SentinelCore — Manuale Utente

Vulnerability Management Platform

Dognet Technologies S.r.l.

© Dognet Technologies S.r.l. — P.IVA 04867480164

Table of contents

1. Introduzione 4
   - 1.1 Cos'è SentinelCore 4
   - 1.2 A chi si rivolge questo manuale 4
   - 1.3 Novità della versione 2.0.0 4
   - 1.4 Edizioni: Community e Pro 5
   - 1.5 Cosa fa SentinelCore 5
   - 1.6 Cosa NON fa (per evitare aspettative sbagliate) 5
   - 1.7 Come è organizzato questo manuale 6
2. 1. Installazione 7
   - 2.1 Modalità A — VM appliance (consigliata) 7
   - 2.2 Modalità B — Pacchetto binario su un server esistente 8
   - 2.3 Verificare i file scaricati 9
   - 2.4 Aggiornare un'installazione esistente 9
3. 2. Primo accesso 11
   - 3.1 Login 11
   - 3.2 Primo cambio password 11
   - 3.3 Attivare l'autenticazione a due fattori (opzionale, consigliato per gli admin) 11
   - 3.4 Tour rapido dell'interfaccia 11
4. 3. Ruoli e permessi 13
   - 4.1 Amministratore (`admin`) 13
   - 4.2 Team Leader (`team_leader`) 13
   - 4.3 Utente (`user`) 13
   - 4.4 Riepilogo rapido 14
   - 4.5 Ruolo all'interno di un team 14
   - 4.6 Permessi granulari (uso avanzato) 14
5. 4. Configurazione 15
   - 5.1 Preferenze 15
   - 5.2 Notifiche 15
   - 5.3 SMTP (solo Amministratore) 16
   - 5.4 Sicurezza 16
   - 5.5 Server MCP (solo Amministratore) 16
   - 5.6 Network Discovery 17
   - 5.7 Logging 17
   - 5.8 Assegnazione vulnerabilità 17
   - 5.9 Override permessi utente 17

© Dognet Technologies S.r.l. — P.IVA 04867480164

5.10 Database 17
6. 5. Team e utenti 18
6.1 Team 18
6.2 Utenti 18
6.3 Competenze (skill) 18
7. 6. Vulnerabilità e punteggio di rischio 19
7.1 Dashboard 19
7.2 Il punteggio di rischio: perché non basta il CVSS 19
7.3 Elenco vulnerabilità 20
7.4 Dettaglio di una vulnerabilità 20
7.5 Accettazione del rischio (risk acceptance) 21
8. 7. Rete e asset 22
8.1 Scansione di rete 22
8.2 La mappa di topologia 22
8.3 Host / asset 24
9. 8. Scanner e integrazioni 26
9.1 Import da file scanner 26
9.2 Connettore OpenVAS diretto (senza esportare file a mano) 26
9.3 Connettore Nessus diretto 27
9.4 Sincronizza ora 28
9.5 Integrazione JIRA 28
9.6 Notifiche 28
9.7 Webhook SOAR in uscita (uso avanzato) 28
10. 9. Report e piani di remediation 29
10.1 Generare un report 29
10.2 Cronologia report 29
10.3 Piani di remediation 29
10.4 Carico di lavoro e classifiche 31
11. 10. Domande frequenti 32

© Dognet Technologies S.r.l. — P.IVA 04867480164

1. Introduzione

1.1 Cos'è SentinelCore

SentinelCore è una piattaforma di **vulnerability management** pensata per team di sicurezza interni. Il suo compito è raccogliere in un unico posto tutte le vulnerabilità della tua infrastruttura — scoperte dalla scansione di rete integrata o importate da scanner di terze parti — assegnare a ciascuna un **punteggio di rischio reale** (non solo il punteggio CVSS "di targa"), instradarle alle persone giuste, tracciarne la risoluzione rispetto a scadenze (SLA) e produrre i report che servono per audit e conformità.

Tutto il prodotto ruota attorno a un unico flusso operativo:

```
scopri → importa → valuta il rischio → assegna → risolvi → verifica → rendiconta
```

Ogni fase di questo flusso corrisponde a una sezione precisa dell'interfaccia, descritta nei capitoli seguenti.

1.2 A chi si rivolge questo manuale

Questo manuale è pensato per due tipi di lettori:

- **Chi installa e amministra** SentinelCore (un amministratore di sistema o un responsabile sicurezza) — capitoli 1–4.
- **Chi lo usa ogni giorno** per gestire vulnerabilità, team e report (analisti, team leader) — capitoli 5 in poi.

Non è richiesta alcuna conoscenza di programmazione: SentinelCore si installa da pacchetti pronti e si usa interamente da interfaccia web.

1.3 Novità della versione 2.0.0

Rispetto alla 1.2.0, la 2.0.0 porta soprattutto questi cambiamenti (i dettagli sono nei capitoli indicati):

- **Mappa di rete rinnovata** — selezione a riquadro, spostamento di gruppi di host, zoom e scorrimento, linee personalizzabili (forma, colore, TAG, animazione), collegamenti scoperti dagli scanner animati, sottoreti raccolte in riquadri comprimibili, viste gerarchica e circolare raggruppate per sottorete (capitolo 7).
- **Dashboard interattiva** — ogni colonna del grafico "Vulnerability Trend" apre il dettaglio di quel giorno, con grafico per severity e collegamenti a vulnerabilità e host (capitolo 6).
- **Punteggio di rischio più chiaro sugli host** — la scheda "Input del risk score" mostra solo i dati che entrano davvero nel calcolo, con i punti che ciascuno porta; i campi doppi sono stati unificati (capitolo 7).
- **Piani di remediation precisi** — un piano è ora l'elenco delle **vulnerabilità** scelte, non degli host interi: si cercano con criteri combinabili (rete/CIDR, tipo di host, team, esposizione, rischio, gravità, KEV, CVE, testo), si aggiungono una per una, tutte insieme o "tutte quelle dell'asset / di rischio X", e le vulnerabilità nuove su un host del piano non ci entrano da sole. Chiusura automatica immediata del piano. È il cambiamento che porta la versione a 2.0.0 (capitolo 9).
- **Dettagli CISA KEV e NVD** — la pagina di una vulnerabilità mostra i dati del catalogo KEV (prodotto, scadenza, azione richiesta, uso ransomware) e l'esito dell'arricchimento NVD, con gli eventi relativi in timeline; gli amministratori possono avviare a mano i due aggiornamenti dalla barra della tabella (capitolo 6).
- **Cloni dell'host in testing e pre-produzione** — nella pagina dell'host si dichiara dove vive una copia, con rete e flag "allineato alla produzione" (capitolo 7).
- **Tabelle più utili** — il tasto **Colonne** sceglie le colonne visibili (e la scelta resta); date e ore in formato europeo ovunque (capitolo 2).
- **Commenti più ricchi** — risposte a qualsiasi livello e autocompletamento delle menzioni `@utente` (capitolo 6).
- **Aggiornamento in tempo reale** — liste, notifiche e dashboard si aggiornano da sole, senza ricaricare la pagina.
- **Sicurezza** — revoca delle sessioni, limite ai tentativi di accesso, codici 2FA non riutilizzabili, scansioni di rete eseguite da un componente privilegiato con elenco di opzioni consentite (capitolo 4).
- **Temi con contrasto verificato** — tutti gli 11 temi rispettano i livelli di leggibilità WCAG AA per testi e colori di gravità (capitolo 4).
- **Release firmate** — i pacchetti e le immagini VM sono accompagnati da checksum e firma verificabili (capitolo 1).

© Dognet Technologies S.r.l. — P.IVA 04867480164

1.4 Edizioni: Community e Pro

SentinelCore è distribuito in due edizioni che condividono lo stesso codice di base e la stessa interfaccia:

- **Community** — gratuita e open source (licenza AGPL). Include l'intero flusso operativo (scoperta, importazione, punteggio di rischio, assegnazione, piani di remediation, report) ed è limitata a **15 host** gestiti.
- **Pro** — a licenza. Alza il tetto degli host a scaglioni (il primo porta a 45 host complessivi — 15 per ambiente — poi 135, 405 e oltre) e aggiunge alcune funzioni esclusive, segnalate in questo manuale con l'etichetta **(Pro)**:
- la **minimappa** della mappa di topologia, comoda sulle reti grandi;
- **limiti e conteggio per ambiente** — produzione, testing e pre-produzione contati separatamente — con l'**ambiente che modula il punteggio di rischio**: lo stesso problema pesa di più in produzione che in testing.

Una sola licenza vale per **tutta la suite SentinelSuite** (SentinelCore Pro e CyberShepherd), con gli stessi limiti di asset.

In alto a sinistra l'interfaccia indica sempre l'**edizione in uso** (`SentinelCore COMMUNITY` o `SentinelCore PRO`) e il numero di versione. Questo manuale descrive l'edizione **Community**: dove una funzione richiede la licenza lo trovi scritto **(Pro)**.

1.5 Cosa fa SentinelCore

- **Network Discovery** — scansione di rete integrata (basata su nmap) con profili configurabili, pianificazione ricorrente e mappa di topologia interattiva degli host scoperti.
- **Importazione da scanner esterni** — legge i risultati di 10 scanner di terze parti (Qualys, Nessus, Burp Suite, OpenVAS/GVM, Nexpose/InsightVM, OWASP ZAP, Nmap, Nikto, Trivy, Grype), normalizza la severità, deduplica i risultati e li collega agli asset.
- **Connettori OpenVAS e Nessus diretti** — connettori integrati interrogano periodicamente un'istanza GVM/OpenVAS o Tenable Nessus (Essentials o Professional, release certificata 10.12.x) e importano automaticamente i report completati, senza bisogno di esportare file a mano.
- **Punteggio di rischio** — un punteggio composito 0–100 che combina CVSS, probabilità di sfruttamento reale (EPSS), impatto di business, esposizione dell'asset e disponibilità di exploit noti, con override automatici per zero-day, CVE sfruttate da ransomware e vulnerabilità attivamente sfruttate (catalogo CISA KEV).
- **SLA e scadenze** — ogni livello di rischio ha una scadenza di rimedio (Critical 1 giorno, High 7 giorni, Medium 30 giorni, Low 90 giorni); il sistema segnala automaticamente gli sforamenti.
- **Assegnazione** — manuale (a team o utente) oppure automatica tramite regole basate su competenze (skill) e bilanciamento del carico.
- **Piani di remediation** — ordini di lavoro che raggruppano vulnerabilità scelte con precisione in piani eseguibili, con stato di avanzamento calcolato sulle vulnerabilità realmente risolte, chiusura automatica al 100%, commenti e verifica finale.
- **Collaborazione** — commenti a thread con menzioni (`@utente` , con autocompletamento), notifiche in-app, classifiche di risoluzione per utenti e team. Le liste e le notifiche si aggiornano in tempo reale.
- **Notifiche** — motore di regole (condizioni, priorità, throttling, orari di silenzio) che invia avvisi via email, Slack e Telegram.
- **Integrazioni** — sincronizzazione bidirezionale con JIRA, arricchimento CVE da NVD, aggiornamento giornaliero EPSS, webhook SOAR in uscita.
- **Reportistica** — report di vulnerabilità (PDF/CSV/JSON/XML), report di gestione, dashboard esecutiva, mappe di calore tecniche.
- **Sicurezza e audit** — autenticazione con cookie httpOnly, protezione CSRF, autenticazione a due fattori (TOTP) con codici non riutilizzabili, limite ai tentativi di accesso, gestione sessioni con revoca da remoto, log di audit (completo per Amministratori e Team Leader, personale per gli Utenti), permessi granulari per utente.
- **Server MCP** — un'interfaccia programmatica (Model Context Protocol) che permette ad agenti AI autorizzati di consultare e, se abilitato, agire su vulnerabilità e rischio — vedi il capitolo dedicato alla configurazione.

