e remediation roadmap per un prodotto embedded connesso

FAC-SIMILE DIMOSTRATIVO

Titolo	CRA Technical Evidence Pack
Codice	SLX-CRA-TEP-001
Versione	1.0
Data	16 agosto 2026
Cliente / Progetto	Caso applicativo - IG-200 Industrial Edge Gateway

Documento pubblico a finalità dimostrativa. I dati del cliente, del prodotto e i finding sono inventati; il contenuto non può essere presentato come assessment reale o evidenza di conformità.

Via Uccellino 9, 44028 Poggio Renatico | www.siliconlogix.it | mpezzullo@siliconlogix.it
Partita IVA: 02189310382

Controllo documento

Titolo	CRA Technical Evidence Pack
Codice documento	SLX-CRA-TEP-001
Cliente	Silicon LogiX · caso applicativo
Prodotto	IG-200 Industrial Edge Gateway · HW Rev. B · IGOS 2.4.1
Revisione	1.0
Stato	FAC-SIMILE / Esempio
Classificazione	Pubblico - Fac-simile dimostrativo
Data	16 agosto 2026

Registro revisioni

Rev.	Data	Descrizione	Autore
1.0	16 agosto 2026	Prima emissione del fac-simile	Silicon LogiX

Uso del documento
Questo fac-simile illustra struttura, terminologia e livello di dettaglio di un possibile deliverable. Prima di un incarico reale il contenuto va adattato al prodotto, al perimetro concordato, alle evidenze disponibili e alla procedura di conformità applicabile.

Posizionamento del deliverable
“CRA Technical Evidence Pack” è una denominazione commerciale del servizio Silicon LogiX, non il nome di un documento previsto dal Regolamento (UE) 2024/2847. Il Pack organizza evidenze tecniche, gap e azioni utili a supportare la documentazione tecnica e il percorso di conformità del fabbricante; non sostituisce la responsabilità del fabbricante, una valutazione legale, la dichiarazione UE di conformità, la marcatura CE o l’eventuale valutazione di un organismo notificato.

0. Executive Summary

Oggetto dell’esempio. Caso applicativo del CRA Technical Evidence Pack su IG-200 Industrial Edge Gateway, con baseline hardware/software versionata, SBOM, superficie esposta, update A/B, finding e remediation. I dati e i risultati del fac-simile sono esemplificativi.

Indicatore	Risultato fac-simile	Lettura
Aree tecniche valutate	22	Controlli e processi selezionati nel perimetro
OK	8	Evidenza sufficiente nel perimetro
PARZIALE	7	Evidenza o controllo incompleto
GAP	5	Intervento tecnico/processo prioritario
NON VERIFICATO	2	Fuori scope o evidenza non disponibile

Top findings

ID	Finding	Stato	Priorità
IG200-F-001	Il percorso recovery non applica la stessa verifica di autenticità del normale update A/B.	GAP	ALTA
IG200-F-002	JTAG/UART accessibili nella configurazione di produzione; policy di protezione non documentata.	GAP	ALTA
IG200-F-003	Snapshot CycloneDX ricostruito; manca una SBOM generata dalla build e legata deterministicamente alla release IGOS.	GAP	ALTA
IG200-F-004	Manca una policy CVD pubblicabile e un contatto dedicato per vulnerability reporting.	GAP	ALTA
IG200-F-007	Nessun gate formalizzato sulle vulnerabilità note prima del rilascio.	GAP	ALTA

Valutazione sintetica
IG-200 dispone di una base tecnica strutturata (TLS 1.3, update A/B, ruoli e factory reset), ma la readiness è limitata dall'assenza di una SBOM di release e da gap nella recovery, nelle interfacce di debug e nel vulnerability handling. La priorità è consolidare questi prerequisiti e renderli tracciabili nella prossima release IGOS.

1. Finalità, utilizzo e limiti del Pack

Finalità. Il Pack organizza in un unico dossier le evidenze tecniche disponibili per la baseline valutata e rende visibili i gap che devono essere chiusi o giustificati. Può essere usato come input alla documentazione tecnica del fabbricante, alle review interne e al confronto con specialisti di conformità.

