

SentinelSuite

SCHEDA TECNICA
E COMMERCIALE

Sicurezza dell'infrastruttura, gestita da te — by Dognet Technologies

Vulnerabilità, asset, firewall, hardening e threat intelligence in **un'unica suite integrata**, che installi sul tuo hardware. I tool lavorano da soli oppure insieme: si scambiano eventi, si interrogano a vicenda e reagiscono secondo regole che decidi tu.

SentinelCore
VULNERABILITÀ
E RISCHIO

FireDog
FIREWALL
E TRAFFICO

CyberShepherd
HARDENING
E CORRELAZIONE

IntelliDog
THREAT
INTELLIGENCE

dog-agent
AGENTE
ENDPOINT

Self-hosted · on-premise

No SaaS · no phone-home

Air-gap supportato

Artefatti firmati **GPG + SHA256**

Server **MCP** su ogni tool

NIS2 · ISO/IEC 27001 · PCI DSS · NIST

Dognet Technologies S.r.l. · Via XXV Aprile 47, 24055 Cologno al Serio (BG)
info@dognet.tech · 352 068 1747

Edizione ottobre 2026
sentinelsuite.dognet-technologies.online

La suite in sintesi

Quattro tool e un agente leggero: visibility, protection, detection, intelligence

Tool indipendenti, un unico perimetro.

SentinelSuite è una toolchain di cybersecurity per team di sicurezza e system integrator, distribuita come appliance e pacchetti firmati da installare sul proprio hardware. Nessun SaaS, nessun phone-home: i dati restano on-premise, anche in ambienti regolati e air-gapped.

4 + 1
tool modulari
e un agente unico

MCP
ogni tool è pilotabile
da un agente AI

0
dati inviati
all'esterno

4
framework coperti:
NIS2, ISO, PCI, NIST



Architettura di SentinelSuite: ogni tool funziona da solo e si integra con gli altri; dog-agent collega gli endpoint.

Componente	Cosa copre	Versione	Edizione	Stack
SentinelCore	Inventario asset, vulnerabilità prioritizzate sul rischio reale, SLA, piani di remediation, report	v1.2.0	Community (open source) + PRO	Rust · React · PostgreSQL
FireDog	Firewall centralizzato per flotte di host: regole, policy DROP di default, traffico bloccato, threat score	v1.0.1	Community (open source)	Django · React · PostgreSQL
CyberShepherd	Hardening per modelli e framework, compliance continua, correlazione eventi su MITRE ATT&CK	—	PRO	Rust · React · PostgreSQL
IntelliDog	Threat intelligence e threat hunting retroattivo sugli eventi di tutta la suite	—	Modulo di espansione · PRO	Modulo di CyberShepherd
dog-agent	Agente endpoint unico: telemetria, heartbeat ed esecuzione dei comandi verso tutti i tool	v1.1.1	Incluso	Rust · binario statico musl

Incluso per i clienti Dognet: l'accesso alle licenze SentinelSuite è compreso nella fascia Essential del contratto di mantenimento. Ogni tool si adotta singolarmente: si parte da quello che serve e si aggiungono gli altri quando il processo è pronto.

SentinelCore v1.2.0

Vulnerability management basato sul rischio reale

DISPONIBILE | COMMUNITY + PRO

COS'È

Tutte le vulnerabilità, un unico flusso.

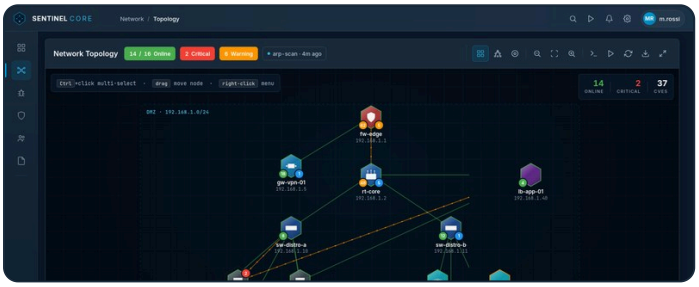
SentinelCore è la piattaforma di vulnerability management della suite, pensata per i team di sicurezza interni. Raccoglie in un unico posto le vulnerabilità dell'infrastruttura, scoperte dalla scansione di rete integrata o importate da scanner di terze parti. A ciascuna assegna un **punteggio di rischio reale**, non il solo CVSS «di targa», la instrada alle persone giuste, ne traccia la risoluzione rispetto alle scadenze (SLA) e produce i report che servono per audit e conformità.