1.6 Cosa NON fa (per evitare aspettative sbagliate)

- **Non è uno scanner di vulnerabilità** in senso stretto: a parte la scoperta di rete/porte basata su nmap, SentinelCore non rileva da solo le vulnerabilità — le riceve da scanner esterni o dai connettori OpenVAS e Nessus.

© Dognet Technologies S.r.l. — P.IVA 04867480164

- **Non è multi-tenant**: un'installazione serve un'unica organizzazione.
- **Non ha alta affidabilità/clustering integrati**: è pensato per un singolo host con un'istanza PostgreSQL.
- **Non richiede né installa agenti** sugli endpoint monitorati: la visibilità viene dalle scansioni di rete e dai dati importati dagli scanner.
- **Non fa patching automatico su larga scala**: i piani di remediation tracciano il lavoro, non lo eseguono al posto tuo.
- **Non ha ancora LDAP/SSO integrato**: l'autenticazione è locale (username/password + 2FA opzionale).

1.7 Come è organizzato questo manuale

Capitolo	Contenuto
1 — Installazione	Le due modalità di distribuzione (VM pronta all'uso, pacchetto binario), requisiti, primo avvio
2 — Primo accesso	Login iniziale, cambio password, tour rapido dell'interfaccia
3 — Ruoli e permessi	I tre ruoli (Amministratore, Team Leader, Utente) e cosa può fare ciascuno
4 — Configurazione	Tutte le sezioni di Impostazioni: preferenze, notifiche, email, sicurezza, MCP, rete, e altro
5 — Team e utenti	Creare team, aggiungere membri, gestire utenti e competenze
6 — Vulnerabilità e rischio	Dashboard, elenco vulnerabilità, punteggio di rischio, stati, assegnazione
7 — Rete e asset	Scansione di rete, topologia, gestione host
8 — Scanner e integrazioni	Importazione da scanner esterni, connettori OpenVAS e Nessus, JIRA, notifiche
9 — Report e piani di remediation	Generare report, cronologia, piani di remediation, carico di lavoro
10 — Domande frequenti	Problemi comuni e loro soluzione

© Dognet Technologies S.r.l. — P.IVA 04867480164

2. 1. Installazione

SentinelCore si distribuisce in due modi. Scegli quello più adatto al tuo contesto.

Modalità	Quando usarla	Cosa serve
A — VM appliance (OVA / qcow2)	Vuoi provare o mettere in produzione SentinelCore nel modo più rapido possibile, senza occuparti di sistema operativo, dipendenze o configurazione manuale	Un hypervisor (VirtualBox, VMware, Proxmox, KVM)
B — Pacchetto binario	Hai già un server Linux (fisico o virtuale) su cui vuoi installare SentinelCore, magari insieme ad altri servizi	Un host Debian 12/13 pulito con accesso `sudo`

Non serve in nessuno dei due casi installare compilatori, Rust, Node.js o altri strumenti di sviluppo: entrambi i pacchetti contengono i binari già compilati.

2.1 Modalità A — VM appliance (consigliata)

2.1.1 Requisiti minimi

Risorsa	Minimo	Consigliato
vCPU	2	4
RAM	2 GB	4 GB
Disco	10 GB	20 GB
Rete	Un indirizzo IP raggiungibile dai browser degli utenti	—

2.1.2 Import dell'immagine

L'appliance viene fornita in due formati equivalenti — scegli quello supportato dal tuo hypervisor:

- **File `.ova`** → VirtualBox (*File → Importa appliance…*) o VMware (*File → Open…*)
- **File `.qcow2`** → Proxmox (importa come disco di una nuova VM) o KVM/QEMU diretto:

```
qemu-system-x86_64 -m 2048 -smp 2 -enable-kvm \
  -drive file=sentinelcore-<versione>-linux-x86_64.qcow2,format=qcow2 \
  -netdev user,id=net0 -device virtio-net-pci,netdev=net0
```

Avvia la VM.

2.1.3 Primo avvio dell'appliance

Al primo avvio di ogni copia (ogni volta che importi o cloni una nuova appliance), un servizio automatico rigenera tutti i segreti univoci dell'istanza — password del database, chiave di firma delle sessioni, chiavi SSH dell'host, certificato TLS — così due appliance nate dalla stessa immagine non condividono mai le stesse credenziali. Questa fase richiede qualche decina di secondi e avviene una sola volta.

Al termine, le credenziali di accesso vengono stampate **sulla console della VM** e salvate nel messaggio del giorno (visibile al login SSH):

```
┌──────────────────────────────────────────────────────┐
│          SentinelCore — Credenziali iniziali istanza          │
└──────────────────────────────────────────────────────┘
  URL:        https://192.168.x.x
  Utente:     admin
  Password:   XxXxXxXx1234Aa1!
  CAMBIA la password al primo accesso (Impostazioni → Profilo).
```


© Dognet Technologies S.r.l. — P.IVA 04867480164

Annota indirizzo, utente e password: ti serviranno per il primo accesso (capitolo successivo). L'indirizzo indicato è quello assegnato via DHCP alla VM sulla rete a cui l'hai collegata.

Importante: cambia la password admin **subito dopo il primo accesso**. L'account iniziale non è protetto da un cambio password obbligatorio a livello di sistema: è una buona pratica di sicurezza che spetta a te applicare.

Da qui in poi l'appliance si comporta come un'installazione normale: ad ogni riavvio successivo non rigenera più nulla.

2.2 Modalità B — Pacchetto binario su un server esistente

2.2.1 Requisiti

- Debian 12 o 13, installazione pulita (l'installer configura da sé PostgreSQL, nginx e gli strumenti di scansione di rete)
- Accesso `sudo`
- Connessione di rete in uscita (per installare i pacchetti di sistema necessari)

2.2.2 Passi

1. Scarica il pacchetto (`sentinelcore-<versione>-linux-x86_64.tar.gz`) e verificane l'integrità e la provenienza, come descritto nella sezione *Verificare i file scaricati* qui sotto:

```
sha256sum -c SHA256SUMS --ignore-missing
```

1. Estrai ed esegui l'installer:

```
tar xzf sentinelcore-<versione>-linux-x86_64.tar.gz
cd sentinelcore-<versione>-linux-x86_64
sudo ./install.sh
```

L'installer rileva automaticamente l'indirizzo IP e l'interfaccia di rete della macchina. Se hai più interfacce o vuoi forzare un nome host specifico:

```
sudo ./install.sh --server-name 10.0.0.5 --iface ens18
```

1. L'installer, in autonomia:
2. installa i pacchetti di sistema necessari (PostgreSQL, nginx, nmap, arp-scan);
3. crea utente e database dedicati con password generata casualmente;
4. applica lo schema del database;
5. genera un certificato TLS auto-firmato per l'istanza e configura nginx per servire tutto in **HTTPS di default** (con redirect automatico da HTTP);
6. configura il servizio di sistema (systemd);
7. crea il primo account **admin**, stampandone le credenziali a fine installazione.
8. Al termine, annota le credenziali admin stampate a schermo e collegati all'indirizzo indicato.

Per esporre l'istanza su Internet con un dominio reale e un certificato Let's Encrypt al posto di quello auto-firmato, consulta la documentazione tecnica `packaging/HTTPS.md` nel repository, oppure richiedila al tuo fornitore.

© Dognet Technologies S.r.l. — P.IVA 04867480164

2.3 Verificare i file scaricati

Dalla versione 2.0.0 ogni release è costruita e firmata in modo automatico, e per ogni versione trovi accanto ai file (pacchetto `.tar.gz`, immagini `.ova` e `.qcow2`):

File	A cosa serve
`SHA256SUMS`	l'elenco dei checksum di tutti i file della release
`SHA256SUMS.asc`	la firma di quell'elenco
`sentinelcore-<versione>-linux-x86_64.tar.gz.asc`	la firma del solo pacchetto binario
`sentinelcore-release.pub.asc`	la chiave pubblica con cui verificare le firme

Per controllare che i file siano autentici e non alterati:

```
gpg --import sentinelcore-release.pub.asc
gpg --fingerprint security@dognet.tech
gpg --verify SHA256SUMS.asc SHA256SUMS
sha256sum -c SHA256SUMS --ignore-missing
```

L'impronta mostrata dal secondo comando deve essere esattamente `18B5 A69F 9767 84E2 5BF2 91F1 8CAD B9F7 D59F 68A1`: se è diversa, non usare i file. Il terzo comando deve dire `Good signature`, il quarto `OK` per ciascun file scaricato.

2.4 Aggiornare un'installazione esistente

Un aggiornamento **non perde dati**: qualunque metodo usi, parte sempre con un backup del database. Vale allo stesso modo per un'installazione da pacchetto, un'appliance VM o un'immagine qcow2, e per le edizioni **Community** e **Pro**.

2.4.1 Metodo consigliato: pacchetto `.deb`

Il modo principale, sia per la Community sia per la Pro, è il pacchetto `.deb` scaricato dalla piattaforma SentinelSuite:

```
# Community
sudo apt install ./sentinelcore_<nuova-versione>_amd64.deb
# Pro
sudo apt install ./sentinelcore-pro_<nuova-versione>_amd64.deb
```

Usa `apt` (non `dpkg -i`), così vengono installate anche le eventuali dipendenze. Il pacchetto riconosce da solo se è un primo install o un aggiornamento ed esegue `upgrade.sh`. Il vantaggio è che il sistema tiene traccia della versione installata: gli aggiornamenti successivi restano puliti.

Una volta su `.deb`, continua con il `.deb`. Aggiornare a mano con il tarball (sotto) un'istanza installata da pacchetto lascia la versione registrata dal sistema disallineata.

2.4.2 Alternativa documentata: tarball + `upgrade.sh`

In alternativa, per installazioni non gestite da pacchetto, c'è il tarball di release con lo script `upgrade.sh`:

```
tar xzf sentinelcore-<nuova-versione>-linux-x86_64.tar.gz
cd sentinelcore-<nuova-versione>-linux-x86_64
sudo ./upgrade.sh
```

Un'installazione partita da tarball può passare in qualsiasi momento al `.deb`: il pacchetto rileva l'app esistente e la aggiorna in-place.

© Dognet Technologies S.r.l. — P.IVA 04867480164

Con entrambi i metodi lo script esegue in automatico, in quest'ordine:

1. **Backup del database** (prima di qualsiasi modifica — se questo passo fallisce, l'aggiornamento si ferma e non viene applicato nulla);
2. arresto del servizio;
3. backup dei file correnti (per un ripristino automatico se il passo successivo fallisce);
4. installazione dei nuovi file (binario, frontend, migrazioni, configurazione di sistema);
5. applicazione delle modifiche al database necessarie alla nuova versione;
6. riavvio del servizio e verifica automatica che risponda correttamente.

Se qualcosa va storto durante l'applicazione delle modifiche al database, lo script **ripristina automaticamente la versione precedente** e riavvia il servizio: non resti mai con un'istanza a metà aggiornata. Il backup del database resta comunque disponibile in `/opt/sentinelsuite/sentinelcore/backups/` per un ripristino manuale in casi eccezionali.

Non serve rieseguire `install.sh` per un aggiornamento: `install.sh` è solo per la primissima installazione.

© Dognet Technologies S.r.l. — P.IVA 04867480164

3. 2. Primo accesso

3.1 Login

Apri il browser all'indirizzo indicato al termine dell'installazione (es. `https://<indirizzo-server>`). Il certificato TLS auto-firmato genererà un avviso di sicurezza nel browser al primo accesso: è normale per un'istanza appena installata — accetta l'eccezione per procedere (oppure configura un certificato valido, vedi capitolo 1).

Accedi con le credenziali admin annotate durante l'installazione:

- **Utente**: `admin`
- **Password**: quella generata e stampata a fine installazione

3.2 Primo cambio password

Subito dopo il primo accesso, vai su **Profilo** (icona utente in alto a destra → *Profilo*) e cambia la password. È l'unica azione di sicurezza che ti consigliamo di fare prima di ogni altra cosa: l'account admin creato dall'installer non forza da solo un cambio password, quindi finché non lo fai la password stampata durante l'installazione resta valida.