- Non è un certificato CRA e non contiene una dichiarazione di conformità.
- Lo stato "OK" indica soltanto che, nel test/perimetro concordato, è stata osservata un'evidenza tecnica coerente con il criterio valutato.
- La classificazione del prodotto, la procedura di valutazione applicabile e le decisioni legali restano responsabilità del fabbricante e delle figure competenti.
- Il Pack va aggiornato quando cambiano baseline, dipendenze, superficie esposta, update path o support period.

Contesto normativo al 16/08/2026
Il CRA è in vigore. Gli obblighi di reporting dell'articolo 14 iniziano ad applicarsi l'11 settembre 2026; i principali obblighi del Regolamento diventano applicabili dall'11 dicembre 2027. Questo fac-simile va quindi considerato uno strumento di readiness e preparazione tecnica.

2. Baseline di prodotto

Nome prodotto	IG-200 Industrial Edge Gateway
Produttore	Silicon LogiX · caso applicativo
Hardware	Rev. B · ARM Cortex-A53 · 1 GB RAM · 8 GB eMMC · 2× GbE · RS-485 isolata · USB service · UART/JTAG
Firmware	IGOS 2.4.1 · U-Boot 2024.01 · Linux 6.1 LTS · Gateway Core 3.2.0 · Web UI 1.8.2
Software terze parti	Linux kernel 6.1.y; BusyBox 1.36.1; OpenSSL 3.0.13; libmodbus 3.1.10 (dati esemplificativi)
Connettività	HTTPS Web UI/REST; MQTT 5/TLS 1.3 outbound; Modbus RTU/TCP verso la rete di campo
Update	Immagini A/B firmate distribuite dal release service; recovery locale via USB service
Support period dichiarato	5 anni dalla data di immissione sul mercato — motivazione da completare nel fac-simile
Assessment boundary	IG-200 HW Rev. B, IGOS 2.4.1, U-Boot, Linux image, Gateway Core, Web UI, interfacce e update A/B. Backend applicativo escluso.

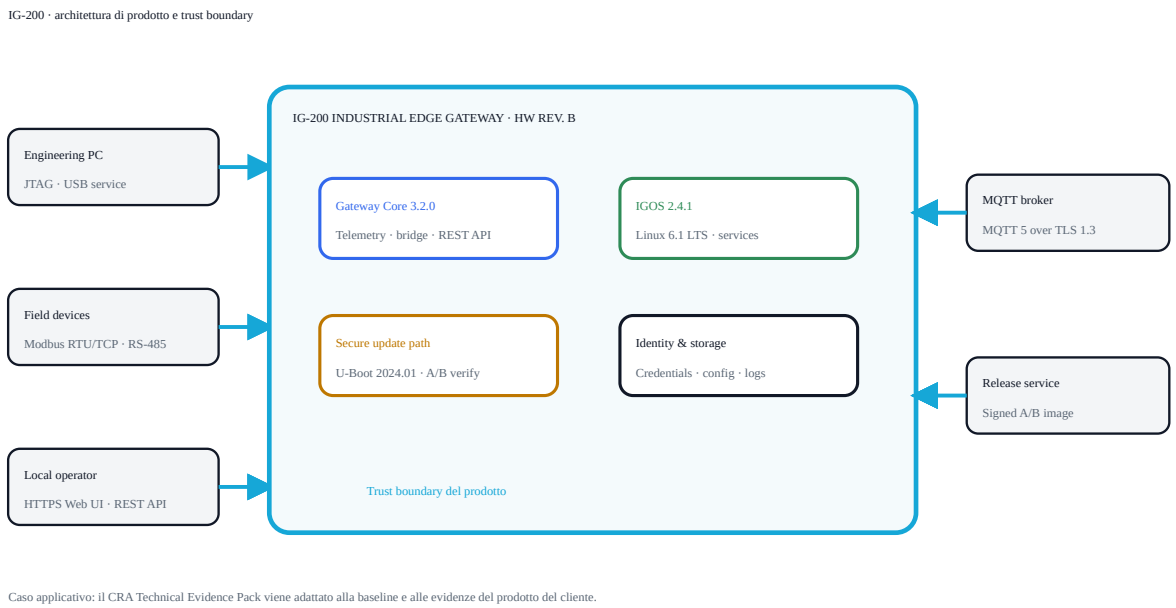

Figura 1 — Architettura IG-200 e principali trust boundary considerati nel Technical Evidence Pack.