Un'unica vista
Asset, servizi e vulnerabilità in una console.

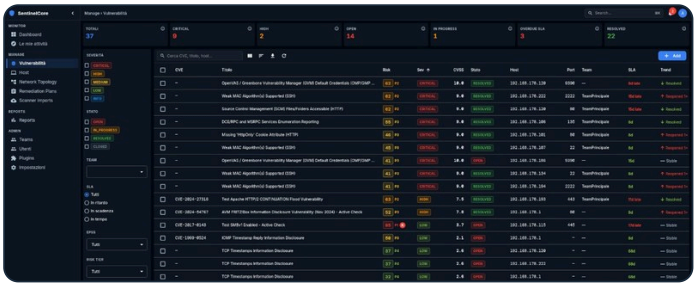
Rischio reale
Priorità dal contesto, non dal solo CVSS.

Team efficaci
Un responsabile e una scadenza per ogni voce.

Report pronti
Evidenze per audit e direzione.



Network Topology: gli host scoperti con il rischio associato (schermata reale)



Gestione vulnerabilità con CVSS, EPSS, stato e SLA (schermata reale)

IL FLUSSO OPERATIVO

Dalla scoperta alla conformità, con un processo continuo

1 Scopri
Scansione di rete integrata (ARP-scan, nmap): host, porte, servizi.

2 Importa
Ricevi i risultati di 10 scanner di terze parti o dal connettore OpenVAS.

3 Valuta
Calcola il rischio su CVSS, EPSS, KEV, esposizione e impatto di business.

4 Assegna
Instrada a team e persone con priorità e scadenza SLA.

5 Risolvi
Piani di remediation, commenti, stato di avanzamento.

6 Verifica
Conferma la chiusura con nuove scansioni o dati aggiornati.

7 Rendiconta
Report per audit e direzione, in PDF, CSV e JSON.

Cosa fa SentinelCore

- **Ricostruisce la rete** come mappa: ogni host compare nella topologia con porte, servizi e rischio.
- **Centralizza le vulnerabilità** di scanner diversi e le riconduce allo stesso asset.
- **Riprioritizza in modo dinamico**: quando una CVE entra nel catalogo KEV o il suo EPSS cambia, cambia la priorità.
- **Assegna e fa rispettare le scadenze**, con segnali al 75%, 90% e 100% della finestra SLA.
- **Notifica sui canali del team**: email, Slack, Telegram, Teams, webhook, PagerDuty, OpsGenie.
- **Sincronizza con JIRA** in entrambe le direzioni (stato, priorità, campi personalizzati).
- **Registra tutto** in un audit log utilizzabile per PCI DSS, ISO 27001, SOC 2 e HIPAA.
- **Si fa pilotare da un agente AI** tramite server MCP in lettura e scrittura.

Cosa non fa SentinelCore

- **Non è uno scanner di vulnerabilità** in senso stretto: oltre alla scoperta di rete e porte, le vulnerabilità arrivano da scanner esterni o dal connettore OpenVAS.
- **Non è multi-tenant:** un'installazione serve una sola organizzazione.
- **Non ha alta affidabilità o clustering integrati:** gira su un singolo host con PostgreSQL dedicato.
- **Non richiede né installa agenti** sugli endpoint: la visibilità viene dalle scansioni di rete e dai dati importati.
- **Non applica patch in automatico:** i piani di remediation tracciano il lavoro, non lo eseguono al posto del team.
- **Non ha LDAP/SSO integrato:** l'autenticazione è locale, con 2FA opzionale.

SentinelCore scheda tecnica

Motore di rischio, SLA, integrazioni, architettura e distribuzione

V1.2.0

MOTORE DI RISCHIO

Un punteggio composito, non un numero fisso

Il rischio di ogni vulnerabilità nasce da cinque fattori e si aggiorna quando uno di essi cambia.