Dalla stessa pagina Profilo puoi anche:

- caricare una foto profilo o scegliere uno dei quattro avatar predefiniti per il tuo ruolo;
- impostare la lingua dell'interfaccia (italiano o inglese);
- collegare un webhook Slack personale, per ricevere lì gli stessi avvisi critici dell'email;
- scegliere il tuo **team principale** (se sei membro di più team), usato come riferimento per i filtri e l'ordinamento delle notifiche.

3.3 Attivare l'autenticazione a due fattori (opzionale, consigliato per gli admin)

In **Impostazioni → Sicurezza** puoi attivare il 2FA basato su app authenticator (Google Authenticator, Authy o equivalenti): il sistema mostra un QR code da inquadrare, poi richiede un codice di conferma per completare l'attivazione. Da quel momento il login richiederà, oltre alla password, il codice a 6 cifre generato dall'app.

3.4 Tour rapido dell'interfaccia

La barra laterale a sinistra è organizzata in quattro aree:

Area	Contenuto	Visibile a
Monitor	Dashboard, Le mie vulnerabilità	Tutti
Gestione	Vulnerabilità, Host, Topologia di rete, Piani di remediation, *Import scanner*	Tutti (le voci segnate * richiedono ruolo Team Leader o Amministratore)
Report	Report	Team Leader e Amministratore
Amministrazione	Team, *Utenti*, Plugin**, Impostazioni	* Team Leader+, ** solo Amministratore

In alto a destra trovi sempre: ricerca globale, campanella delle notifiche in-app, e il menu del tuo profilo utente.

I dati si **aggiornano da soli**: quando un collega crea un utente, assegna una vulnerabilità o cambia un piano, le liste che hai aperto si ricaricano senza che tu debba premere F5. Passando il mouse su un utente o su un team compare una piccola scheda informativa (ruolo, team, contatti).

© Dognet Technologies S.r.l. — P.IVA 04867480164

3.4.1 La barra delle tabelle

Sopra ogni tabella trovi la ricerca e, a destra, alcune icone:

- **Colonne** — apre l'elenco delle colonne con una spunta ciascuna: scegli quali vedere. La scelta viene ricordata per quella tabella;
- **Esporta** — scarica la tabella (dove disponibile);
- **Aggiorna** — ricarica i dati;
- nella tabella **Vulnerabilità**, per gli amministratori, **Avvia aggiornamenti** (vedi capitolo 6).

L'ordinamento si cambia cliccando sull'intestazione di una colonna. **Date e orari** sono ovunque in formato europeo: GG/MM/AAAA e ore a 24 ore (es. `09/10/2026, 00:38:58`), anche con l'interfaccia in inglese.

Il capitolo successivo spiega nel dettaglio cosa può fare ciascuno dei tre ruoli disponibili.

© Dognet Technologies S.r.l. — P.IVA 04867480164

4. 3. Ruoli e permessi

SentinelCore ha tre ruoli. Un utente ne ha esattamente uno, assegnato da un amministratore.

4.1 Amministratore (`admin`)

Controllo completo della piattaforma. Oltre a tutto ciò che possono fare Team Leader e Utente, l'Amministratore è l'unico che può:

- creare, modificare ed eliminare vulnerabilità, asset e team;
- assegnare vulnerabilità a team/utenti (singolarmente o in blocco);
- gestire gli utenti (creazione, blocco, sessioni attive, ruoli);
- definire le regole di assegnazione automatica e la politica generale (automatica/manuale);
- definire le regole di notifica e i canali di invio;
- importare file da scanner esterni;
- eliminare i piani di remediation (creare e modificare è consentito anche al Team Leader);
- gestire il ciclo di vita dell'accettazione del rischio (risk acceptance: approvare, rifiutare, rinnovare);
- registrare e verificare le risoluzioni;
- gestire i plugin (inclusa la configurazione dei connettori OpenVAS e Nessus);
- configurare l'integrazione JIRA e i webhook SOAR;
- accedere al log di audit completo (come il Team Leader);
- modificare tutte le **Impostazioni** di sistema (rete, sicurezza, notifiche, MCP, ecc.);
- creare chiavi API con permessi di **scrittura** per il server MCP (vedi capitolo 4).

4.2 Team Leader (`team_leader`)

Un coordinatore con visibilità e alcune capacità di gestione più ampie di un Utente semplice, ma senza i poteri di sistema di un Amministratore:

- vede e naviga le sezioni **Piani di remediation**, **Import scanner** e **Report**, non visibili a un Utente semplice;
- **crea e modifica i piani di remediation**, comprese le liste di host dei piani in bozza (l'eliminazione resta all'Amministratore);
- vede il **log di audit completo** di tutti gli utenti;
- vede e naviga **Team** e **Utenti** — in particolare può modificare email, password e competenze (skill) dei membri del **proprio** team;
- per il resto ha le stesse capacità di un Utente (vedi sotto).

4.3 Utente (`user`)

Il ruolo operativo di base: un analista che lavora sulle vulnerabilità assegnate a sé o al proprio team.

Un Utente può:

- vedere vulnerabilità, asset, topologia di rete, team e piani condivisi;
- avviare scansioni di rete, modificare i dispositivi scoperti, assegnarli in blocco;
- commentare e menzionare colleghi (`@utente`) su vulnerabilità, asset e piani;
- generare, scaricare e ricevere via email i report a cui ha accesso;
- gestire il proprio profilo, il 2FA, le proprie chiavi API e le proprie sessioni attive;
- consultare il proprio carico di lavoro, le proprie statistiche di risoluzione e le classifiche.

© Dognet Technologies S.r.l. — P.IVA 04867480164

Dell'audit log un Utente vede **solo le proprie azioni** (login, modifiche), mai quelle degli altri account. La **timeline** di una vulnerabilità, invece, è leggibile da ogni utente autenticato.

Un Utente **non** può creare/modificare/eliminare vulnerabilità o asset, assegnare lavoro ad altri, gestire team o utenti, importare scanner, o accedere alle Impostazioni di sistema.

4.4 Riepilogo rapido

Capacità	Utente	Team Leader	Amministratore
Visualizzare vulnerabilità, asset, topologia, team, report	✅	✅	✅
Avviare scansioni di rete, modificare/assegnare dispositivi	✅	✅	✅
Commentare, menzionare, gestire il proprio profilo/ 2FA/sessioni	✅	✅	✅
Vedere Piani di remediation, Import scanner, Report nel menu	❌	✅	✅
Modificare email/password/skill dei membri del proprio team	❌	✅ (solo il proprio team)	✅ (tutti)
Creare/modificare/eliminare vulnerabilità e asset	❌	❌	✅
Assegnare vulnerabilità a team/utenti	❌	❌	✅
Creare/eliminare team, gestire regole di assegnazione	❌	❌	✅
Gestire utenti (creazione, blocco, ruoli)	❌	❌	✅
Importare file da scanner esterni	❌	❌	✅
Creare e modificare piani di remediation	❌	✅	✅
Eliminare piani di remediation, gestire risk acceptance	❌	❌	✅
Gestire plugin, connettori OpenVAS e Nessus, JIRA, webhook SOAR	❌	❌	✅
Log di audit	Solo le proprie azioni	Completo	Completo
Impostazioni di sistema	❌	❌	✅

4.5 Ruolo all'interno di un team

Indipendentemente dal ruolo di piattaforma, ogni appartenenza a un team ha un proprio ruolo interno — **leader** o **contributor** — assegnabile da un amministratore o da un team leader dalla pagina **Team**. Questo ruolo è indipendente dal ruolo di piattaforma: un Utente può essere "leader" all'interno del proprio team, senza per questo diventare un `team_leader` di piattaforma.

4.6 Permessi granulari (uso avanzato)

Oltre ai tre ruoli, un amministratore può concedere **permessi puntuali** a un singolo utente su una risorsa specifica (con scadenza opzionale), per gestire eccezioni senza dover cambiare il ruolo di base della persona. È una funzionalità pensata per casi particolari, non per la gestione quotidiana dei permessi.

© Dognet Technologies S.r.l. — P.IVA 04867480164

5. 4. Configurazione

Tutte le impostazioni di sistema si trovano in **Impostazioni** (visibile a tutti i ruoli, ma la maggior parte delle sezioni è modificabile solo da un Amministratore). Il menu laterale della pagina elenca le sezioni descritte qui sotto. Se apri una sezione riservata all'Amministratore senza averne i permessi, la pagina lo dice con un avviso esplicito invece di restare vuota o in caricamento.

5.1 Preferenze

Scelta del tema grafico dell'interfaccia: 11 temi, tra cui SentinelCore Professional Dark (predefinito), Dognet Professional e Dognet Black, i quattro temi Entuity (Light, Dark, Midnight Blue, Arctic Blue), e i temi Minimal, Modern Tech, Cyberpunk ed Enterprise. È una preferenza personale, salvata per l'utente che l'ha impostata.

I colori di testi, pulsanti e livelli di gravità (Critical/High/Medium/Low) di ogni tema sono verificati per rispettare i rapporti di contrasto WCAG AA, quindi restano leggibili in qualsiasi tema, chiaro o scuro.

5.2 Notifiche

Il canale **in-app** (la campanella in alto) è sempre attivo, indipendentemente da tutto quello che segue. Questa pagina decide invece **cosa** ti arriva anche via **email e Slack personale** (il webhook impostato in Profilo) — perché queste email/Slack arrivino davvero, un amministratore deve aver configurato un server SMTP funzionante (sezione successiva) e/o tu stesso un webhook Slack in Profilo.

Interruttori generali:

- **Email** — interruttore generale del canale email;
- **Avviso vulnerabilità critical** — invia un'email quando viene scoperta una vulnerabilità critical assegnata al tuo team;
- **Report settimanale** — invia un'email di riepilogo settimanale delle vulnerabilità.

Eventi personali (visibili a tutti i ruoli — riguardano il lavoro assegnato a te o al tuo team):

- Ti viene assegnata una vulnerabilità (a te direttamente o al tuo team);
- Il tuo team riceve un nuovo piano di remediation — un piano ancora in **bozza** non genera nessuna notifica: l'avviso parte quando il piano esce dalla bozza (diventa Attivo).

Eventi operativi (visibili solo a Team Leader e Amministratore — riguardano la gestione del team/dell'istanza, non solo il tuo lavoro):

- Un utente cambia lo stato di una vulnerabilità (presa in carico, risolta, chiusa);
- Viene creata una nuova vulnerabilità (manualmente o da un import scanner — in questo caso ricevi un riepilogo del batch, non un'email per ogni riga importata);
- Viene scoperto un nuovo host dal Network Discovery;
- Una scansione di rete **periodica** (quella pianificata in Impostazioni → Network Discovery, non gli avvii manuali) è completata;
- Uno o più host risultano offline in una scansione.

Le **menzioni** (`@nomeutente` in un commento) generano invece sempre una notifica in-app, e solo per le persone citate: nessun altro membro del team viene avvisato.

Ognuna di queste preferenze è indipendente dalle altre: puoi ad esempio ricevere email sulle vulnerabilità assegnate ma non sui report settimanali, o viceversa.

© Dognet Technologies S.r.l. — P.IVA 04867480164

5.3 SMTP (solo Amministratore)

Configurazione del server di posta usato per gli avvisi critici, i report settimanali e le notifiche di avanzamento dei piani di remediation:

Campo	Descrizione
Server SMTP	Hostname del server di invio (es. `smtp.gmail.com`)
Porta	Porta SMTP (tipicamente 587 per STARTTLS)
Username	Utente per l'autenticazione SMTP
Password	Password SMTP — una volta salvata, il campo resta vuoto: lascialo vuoto se non vuoi cambiarla
Indirizzo mittente	Se vuoto, viene usato lo username come mittente
Invio email abilitato	Interruttore generale: se spento, nessuna email parte anche se le regole di notifica sono configurate

Dopo aver inserito i parametri, usa il pulsante **Testa connessione**: invia una vera email di prova alla casella dell'amministratore che ha premuto il pulsante — se arriva, la configurazione è corretta. Puoi testare anche prima di salvare, per verificare i parametri senza doverli prima confermare.