3. Uso previsto, ambiente e asset da proteggere

3.1 Uso previsto

Il dispositivo è destinato a essere integrato in una macchina industriale e a svolgere funzioni di acquisizione telemetria, esposizione dati locali, ricezione di parametri autorizzati e invio dati a un broker MQTT. Non è progettato per essere direttamente esposto a Internet.

3.2 Ambiente ragionevolmente prevedibile

- Rete di stabilimento con possibili segmenti legacy e dispositivi di terze parti.
- Accesso locale di manutentori tramite browser e USB service.
- Connessione outbound verso broker/servizio remoto configurato dal cliente.
- Possibilità di accesso fisico al quadro macchina da parte di personale tecnico.
- Ciclo di vita superiore a una singola release firmware, con necessità di security update in campo.

3.3 Asset critici

Asset	Obiettivo di sicurezza	Impatto se compromesso
Firmware e boot chain	Integrità / autenticità	Esecuzione di codice non autorizzato, persistenza
Credenziali e chiavi	Confidenzialità / integrità	Accesso non autorizzato, impersonificazione
Configurazione macchina	Integrità / disponibilità	Parametri errati, indisponibilità del servizio

Asset	Obiettivo di sicurezza	Impatto se compromesso
Telemetria	Integrità / confidenzialità secondo contesto	Decisioni errate, leakage di dati operativi
Update package	Autenticità / integrità	Installazione di release alterate
Log di sicurezza	Integrità / disponibilità	Ridotta capacità di rilevare/ricostruire eventi

4. Architettura, trust boundary e flussi

Flusso	Origine → Destinazione	Protocollo	Trust decision
F1	Browser manutentore → Web UI	HTTPS	Autenticazione locale; TLS richiesto
F2	PLC/SCADA → IG-200	Modbus TCP	Rete di campo; nessuna assunzione di trust assoluto
F3	IG-200 → Broker	MQTT 5/TLS 1.3	Verifica certificato server + credenziale dispositivo
F4	Release service → IG-200	HTTPS/package	Pacchetto firmato; verifica nel bootloader
F5	Engineering PC → JTAG	Debug fisico	Da limitare/proteggere sulle unità di produzione
F6	Engineering PC → USB service/recovery	Servizio locale	Recovery autenticata e vincolata alla stessa policy di image verification

> **Osservazione chiave**
> Le difese di rete esterne non vengono considerate sostitutive dei controlli di sicurezza del prodotto. Il rischio viene valutato anche rispetto a usi ragionevolmente prevedibili e condizioni operative reali.

5. Software inventory e SBOM

Stato. Partendo dall'inventario preliminare, l'assessment ha ricostruito uno snapshot CycloneDX per IGOS 2.4.1. Lo snapshot non è ancora generato in modo deterministico dalla pipeline né associato all'immagine A/B di release; il finding IG200-F-003 resta quindi aperto.

Componente	Versione esempio	Origine	Funzione	Evidence
Gateway Core	3.2.0	Proprietario	Protocol bridge / REST API	Build manifest
U-Boot	2024.01	Open source	Boot, verify, rollback	Repository tag
Linux kernel	6.1.y	Open source	kernel	component manifest
BusyBox	1.36.1	Open source	userland/services	component manifest

Componente	Versione esempio	Origine	Funzione	Evidence
OpenSSL	3.0.13	Open source	TLS / crypto	component manifest
libmodbus	3.1.10	Open source	Modbus RTU/TCP	manual inventory

Finding collegato · IG200-F-003
La SBOM di release non è ancora disponibile. Azione raccomandata: generarla nella pipeline IGOS, versionarla e associare digest e component inventory all'immagine A/B distribuita.

6. Superficie esposta e interfacce

Interfaccia	Esposizione	Controllo osservato	Stato	Note
Ethernet HTTPS / REST	Locale / rete stabilimento	TLS + login ruoli	OK	HTTP non esposto; redirect disabilitato
MQTT 5/TLS 1.3	Outbound	TLS server auth + device credential	OK	Backend fuori scope
Modbus TCP	Rete campo	ACL applicative e matrice comandi incomplete	PARZIALE	Dipende dall'architettura di rete; limitare funzioni/porte
USB service	Fisica	Recovery tool	PARZIALE	Verifica recovery non equivalente al normale update A/B
JTAG	Fisica	Connettore test pad	GAP	Policy JTAG di produzione non documentata
UART service	Interna	Header non popolato	PARZIALE	Definire policy produzione e logging

7. Cybersecurity risk assessment — estratto

Metodo fac-simile. Rischio inerente = Probabilità (1–5) × Impatto (1–5). Il valore residuo viene ricalcolato considerando soltanto controlli verificati/documentati. La matrice è un metodo interno di prioritizzazione, non una scala prescritta dal CRA.