- **CVSS base** · gravità tecnica
- **EPSS** · probabilità di sfruttamento
- **Exploit** · disponibilità nota
- **Esposizione** dell'asset
- **Impatto** di business

Barre illustrative: i fattori concorrono al punteggio, non rappresentano i pesi reali. Un canale di **override** porta in cima zero-day, CVE legate a ransomware e voci del catalogo CISA KEV; EPSS si aggiorna ogni giorno, NVD arricchisce i metadati delle CVE.

SLA

La gravità diventa una scadenza

1 g	7 g	30 g	90 g
CRITICAL	HIGH	MEDIUM	LOW

Ogni fascia ha la sua finestra di risoluzione. Il sistema segnala l'avvicinarsi della scadenza al **75%** e al **90%** e la violazione al **100%**; throttling e quiet-hours tengono pulito il canale delle notifiche.

RUOLI E ACCESSI

Tre ruoli (**admin**, **team leader**, **user**), 2FA TOTP, sessioni revocabili da remoto, autenticazione JWT in cookie `httpOnly` con token CSRF sulle operazioni di scrittura.

IMPORTER · 10 SCANNER

- Qualys
- Nessus
- Burp Suite
- OpenVAS / GVM
- Nexpose / InsightVM
- OWASP ZAP
- Nmap
- Nikto
- Grype
- Trivy

NOTIFICHE · 7 CANALI

- Email
- Slack
- Telegram
- Microsoft Teams
- Webhook
- PagerDuty
- OpsGenie

INTEGRAZIONI E FEED

- JIRA bidirezionale
- NVD
- EPSS giornaliero
- CISA KEV
- Feed CVE offline
- Plugin

ARCHITETTURA

Console web
React 18 · MUI
Cytoscape · ECharts

→

Backend
Rust · Axum · sqlx
CSRF · RBAC · JWT

→

Database
PostgreSQL 15+
JSONB · trigger · GIN

Worker in background: assegnazione, riscansione automatica, allerta critiche, aggiornamento EPSS e KEV, arricchimento NVD, sync JIRA, polling OpenVAS, controllo SLA, avanzamento dei piani, generazione report, report settimanale, digest notifiche, retention dei log.

SERVER MCP

Endpoint unico `POST /api/mcp` · JSON-RPC 2.0

Lettura: `list_vulnerabilities` `get_vulnerability` `get_risk_summary`

Scrittura: `assign_vulnerability` `update_vulnerability_status` `accept_risk` `trigger_scan`

Ogni tool di scrittura è vincolato allo scope della chiave API che lo invoca. Nessun gateway esterno.

REQUISITI MINIMI

Sistema	Debian 12 / 13 · x86_64
CPU	4 vCPU · x86-64-v2
RAM	4 GB · 8 GB oltre 500 host
Disco	20 GB SSD
Rete	1 NIC · accesso L2 ai target
Console	HTTPS :443

FORMATI DI RILASCIO

.tar.gz	Installer Debian · 16 MB
.ova	VirtualBox / VMware · 678 MB
.qcow2	KVM / Proxmox · 702 MB
Sorgenti	GitHub · licenza AGPL-3.0

Ogni artefatto è firmato GPG e pubblicato con checksum SHA256 separato.

INSTALLAZIONE E AGGIORNAMENTO

`install.sh` configura database, nginx con HTTPS, nmap, arp-scan e servizio systemd, e crea il primo amministratore senza richiedere input.

`upgrade.sh` aggiorna sul posto: backup del database, migrazioni, verifica di salute e ripristino automatico se una migrazione fallisce.

Documentazione: manuale utente completo in italiano (installazione, ruoli e permessi, rete e asset, vulnerabilità e rischio, report e remediation), consultabile online e in PDF dal sito della suite.

FireDog v1.0.1

Gestione centralizzata del firewall per flotte di host Linux

DISPONIBILE | COMMUNITY · OPEN SOURCE

COS'È

Un pannello, tutti i firewall.

FireDog è la piattaforma di gestione centralizzata del firewall per flotte di host Linux. Invece di configurare **iptables** a mano su ogni server, un unico pannello web, il **master**, permette di definire e distribuire le regole a tutti gli host gestiti, di osservarne il traffico bloccato e le minacce rilevate, e di reagire da un solo posto.

