SCARR: nuove funzionalità per la sicurezza delle reti

Vincenzo Caracciolo

GARR

WORKSHOP GARR 2021

NET MAKERS

Consortium GARR

SCARR (SCAnsioni Ripetute a Richiesta)

Cos'è?

Servizio per effettuare scansioni di vulnerabilità

A chi è rivolto?

Agli APM GARR, per scansioni sulla propria rete di competenza

Come si usa?

Fruibile in modalità self-service

Dove lo trovo

https://scarr.garr.it/
scarr-service@garr.it

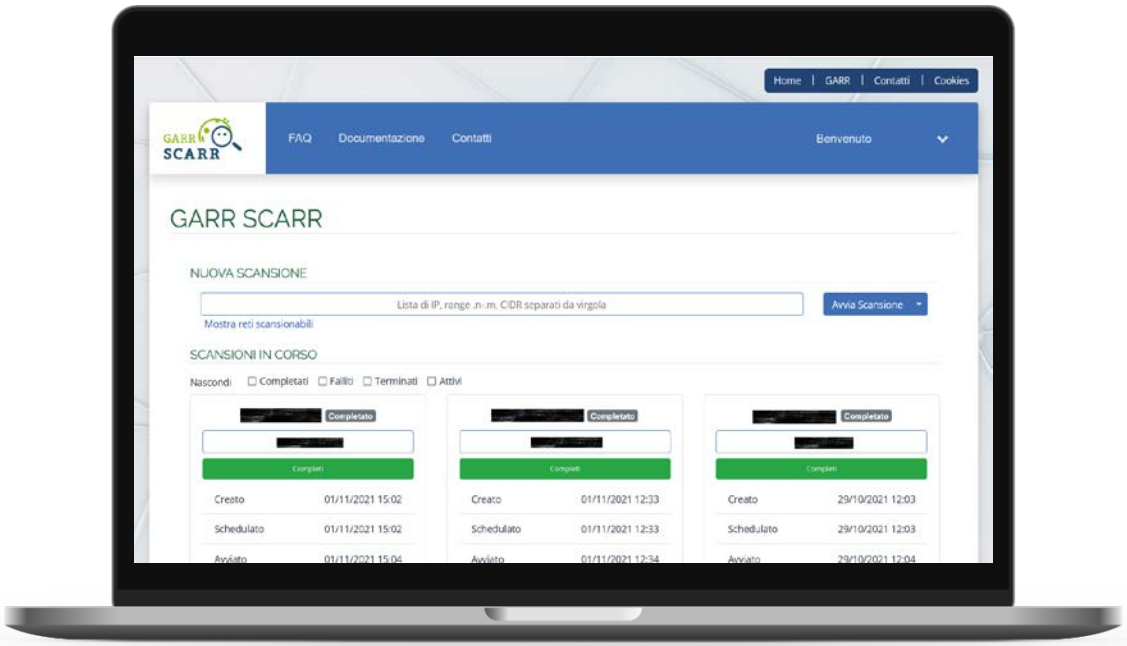
Funzionalità

Scansioni

Scansioni di indirizzi IP in classe C. Esecuzione asincrona e split in task paralleli

Scheduling

Possibilità di prenotare a calendario e ripetere a differenti intervalli temporali le richieste



