

ESEMPIO DI CONSEGNA / VA

Vulnerability assessment

Inventario. Applicabilità. Priorità motivata.



Perimetro del campione

Tre asset fittizi APP-01, DEP-02 e HOST-03. Nessun punteggio scanner, EPSS o CVSS è inventato o presentato come misurazione reale.

Come leggere questo documento

Questo estratto rende visibile la struttura di una consegna. Riscontri, attività e date del racconto sono sintetici, salvo l'impronta del file campione ricalcolabile. Il contenuto di un incarico effettivo viene definito con il committente.

Il percorso documentato.

01 / Inventario minimo

Per ogni asset: proprietario, funzione, prodotto, versione, esposizione e criticità del servizio. Per DEP-02 occorre anche il lockfile o una SBOM con versioni effettive.

02 / Riscontri del campione

APP-01: versione non documentata, applicabilità da verificare. DEP-02: componente elencato nell'inventario, corrispondenza al pacchetto ancora da confermare. HOST-03: configurazione riferita dal responsabile, non osservata direttamente.

03 / Decisione sulla priorità

Prima azione: completare versioni e perimetro. Se una CVE risulta applicabile, leggere fonte del produttore, gravità e vettore, EPSS con data, presenza KEV, esposizione e controlli. Non sommare questi indicatori in un punteggio arbitrario.

04 / Remediation e verifica

Registro: rilievo, responsabile, azione, scadenza concordata, prova di correzione, esito del retest e rischio residuo. Una segnalazione non verificata conserva lo stato "da confermare".

Criterio di riesame

Il pannello EPSS dell'Hub consente una consultazione reale per CVE. Ogni risultato mostra la data della fonte e distingue dato assente da errore di accesso; non dimostra da solo che un asset sia vulnerabile.

Approfondisci: <https://consuleria.org/vulnerability-assessment/>