5.4 Sicurezza

- **Autenticazione a due fattori (2FA)** — attiva/disattiva il 2FA per il proprio account (vedi capitolo 2).
- **Timeout sessione** — tempo di inattività (15 minuti, 30 minuti, 1 ora, 2 ore o 8 ore) dopo il quale la sessione scade automaticamente e viene richiesto un nuovo login. Si applica per utente, non globalmente. L'inattività conta davvero anche con la pagina aperta: gli aggiornamenti automatici in background non mantengono viva la sessione, mentre l'uso reale (clic, tastiera) sì.
- **Sessioni attive** — dal proprio profilo ciascuno può vedere e chiudere le proprie sessioni. Le sessioni di un utente vengono chiuse automaticamente quando la sua password cambia, quando l'account viene bloccato o eliminato.
- **Protezioni dell'accesso** — i tentativi di login (e di conferma 2FA) sono limitati per indirizzo IP, per rallentare chi prova password a caso; un codice 2FA già usato non viene accettato una seconda volta.

5.5 Server MCP (solo Amministratore)

Questa sezione espone SentinelCore ad **agenti AI autorizzati** tramite il protocollo MCP (Model Context Protocol), per consultare — e, se la chiave lo consente, agire su — vulnerabilità e punteggi di rischio in modo programmatico.

- **Endpoint** — l'indirizzo a cui un client MCP deve connettersi, con relativo frammento di configurazione JSON pronto da copiare.
- **Chiavi API** — ogni agente si autentica con una chiave dedicata, non con le credenziali di un utente umano. Per ogni chiave puoi vedere nome, prefisso, ambito (scope), data di creazione, ultimo utilizzo e scadenza, e revocarla in qualsiasi momento.
- **Ambito (scope) della chiave**:
- **read** — l'agente può solo consultare dati (vulnerabilità, rischio, asset);
- **write** — l'agente può anche compiere azioni (es. cambiare lo stato di una vulnerabilità, assegnarla, avviare una scansione). **Solo un Amministratore può creare una chiave con scope write** — è un ambito potenzialmente ad alto impatto, da concedere con cautela e solo ad agenti realmente fidati.

Se non usi integrazioni con agenti AI, questa sezione può restare semplicemente inutilizzata: non ha alcun effetto sul resto del sistema finché non generi una chiave.

© Dognet Technologies S.r.l. — P.IVA 04867480164

5.6 Network Discovery

Configura la scansione di rete automatica periodica (vedi anche capitolo 7):

- **Auto-rescan** — abilita/disabilita la scansione ricorrente e ne imposta la frequenza (da ogni ora a ogni 2 settimane);
- **Subnet di destinazione** — una o più subnet CIDR da scansionare (es. `192.168.1.0/24`); per subnet non direttamente raggiungibili serve una rotta statica configurata sul server;
- **Opzioni nmap** — tipo di scansione (full/ARP/ping), timing (da T0 "paranoid" a T5 "insane"), porte TCP da controllare, numero di porte UDP top da controllare, rilevamento OS e rilevamento versione dei servizi;
- **Modalità avanzata** — è possibile scrivere a mano gli argomenti nmap, per chi conosce lo strumento e vuole un controllo fine; l'anteprima del comando che verrà eseguito è sempre visibile prima di salvare. Per sicurezza le scansioni girano tramite un componente privilegiato dedicato che accetta solo un **elenco di opzioni consentite** e target validi (IP, CIDR, intervalli, nomi host): opzioni che leggono o scrivono file (come `-iL` o `-oN`) o script NSE vengono rifiutate, e un'opzione non ammessa produce un errore chiaro invece di una scansione parziale.

5.7 Logging

Configurazione del file di log applicativo: livello (da `trace`, il più dettagliato, a `error`, il più silenzioso — default `warn`), percorso del file di destinazione, giorni di conservazione degli archivi compressi. Le modifiche a livello e destinazione richiedono un riavvio del servizio per essere applicate; la conservazione (retention) invece si applica subito.

5.8 Assegnazione vulnerabilità

Decide come vengono prese in carico le vulnerabilità non ancora assegnate:

- **Automatica** — un processo in background assegna le nuove vulnerabilità dopo un ritardo configurabile (default 24 ore), abbinandole a team/utenti in base alle competenze (skill) dichiarate;
- **Manuale** — restano in attesa finché un amministratore non le assegna a mano (con un eventuale ritardo di "fallback manuale" oltre il quale scatta comunque un'assegnazione automatica di sicurezza).

5.9 Override permessi utente

Per policy predefinita, un Utente semplice che vuole modificare alcuni dati sensibili (campi di un dispositivo, titolo/descrizione di una vulnerabilità, ricalcolo del punteggio di rischio) non li modifica direttamente: crea una **proposta** che un amministratore o il team leader del team competente approva o rifiuta. Questa sezione permette di **disattivare quel workflow di proposta** per capacità specifiche, dando agli utenti modifica diretta:

Capacità	Se attiva
Modifica device	L'utente modifica direttamente criticità, tag, note e proprietario di un dispositivo, senza passare da una proposta
Modifica metadata vulnerabilità	L'utente modifica direttamente titolo e descrizione di una vulnerabilità (punteggio di rischio, CVSS e severity restano comunque riservati ad admin/team leader)
Ricalcolo punteggio di rischio	L'utente può forzare da solo il ricalcolo del punteggio di rischio di una vulnerabilità nel proprio ambito

Ogni modifica diretta fatta grazie a un override attivo resta comunque tracciata nella cronologia dell'oggetto modificato.

5.10 Database

Una vista di sola lettura sullo stato del database: stato online/offline, nome del database, dimensione totale, connessioni attive rispetto al limite massimo, e conteggio righe per ciascuna tabella. Utile per una diagnosi rapida senza dover accedere al server via terminale.

© Dognet Technologies S.r.l. — P.IVA 04867480164

6. 5. Team e utenti

6.1 Team

La pagina **Team** (visibile a Team Leader e Amministratore) elenca i team esistenti. Per ciascun team puoi configurare:

- **Nome, descrizione e avatar** — ogni team può avere un'immagine scelta tra gli avatar predefiniti per i gruppi, così si riconosce a colpo d'occhio nelle liste e nelle schede
- **Competenze (skill)** — l'elenco di competenze del team, usato dal motore di assegnazione automatica per abbinare le vulnerabilità al team più adatto
- **Contatti e integrazioni**:
- email di contatto del team;
- webhook Slack del team — il canale condiviso su cui arrivano gli avvisi automatici (es. scoperta di una vulnerabilità critical), indipendente dalle notifiche email personali di ciascun membro. Un pulsante **Testa** invia subito un messaggio di prova sul canale, per verificare che l'URL sia corretto prima di salvare;
- chat ID Telegram del team, per chi usa quel canale (richiede che un amministratore abbia configurato un bot Telegram per l'istanza).
- **Membri del team** — puoi aggiungere un utente esistente della piattaforma (cercandolo per nome/email) oppure un membro "esterno" che non ha un proprio account SentinelCore ma partecipa via nome ed email (utile per referenti esterni destinatari di notifiche, non per l'uso operativo del prodotto). Ogni membro ha un ruolo interno al team: **leader** o **contributor**.

6.2 Utenti

La pagina **Utenti** (visibile a Team Leader e Amministratore) mostra l'elenco di tutti gli account: username, email, ruolo di piattaforma e competenze (skill) individuali.

- Un **Amministratore** può creare nuovi account, cambiarne username e ruolo, e (a seconda della configurazione dell'istanza) sbloccare account bloccati per troppi tentativi di login falliti.
- Un **Team Leader** può modificare email, password e competenze dei membri del **proprio** team, ma non cambiarne username o ruolo di piattaforma — quelle operazioni restano riservate all'Amministratore.

Passando il mouse sul nome di un utente o di un team (in elenchi, assegnazioni, menzioni) compare una piccola scheda con le informazioni principali, senza dover aprire la pagina dedicata. Il ruolo, il team e i contatti di un team sono visibili a tutti gli utenti autenticati: servono a sapere a chi rivolgersi e a poter assegnare o menzionare le persone giuste.

Quando un amministratore o team leader imposta una password temporanea per un altro utente, all'account viene marcato l'obbligo di cambiarla al primo accesso successivo.

6.3 Competenze (skill)

Le competenze sono un catalogo condiviso (es. "Linux", "Windows Server", "Networking", "Web Application", ecc.) assegnabile sia a livello di team sia di singolo utente. Sono il criterio con cui il motore di **assegnazione automatica** (capitolo 4, sezione "Assegnazione vulnerabilità") sceglie a chi instradare una nuova vulnerabilità: più le competenze di un team/utente combaciano con la natura della vulnerabilità scoperta (es. servizio, sistema operativo), più è probabile che venga scelto.

© Dognet Technologies S.r.l. — P.IVA 04867480164

7. 6. Vulnerabilità e punteggio di rischio

7.1 Dashboard

La pagina iniziale (**Dashboard**) mostra un riepilogo dello stato generale: conteggi per severità, andamento nel tempo, e una tabella delle vulnerabilità critiche/alte più recenti — ordinata per **punteggio di rischio**, non per il semplice punteggio CVSS dello scanner (vedi sotto perché la differenza conta).

7.1.1 Il grafico "Vulnerability Trend" e il dettaglio di un giorno

Ogni colonna del grafico rappresenta le vulnerabilità **aperte in quel giorno** (scoperte entro quel giorno e non ancora risolte alla sua fine), negli ultimi 30 giorni. **Cliccando su una colonna** si apre al centro dello schermo un pannello con il dettaglio di quel giorno, e la colonna scelta cambia colore:

- **Titolo** — la data, con due frecce agli estremi (sinistra e destra) per passare al giorno precedente o successivo senza chiudere il pannello; funzionano anche le frecce ← → della tastiera, e Esc chiude;
- **A sinistra (circa metà pannello)** — un grafico a rosa per severity: tutte le fette hanno lo stesso angolo e la **lunghezza** dice quante vulnerabilità ci sono; il totale è scritto al centro, il numero dentro ogni fetta, e ogni fetta ha la sua etichetta esterna con nome, numero e percentuale, collegata da una linea;
- **A destra** — tre numeri (vulnerabilità aperte quel giorno con la differenza rispetto al giorno prima, nuove, risolte), le **vulnerabilità più critiche** di quel giorno e gli **host più esposti**. Cliccando una vulnerabilità o un host si apre la sua pagina di dettaglio; in fondo i pulsanti *Tutte le vulnerabilità* e *Tutti gli host* portano agli elenchi.

7.1.2 La colonna "Trend" delle vulnerabilità recenti

Nella tabella delle vulnerabilità critiche/alte (e nell'elenco Vulnerabilità) la colonna **Trend** non è un grafico: è un indicatore basato su dati reali, perché per la singola vulnerabilità non esiste una serie storica. Mostra una freccia rossa verso l'alto se la vulnerabilità è stata **riaperta** (con il numero di volte), una freccia verde verso il basso se è **risolta**, una freccia blu se è **in corso**, un trattino se è **stabile**.

7.2 Il punteggio di rischio: perché non basta il CVSS

Ogni vulnerabilità importata porta con sé un punteggio CVSS (la "gravità tecnica" assegnata dallo scanner o dal database CVE), ma SentinelCore calcola per ciascuna anche un **punteggio di rischio** proprietario, su scala 0–100, che combina:

- il punteggio **CVSS** di base;
- la probabilità reale di sfruttamento (**EPSS**, aggiornata quotidianamente);
- l'**impatto di business** dell'asset coinvolto (quanto è critico quel sistema per l'organizzazione);
- l'**esposizione** dell'asset (è raggiungibile da Internet? è su una rete interna segmentata?);
- la **disponibilità di exploit** noti e pubblici.

