WORKSHOP GARR 2026

NET MAKERS

SecHawk: dalla scansione SCARR al monitoraggio proattivo nella rete GARR

Lorenzo Fava

GARR

SCARR

Servizio di scansione di vulnerabilità di GARR, basato su OpenVAS.

ACCESSO	interfaccia web · API
UNA RICHIESTA	cosa scansionare · quando · ogni quanto · chi avvisare
REPORT	in più formati, per esempio pdf o xml

SecHawk legge il report in formato xml.

> **SecHawk nasce attorno a SCARR:** è il motore di tutte le scansioni.

Il punto di partenza: scansioni a mano

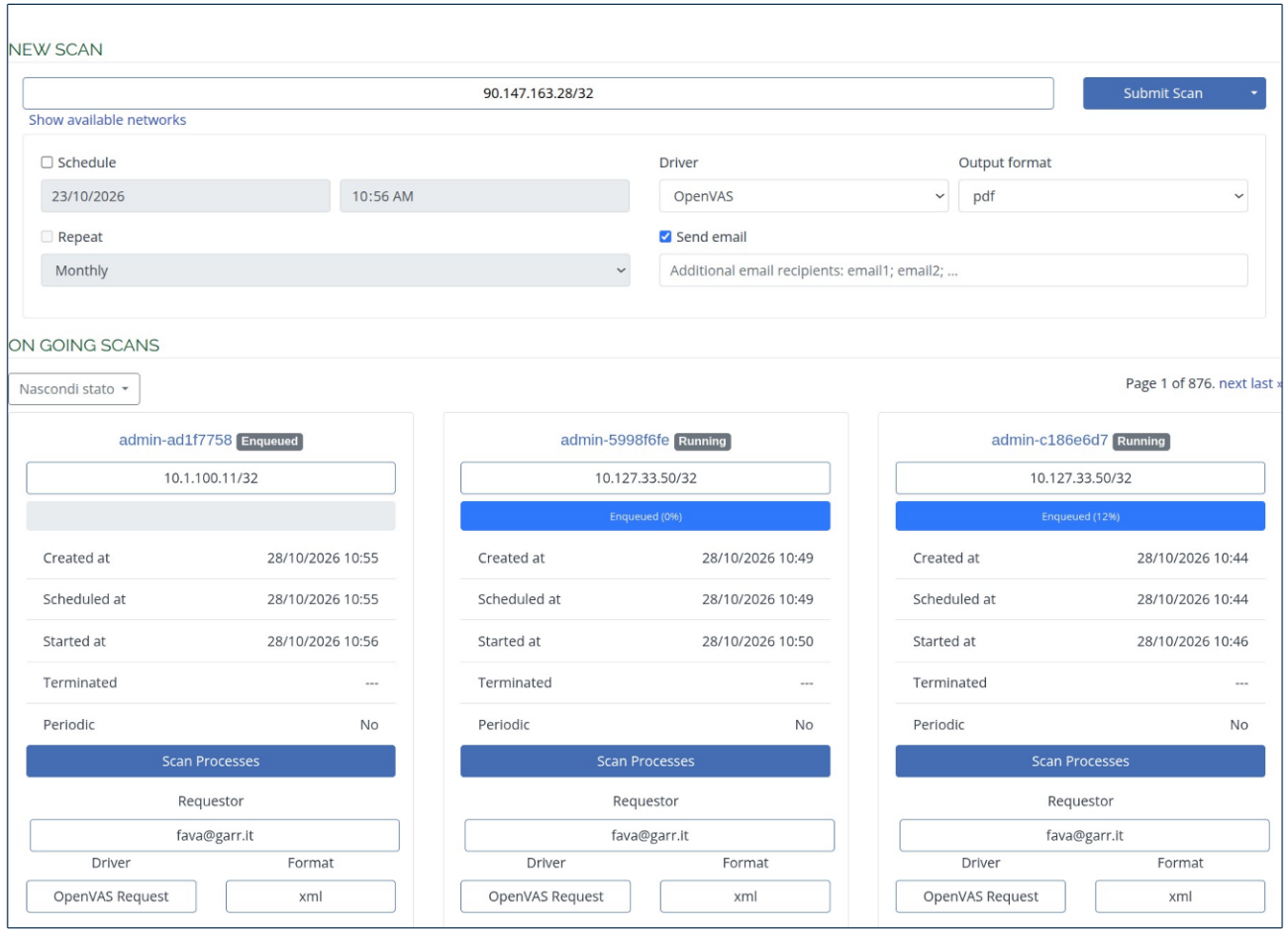
01 Lanciare le scansioni su SCARR per la regione cloud GARR