I COMPONENTI

Master

un host o una VM dedicata

Backend Django e frontend React: editor delle policy, dashboard del traffico in tempo reale, API REST e server MCP. Riceve heartbeat, statistiche e minacce dagli agenti via WebSocket.

Strumenti firewall

su ogni target, in `/opt/sentinelsuite/firedog`

`firewall-manager` (CLI delle regole), `traffic-analyzer` (analisi PCAP con threat scoring) e `firewall-init.sh` (policy DROP e protezioni anti-attacco).

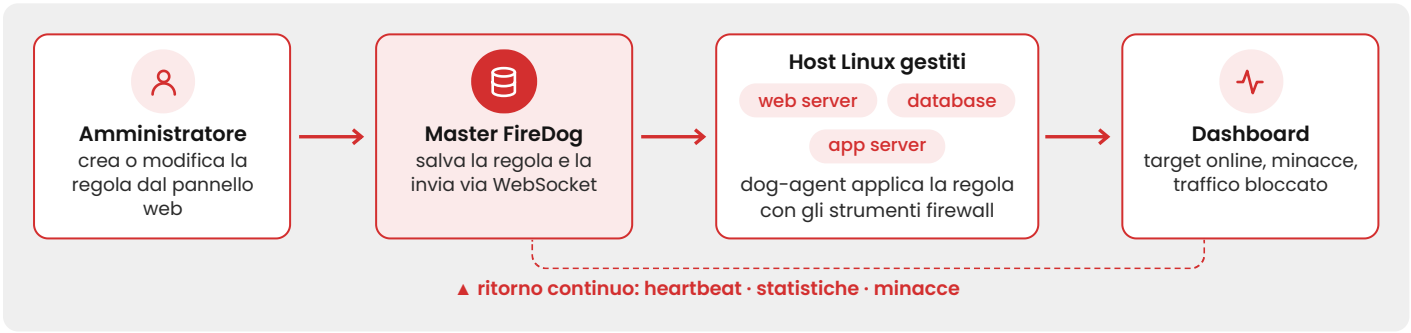
dog-agent

su ogni target, `/usr/bin/dog-agent`

Binario Rust statico condiviso con il resto della suite: autentica il target al master con un pairing a due fasi, invia telemetria ed esegue i comandi regola ricevuti.

FLUSSO OPERATIVO

Dal pannello alla protezione, in tempo reale



1 Definizione

L'amministratore crea o modifica le regole dal pannello, per singolo host o per interfaccia di rete.

2 Distribuzione

Il master salva la regola e la invia agli agenti. Se un agente non è connesso, la regola resta in attesa di riconciliazione.

3 Esecuzione

dog-agent riceve il comando, applica la regola tramite gli strumenti firewall e sorveglia il traffico.

4 Feedback

Il traffico bloccato è salvato in PCAP, analizzato e mostrato in tempo reale con il punteggio di minaccia.

Cosa fa FireDog

- **Gestisce le regole da un solo posto** e le distribuisce in tempo reale; nessun accesso SSH ai target è coinvolto.
- **Applica la policy DROP di default** su INPUT e OUTPUT: passa solo ciò che è stato autorizzato.
- **Protegge da SYN flood, port scan e brute force SSH**, con soglie e durata del ban configurabili.
- **Supporta host con più interfacce di rete**: regole per singola NIC e contatori rx/tx dedicati.
- **Cattura e analizza il traffico bloccato** in formato PCAP e assegna un punteggio di minaccia.
- **Registra ogni scrittura** in un audit log con utente, azione e valori.
- **Espone un server MCP** per agenti AI autorizzati, in lettura e in scrittura.

Cosa non fa FireDog

- **Non gestisce ancora host Windows:** la versione attuale è per sistemi Linux; il supporto arriva con la prossima release.
- **Non sostituisce i sistemi di rete:** non è un router, non gestisce NAT, VPN o bilanciamento del carico.
- **Non è un IDS/IPS completo:** si basa su iptables e sull'analisi del traffico bloccato.
- **Non analizza il traffico permesso:** lavora sul PCAP del solo traffico bloccato.
- **Non configura servizi applicativi** come web server o database.
- **Non decide le regole da solo:** le azioni sono guidate dall'amministratore o da agenti AI autorizzati via MCP.