Sopra a questo calcolo composito esistono override che forzano il punteggio verso l'alto indipendentemente dal resto, per tre categorie che meritano sempre priorità assoluta: vulnerabilità **zero-day**, CVE **sfruttate attivamente da campagne ransomware** e CVE presenti nel catalogo **CISA KEV** (Known Exploited Vulnerabilities — sfruttate attivamente "in the wild").

© Dognet Technologies S.r.l. — P.IVA 04867480164

Il punteggio di rischio determina anche il **livello di rischio** (risk tier) della vulnerabilità — Critical / High / Medium / Low — a cui è agganciata la scadenza SLA di rimedio:

Livello di rischio	Scadenza (SLA)
Critical	1 giorno
High	7 giorni
Medium	30 giorni
Low	90 giorni

7.3 Elenco vulnerabilità

La pagina **Vulnerabilità** mostra tutte le vulnerabilità note, filtrabili per severità, stato, team/utente assegnato, asset e testo libero. Per ogni riga sono visibili severità, punteggio di rischio, stato e assegnazione corrente.

Con il **tasto destro** su una riga (o su più righe selezionate) trovi le azioni rapide, tra cui **Aggiungi al piano di remediation (bozza)**: apre l'elenco dei piani ancora in bozza e aggiunge a quello scelto gli host delle vulnerabilità selezionate (vedi capitolo 9).

7.3.1 Stati di una vulnerabilità

- **Open** — scoperta, non ancora in lavorazione;
- **In progress** — qualcuno la sta lavorando;
- **Resolved** — risolta;
- **Closed** — chiusa (dopo verifica, se prevista dal piano di remediation);
- **Reopened** — era risolta/chiusa ma è stata rilevata di nuovo in una scansione successiva: viene segnalata separatamente dalle "open" ordinarie perché indica una regressione, non solo un ritardo.

7.3.2 Assegnazione

Un Amministratore può assegnare una vulnerabilità (o più in blocco) a un team o a un utente specifico. In alternativa, se la policy "Assegnazione vulnerabilità" (capitolo 4) è impostata su **automatica**, il sistema la assegna da solo dopo il ritardo configurato, in base alle competenze di team/utenti disponibili.

Ogni utente trova le vulnerabilità assegnate a sé (direttamente o tramite il proprio team) nella voce di menu **Le mie vulnerabilità**, e il proprio carico di lavoro complessivo — insieme a statistiche di risoluzione e classifiche — nella dashboard dedicata al carico di lavoro.

7.4 Dettaglio di una vulnerabilità

Aprendo una vulnerabilità trovi: descrizione tecnica, riferimenti CVE/CWE, cronologia degli eventi (timeline), e una sezione **commenti** dove puoi discutere il caso con il team:

- le risposte si possono annidare a **qualsiasi livello** (non solo due); oltre una certa profondità il rientro smette di crescere, così il thread resta leggibile;
- scrivendo `@` compare l'**autocompletamento** con tutti gli utenti della piattaforma: scegline uno per menzionarlo. **Solo le persone menzionate** ricevono la notifica in-app, non l'intero team;
- l'etichetta **Internal** è solo un'indicazione ("nota interna"): non limita chi può leggere il commento.

Nella parte centrale, sotto descrizione e rimedio, trovi **Threat intelligence** e **Asset interessato**; a destra riepilogo del rischio, riapertura, sorgenti e assegnazione. Le righe della stessa CVE su host diversi sono vulnerabilità distinte: dall'elenco ogni riga apre proprio la sua.

Per le CVE presenti nel catalogo **CISA KEV** il dettaglio mostra una scheda dedicata con i dati del catalogo: vendor e prodotto, nome della vulnerabilità, data di inserimento, azione richiesta, scadenza e indicazione di uso in campagne ransomware. Se la CVE è stata arricchita da **NVD**, la scheda riporta anche l'esito dell'arricchimento.

© Dognet Technologies S.r.l. — P.IVA 04867480164

La **timeline** registra anche questi passaggi automatici: *eseguito arricchimento NVD* (o *CVE non trovata su NVD*), *riscontrato nel catalogo KEV*, *rimosso dal catalogo KEV* e *segnalato come sfruttato da ransomware*.

Se il catalogo KEV non è ancora stato scaricato, la scheda lo dice ("Catalogo CISA KEV non ancora scaricato") invece di dichiarare la CVE non presente.

Avviare gli aggiornamenti a mano (Amministratore). Il catalogo KEV e l'arricchimento NVD si aggiornano da soli ogni 24 ore e all'avvio del servizio. Dalla tabella **Vulnerabilità**, l'icona **Avvia aggiornamenti** offre *KEV + NVD*, *solo KEV* o *solo NVD*: il KEV parte subito e mostra quante vulnerabilità risultano nel catalogo, l'arricchimento NVD prosegue in background.

Quando crei una vulnerabilità a mano, il modulo si apre sempre **vuoto**: i dati dell'ultima vulnerabilità inserita non vengono riproposti.

La **timeline** della vulnerabilità (cronologia degli eventi) è leggibile da ogni utente autenticato, indipendentemente dal ruolo o dal team.

7.5 Accettazione del rischio (risk acceptance)

Per vulnerabilità che, per motivi tecnici o di business, si decide consapevolmente di **non risolvere** (o non nell'immediato), un Amministratore può avviare un percorso di accettazione del rischio: la decisione viene approvata, motivata, e resta soggetta a rinnovo/revisione periodica invece di restare silenziosamente "aperta" a tempo indefinito.

Il punteggio di rischio descritto sopra è il dato usato ovunque nell'applicazione compaia una nozione di "priorità" o "rischio" — dashboard, tabelle, e soprattutto i report (capitolo 9): il CVSS grezzo resta visibile solo come dettaglio tecnico della singola vulnerabilità, mai come criterio di ordinamento o di somma aggregata.

© Dognet Technologies S.r.l. — P.IVA 04867480164

8. 7. Rete e asset

SentinelCore distingue due percorsi distinti che è utile non confondere:

- **Network Discovery** — scopre *dispositivi* sulla rete (IP, MAC, hostname, sistema operativo, porte aperte) e li mostra come nodi di una topologia. Non genera da sola vulnerabilità: mappa "cosa c'è in rete".
- **Import scanner** (capitolo 8) — importa *vulnerabilità* trovate da uno scanner esterno o dai connettori OpenVAS e Nessus, e le collega agli asset noti.

8.1 Scansione di rete

Dalla pagina **Discovery** puoi avviare una scansione manuale immediata, oltre a quella pianificata configurabile in Impostazioni (capitolo 4). Puoi scegliere al volo tipo di scansione, timing e opzioni, oppure usare i valori di default configurati dall'amministratore.

Al termine, la mappa di **topologia di rete** mostra i dispositivi scoperti come nodi, con indicazione visiva di stato (online/offline) e del numero di vulnerabilità note per dispositivo.

8.2 La mappa di topologia

La pagina **Topologia di rete** è una mappa interattiva dei dispositivi. Team Leader e Amministratori dispongono di tutti i comandi qui sotto; gli Utenti consultano la mappa (zoom, scorrimento trascinando lo sfondo, dettaglio degli host). La disposizione salvata è **una sola, condivisa da tutti**.

8.2.1 Muoversi e selezionare

Azione	Come
Spostare un host	trascinalo; se fa parte di una selezione si muove **l'intera selezione**, mantenendo le distanze
Selezionare più host	trascina un riquadro sullo sfondo vuoto, oppure `Ctrl` +clic sui singoli host; `Esc` annulla la selezione
Zoom	`Ctrl` +rotellina (centrato sul puntatore) o i pulsanti lente nella barra
Scorrere la mappa	tasto centrale del mouse trascinando (chi può solo consultare la mappa scorre trascinando lo sfondo), oppure le **frecce** direzionali della tastiera
Inquadrare tutto	pulsante **Fit**: adatta zoom e posizione a tutto ciò che è visibile nella finestra, senza ingrandire troppo
Salvare la disposizione	pulsante **Salva** nella barra: si accende quando c'è qualcosa da salvare
Schermo intero	pulsante in alto a destra; menu e finestre restano visibili anche a schermo intero

I nodi non possono finire sotto l'intestazione o i pannelli che stanno sopra la mappa: c'è un'area sicura in alto e a sinistra, e un host trascinato si ferma al bordo. Le disposizioni salvate in versioni precedenti che avevano nodi troppo in alto vengono abbassate automaticamente all'apertura, senza segnarle come modificate. Sulle reti grandi la mappa si **apre già centrata** sugli host, così non devi cercarli.

(Pro) L'edizione Pro mostra in alto a destra una **minimappa**: una vista in miniatura dell'intera rete con un rettangolo che indica la porzione visibile. Cliccando o **trascinando il rettangolo** ci si sposta rapidamente — molto utile quando gli host sono troppi per stare tutti nella finestra.

Con il **tasto destro** su uno o più host si apre il menu dei dispositivi: dettaglio, **nascondi icona** (l'host resta nel sistema, sparisce solo dalla mappa; il pulsante con l'occhio li mostra di nuovo), **colore** del nodo, assegnazione e altre azioni.

© Dognet Technologies S.r.l. — P.IVA 04867480164

8.2.2 Le tre viste

Il selettore in alto cambia la disposizione:

- **Subnet Grid** — gli host sono raccolti per sottorete (`/24`) in riquadri, e **la disposizione è quella salvata**;
- **Hierarchical** — a livelli: router e firewall in alto, poi switch, server ed endpoint;
- **Circular Topology** — gli host su un cerchio.

Nelle viste Hierarchical e Circular gli host sono **raggruppati per sottorete**: ogni sottorete è un blocco con il suo riquadro (nella gerarchica i blocchi stanno uno accanto all'altro, a capo dopo tre; nella circolare stanno su un cerchio grande, con gli host di ciascuna su un cerchio piccolo). Il pulsante ▣ toglie o rimette il raggruppamento. È molto comodo con reti grandi, perché un gruppo si può comprimere.

Se sposti degli host in una di queste viste e salvi, la **posizione viene ricordata per quella vista**: Subnet Grid, Hierarchical e Circular (raggruppata o no) hanno ciascuna la propria disposizione e non si sovrascrivono a vicenda.

8.2.3 Sottoreti: riquadri mobili e comprimibili

Il riquadro di una sottorete **segue gli host**: se ne sposti uno il riquadro si adatta. Trascinando l'**intestazione** del riquadro (la fascia con il nome della rete, ad esempio `10.10.0.0/24`) si spostano insieme tutti gli host del gruppo. Il triangolino a sinistra del nome **comprime il gruppo** in una scheda con la rete e il numero di host; cliccandolo di nuovo il gruppo si riapre. Quando due gruppi compressi sono collegati da più linee, vedi **una sola linea** con la scritta "N links", per non sovrapporre decine di tratti: per modificare le singole linee riapri i gruppi. Quali gruppi sono compressi è una preferenza personale, ricordata per ogni utente.

8.2.4 Le linee di collegamento

- **Linee azzurre tratteggiate e animate** — sono i collegamenti **scoperti dagli scanner**: indicano asset che possono comunicare tra loro. Passando il mouse compare il tipo di collegamento, gli hop e la latenza. Il pulsante `⇄N` nella barra le mostra o le nasconde (se sono molte, oltre 120, restano ferme per non appesantire la mappa; se il sistema operativo è impostato per ridurre le animazioni, restano sempre ferme).
- **Linee arancioni** — sono i collegamenti **manuali**, disegnati da te: trascina il piccolo punto arancione che compare in alto a destra di un host fino a un altro host. Vanno salvate con il pulsante Salva.