02 Scaricare i report

03 Estrarre le vulnerabilità con degli script

04 Risalire a progetto e utente di ogni IP

05 Scrivere a mano una mail a ogni utente



SCARR, nuova scansione e scansioni in corso

SecHawk v0: da report a mail, in automatico

SecHawk

AUTOMATICO, A OGNI SCANSIONE COMPLETATA

SCARR
scansione completata

Download
dei report completati

Arricchimento
API dei progetti: mail del proprietario, VM, progetto

Mail
testo leggibile per il proprietario

COSA ARRIVA ALL'UTENTE

Una mail per proprietario, raggruppata per progetto e per host.

Vulnerabilità ordinate per gravità.

Scritta perché chi la riceve capisca cosa fare.

USO INTERNO

Una dashboard minimale su Grafana: solo per noi, e poco leggibile.

Dal cloud a tutte le nostre reti

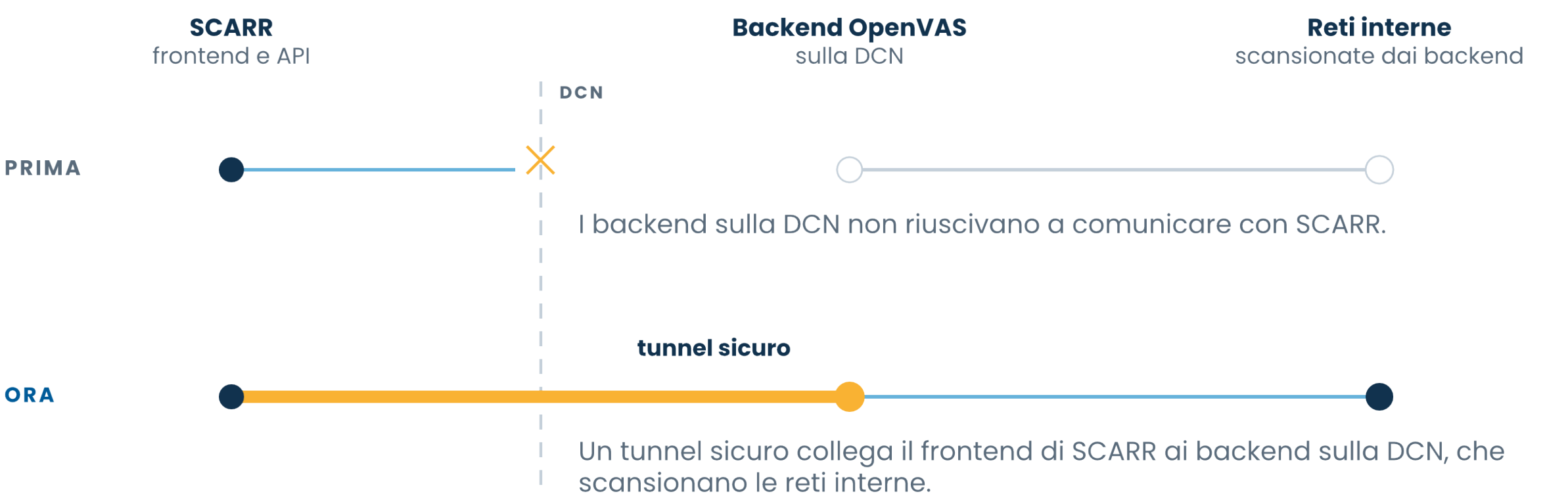
Siamo partiti automatizzando gli avvisi per la cloud GARR. Poi abbiamo scelto di estendere il sistema a tutte le nostre reti interne, e per farlo la mail non bastava più.