Real time

Monitoraggio delle scansioni richieste e consultazione di quelle concluse

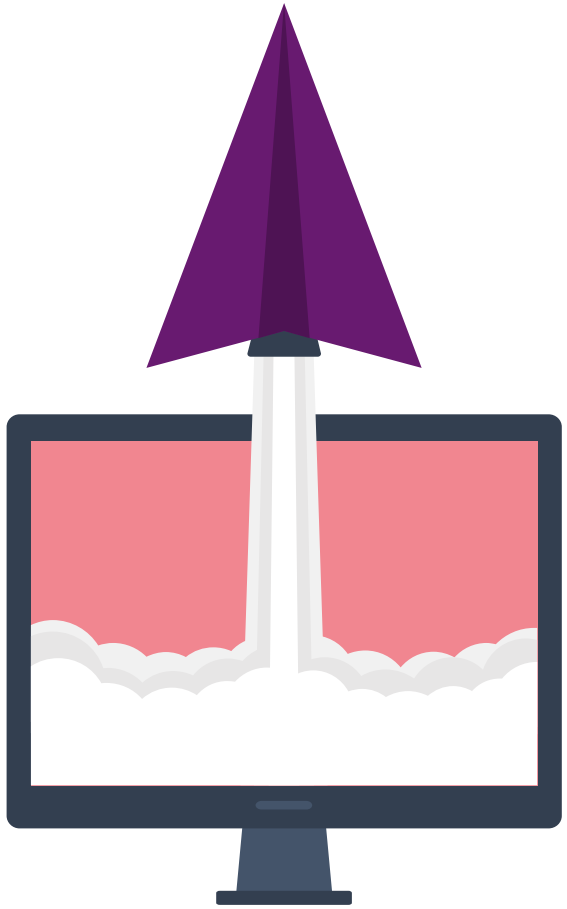
Report

Report dettagliato delle vulnerabilità riscontrate con suggerimenti sulle azioni da intraprendere per mitigarle

Ulteriori informazioni: https://www.eventi.garr.it/it/ws19/programma/speaker/545-gianni-marzulli