Scenario	Asset	P	I	Rischio	Controlli	Residuo
Installazione di IGOS non autorizzato via recovery	Firmware	3	5	15 · Alto	Verify incompleta sulla recovery	12 · Alto
Accesso debug a dispositivo in campo	Chiavi/config	3	4	12 · Alto	Accesso fisico al quadro	9 · Medio
Credenziale Web UI amministrativa compromessa	Config/Web UI	3	4	12 · Alto	Password unique + lockout parziale	6 · Medio

Scenario	Asset	P	I	Rischio	Controlli	Residuo
Manipolazione traffico cloud	Telemetria	2	4	8 · Medio	MQTT 5/TLS 1.3 + server validation	3 · Basso
Vulnerabilità in un componente Linux non rilevata	Firmware	3	4	12 · Alto	Inventario manuale + review ad hoc	8 · Medio
Perdita tracciabilità evento security	Log	3	3	9 · Medio	Logging limitato	6 · Medio

8. Mappatura tecnica — Allegato I, Parte I

Ref.	Area sintetica	Evidenza attesa	Stato	Osservazione
I.1	Livello di cybersecurity appropriato al rischio	Risk assessment documentato, security baseline	PARZIALE	Risk model presente; baseline da formalizzare
I.2(a)	Assenza di vulnerabilità note sfruttabili al market release	Dependency/vulnerability gate release	NON VERIFICATO	Processo di release non valutato end-to-end
I.2(b)	Secure by default	Credenziali uniche; servizi minimi; reset sicuro	PARZIALE	Modbus, REST e service interfaces da rivedere
I.2(c)	Vulnerabilità gestibili tramite security update	OTA + recovery + rollback	PARZIALE	Recovery path non applica verify equivalente
I.2(d)	Protezione da accessi non autorizzati	Ruoli, autenticazione, lockout	PARZIALE	JTAG/UART non governati in produzione
I.2(e)	Confidenzialità dei dati	TLS; storage sensibile	OK	TLS verificato sul flusso MQTT/HTTPS
I.2(f)	Integrità di dati/comandi/configurazione	TLS; signed update; config checks	PARZIALE	Update recovery gap
I.2(g)	Data minimisation	Telemetria limitata a dataset configurato	OK	Nessun dato personale nell'esempio
I.2(h)	Disponibilità delle funzioni essenziali	Watchdog; recovery; safe mode	OK	Test di recovery documentato
I.2(i)	Riduzione impatto su reti/servizi	Rate limit / reconnect backoff	OK	MQTT reconnect backoff verificato
I.2(j)	Limitazione attack surface	Service inventory; debug policy	GAP	Inventario servizi e policy JTAG/UART incompleti
I.2(k)	Mitigazione impatto incidenti	Least privilege; service isolation; watchdog	PARZIALE	Permessi, capability e hardening servizi non baselineizzati
I.2(l)	Security logging/monitoring	Auth/update/security events	PARZIALE	Log insufficienti per alcune azioni admin

Ref.	Area sintetica	Evidenza attesa	Stato	Osservazione
I.2(m)	Rimozione sicura di dati/impostazioni	Factory reset + key erase	OK	Procedura verificata su campione

Nota interpretativa
La tabella è un mapping tecnico di lavoro. La formulazione ufficiale e l'applicabilità dei requisiti devono essere sempre ricontrollate sul testo vigente del Regolamento e sulla valutazione dei rischi specifica del prodotto.