I LIMITI DELLA MAIL

01	**Non vede le reti interne** Le scansioni coprivano solo il cloud: le reti interne restavano al buio.	1
02	**Non sa a chi scrivere** Un IP interno non ha progetto né proprietario: prima bisogna sapere cosa c'è.	2
03	**Non ha memoria** Ogni mail è una fotografia: non dice da quando c'è, né se è stata risolta.	2
04	**Non dà una vista d'insieme** Tante mail sparse, nessun posto dove vedere stato e priorità.	2

1 · Vedere: scansioni delle reti interne → **2 · Tenere traccia: SecHawk v1**

Primo passo: scansionare le reti interne



SecHawk v1

SecHawk

Dalla mail alla piattaforma: non basta avvisare, bisogna tenere traccia.

01	**Inventario vivo**	Host con identità, progetto e owner sempre aggiornati
02	**Storia delle vulnerabilità**	Prima vista, ultima vista, risolta, riaperta
03	**Scansioni autonome**	Pianificate da una policy di priorità, non a mano
04	**Multi-tenant**	Ogni team vede solo il proprio perimetro
05	**Open data**	API ed export per altri sistemi
06	**Una dashboard vera**	Il punto di accesso per tutti

Architettura

WORKSHOP GARR 2026

NET MAKERS

Le azioni

SecHawk

FUORI DA SECHAWK

SCARR
esegue le scansioni e restituisce i report

NetBox e OpenStack
sanno di chi è ogni macchina

Fonti sulle minacce
exploit noti, probabilità di sfruttamento

SECHAWK

1 **Pianifica** decide chi scansionare e quando

2 **Raccoglie** scarica i report delle scansioni completate

3 **Interpreta** estrae le vulnerabilità e ne tiene la storia

4 **Arricchisce** associa ogni macchina a progetto e proprietario, e aggiunge informazioni sulle minacce

ARCHIVIO CONDIVISO database e storage

VERSO GLI UTENTI

Email ai proprietari
avvisi a chi deve intervenire

Dashboard e API
per team GARR

I componenti

SecHawk

Una pipeline ogni 15 minuti

PIPELINE · CRONJOB OGNI 15'

SCARR
sorgente delle scansioni

01
monitor
scarica i report buoni (senza errori, solo /32 autorizzati) su S3

02
xml-parser
XML → JSON; classifica gli IP. Report inutilizzabile: errore

03
vuln-logger
upsert in MongoDB per host, IP, porta, CVE, OID; marca le risolte

04
sechawk-sync
host da NetBox/OpenStack; dismette quelli spariti da 30 giorni

S3 incoming → processing → parsed → archive

MONGODB vulnerabilità · host · storico

SERVIZI DI SUPPORTO

PIANIFICAZIONE
scheduler
Una scansione per IP (/32), cooldown di 168 h, max 15 attive. Priorità: mai scansionato per primo, poi ritardo e gravità.

PARLA CON · SCARR

INTELLIGENCE
enrichment
Sincronizza KEV, EPSS, ExploitDB, Metasploit e NVD; aggiorna i dettagli CVE.

SCRIVE IN · MongoDB

CONSULTAZIONE
sechawk-api → dashboard
sechawk-api (FastAPI) e sechawk-dashboard (React + Nginx); SSO Keycloak e notifiche SMTP.