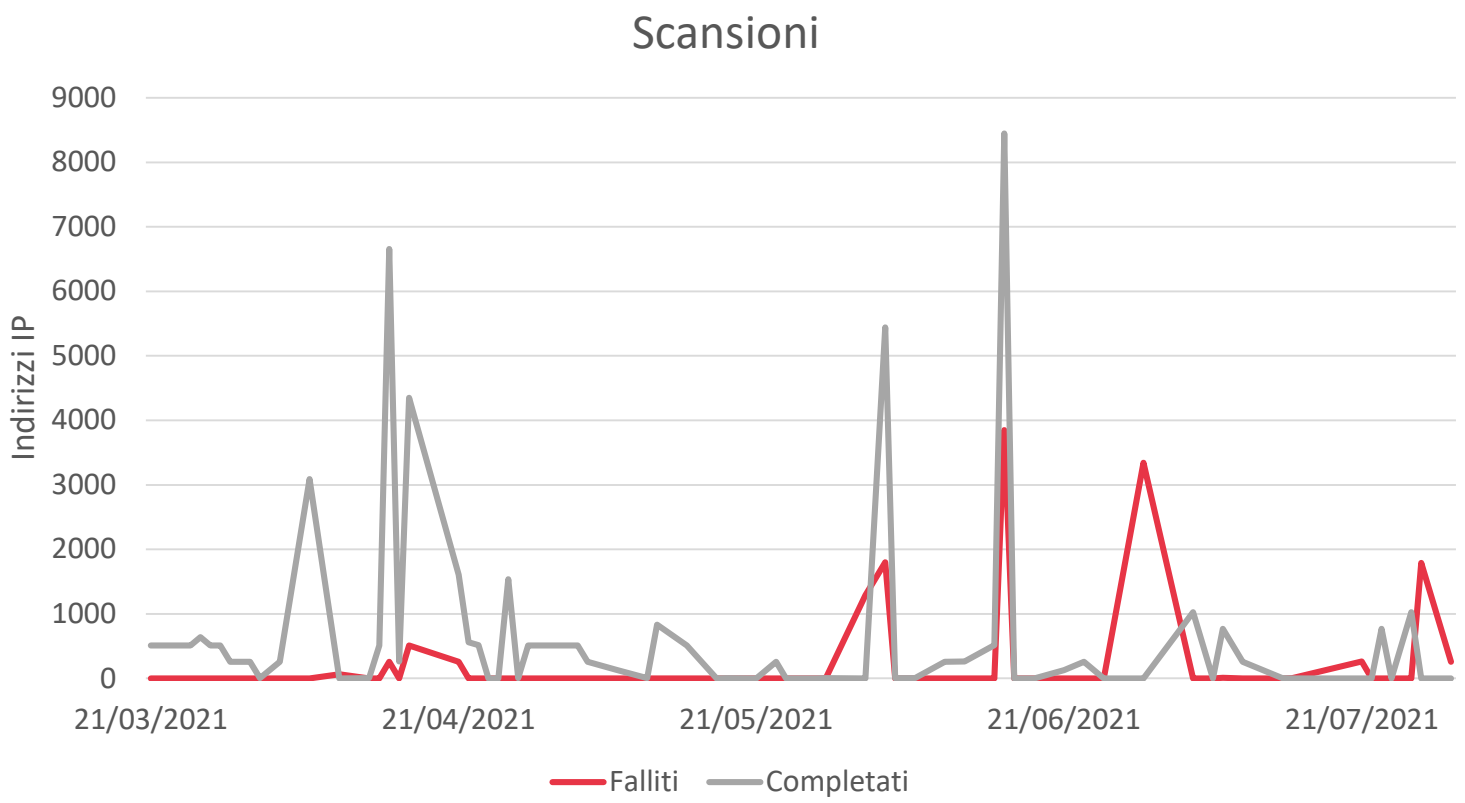
Statistiche dal lancio a inizio 2021

1. 1492
   Scansioni richieste
2. 119
   Enti utilizzatori
3. 438482
   Indirizzi IP scansionati



4. 6251
   Task eseguiti
5. 78,62%
   Task completati
6. 11,66%
   Task terminati
7. 9,72%
   Task falliti

Migliorie necessarie



END OF LIFE

Release di Greenbone in uso rilasciata da tre anni

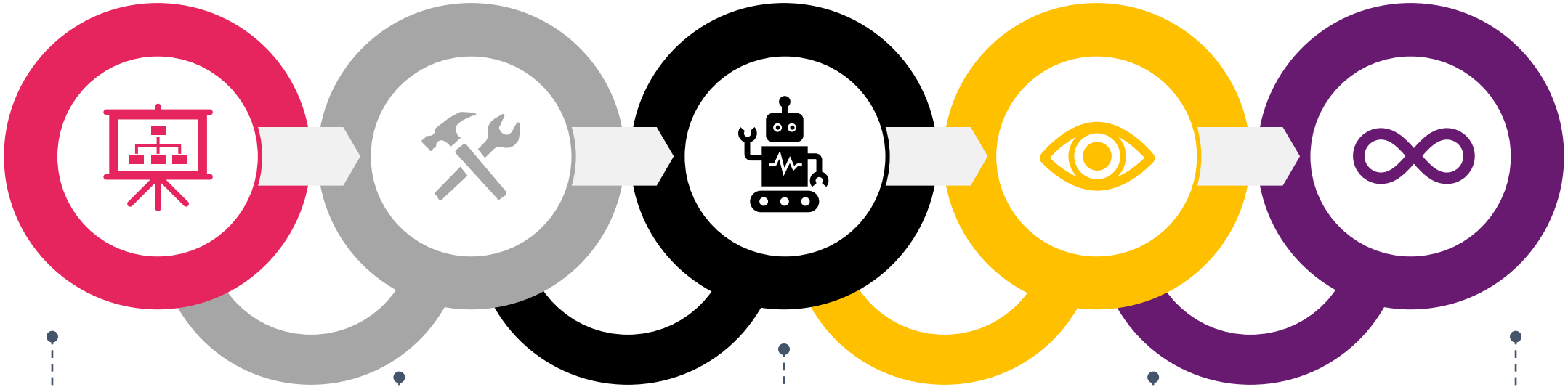
CONGESTIONE

Backend congestionati a causa di scansioni con subnet molto grandi

METODOLOGIA

Una metodologia di sviluppo non adatta a un fast update and deploy

Metodologia DevOps



Analisi requisiti e sviluppo software

Processi standardizzati

Automazione e CI/CD best practices

Monitoraggio

Release frequenti

Ridotto drasticamente il consumo di memoria (40MiB per scansione, 50% di RAM in meno nel nostro caso)

Introduzione di un sistema di code per l'avvio delle scansioni

Avvio delle scansioni in base alle risorse disponibili (evita congestioni)

