



SentinelCore

Manuale Utente — installazione, configurazione e uso
quotidiano della piattaforma di vulnerability
management

Versione documento: **1.2.0** · Agosto 2026

Indice

Introduzione

Cos'è SentinelCore

A chi si rivolge questo manuale

Cosa fa SentinelCore

Cosa NON fa (per evitare aspettative sbagliate)

Come è organizzato questo manuale

1. Installazione

Modalità A — VM appliance (consigliata)

Modalità B — Pacchetto binario su un server esistente

Aggiornare un'installazione esistente

2. Primo accesso

Login

Primo cambio password

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

Tour rapido dell'interfaccia

3. Ruoli e permessi

Amministratore (`admin`)

Team Leader (`team_leader`)

Utente (`user`)

Riepilogo rapido

Ruolo all'interno di un team

Permessi granulari (uso avanzato)

4. Configurazione

Preferenze

Notifiche

SMTP (solo Amministratore)

Sicurezza

Server MCP (solo Amministratore)

Network Discovery

Logging

Assegnazione vulnerabilità

Override permessi utente

Database

5. Team e utenti

Team

Utenti

Competenze (skill)

6. Vulnerabilità e punteggio di rischio

Dashboard

Il punteggio di rischio: perché non basta il CVSS

Elenco vulnerabilità

Dettaglio di una vulnerabilità

Accettazione del rischio (risk acceptance)

7. Rete e asset

Scansione di rete

Host / asset

8. Scanner e integrazioni

Import da file scanner

Connettore OpenVAS diretto (senza esportare file a mano)

Integrazione JIRA

Notifiche

Webhook SOAR in uscita (uso avanzato)

9. Report e piani di remediation

Generare un report

Cronologia report

Piani di remediation

Carico di lavoro e classifiche

10. Domande frequenti

Introduzione

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.

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.

Cosa fa SentinelCore

- **Network Discovery** — scansione di rete integrata (basata su nmap) con profili configurabili, pianificazione ricorrente e mappa di topologia 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, Gripe), normalizza la severità, deduplica i risultati e li collega agli asset.

- **Connettore OpenVAS diretto** — un connettore integrato interroga periodicamente un'istanza GVM/OpenVAS e importa 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** — raggruppano vulnerabilità e dispositivi in piani eseguibili, con stato di avanzamento, commenti e verifica finale.
- **Collaborazione** — commenti con menzioni (@utente), notifiche in-app, classifiche di risoluzione per utenti e team.
- **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), gestione sessioni con revoca da remoto, log di audit completo, 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.

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 dal connettore OpenVAS.
- **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).

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, connettore OpenVAS, 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

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 <code>sudo</code>

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.

Modalità A — VM appliance (consigliata)

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	—

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.

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).              │
└────────────────────────────────────────────────────────────────────────────────┘
```

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.

Modalità B — Pacchetto binario su un server esistente

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)

Passi

1. Scarica il pacchetto (`sentinelcore-<versione>-linux-x86_64.tar.gz`) e verificane l'integrità, se disponi del checksum:

```
sha256sum -c sentinelcore-<versione>-linux-x86_64.tar.gz.sha256
```

2. 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
```

3. L'installer, in autonomia:

- installa i pacchetti di sistema necessari (PostgreSQL, nginx, nmap, arp-scan);
- crea utente e database dedicati con password generata casualmente;
- applica lo schema del database;
- genera un certificato TLS auto-firmato per l'istanza e configura nginx per servire tutto in **HTTPS di default** (con redirect automatico da HTTP);
- configura il servizio di sistema (systemd);

- crea il primo account **admin**, stampandone le credenziali a fine installazione.

4. 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.

Aggiornare un'installazione esistente

Per passare da una versione di SentinelCore alla successiva **senza perdere dati**, usa lo script `upgrade.sh` incluso in ogni nuovo pacchetto binario (funziona allo stesso modo sia per un'installazione da pacchetto, sia per un'appliance VM, sia per un'immagine qcow2):

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

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/sentinel-suite/sentinelcore/backups/` per un ripristino manuale in casi eccezionali.