PER · team GARR

La vita di un host

Dalla subnet alla vulnerabilità

WORKSHOP GARR 2026

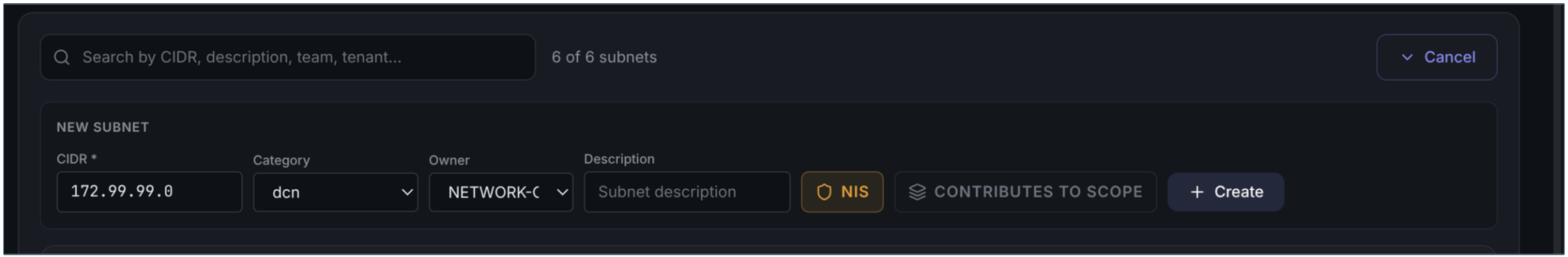
NET MAKERS

L'admin aggiunge una subnet

SecHawk

T0

La subnet è subito operativa: classifica gli host e autorizza le scansioni.



POST /subnets

subnet	**172.99.99.0/24**
tenant	**dcn**
team	**network-ops**
nis_relevant	**true**
status	**active**

01 Validazione: CIDR valido, niente duplicati, sovrapposizioni solo se annidate.

02 Ricalcolo di categoria, team e NIS sugli host presenti. Vince la subnet più specifica; il resto si eredita.

03 Nessuna chiamata a NetBox e nessuna scansione: la discovery arriva al prossimo sync.

Da IP a host: l'identità arriva da NetBox

SecHawk

T+1h

Di solito i dati arrivano da OpenStack o NetBox: qui da NetBox, perché l'IP è di un device.

DA IP A SITE · FONTE: NETBOX

172.99.99.99 → **dcn-sw-core-01** → **Bologna**

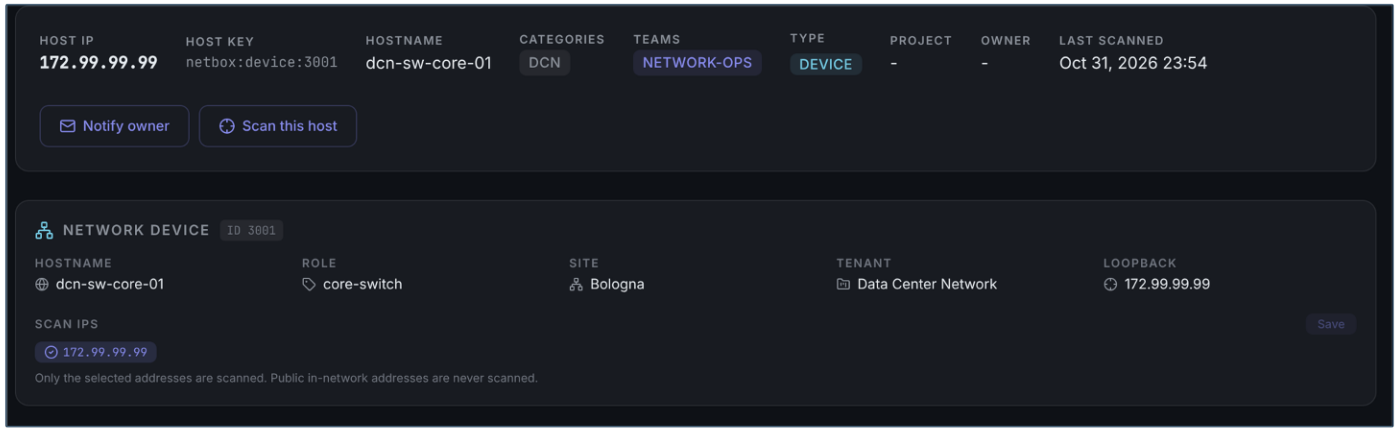
Loopback assegnato a un device

Device di rete · ruolo ammesso

Site · tenant Data Center Network

L'HOST IN hosts · CATEGORIA E TEAM DALLA SUBNET

hostname	**dcn-sw-core-01**
host key	**netbox:device:3001**
site	**Bologna**
categoria	**dcn · network-ops**
progetto	**-**
owner	**-**