Nuova funzionalità per identificare più velocemente se gli host sono attivi

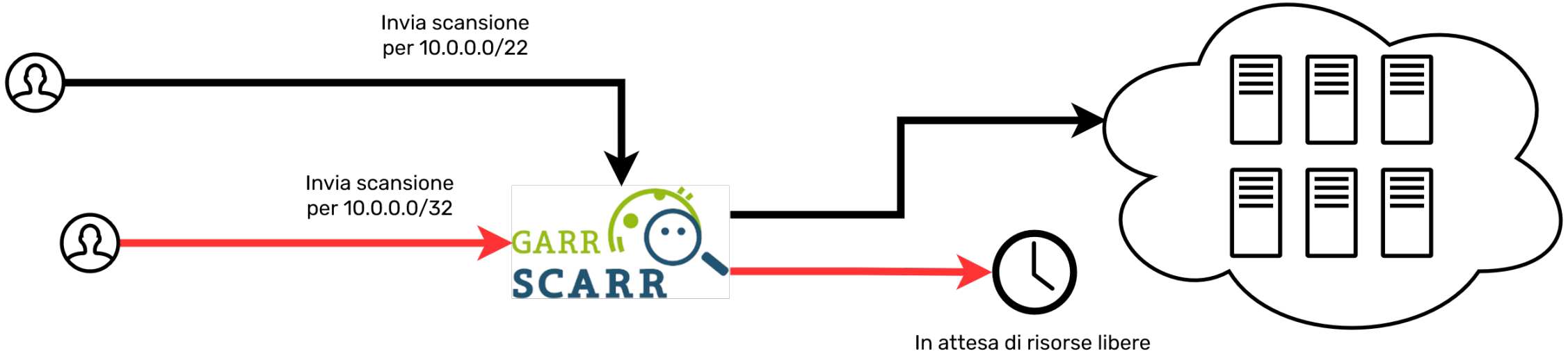
Greenbone

Sustainable Resilience

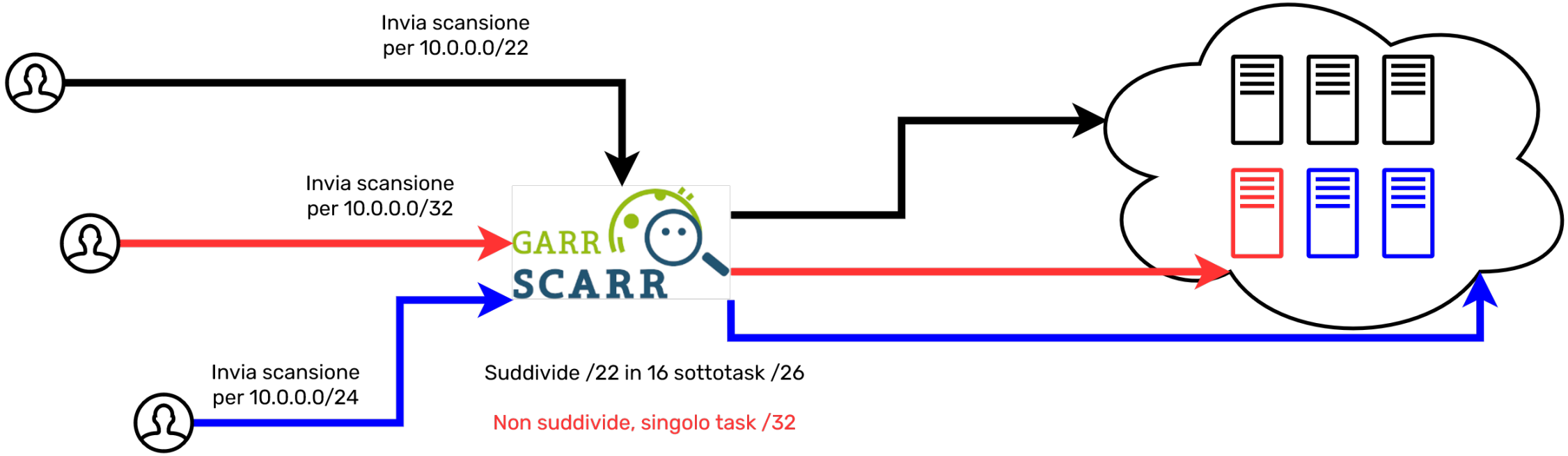
v9 → v20

Community Edition

Nuova gestione delle code



Nuova gestione delle code

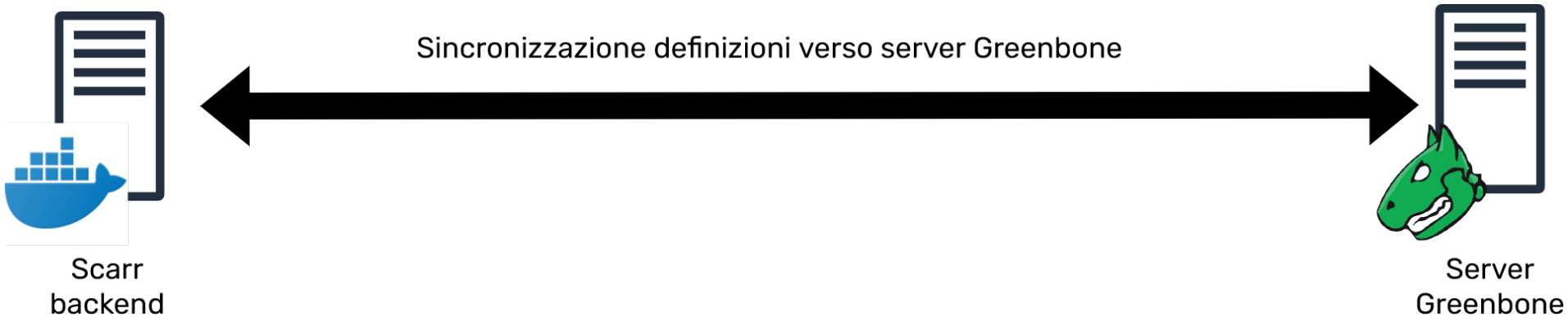


Greenbone security feed

Sono un insieme di test di vulnerabilità con cui lo scanner controllerà tutti i dispositivi.

1. NVTs (Network Vulnerability Tests)
2. SCAP (Security Content Automation Protocol)