Con la prossima release: `firewall-manager` portato su PowerShell e dog-agent compilato per Windows 11 e Windows Server; supporto a Oracle Linux e Arch Linux; integrazioni tra i tool della suite.

FireDog scheda tecnica

Protezioni, cattura del traffico, server MCP, requisiti e installazione

V1.0.1

PROTEZIONI INTEGRATE

Default deny, poi le eccezioni

- Policy **DROP** su INPUT e OUTPUT
- **SYN flood:** limite di 50 connessioni al secondo (burst 100), configurabile
- **Port scan:** rilevamento e blocco
- **Brute force SSH:** soglia e finestra configurabili (20 tentativi in 60 secondi di default)
- **Ban** temporaneo o permanente tramite ipset persistente, gestibile con `--list-bans` e `--unban`

TRAFFICO E MINACCE

Vedere cosa viene respinto

- Log separati INPUT e OUTPUT in **PCAP** tramite ulogd2
- Retention automatica con logrotate
- `traffic-analyzer` assegna a ogni sorgente un **threat score** con i motivi del punteggio
- Statistiche e minacce in streaming verso la dashboard del master
- Elenco dei peer remoti pubblici osservati per ogni target

CONFIGURAZIONE DEL TARGET

`/etc/firewall/firedog.conf`

- **Interfacce monitorate** e riportate al master
- **Porte sempre aperte** prima della policy DROP
- **Protezione SSH:** tentativi, finestra, durata del ban
- Creato alla prima installazione e mai sovrascritto dagli aggiornamenti
- Regole per singola NIC con `-i` / `-o`

SERVER MCP · POST /api/mcp · JSON-RPC 2.0

16 tool per interrogare e governare il firewall da un agente AI

Target

`list_targets`
`get_target`
`list_interfaces`
`get_policy_summary`

Regole

`list_rules`
`get_rule`
`create_rule` ADMIN
`delete_rule` ADMIN

Minacce e blocchi

`list_threats` · `get_threat`
`resolve_threat` ADMIN
`list_blocked_ips`
`block_ip` · `unblock_ip`
ADMIN

Traffico

`list_traffic_stats`
`list_network_flows`

Snapshot dei volumi e peer remoti osservati.

La chiave MCP si genera in **Settings › API Keys MCP** ed eredita ruolo e permessi dell'utente che l'ha creata: i tool marcati Admin funzionano solo con la chiave di un amministratore. Ogni scrittura via MCP finisce nell'audit log con il prefisso `MCP <tool>`, distinguibile dalle modifiche fatte da interfaccia.

REQUISITI · MASTER

Sistema	Debian 12+ · Ubuntu 22.04+
Runtime	Python 3.11–3.13 · Node 20
Servizi	PostgreSQL · Redis · nginx
RAM	2 GB · 4 GB consigliati
Porte	TCP 80 / 443 via nginx

REQUISITI · TARGET

Sistema	Debian / Ubuntu · openSUSE / SLES
Firewall	iptables + ulogd2
Percorso	`/opt/sentinelsuite/firedog`
Agente	dog-agent · .deb / .rpm
Avvio	systemd

DISTRIBUZIONE

Sorgenti	GitHub · ramo `stabile`
Licenza	AGPL-3.0
Master	guida `INSTALL.md` · unit systemd
Target	script `get-firedog.sh`
Manuale	in italiano, online

target — installazione degli strumenti firewall

```
# scarica l'installer, ispezionalo, poi eseguilo
curl -fsSL https://raw.githubusercontent.com/Dognet-Technologies/
  firedog/stabile/firedog-package/get-firedog.sh -o get-firedog.sh
less get-firedog.sh
sudo bash get-firedog.sh # installa e attiva la policy DROP
sudo bash get-firedog.sh --skip-init # solo strumenti, attivazione dopo
```

PAIRING A DUE FASI

1. **Chiave API.** L'agente si presenta con la chiave generata in Settings › API Keys Agent.
2. **Identità.** Il master verifica l'impronta `SHA512(ip + hostname + mac)` contro la scheda del target.
3. **Canale attivo.** Da qui partono heartbeat, statistiche, minacce e comandi regola.