Con il **tasto destro su una linea manuale** si apre un menu per personalizzarla:

Opzione	Scelte
Shape (forma)	Straight (diritta), Curved (curva), 90° rounded (a gomito con angoli arrotondati)
Stroke (tratto)	Solid, Dashed (tratteggiato), Dotted (puntinato)
Start / End	forma dell'estremità: None, Arrow (freccia), Dot (punto), Diamond (rombo)
Color	sei colori
Tag	*Lateral movement* (movimento laterale: rosso, tratteggiato, animato) e *Monitored segment* (segmento monitorato: azzurro); il tag imposta colore, tratto e animazione, che puoi poi ritoccare, e scrive la dicitura sulla linea
Animation	Still (ferma) o Flowing (con scorrimento)
Edit label…	scrive un'etichetta mostrata sulla linea
Delete	elimina la linea

Le linee si fermano al bordo degli host e sono cliccabili in una fascia più larga del tratto, per essere facili da prendere.

© Dognet Technologies S.r.l. — P.IVA 04867480164

8.3 Host / asset

La pagina **Host** elenca tutti gli asset conosciuti (scoperti via rete o creati manualmente), con hostname, indirizzo IP, sistema operativo, tipo di dispositivo, criticità e stato. Quando un host non ha un hostname noto (succede spesso in reti virtuali o dietro NAT, dove nessun protocollo di risoluzione risponde) il suo nome è l'indirizzo IP, mostrato **una volta sola** e senza la maschera `/32`.

Da qui puoi:

- aprire il dettaglio di un singolo host — mostra le informazioni dell'asset (non avvia direttamente azioni sulle sue vulnerabilità: quelle si gestiscono dalla pagina Vulnerabilità, filtrando per quell'asset);
- modificare in blocco più dispositivi selezionati (es. assegnare un proprietario, un livello di criticità, dei tag);
- **aggiungere gli host selezionati a un piano di remediation in bozza** (tasto destro → *Aggiungi al piano di remediation (bozza)*, vedi capitolo 9);
- eliminare in blocco dispositivi non più rilevanti.

8.3.1 Limite di host e stato «oltre licenza»

L'edizione **Community** gestisce fino a **15 host**. Quando ne scopri o ne crei di più, i 15 **più vecchi** (per data di prima scoperta) restano pienamente gestiti; gli altri passano in stato **«oltre licenza»**: restano **visibili e contati** nelle liste e nella mappa — così sai che esistono — ma **non vengono gestiti**, cioè non importano vulnerabilità e non entrano nei piani di remediation. Nella tabella Host la riga mostra l'indicatore **Oltre licenza**.

Il limite si applica **da solo**: scoprendo nuovi host o eliminandone, lo stato «oltre licenza» si ricalcola senza bisogno di riavviare nulla. Per gestirne di più serve l'edizione **(Pro)**, che alza il tetto a scaglioni e conta gli host **per ambiente** (produzione, testing, pre-produzione) separatamente.

8.3.2 Il dettaglio di un host: la scheda "RBRE & Compliance"

Aprendo il dettaglio di un host, nella scheda **System Configuration** trovi **RBRE & Compliance** (RBRE = Risk-Based Remediation Engine; il nome resta in inglese anche con l'interfaccia in italiano). È divisa in riquadri, e la differenza tra l'uno e l'altro è netta:

1. "Input del risk score" — evidenziato, con l'etichetta **Pilota il risk score**. Contiene **solo ed esclusivamente** i dati dell'host che entrano davvero nel calcolo del punteggio di rischio delle sue vulnerabilità (insieme a CVSS, EPSS ed exploit, che sono della vulnerabilità, non dell'host). Accanto a ogni valore trovi i **punti** che porta al calcolo; in modifica, sotto il campo, vedi i punti di tutti i valori possibili:

Campo	Valori e punti	Note
Business Criticality	Mission Critical 15 · Core Business 11 · Supporto 6 · Lab/Test 2	È il fattore con più peso. "Mission Critical" segnala un sistema il cui fermo blocca il business; "Lab/Test" un ambiente il cui compromesso ha impatto minimo.
Exposure Level	Internet Facing 12 · DMZ 10 · Internal 5 · Segmented 0	Quanto l'host è raggiungibile da un attaccante.
Data Classification	Public / Internal: nessun bonus · Sensitive / Critical: +5	Segnala che l'host tratta dati sensibili.
Data Processor (GDPR)	acceso: +5	Anch'esso segnala dati personali. **Non si somma** a Data Classification: i dati sensibili valgono +5 **una volta sola**, che a motivarli sia la classificazione, il flag, o entrambi.
IP pubblico *(sola lettura)*	Sì: esposizione al massimo (12)	Rilevato **automaticamente** dall'indirizzo (tutto ciò che non è nei range privati RFC 1918, loopback o link-local). Un IP pubblico porta l'esposizione al massimo qualunque sia l'Exposure Level; non c'è nulla da impostare a mano.

© Dognet Technologies S.r.l. — P.IVA 04867480164

2. "Contesto di remediation" e **3. "Compliance e note"** — sono **solo informativi**: Remediation Difficulty, Patch Available, Deployment Impact, Compensating Controls, Compliance Requirements, tag e note aiutano chi pianifica e assegna gli interventi e chi fa reportistica, ma **non entrano in nessun calcolo**.

Cosa è cambiato rispetto alle versioni precedenti. Prima esistevano campi doppi che dicevano la stessa cosa e potevano contraddirsi (ad esempio *Criticality* e *Business Criticality*, oppure *Internet Facing* ed *Exposure Level*). Ora sono unificati: **Criticality** deriva da Business Criticality, **Internet Facing** da Exposure Level e **Has Public IP** dall'indirizzo, e non si inseriscono più a mano — servono solo a ordinare gli host nei piani di remediation. Il campo *Device Use Case*, che aveva la stessa lista del tipo di dispositivo e non influenzava nulla, non è più mostrato. Il tipo di dispositivo si sceglie nella scheda *System Information* e guida l'icona.

Per policy predefinita, un utente semplice non modifica questi campi direttamente ma propone una modifica che un admin/team leader approva — vedi "Override permessi utente" nel capitolo 4 per attivare la modifica diretta.

8.3.3 Cloni in altre reti (testing e pre-produzione)

Di solito gli host sono asset **in produzione**, ma può esistere una copia dello stesso asset in una rete di **testing** e/o di **pre-produzione**: è dove conviene provare una remediation o una modifica prima di applicarla in produzione. La scheda **Cloni in altre reti** (sotto RBRE & Compliance, con la sua matita di modifica) serve a dichiararlo:

- **Clone in rete di Testing** e **Clone in rete di Pre-produzione** sono due caselle indipendenti. Spuntandone una si abilitano i campi del clone:
- **IP del clone** — l'indirizzo IP dell'host nell'altra rete (obbligatorio). Deve essere un IP **interno**: hostname, URL e indirizzi esterni (pubblici) vengono segnalati come errore e non si salvano;
- **Rete del clone** — la rete in cui sta il clone, in formato CIDR (es. `10.20.0.0/24`, obbligatoria). Deve contenere l'IP del clone e stare interamente in un blocco interno (`10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16`, `fc00::/7`). Di norma le reti di testing e di pre-produzione hanno indirizzamenti diversi da quella di produzione;
- **ID del dog_agent sul clone** — l'identificativo dell'agent che gira su quel clone (obbligatorio). Sono ammessi lettere, numeri e i simboli `. _ : -`. Nel suo `config.toml` quell'agent deve dichiarare `environment = "testing"` o `environment = "preproduction"`, secondo la rete del clone;
- **Allineato alla produzione** — una spunta per dichiarare esplicitamente che il clone ha le stesse versioni dei servizi e gli stessi aggiornamenti. Dovrebbe esserlo sempre, ma scriverlo dice a chi lo usa se può fidarsi del test.
- Togliendo la spunta, i dati di quel clone vengono cancellati: non restano valori vecchi dimenticati.
- Modifica e salvataggio seguono le stesse regole degli altri dati del dispositivo (Amministratore e Team Leader del team dell'host; un Utente solo con l'override di modifica diretta, vedi capitolo 4).

È un'informazione **solo organizzativa**: oggi non entra in nessun calcolo (né nel punteggio di rischio né nei piani di remediation) e non avvia nessuna azione sul clone. È predisposta perché in futuro venga **esportata verso le integrazioni tra gli host** della suite.

(Pro) Nell'edizione Pro testing e pre-produzione diventano **ambienti con un proprio conteggio** di host (ciascuno con il suo tetto, in base allo scaglione di licenza) e l'ambiente **modula il punteggio di rischio**: produzione a peso pieno, pre-produzione ridotto, testing molto ridotto. Nell'edizione Community l'informazione resta solo organizzativa, come descritto qui sopra.

8.3.4 Il riepilogo remediation di un host

In fondo alla stessa pagina la scheda **Remediation Summary** riguarda **solo l'host che stai guardando** (il suo nome è scritto nell'intestazione). I numeri contano i **piani di remediation che includono questo host**, escluse le bozze e i piani annullati: un piano con quattro host conta 1 su ciascuno dei quattro, quindi due host dello stesso piano mostrano lo stesso numero.

- **Piani in corso** — piani non ancora conclusi per questo host, con un link a ciascuno;
- **Piani completati** — piani in cui l'host risulta completato (tutte le sue vulnerabilità risolte);
- **Falliti o saltati**;
- **Ultima remediation conclusa su questo host** — nome del piano (con link), esito e data.

© Dognet Technologies S.r.l. — P.IVA 04867480164

9. 8. Scanner e integrazioni

9.1 Import da file scanner

La pagina **Import scanner** (Team Leader e Amministratore) permette di caricare il file di risultati esportato da uno scanner di terze parti. SentinelCore riconosce il formato e ne estrae le vulnerabilità, normalizzando la severità su una scala comune ed evitando duplicati quando la stessa vulnerabilità viene rilevata più volte.

Scanner supportati:

Scanner	Formato tipico
Qualys	XML
Nessus	.nessus (XML)
Burp Suite	XML
OpenVAS / GVM	XML
Nexpose / InsightVM	XML
OWASP ZAP	XML/JSON
Nmap	XML
Nikto	XML/CSV
Trivy	JSON
Grype	JSON

9.2 Connettore OpenVAS diretto (senza esportare file a mano)

Se disponi di un'istanza OpenVAS/GVM, un Amministratore può configurarne la connessione diretta dalla pagina **Plugin** → *Greenbone/OpenVAS* → **Configura**: host e **porta** del servizio GMP (oppure il percorso del socket unix, solo se SentinelCore gira sulla stessa macchina di GVM), credenziali GMP, nome del task da seguire, intervallo di polling e quanti giorni di storico importare al primo avvio. Una volta configurato, il connettore interroga periodicamente GVM e importa da solo i report completati del task — non serve più esportare e caricare file manualmente.

9.2.1 Prerequisiti (importante)

Il connettore dialoga con GVM tramite `gvm-cli` (dal pacchetto *gvm-tools*), che va **installato sul server SentinelCore**, e richiede che GVM esponga **GMP su TCP+TLS** (tipicamente la porta **9390**).

1. Installa gvm-tools sul server SentinelCore. Su Debian 13 il pacchetto non è nei repository apt: si installa con pip.

```
sudo python3 -m pip install gvm-tools --break-system-packages
```

Verifica con `gvm-cli --version`. Dev'essere in `/usr/local/bin` (nel PATH del servizio `sentinelcore`).

2. Esponi GMP su TCP+TLS (porta 9390). Il connettore si collega al **Greenbone Management Protocol (GMP)** via TLS sulla porta **9390** per elencare e scaricare i report. Le installazioni GVM recenti tengono `gvmd` **solo sul socket unix locale**: da un'altra macchina non è raggiungibile finché non esponi GMP su TCP. Le porte **9392** / **443** che vedi aperte sul server OpenVAS sono la **web UI (GSA)**, *non* GMP — un test TLS lì dà `WRONG_VERSION_NUMBER`.