3. CERT (Computer Emergency Response Team)

Sincronizzazione delle definizioni



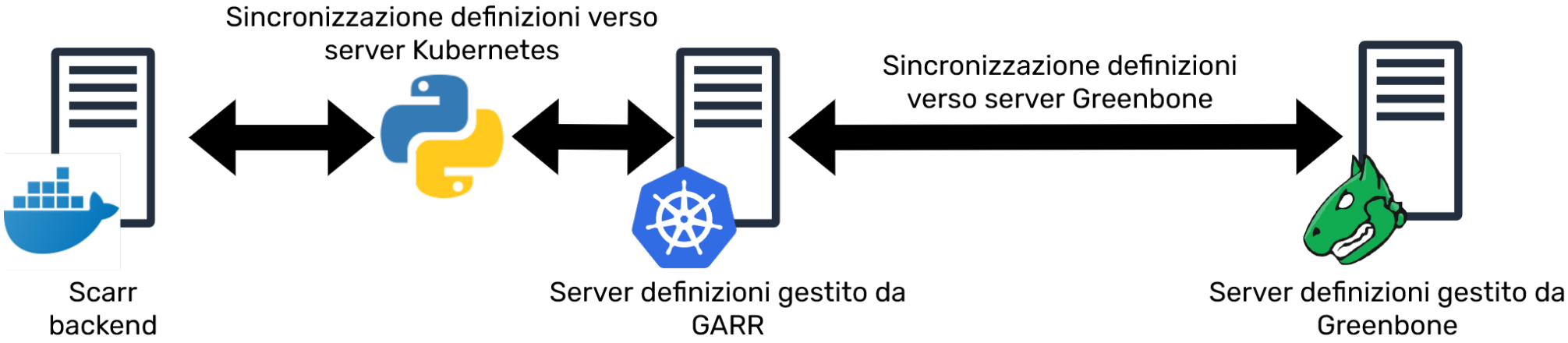
Connessioni limitate

Velocità in download limitata

Scarsa scalabilità

Downtime del backend

Sincronizzazione delle definizioni



Connessioni illimitate

Nessun limite imposto alla velocità di download

Elevata scalabilità

Nessun downtime del backend

Statistiche dopo l'aggiornamento

1. 102
   Scansioni richieste
2. 42
   Enti utilizzatori
3. 28370
   Indirizzi IP scansionati