9. Mappatura tecnica — Allegato I, Parte II (vulnerability handling)

Ref.	Area	Evidenza corrente	Stato	Azione
II.1	Componenti/vulnerabilità + SBOM machine-readable	Inventario preliminare; SBOM release assente	PARZIALE	Automatizzare e collegare alla release
II.2	Remediation senza ritardo / security updates	Processo interno non formalizzato	GAP	Definire SLA/triage e release flow
II.3	Test e review di sicurezza regolari	Test di regressione; review sporadiche	PARZIALE	Definire cadence e security gates
II.4	Disclosure informazioni su vulnerabilità corrette	Nessun template advisory	GAP	Preparare advisory workflow
II.5	Coordinated vulnerability disclosure policy	Assente	GAP	Pubblicare policy e scope
II.6	Canale per segnalazione vulnerabilità	Support mailbox generica	PARZIALE	Creare security contact dedicato
II.7	Distribuzione sicura aggiornamenti	Signed A/B update; recovery differente	PARZIALE	Uniformare verification policy
II.8	Security update tempestivi e accompagnati da advisory	Release notes generiche	PARZIALE	Separare contenuti security e istruzioni utente

10. Update, rollback e recovery

Percorso	Pacchetto	Verifica	Rollback	Stato
Remote A/B update	Signed bundle	Firma + hash nel bootloader	A/B slot + last-known-good	OK
Local service update	Signed bundle	Firma + hash nel bootloader	Manuale	OK

Percorso	Pacchetto	Verifica	Rollback	Stato
USB recovery	Raw image service	Hash soltanto	Recovery-only	GAP
Factory programming	Provisioning image via JTAG	Controllo procedurale	N/A	PARZIALE

IG200-F-001 · High
La recovery path rappresenta una deviazione dalla catena di fiducia del normale update A/B. La remediation prioritaria è applicare la stessa autenticazione dell'immagine a ogni percorso che può installare firmware persistente, incluse procedure di recovery/manutenzione.

11. Vulnerability handling e support period

Processo	Stato corrente	Target minimo
Vulnerability intake	Support mailbox generica	security@ / web form + CVD policy
Triage	Gestito caso per caso da R&D	Severity + ownership + target remediation
Dependency monitoring	Manuale prima di release principali	Automazione continua/SBOM diff
Security advisory	Release note generica	Template advisory con prodotto/versione/impatto/mitigazione
Reporting CRA	Non ancora formalizzato	Runbook interno per obblighi applicabili dal 11/09/2026
Support period	5 anni dichiarati	Motivazione documentata, dipendenze e capacità di patching
EOL/EOS	Comunicazione commerciale	Processo con end-date support, decommissioning e archive policy

IG200-F-004 · High
Manca una policy di coordinated vulnerability disclosure utilizzabile pubblicamente e un punto di contatto dedicato. Il gap è di processo, ma incide direttamente sulla capacità di ricevere, triagiare e documentare vulnerabilità.

12. Security test evidence

Test / review	Baseline	Esito	Evidence ID	Nota
Update tamper test	IGOS 2.4.1	Pass su OTA / Fail su recovery	IG200-E-UPD-004	Recovery accetta immagine non autenticata
TLS server validation	IGOS 2.4.1	Pass	IG200-E-NET-011	Certificato invalido rifiutato

Test / review	Baseline	Esito	Evidence ID	Nota
Default credential review	IGOS factory image	Pass	IG200-E-ID-003	Password iniziale unique per unità
Debug access review	HW Rev. B	Fail readiness	IG200-E-HW-007	JTAG accessibile nella configurazione di produzione
Factory reset / data erase	IGOS 2.4.1	Pass	IG200-E-DATA-002	Credenziali e config rimosse
Security log coverage	IGOS 2.4.1	Partial	IG200-E-LOG-006	Mancano eventi su alcune modifiche ruolo

Nota: in un incarico reale ogni Evidence ID rimanderebbe a report, screenshot, hash, test log, commit/tag o documento sotto controllo versione.