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

primitissima installazione.

2. Primo accesso

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

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 due 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.

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.

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, <i>Import scanner</i>	Tutti (le voci segnate * richiedono ruolo Team Leader o Amministratore)
Report	Report	Team Leader e Amministratore
Amministrazione	Team, <i>Utenti</i> , 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.

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

3. Ruoli e permessi

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

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;
- gestire i piani di remediation;
- 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 del connettore OpenVAS);
- configurare l'integrazione JIRA e i webhook SOAR;
- accedere al log di audit;
- 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).

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;
- 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).

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.

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.

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	✗	✗	✓

Capacità	Utente	Team Leader	Amministratore
Assegnare vulnerabilità a team/utenti	✗	✗	✓
Creare/eliminare team, gestire regole di assegnazione	✗	✗	✓
Gestire utenti (creazione, blocco, ruoli)	✗	✗	✓
Importare file da scanner esterni	✗	✗	✓
Gestire piani di remediation, risk acceptance	✗	✗	✓
Gestire plugin, connettore OpenVAS, JIRA, webhook SOAR	✗	✗	✓
Accedere al log di audit e alle Impostazioni di sistema	✗	✗	✓

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.

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.

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.

Preferenze

Scelta del tema grafico dell'interfaccia (chiaro/scuro e varianti). È una preferenza personale, salvata per l'utente che l'ha impostata.

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.

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.

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

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. <code>smtp.gmail.com</code>)
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.

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.

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.

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.

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.

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).

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.

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.

5. Team e utenti

Team

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

- **Nome e descrizione**
- **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**.

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.

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.

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.

6. Vulnerabilità e punteggio di rischio

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).

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”).

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

Livello di rischio	Scadenza (SLA)
Low	90 giorni

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.

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.

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.

Dettaglio di una vulnerabilità

Aperto una vulnerabilità trovi: descrizione tecnica, riferimenti CVE/CWE, cronologia degli eventi (timeline), e una sezione **commenti** dove puoi discutere il caso con il team e menzionare colleghi specifici con `@nomeutente` — chi viene menzionato riceve una notifica in-app.

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.

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 dal connettore OpenVAS, e le collega agli asset noti.

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 collegati, con indicazione visiva di stato (online/offline) e, se disponibili, del numero di vulnerabilità note per dispositivo.

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. 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);
- eliminare in blocco dispositivi non più rilevanti.

Quali campi di un host influenzano davvero il punteggio di rischio

Aperto il dettaglio di un host trovi la scheda “**System Configuration**” → “**RBRE & Compliance**” (il nome resta in inglese anche con l’interfaccia in italiano). Contiene diversi campi, ma **solo tre** di questi entrano davvero nel calcolo del punteggio di rischio delle

vulnerabilità di quell'host — gli altri sono informativi/organizzativi. Sapere quali sono ti permette di alzare o abbassare consapevolmente il rischio calcolato per un host, invece di scoprirlo per tentativi:

Campo (nome in UI)	Valori	Effetto sul punteggio
Business Criticality	Mission Critical / Core Business / Supporto / Lab-Test	È il fattore con più peso: da solo può valere fino a 15 punti su 100. "Mission Critical" segnala un sistema il cui fermo blocca il business (es. gateway di pagamento, autenticazione, infrastruttura core); "Lab/Test" un ambiente di sviluppo il cui compromesso ha impatto reale minimo.
Exposure Level	Internet Facing / DMZ / Internal / Segmented	Fino a 12 punti. "Internet Facing" (o un IP pubblico rilevato automaticamente sull'host) porta il massimo; "Segmented" (rete isolata) porta il minimo — un attaccante deve prima superare un altro livello di rete per raggiungerlo.
Data Classification (<i>oppure il flag Data Processor (GDPR) acceso</i>)	Public / Internal / Sensitive / Critical	+5 punti fissi se il valore è "Sensitive" o "Critical", oppure se il flag "Data Processor (GDPR)" è acceso — segnala che l'host tratta dati personali/sensibili, indipendentemente dalla classificazione testuale.