4. 421
   Task eseguiti
5. 89,22%
   Task completati
6. 7,84%
   Task terminati
7. 2,94%
   Task falliti

Miglioramenti futuri

- Aggiornamento a Greenbone 21
- Sistema di reportistica avanzato
- Migliore gestione dei fallimenti

Conclusioni

01

Apprezzato

L'utilizzo del servizio è sempre costante da parte della comunità GARR

02

Semplice

Interfaccia di utilizzo minimale

03

Audit

Strumento utile a fare una valutazione semi-automatica e sistematica di un sistema.

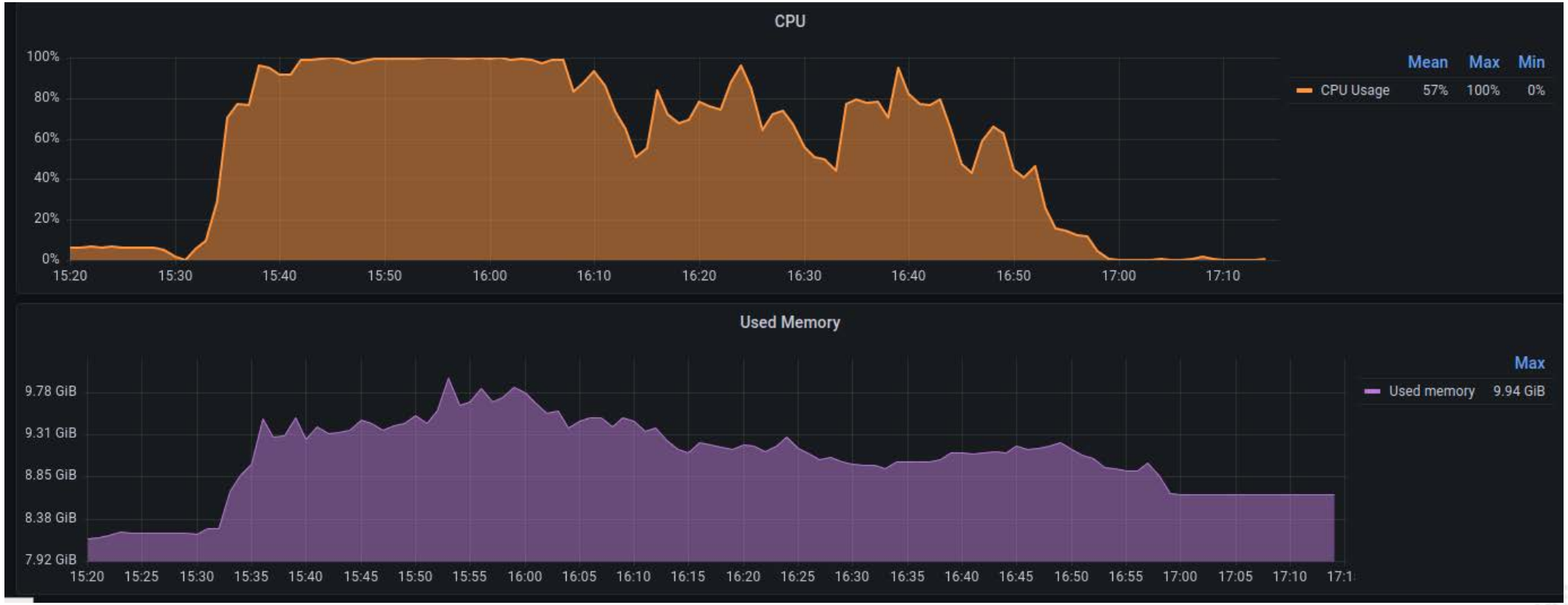
04

Compreso

Non propone la verità assoluta ma è uno strumento che va compreso e analizzato

Grazie per l'attenzione

Utilizzo RAM e CPU Greenbone 9



Utilizzo RAM e CPU Greenbone 20