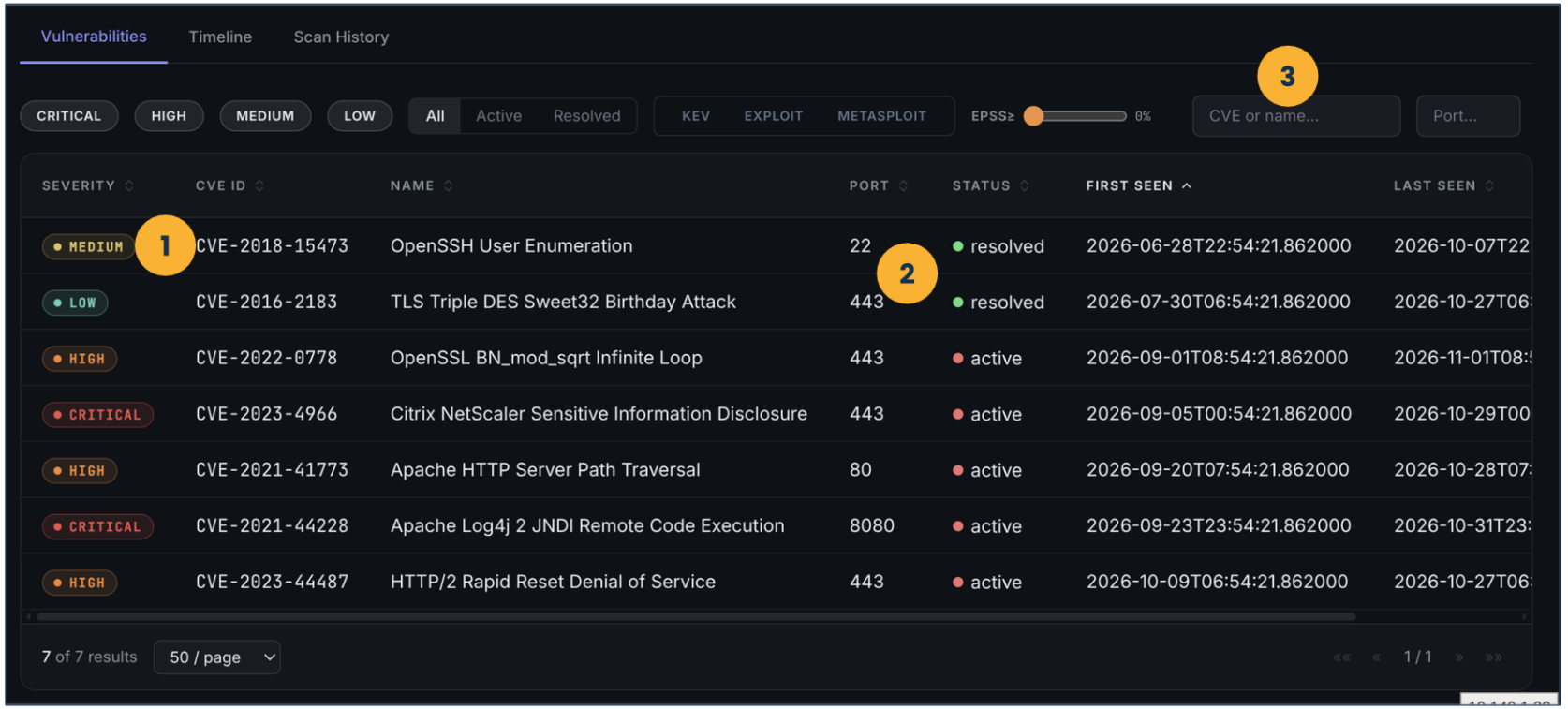
Le vulnerabilità restano legate all'host, non all'IP.

Cosa trova su dcn-sw-core-01

SecHawk

T+2h

Il report diventa una tabella: 7 vulnerabilità, 5 attive e 2 risolte.



1 Severità
2 critical e 3 high attive; medium e low risolte. Critical da CVSS 9.

2 Stato
Nuova, risolta, riaperta: restano in tabella con prima e ultima visita, senza duplicati.

3 Filtri
Severità, stato, KEV, exploit, Metasploit, EPSS, CVE e porta.

Il VPR nel dettaglio

SecHawk

T+2h





1. **VPR**
   Pesa CVSS, EPSS, KEV, exploit e Metasploit. Con CVSS 10: Log4Shell 10,0, senza segnali 4,03.