Non entrano invece nel calcolo (anche se si trovano nella stessa scheda e potrebbero sembrare correlati): "Criticality (legacy)", Device Use Case, Remediation Difficulty, gli switch "Internet Facing"/"Has Public IP"/"Patch Available", e il campo libero "Deployment Impact". Sono utili per organizzazione e reportistica interna, ma oggi non spostano il punteggio di rischio di una singola unità.

Un IP pubblico viene comunque rilevato **automaticamente** dal sistema guardando l'indirizzo della vulnerabilità stessa (tutto ciò che non rientra nei range privati RFC 1918/loopback/link-local) — non serve marcare nulla a mano perché questa parte funzioni; è “Exposure Level” il campo che aggiunge un giudizio più fine (es. DMZ vs Internet Facing) sopra a quel rilevamento automatico.

Il resto della scheda **Host** (proprietario, note, tag, tipo dispositivo) resta comunque utile per organizzazione interna, filtri e ricerca, anche se non influenza il punteggio.

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. Scanner e integrazioni

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

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**: host/porta (o socket) del servizio GMP, credenziali, intervallo di polling e quanti giorni indietro considerare al primo avvio. Una volta configurato, il connettore interroga periodicamente GVM e importa da solo i report completati — non serve più esportare e caricare file manualmente per quella sorgente.

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.

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), e un bot Telegram configurato dall'amministratore per l'istanza.

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.

9. Report e piani di remediation

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.

Cronologia report

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

Piani di remediation

Un **piano di remediation** (Amministratore) raggruppa una o più vulnerabilità e i dispositivi coinvolti in un unico obiettivo tracciabile: ha un titolo, uno stato di avanzamento, una sezione commenti per coordinare il lavoro tra le persone coinvolte, e — al completamento — una fase di verifica per confermare che il rimedio applicato abbia effettivamente 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.

Creare un piano: cosa significano i campi della sezione “Pianificazione”

- **Priorità** (P1 Critica / P2 Alta / P3 Media / P4 Bassa) — è **solo un’etichetta informativa** sul piano stesso, utile per ordinarlo/segnalarlo nella lista piani: non filtra né influenza in alcun modo quali device o vulnerabilità finiscono nel piano. Per selezionare cosa includere in base al rischio reale usa i filtri della sezione “Selezione device” (sotto), non la priorità.
- **Stato** — il ciclo di vita del piano:
 - *Bozza*: in preparazione, il team assegnato non lo vede ancora;
 - *Attivo*: comunicato al team, pronto ma non ancora iniziato;
 - *In corso*: il team ci sta lavorando (si imposta a mano);
 - *Completato*: si imposta **da solo automaticamente** quando il 100% delle vulnerabilità del piano risulta risolto — non serve chiuderlo a mano;
 - *Annullato*: piano abbandonato.
- **Team assegnato** — il team responsabile dell’esecuzione del piano (facoltativo, “Nessuno” se non ancora deciso).

Solo in fase di **creazione** (non modificabile dopo, perché i device del piano sono già fissati) puoi anche filtrare automaticamente quali device includere, nella sezione “Selezione device”:

- **Solo device di questo team** — limita ai dispositivi assegnati a un team specifico;
- **Fascia di rischio** — filtra per `risk_tier` del nostro motore di prioritizzazione (Critical/High/Medium/Low/Info, capitolo 6) — **non** per la sola severity CVSS;
- **Ambito fascia di rischio** — “Questo tier e superiori” include anche le fasce più critiche di quella scelta; “Solo questo tier” seleziona esclusivamente quella fascia;
- **Solo device internet-facing** — limita ai dispositivi esposti su Internet (vedi capitolo 7 per come viene determinata l’esposizione).

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.

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.

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/sentinel suite/sentinelcore/backups/`).