© Dognet Technologies S.r.l. — P.IVA 04867480164

9.2.2 Caso Greenbone Community (Docker)

Con i **container Greenbone Community** (docker compose), `gvmd` gira in un container col socket in un volume `..._gvmd_socket_vol`. Per esporre GMP su 9390 si usa un relay **socat con TLS** verso quel socket. **Sull'host dei container OpenVAS:**

```
# 1. certificato self-signed per il relay TLS
openssl req -x509 -newkey rsa:2048 -nodes -keyout gmp.key -out gmp.crt \
  -days 3650 -subj "/CN=gvm-gmp"
cat gmp.key gmp.crt > gmp.pem && chmod 600 gmp.pem

# 2. individua il volume col socket di gvmd
docker volume ls | grep -i gvmd        # es. greenbone-community-edition_gvmd_socket_vol

# 3. relay socat TLS:9390 -> socket unix di gvmd (sostituisci <VOLUME>)
docker run -d --name gmp-tls-relay --restart unless-stopped \
  -p 9390:9390 \
  -v <VOLUME>:/run/gvmd \
  -v "$PWD/gmp.pem:/gmp.pem:ro" \
  alpine/socat \
  OPENSSL-LISTEN:9390,reuseaddr,fork,cert=/gmp.pem,verify=0 UNIX-CONNECT:/run/gvmd/gvmd.sock
```

Verifica dal server SentinelCore prima di usare la UI:

```
gvm-cli --gmp-username <utente> --gmp-password <password> \
  tls --hostname <ip-openvas> --port 9390 --xml "<get_version/>"
```

Una risposta `<get_version_response status="200" ...><version>22.x</version>` conferma che GMP è raggiungibile. A quel punto nel connettore imposti **host** = IP di OpenVAS e **porta** = `9390`, e il **Test connessione** passa (mostra la versione GMP). Il cert self-signed del relay va bene: la connessione è autenticata con le credenziali GMP, non col certificato.

Il connettore è **in sola lettura**: legge i report completati del task configurato e li importa con la stessa deduplica dell'import da file. Le voci informative (severità *Info*) non vengono importate.

9.3 Connettore Nessus diretto

Lo stesso tipo di collegamento è disponibile per **Tenable Nessus**, sia nell'edizione gratuita *Essentials* sia in *Professional*. Non serve indicare quale delle due usi: SentinelCore la riconosce da solo e la mostra nel test di connessione. La release certificata è la **10.12.x**. Le altre 10.x vengono segnalate come «non certificate» ma di norma funzionano; le versioni con un numero principale diverso vengono indicate come non supportate.

Dalla pagina **Plugin**, un Amministratore apre il menu contestuale della riga *Tenable Nessus* → **Configura** e inserisce:

- l'**URL** di Nessus (es. `https://nessus.lan:8834`). Se Nessus usa ancora il certificato self-signed dell'installazione, disattiva la verifica TLS;
- le **chiavi API**, consigliate: in Nessus si trovano in *Settings* → *My Account* → *API Keys* → *Generate*. La secret key viene mostrata una sola volta, e rigenerarla invalida quella precedente. In alternativa puoi usare **utente e password**, se la tua edizione non mostra la scheda delle chiavi API;
- facoltativamente il **nome della scansione** da seguire. Lasciandolo vuoto vengono importate tutte le scansioni visibili all'utente;
- l'**intervallo di polling**, cioè ogni quanti minuti cercare esecuzioni nuove (da 1 a 1440, predefinito 30), e quanti giorni di storico importare al primo avvio.

Test connessione verifica raggiungibilità e credenziali senza salvare. Mostra edizione, versione, numero di scansioni visibili, il modo in cui verranno letti i risultati e un avviso se la scansione indicata non esiste. Dopo il salvataggio attiva il plugin con **Attiva**/**Disattiva**.

Il connettore è **in sola lettura**: non crea e non avvia scansioni, che restano gestite in Nessus. A ogni giro legge le esecuzioni completate dopo l'ultima importata e le importa con la stessa deduplica dell'import da file. *Professional* e le altre edizioni le scaricano in formato `.nessus`. *Essentials* non permette l'export via API, quindi i risultati vengono letti dalle pagine di dettaglio di host e plugin: il contenuto importato è lo stesso. Ricorda che Essentials limita ogni scansione a 5 indirizzi IP. Le voci puramente informative (severità *Info*) non vengono importate. Se un'esecuzione non si riesce a scaricare, il connettore si ferma lì e la riprova al giro successivo, senza saltarla. Per le credenziali conviene un utente Nessus dedicato che possa solo vedere i risultati.

Nello storico di **Scanner imports** la colonna *Scanner* riporta l'edizione rilevata, per esempio *Nessus Essentials* o *Nessus Professional*.

© Dognet Technologies S.r.l. — P.IVA 04867480164

9.4 Sincronizza ora

I connettori che importano report (OpenVAS e Nessus) hanno nella finestra di configurazione il pulsante **Sincronizza ora**. Avvia subito un giro, senza aspettare l'intervallo di polling: è utile appena finisce una scansione lanciata a mano. Usa la configurazione salvata, quindi salva prima eventuali modifiche, e il plugin deve essere attivo. Se in quel momento il giro automatico è già in corso, il pulsante lo segnala invece di importare due volte.

9.5 Integrazione JIRA

Per team che tracciano il lavoro anche su JIRA, un Amministratore può configurare la sincronizzazione bidirezionale: creazione automatica di ticket per nuove vulnerabilità (secondo criteri configurabili) e aggiornamento di stato in entrambe le direzioni.

9.6 Notifiche

Le **regole di notifica** (accessibili dalla relativa voce di menu, gestite da un Amministratore) decidono chi viene avvisato, quando e su quale canale, in base a condizioni configurabili (es. severità, team assegnato). Per ciascuna regola puoi impostare:

- priorità e condizioni di attivazione;
- canali di invio: email, Slack, Telegram;
- se l'invio è immediato o raggruppato, con un intervallo minimo tra due notifiche simili (throttling) per evitare di sommergere le persone di messaggi;
- eventuali "orari di silenzio" in cui non inviare notifiche non urgenti.

Perché email/Slack/Telegram funzionino davvero servono, rispettivamente: un server SMTP configurato (capitolo 4), un webhook Slack (personale in Profilo, o di team nella pagina Team — entrambi testabili con un pulsante dedicato prima di fidarsene; l'indirizzo viene controllato e deve essere un vero *Incoming Webhook* di Slack, `https://hooks.slack.com/…`), e un bot Telegram configurato dall'amministratore per l'istanza.

9.7 Webhook SOAR in uscita (uso avanzato)

Per integrazioni con piattaforme SOAR esterne, SentinelCore può inviare eventi in uscita verso un webhook configurato da un Amministratore — utile per orchestrare automazioni di risposta al di fuori di SentinelCore stesso.

© Dognet Technologies S.r.l. — P.IVA 04867480164

10. 9. Report e piani di remediation

10.1 Generare un report

Dalla pagina **Report → Nuovo report** (Team Leader e Amministratore) puoi generare un **report di gestione** per un intervallo di date, opzionalmente filtrato per team e/o singolo asset. Il report che ne risulta include diverse sezioni:

- **Riepilogo esecutivo** — conteggi di vulnerabilità totali, nuove, risolte, aperte, in lavorazione, riaperte nel periodo, rischio eliminato e rischio residuo;
- **Metriche di gestione** — tempo medio di risoluzione (MTTR) per livello di rischio, rispetto delle SLA, distribuzione per anzianità delle vulnerabilità ancora aperte;
- **Analisi del rischio** — le vulnerabilità aperte più critiche e quelle risolte più rilevanti nel periodo;
- **Performance dei team** — confronto tra team su volumi e tempi di risoluzione;
- **Dettaglio vulnerabilità** — elenco puntuale delle vulnerabilità aperte e in lavorazione.

Quando generi un report filtrato per un team specifico, **tutte** le sezioni rispettano quel filtro: vedrai solo dati relativi a quel team, non all'intera organizzazione.

Importante: in ogni report, ovunque compaia un valore di "rischio" — rischio eliminato, rischio residuo, la colonna nelle tabelle di dettaglio vulnerabilità, il rischio eliminato per team — il dato mostrato è sempre il **punteggio del motore di prioritizzazione** (risk score/tier, vedi capitolo 6), non il semplice punteggio CVSS. Il CVSS resta visibile come informazione tecnica altrove (dettaglio della singola vulnerabilità), ma non è mai il criterio con cui i report ordinano o sommano il rischio.

10.2 Cronologia report

Report → Cronologia elenca tutti i report generati in precedenza, con possibilità di riaprirli, scaricarli o eliminarli (in blocco, se necessario).

10.3 Piani di remediation

Un **piano di remediation** (creato e modificato da Team Leader e Amministratori; l'eliminazione è riservata all'Amministratore) è un **ordine di lavoro**: un amministratore decide che un insieme preciso di vulnerabilità va sistemato e lo affida a un team. Il criterio non è per forza il rischio: può essere "tutte le vulnerabilità critiche", ma anche "quelle di rischio basso su questa rete perché siamo sotto audit". Per questo il piano contiene **vulnerabilità scelte con precisione**, non host interi: gli host del piano sono quelli delle sue vulnerabilità, e **una vulnerabilità nuova comparsa su un host del piano non ci entra da sola**. L'avanzamento è la percentuale di vulnerabilità del piano realmente risolte o chiuse (la colonna *Progress* della lista, ad esempio "50% (4/8)"). Ha un titolo, uno stato, una sezione commenti per coordinare il lavoro e, al completamento, una fase di verifica per confermare che il rimedio abbia funzionato (es. dopo una nuova scansione).

È lo strumento giusto quando la risoluzione di più vulnerabilità richiede un intervento coordinato (es. un aggiornamento pianificato su un gruppo di server), invece di lavorare le vulnerabilità una per una senza un contesto comune.

10.3.1 Il ciclo di vita di un piano

- **Bozza** — in preparazione: il team assegnato **non lo vede e non riceve notifiche**. È l'unico stato in cui si può cambiare il contenuto del piano.
- **Attivo** — comunicato al team (qui parte la notifica), pronto ma non ancora iniziato. Da ora l'elenco degli host è bloccato.
- **In corso** — il team ci sta lavorando (si imposta a mano).
- **Completato** — passa **da solo e subito**, nello stesso istante in cui l'ultima vulnerabilità del piano viene risolta o chiusa: non serve chiuderlo a mano e non c'è da aspettare. Anche gli host del piano risultano completati (un host si completa già prima, quando le sue vulnerabilità sono tutte risolte), la lista dei piani si aggiorna da sola e il team assegnato riceve l'avviso di completamento (email, Slack,

© Dognet Technologies S.r.l. — P.IVA 04867480164

Telegram secondo le sue impostazioni) entro un minuto. Una bozza non si chiude mai da sola, e un piano concluso non si riapre se una vulnerabilità viene riaperta in seguito.

- **Annullato** — piano abbandonato.

10.3.2 Creare un piano

Da **Piani di remediation → Nuovo piano**. Il modulo ha queste sezioni:

- **Informazioni generali** — nome e descrizione.
- **Pianificazione**:
- **Priorità** (P1 Critica … P4 Bassa) — è **solo un'etichetta informativa** sul piano, utile per ordinarlo e segnalarlo nella lista: non influenza quali vulnerabilità finiscono nel piano;
- **Stato** — vedi sopra (un piano nuovo parte in bozza);
- **Data scadenza** e **Team assegnato** — facoltativi.
- **Contenuto del piano** — dove scegli quali vulnerabilità includere (sotto).

10.3.3 Scegliere il contenuto del piano

Nella sezione **Contenuto del piano** vedi in alto le vulnerabilità già incluse, raggruppate per host (con il totale "N vulnerabilità su M host"), e sotto il riquadro **Cerca vulnerabilità da aggiungere**. I criteri sono tutti facoltativi e **si combinano** (tutti insieme devono essere veri; più valori dello stesso criterio sono alternativi):

- **Testo libero** — titolo, CVE, nome host o IP;
- **Reti / IP** — uno o più CIDR o IP, per esempio `10.0.1.0/24` (le reti non valide vengono segnalate);
- **CVE** — una o più;
- **Team proprietario dell'host** ed **Esposizione** (esposti su internet / solo interni);
- **Tipo di host** — server, firewall, database…;
- **Livello di rischio** del nostro motore di prioritizzazione (Critical…Info, capitolo 6) e **Gravità** dello scanner;
- **Solo sfruttate (catalogo KEV)**.