13. Findings register — estratto

ID	Area	Finding	Stato	Priorità	Owner	Recommended action
IG200-F-001	Update/ Recovery	Recovery image senza verifica di autenticità equivalente	GAP	ALTA	Firmware/ Bootloader	Allineare recovery a signed-image verification; aggiungere negative test
IG200-F-002	Hardware hardening	JTAG/UART disponibili in produzione; policy non documentata	GAP	ALTA	HW/Firmware	Definire protection state, provisioning e recovery autorizzata
IG200-F-003	SBOM	Snapshot CycloneDX ricostruito; manca una SBOM generata e legata deterministicamente alla release	GAP	ALTA	Build/Release	Generazione automatica; digest associato all'immagine IGOS
IG200-F-004	Vulnerability handling	CVD policy e security contact dedicato assenti	GAP	ALTA	Product/ Security	Definire policy, canale, triage e disclosure workflow
IG200-F-005	Lifecycle	Support period senza razionale tecnico documentato	PARZIALE	MEDIA	Product/R&D	Documentare expected use, component support e capacità update
IG200-F-006	Logging	Copertura incompleta eventi amministrativi/security	PARZIALE	MEDIA	Firmware	Estendere event taxonomy e retention/export
IG200-F-007	Release gate	Nessun gate formalizzato su vulnerabilità note prima del rilascio	GAP	ALTA	Release/ Security	Vulnerability check + exception approval + evidence
IG200-F-008	Attack surface	Servizi di rete, privilegi e policy UART/service non completamente inventariati	PARZIALE	MEDIA	Gateway/ Manufacturing	Mappare socket/privilegi; definire UART/service policy e controllo BOM

ID	Area	Finding	Stato	Priorità	Owner	Recommended action
IG200-F-009	Identity	Provisioning e lockout account amministratore da completare	PARZIALE	MEDIA	Firmware	Rate limit/backoff + audit event
IG200-F-010	Decommissioning	Factory reset verificato ma istruzioni utente non ancora formalizzate	PARZIALE	BASSA	Product Docs	Aggiungere secure decommissioning instructions

14. Remediation roadmap

Finestra	Obiettivo	Azioni principali	Output verificabile
0–30 giorni	Chiudere prerequisiti critici	IG200-F-001 recovery verify; IG200-F-002 debug policy; IG200-F-003 SBOM; IG200-F-004 CVD/contact; IG200-F-007 release gate	U-Boot/recovery test; JTAG policy; SBOM pipeline; CVD draft; release checklist
30–60 giorni	Rendere la release tracciabile	IG200-F-006 logging; IG200-F-008 service inventory; IG200-F-009 auth hardening	Service inventory; event catalog; negative auth tests; SBOM delta check
60–90 giorni	Consolidare lifecycle evidence	IG200-F-005 support-period rationale; IG200-F-010 user/decommission docs; retest finding	Lifecycle memo; updated user instructions; closure evidence
Continuativo	Mantenere evidenze e vulnerabilità	Dependency monitoring; security review cadence; advisory/reporting runbook	Dashboard/process records; recurring review evidence

Remediation support
Silicon LogiX può proseguire dall'assessment all'implementazione delle modifiche su firmware/software, alla revisione dell'update chain, all'automazione SBOM e alla produzione delle evidenze di chiusura. Ogni attività di remediation viene però quotata e baselineizzata separatamente.

15. Mappa delle evidenze verso l'Allegato VII

Ref.	Elemento	Dove si trova	Copertura	Nota
VII.1	Descrizione generale, uso previsto, versioni SW, immagini/info utente	Sez. 2–3 + product docs	PARZIALE	Istruzioni utente da completare
VII.2(a)	Design/development, schemi, system architecture	Sez. 4 + Figura 1 + IG200-E-ARCH-*	OK	Architettura baseline disponibile
VII.2(b)	Vulnerability handling, SBOM, CVD, contatto, secure update	Sez. 5, 10, 11	PARZIALE	CVD/contact gap; recovery gap
VII.2(c)	Produzione/monitoring/validation process	Manufacturing docs	NON VERIFICATO	Fuori scope del fac-simile

Ref.	Elemento	Dove si trova	Copertura	Nota
VII.3	Cybersecurity risk assessment	Sez. 7–9	PARZIALE	Da estendere alla documentazione finale del fabbricante
VII.4	Informazioni per determinare support period	Sez. 11	PARZIALE	IG200-F-005
VII.5	Standard/common specs/cert schemes o soluzioni adottate	Open item	NON VERIFICATO	Da definire sul percorso reale
VII.6	Report dei test di conformità/security	Sez. 12 + evidence index	PARZIALE	Solo test selezionati nel fac-simile
VII.7	EU declaration of conformity	Non inclusa	N/A	Responsabilità del fabbricante
VII.8	SBOM su richiesta motivata dell'autorità, ove applicabile	SBOM snapshot / machine-readable	PARZIALE	Artifact di esempio