Policy DROP senza tagliarsi fuori. Nel file di configurazione si dichiarano le porte che devono restare aperte all'avvio, così l'attivazione della policy DROP non interrompe l'accesso all'host, e le interfacce da monitorare sugli host con più schede di rete. Con `--skip-init` si installano gli strumenti e si attiva il firewall in un secondo momento.

CyberShepherd

Hardening, compliance continua e correlazione degli eventi host

EDIZIONE PRO

COS'È

Harden. Monitor. Correlate.

CyberShepherd mette in sicurezza gli host Linux e poi controlla che restino sicuri. Applica modelli di hardening allineati ai framework di riferimento, misura la conformità nel tempo e correla gli eventi di sistema, mappandoli sulla matrice **MITRE ATT&CK**.

Nell'edizione PRO è anche il punto di governo della suite: da qui si definiscono i playbook e la policy delle risposte automatiche che SentinelCore e FireDog applicano.

FRAMEWORK DI RIFERIMENTO

NIS2 · NIST · ISO/IEC 27001 · PCI DSS · CIS · MITRE ATT&CK · MITRE D3FEND

Ogni controllo di hardening porta il riferimento ai framework che soddisfa; ogni evento correlato porta la tattica ATT&CK e la tecnica difensiva D3FEND che lo mitiga.

IL FLUSSO OPERATIVO

Dal modello alla prova di conformità

1 Profila
Scegli il modello adatto al ruolo dell'host e al framework da rispettare.

2 Indurisci
Applica servizi, regole auditd e parametri sysctl tramite dog-agent.

3 Raccogli
Ricevi eventi di audit, metriche e stato dei controlli dagli host.

4 Correla
Trasforma gli eventi grezzi in eventi di sicurezza mappati su ATT&CK.

5 Allerta
Notifica violazioni e correlazioni via email, Slack e Discord.

6 Verifica
Ripeti le scansioni di compliance e conserva lo storico.

Hardening per modelli

- Template dichiarativi applicati dall'agente
- System hardening, IAM, cifratura
- Sicurezza di rete, logging e monitoraggio
- Baseline di audit CIS, ISO 27001, NIST, PCI

Compliance continua

- Scansioni pianificate e su richiesta
- Oltre 16 policy di controllo comportamentale
- Tracciamento automatico delle violazioni
- Storico su serie temporali (InfluxDB)

Correlazione degli eventi

- Frequenza e sequenza nel tempo
- Identità reale dell'utente e sessione
- Lignaggio dei processi, file, rete
- Criticità dell'asset coinvolto

COSA RICONOSCE LA CORRELAZIONE · TATTICHE MITRE ATT&CK

Credential access
brute force, accesso a file di credenziali

Privilege escalation
salti di privilegio attribuiti all'utente reale

Execution
esecuzioni sospette, shell inverse

Persistence
modifiche a cron, systemd, chiavi SSH

Lateral movement
catene di accesso tra host

Command & control
beaconing verso la stessa destinazione

Exfiltration
trasferimenti anomali verso l'esterno

Defense impairment
manomissione o silenzio del sensore

Sorgente primaria: **auditd**; sensore **eBPF** come plugin opzionale, disattivato di default. Schema delle tattiche: MITRE ATT&CK v19.

Cosa fa CyberShepherd

- **Applica l'hardening** in modo ripetibile su servizi, audit e kernel.
- **Misura la conformità** ai framework e ne conserva lo storico.
- **Correla gli eventi host** e li colloca sulla matrice ATT&CK.
- **Si estende con plugin**, compresi quelli verso IDS/IPS di terze parti.
- **Espone un server MCP** per allerte, correlazioni, compliance e hardening.
- **Governa le integrazioni** della suite: playbook, policy, approvazioni, audit.

Cosa non fa CyberShepherd

- **Non sostituisce IDS/IPS,** firewall perimetrali e router: li integra tramite plugin.
- **Non è un SIEM generalista:** si concentra sugli host gestiti dalla suite.
- **Non esegue azioni intrusive di propria iniziativa:** passano dalla policy e dall'approvazione prevista.
- **Non clona gli host:** gli ambienti di test e preproduzione li crea e li dichiara il cliente.

IntelliDog

Threat intelligence e threat hunting, anche retroattivo

MODULO DI ESPANSIONE · PRO

COS'È

Quello che il mondo sa, cercato in casa tua.