Premi **Cerca**: compaiono i totali ("N vulnerabilità su M host corrispondono") e i risultati raggruppati per host. Da lì:

- spunta le singole vulnerabilità (o l'intestazione di un host per tutte le sue) e premi **Aggiungi N selezionate**;
- oppure **Aggiungi tutte (N)** per includere tutto ciò che la ricerca ha trovato;
- oppure, sull'**intestazione di un host** (menu ⋮ o tasto destro), **Aggiungi tutte le vulnerabilità dell'asset** o **Aggiungi quelle di rischio X o superiore**.

Una ricerca senza criteri non è ammessa: non significa "tutto". Le vulnerabilità già nel piano non vengono riproposte, e con più di 500 risultati l'elenco mostra solo i primi (i totali restano esatti): in modifica **Aggiungi tutte** le comprende comunque tutte, in creazione conviene restringere i criteri.

Per **togliere** una vulnerabilità usa la X sulla sua riga, per togliere un intero host la X sull'intestazione, **Svuota il piano** per ricominciare.

- Creando un nuovo piano, le vulnerabilità scelte vengono salvate insieme al piano (una nota sotto l'elenco lo ricorda).
- Modificando un piano **in bozza**, aggiunta e rimozione sono **immediate**.
- Su un piano che **non è più in bozza** il contenuto è in sola lettura, con la nota *"Il contenuto di un piano si può cambiare solo finché è in bozza"* (anche il server rifiuta la modifica).
- I piani creati prima di questa versione conservano le vulnerabilità che coprivano di fatto (tutte quelle dei loro host al momento dell'aggiornamento); da lì in poi non assorbono più vulnerabilità nuove.

© Dognet Technologies S.r.l. — P.IVA 04867480164

10.3.4 Aggiungere a un piano in bozza da altre pagine

Dalle pagine **Host** e **Vulnerabilità**, con il **tasto destro**, trovi la voce **Aggiungi al piano di remediation (bozza)**: si apre l'elenco dei piani **in bozza** (se non ce ne sono, la voce dice "Nessun piano in bozza"). Scegli il piano e l'azione si applica a **tutta la selezione** (più righe selezionate) oppure alla riga sotto il puntatore.

- Da **Host** si aggiungono **tutte le vulnerabilità aperte** degli host selezionati.
- Da **Vulnerabilità** si aggiungono **solo le vulnerabilità selezionate**, non quelle del loro host.
- Un messaggio riassume l'esito, ad esempio *"3 vulnerabilità aggiunte al piano «Patch Q4» · 1 già presenti"*. Le vulnerabilità che non hanno un dispositivo di rete collegato non possono stare in un piano.
- La voce è disponibile a Team Leader e Amministratori.

10.4 Carico di lavoro e classifiche

La dashboard **Carico di lavoro** mostra, per te e per il tuo team, quante vulnerabilità sono assegnate, quante risolte, e l'andamento nel tempo. Le classifiche di risoluzione permettono di vedere, in modo trasparente, chi sta contribuendo di più alla riduzione del rischio complessivo — pensate come stimolo collaborativo, non come strumento di controllo individuale.

© Dognet Technologies S.r.l. — P.IVA 04867480164

11. 10. Domande frequenti

Il browser mostra un avviso di sicurezza/certificato non valido al primo accesso. Normale se non hai ancora configurato un certificato TLS valido: SentinelCore genera un certificato auto-firmato per l'istanza. Puoi accettare l'eccezione nel browser, oppure configurare un dominio reale con certificato Let's Encrypt (vedi la documentazione tecnica `packaging/HTTPS.md`).

Ho dimenticato la password: come la recupero? Non esiste un recupero password "self-service" via email: è una scelta di sicurezza deliberata. Chiedi a un Amministratore, o al Team Leader del tuo team, di impostarti una password temporanea da **Utenti** — al login successivo ti verrà chiesto di sceglierne una nuova. Se sei l'unico account amministratore e hai perso l'accesso, serve un intervento diretto sul server da parte di chi lo gestisce.

Il pulsante "Testa" dell'SMTP dice che l'invio è fallito. Verifica in ordine: server e porta corretti, username/password corretti (se hai lasciato vuota la password pensando restasse quella già salvata, verifica che sia davvero già stata impostata in precedenza), che il server SMTP sia raggiungibile dal server SentinelCore (non dal tuo browser — è il backend a connettersi), e che non ci sia un firewall che blocca la porta usata.

Il pulsante "Testa" del webhook Slack non funziona. Controlla che l'URL sia un vero "Incoming Webhook" di Slack (inizia con `https://hooks.slack.com/`) generato dalla configurazione dell'app Slack, non un link generico al canale.

Le email di riepilogo/avviso non arrivano anche se SMTP è configurato. Controlla che l'interruttore "Invio email abilitato" in Impostazioni → SMTP sia acceso, e che l'utente destinatario abbia le relative opzioni attive in Impostazioni → Notifiche (o Profilo, per gli avvisi personali via Slack).

Un report filtrato per team mostra dati dell'intera azienda. Se questo accade, verifica di essere su una versione aggiornata: nelle versioni precedenti alla 1.2.0 alcune sezioni del report di gestione (Metriche, Analisi del rischio, Dettaglio vulnerabilità) non applicavano correttamente il filtro per team — un problema corretto a partire da quella versione. Aggiorna l'istanza (capitolo 1) se non l'hai già fatto.

La scansione di rete non trova nulla, o trova meno dispositivi del previsto. Verifica che la subnet configurata sia effettivamente quella su cui si trova SentinelCore (o che esista una rotta verso di essa), e che il tipo di scansione scelto sia adatto: uno scan "ping" o "ARP" trova meno informazioni di uno scan "full", che richiede però privilegi di rete più ampi sul server.

Il connettore OpenVAS/GVM dà errore sul test di connessione (`gvm-cli` non trovato, oppure `WRONG_VERSION_NUMBER` / timeout). Il connettore ha due prerequisiti, entrambi descritti in «Connettore OpenVAS diretto» nel capitolo 8. Primo: lo strumento `gvm-cli` (pacchetto *gvm-tools*) dev'essere installato sul server SentinelCore (su Debian 13 via `pip … --break-system-packages`); se manca, il test dice che `gvm-cli` non è nel PATH. Secondo: GVM deve esporre **GMP su TCP+TLS, tipicamente la porta 9390**. Perché 9390 e non la web UI? Perché il connettore parla il protocollo **GMP**, non HTTP: le porte della console web (spesso 9392 o 443) rispondono ma non sono GMP, e un test TLS lì dà `WRONG_VERSION_NUMBER`. Le installazioni GVM recenti (inclusi i container Greenbone Community) tengono `gvmd` sul solo socket unix locale: finché non esponi GMP su TCP — col relay socat TLS descritto nel capitolo 8 — da SentinelCore non è raggiungibile. Verifica con `gvm-cli … tls --port 9390 --xml "<get_version/>"` prima di usare la UI.

Non vedo alcune voci di menu che mi aspetto (Team, Utenti, Report, Piani di remediation, Import scanner). Sono visibili solo a Team Leader e Amministratore. Se il tuo ruolo è "Utente", è normale non vederle — vedi il capitolo 3 per il dettaglio dei permessi per ruolo.

Dopo un aggiornamento il servizio non riparte. Lo script di aggiornamento esegue da solo un controllo di salute e, se le migrazioni del database falliscono, ripristina automaticamente la versione precedente. Se invece le migrazioni sono andate a buon fine ma il servizio non risponde comunque, consulta i log (`journalctl -u sentinelcore -n 100`) e, in caso di dubbio, usa il backup del database creato automaticamente prima dell'aggiornamento (si trova in `/opt/sentinelsuite/sentinelcore/backups/`).

Ho risolto tutte le vulnerabilità di un piano ma lo stato è ancora "Attivo". Dalla 2.0.0 il piano passa a *Completato* da solo, nello stesso istante in cui l'ultima vulnerabilità viene risolta o chiusa. Se non succede, verifica che il piano non sia in **bozza** (le bozze non si chiudono da sole), che contenga almeno un host con vulnerabilità collegate, e che nessuna vulnerabilità dei suoi host sia ancora aperta o in lavorazione (la colonna *Progress* lo mostra). Se la lista che hai aperto non è aggiornata, ricarica la pagina; di norma si aggiorna da sola.

Aggiungendo vulnerabilità a un piano in bozza, il messaggio dice "senza dispositivo di rete". Un piano contiene dispositivi di rete, non singole vulnerabilità: una vulnerabilità o un asset inseriti a mano e mai collegati a un dispositivo scoperto dalla rete (o importato) non possono stare in un piano. Esegui una scansione di rete che scopra l'host, oppure verifica nel dettaglio dell'host che sia collegato a un dispositivo.

© Dognet Technologies S.r.l. — P.IVA 04867480164

Non riesco a togliere o aggiungere host a un piano. Gli host si cambiano solo finché il piano è in **bozza** e solo da Team Leader e Amministratori. Per un piano già Attivo, riportalo allo stato Bozza dal menu *Cambia stato* se devi modificarne gli host.

Nella mappa di topologia un host è finito sotto l'intestazione o i pannelli. Dalla 2.0.0 gli host non possono più uscire dall'area sicura in alto e a sinistra, e una disposizione salvata con host troppo in alto viene abbassata da sola all'apertura. Se vuoi comunque ripartire da una disposizione ordinata, passa dalla vista **Hierarchical** o **Circular** (che calcolano la disposizione da sole) e torna a **Subnet Grid**.

Cambiando vista (Hierarchical / Circular) non succedeva nulla. Era un difetto delle versioni precedenti: la disposizione salvata prevaleva su qualunque vista. Dalla 2.0.0 ogni vista ha la sua disposizione, calcolata o salvata a parte.

La sessione mi si chiude anche se lavoro. Il timeout di inattività è impostato per ogni utente in Impostazioni → Sicurezza. Conta l'uso reale della pagina (clic, tastiera): gli aggiornamenti automatici in background non tengono viva la sessione. Se vieni disconnesso mentre lavori, aumenta il valore.

Un host non mostra l'hostname, solo l'indirizzo IP. In reti virtuali o dietro NAT nessun protocollo di risoluzione (DNS inverso, mDNS, NetBIOS) risponde, quindi il nome non è recuperabile dalla scansione. Puoi impostarlo a mano dalla scheda *System Information* dell'host. Nelle reti reali, con DNS inverso o NetBIOS attivi, il nome viene in genere recuperato da solo.

Un host è segnato come "oltre licenza": cosa significa? L'edizione Community gestisce fino a 15 host; i 15 più vecchi restano gestiti, gli host in più diventano «oltre licenza» — visibili e contati, ma senza importazione di vulnerabilità né inserimento nei piani. Basta scendere sotto i 15 host (eliminandone qualcuno) perché tornino gestiti, oppure passare all'edizione Pro, che alza il limite. Lo stato si ricalcola da solo, senza riavviare nulla. Vedi "Limite di host e stato «oltre licenza»" nel capitolo 7.

Che differenza c'è tra l'edizione Community e la Pro? La Community è gratuita e open source, completa nel flusso di lavoro, con un tetto di 15 host. La Pro è a licenza: alza il tetto a scaglioni, conta gli host per ambiente (produzione / testing / pre-produzione) e aggiunge funzioni come la minimappa della topologia e l'ambiente che modula il rischio. L'edizione in uso è indicata in alto a sinistra. Vedi "Edizioni: Community e Pro" nell'introduzione.

© Dognet Technologies S.r.l. — P.IVA 04867480164