16. Evidence index — esempio

Evidence ID	Descrizione	Tipo	Versione/Data	Livello
IG200-E-ARCH-001	System architecture IG-200 HW Rev. B	Diagramma/ Documento	1.2	Documentato
IG200-E-SBOM-002	CycloneDX snapshot ricostruito IGOS 2.4.1	JSON	sha256: example…	Documentato
IG200-E-UPD-004	Update tamper negative test	Test report	2026-08-10	Verificato
IG200-E-HW-007	Debug access inspection	Test note/photo	2026-08-10	Verificato
IG200-E-NET-011	TLS invalid cert test	Test log	2026-08-11	Verificato
IG200-E-ID-003	Factory credential provisioning note	Manufacturing note	rev 0.7	Documentato
IG200-E-DATA-002	Factory reset verification	Test report	2026-08-11	Verificato
IG200-E-LOG-006	Security event coverage	Review note	2026-08-12	Verificato

A. SBOM Snapshot — esempio illustrativo

Nota. Le versioni riportate sono esclusivamente illustrative. In un incarico reale ogni entry deve essere derivata dalla build/release valutata e includere gli identificatori necessari a garantirne la tracciabilità.

Component	Version	License	Supplier	Role	Identifier
Gateway Core	3.2.0	proprietary	Silicon LogiX	gateway application	pkg:generic/gateway-core@3.2.0
U-Boot	2024.01	GPL-2.0-or-later	DENX / U-Boot project	bootloader	pkg:generic/u-boot@2024.01
Linux kernel	6.1.y	GPL-2.0-only	Linux community	kernel	pkg:generic/linux@6.1
BusyBox	1.36.1	GPL-2.0-only	BusyBox project	userland	pkg:generic/busybox@1.36.1
OpenSSL	3.0.13	Apache-2.0	OpenSSL project	crypto/TLS	pkg:generic/openssl@3.0.13
libmodbus	3.1.10	LGPL-2.1-or-later	libmodbus project	industrial protocol	pkg:generic/libmodbus@3.1.10

B. Finding record — formato completo

Finding ID	IG200-F-001
Titolo	Recovery path: autenticità immagine non uniformemente verificata
Area	Update / boot chain
Stato	GAP
Priorità	ALTA
Baseline	HW Rev. B · IGOS 2.4.1 · U-Boot 2024.01
Evidence	IG200-E-UPD-004, IG200-E-ARCH-001
Owner suggerito	Firmware / Product Security
Target	IGOS 2.5.x

Osservazione

L’aggiornamento A/B standard verifica firma e digest dell’immagine prima dell’attivazione. La modalità USB recovery, pensata per ripristino in assistenza, verifica soltanto l’integrità tramite hash e non applica la stessa autenticazione della normale catena di update.

Impatto tecnico

Un attore con accesso al canale recovery potrebbe tentare di installare un'immagine non autorizzata. Il finding indebolisce la fiducia nella boot/update chain e rende incoerenti le evidenze tra i diversi percorsi di installazione firmware.

Recommended action

Uniformare formato e policy di verifica delle immagini su update A/B, service update e recovery. Aggiungere test negativi per firma non valida, downgrade non autorizzato, immagine corrotta e interruzione dell'update. Documentare eventuali eccezioni e recovery autorizzate.

Closure evidence

- Test report con rifiuto di immagini non firmate/modificate su ogni percorso.
- Versione bootloader/recovery aggiornata e collegata alla baseline prodotto.
- Descrizione della update chain e delle chiavi/ruoli senza esporre materiale segreto.
- Release note e approvazione del finding closure.

Riferimenti normativi e informativi

Regolamento (UE) 2024/2847 (Cyber Resilience Act) — testo ufficiale EUR-Lex: Regulation (EU) 2024/2847

Commissione europea — Cyber Resilience Act: pagina ufficiale

Commissione europea — guidance CRA C(2026) 5252: Guidance C(2026) 5252

Verificato al 16/08/2026. La guidance non vincolante della Commissione C(2026) 5252 del 27/07/2026 è inclusa tra i riferimenti; atti di esecuzione, standard armonizzati, common specifications e guidance successivi devono essere riesaminati prima di ogni incarico reale.