IntelliDog è il modulo di threat intelligence di CyberShepherd. Raccoglie indicatori di compromissione dalle fonti riconosciute e li cerca nei dati che la suite ha già: traffico di FireDog, vulnerabilità di SentinelCore, eventi host di CyberShepherd.

La ricerca vale anche all'indietro: quando un indicatore diventa noto oggi, IntelliDog verifica se è già passato dai tuoi sistemi nelle settimane precedenti.

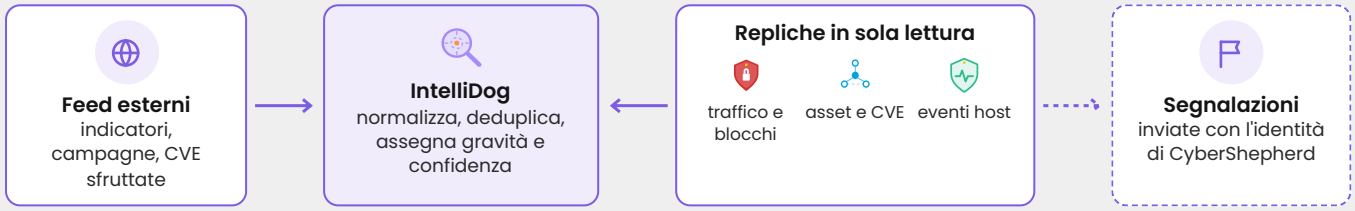
FONTI DI INTELLIGENCE

- **MISP** condivisione di minacce e campagne
- **AlienVault OTX** pulse e indicatori
- **AbuseIPDB** reputazione degli IP
- **Shodan** esposizione su Internet

Più il catalogo CISA KEV e feed personalizzati in formato CSV e JSON.

IL FLUSSO DEI DATI

Dagli indicatori alla segnalazione, senza toccare i tool in produzione



IntelliDog legge copie PostgreSQL dei dati dei tool: le ricerche, anche pesanti, non rallentano i sistemi che stanno lavorando.

Caccia sullo storico

Una volta alla settimana cerca gli indicatori nello storico di tutti i tool. Quando arriva un segnale forte, come una CVE aggiunta al catalogo KEV o una campagna attiva segnalata in MISP, parte subito una ricerca mirata su quel solo elemento.

Sei modi di correlare

- **Indirizzi IP** nel traffico del firewall
- **Domini** contattati (con un IDS integrato)
- **CVE** presenti sugli asset
- **Hash** di file noti come malevoli
- **Pattern** nei log
- **Comportamenti** anomali

Indicatori pesati

Ogni indicatore ha tipo, gravità, livello di confidenza, età e marcatura TLP. Il peso conta: molti IP appartengono a infrastrutture condivise come CDN e hosting, e bloccarli alla cieca interromperebbe servizi legittimi.

COSA OTTIENI IN CONSOLE

Panoramica	Feed	Indicatori	Rilevamenti	Threat hunting
stato dei feed e rilevamenti recenti	fonti, aggiornamenti, esiti	ricerca e filtri sugli IoC	presa in carico e chiusura	ricerche personalizzate sullo storico

Cosa fa IntelliDog

- **Acquisisce indicatori** di continuo dalle fonti di intelligence configurate.
- **Li cerca nei tuoi dati,** anche in quelli raccolti prima che l'indicatore fosse noto.
- **Classifica gli host coinvolti:** vulnerabili, in contatto con l'attaccante, o entrambe le cose.
- **Cambia il peso delle vulnerabilità:** una CVE media sfruttata in una campagna attiva diventa urgente.
- **Propone le contromisure** agli altri tool, come regole di blocco per FireDog.
- **Usa standard aperti:** STIX e MISP per l'intelligence, TLP per la condivisione.

Cosa non fa IntelliDog

- **Non funziona da solo:** è un modulo di CyberShepherd e richiede l'edizione PRO.
- **Non agisce direttamente sui sistemi:** segnala. Le risposte passano dalla policy definita in CyberShepherd.
- **Non ha impostazioni di collegamento proprie:** parla con gli altri tool attraverso CyberShepherd.
- **Non scrive nei database dei tool:** lavora su repliche in sola lettura.
- **Non sostituisce l'analista:** un contatto senza vulnerabilità resta un caso da investigare.

dog-agent v1.1.1 · MCP

Un solo agente sugli endpoint, un solo linguaggio per governare la suite

DISPONIBILE · INCLUSO

DOG-AGENT · COS'È

Piccolo, silenzioso, onesto.