2. **EPSS**
   Probabilità di sfruttamento nei prossimi 30 giorni

3. **CVSS**
   Vettore e metriche, una per una

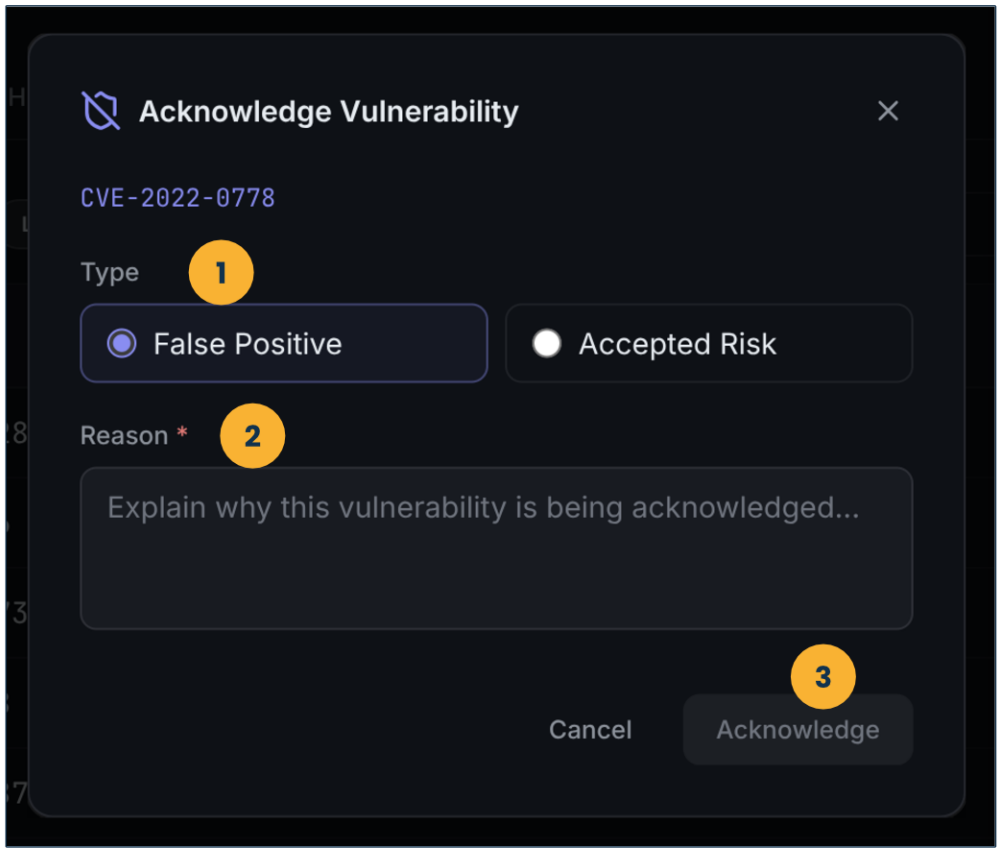
4. **Exploit e patch**
   Se c'è un exploit pubblico e se c'è una patch

ACK: falso positivo o rischio accettato

SecHawk

T+2h

Un finding si può marcare come gestito, sempre con una motivazione.



1 **Il tipo**
Falso positivo: la vulnerabilità non esiste. Rischio accettato: esiste, ma si decide di conviverci.

2 **La motivazione**
È obbligatoria: finché è vuota, il pulsante Acknowledge resta disabilitato.

3 **Il registro**
Ogni azione finisce nell'audit log, in sola aggiunta.

La dashboard: panoramica

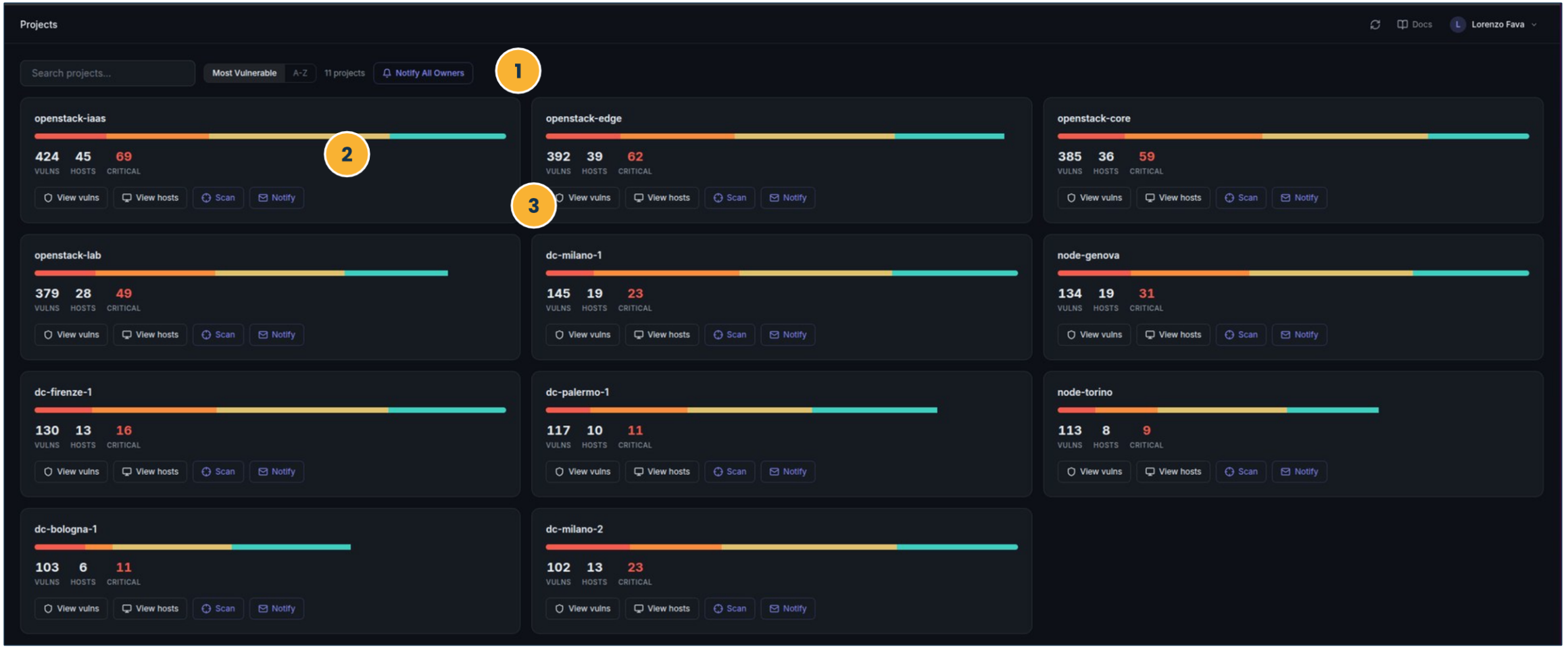
SecHawk



1. **KPI di severità**
   Critical, high, medium, low, risolte
2. **Threat intelligence**
   KEV, exploit, Metasploit, EPSS alto
3. **Trend**
   Vulnerabilità per severità, nel tempo
4. **Scansioni al giorno**
   Quante, e quando
5. **Distribuzione**
   Per severità, con il totale

La dashboard: vista per progetto

SecHawk



1 Notify All Owners **2** Vulnerabilità, host e critical per progetto **3** View vulns · View hosts · Scan · Notify

Cosa ci portiamo a casa

Scansioni a mano
report, script, una mail alla volta

SecHawk v0
dal report alla mail, in automatico

Reti interne
scansioni dalla DCN, via tunnel

SecHawk v1
tracciabilità e dashboard

2.074
host in inventario
2.021 attivi, su 67 subnet

276
scansioni al giorno
media degli ultimi 30 giorni

7,3 giorni
per riscansionare ogni host
cooldown minimo di 7 giorni per host

PROSSIMI PASSI

Più copertura delle reti, più integrazioni, più automazione.

Domande?

Lorenzo Fava · Consortium GARR

WORKSHOP GARR 2026

NET MAKERS