Un unico binario Rust statico per tutta la suite. Si installa una volta sull'host e riferisce ai prodotti in uso, uno o più insieme, su un canale WebSocket autenticato. Per ogni prodotto basta un blocco `[[targets]]` nel file `/etc/dog-agent/agent.conf`, con la propria chiave API.

<12 MB di memoria residente	**1,8** MB il pacchetto .deb
0 dipendenze a runtime	**1** agente per tutti i tool

Inventario

Pacchetti installati e versioni a ogni esecuzione, da confrontare con feed CVE e policy.

Porte e servizi

Socket in ascolto e processi proprietari: la vista dell'host, da incrociare con scansioni e regole.

Drift di configurazione

Hash dei file sorvegliati e segnalazione delle modifiche tra un controllo e l'altro.

Comandi e telemetria

Heartbeat, statistiche e minacce verso il master; esecuzione delle regole ricevute.

REQUISITI

Sistema	Linux · x86_64 / arm64
Kernel	4.19+ · nessuna dipendenza da libc
Memoria	< 12 MB · picco 32 MB in scansione
Disco	40 MB + buffer locale
Privilegi	non privilegiato dove possibile

PACCHETTI

.deb	Debian / Ubuntu · 1,8 MB
.rpm	openSUSE / SLES / RHEL · 1,9 MB
Build	musl statica · TLS con rustls
Servizio	unit systemd inclusa
Sorgenti	GitHub · checksum SHA256
In arrivo	Windows 11 · Windows Server

ARRUOLAMENTO

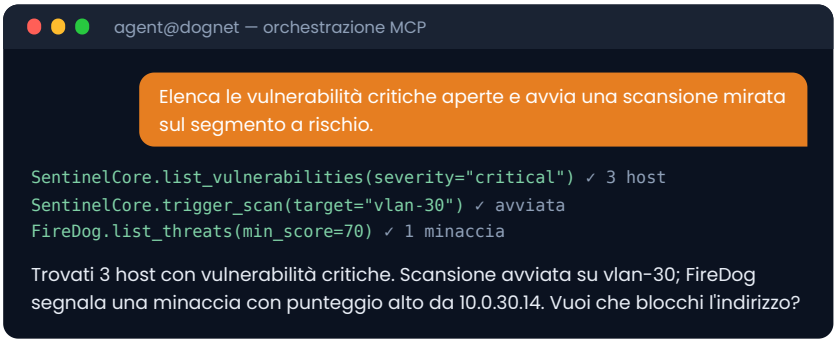
1. **Installa** il pacchetto: il servizio resta inattivo finché non è configurato.
2. **Configura** un blocco `[[targets]]` per ogni prodotto.
3. **Avvia:** il pairing a due fasi parte da solo alla prima connessione.

GESTIONE VIA AGENTE AI · MODEL CONTEXT PROTOCOL

Non solo dashboard: orchestrazione.

Ogni prodotto della suite espone un proprio server **MCP**: l'intera infrastruttura diventa pilotabile in linguaggio naturale da un agente AI, come Claude, che gira nel perimetro del cliente. Si può usare un agente per tool oppure uno solo per tutta la suite.

- **Stesso contratto su tutti i tool:** endpoint `POST /api/mcp`, JSON-RPC 2.0
- **Chiavi dedicate**, distinte da quelle degli agenti endpoint e da quelle tra tool
- **Permessi ereditati** dalla chiave: lettura per tutti, scrittura solo dove autorizzata
- **Tracciabilità:** ogni scrittura via MCP è registrata nell'audit log
- **Nessun dato esce:** coerente con NIS2 e con gli ambienti air-gapped



Esempio illustrativo dell'orchestrazione via agente

Server MCP	In lettura	In scrittura
SentinelCore	vulnerabilità, dettaglio, riepilogo del rischio	assegnazione, cambio di stato, accettazione del rischio, avvio scansione
FireDog	target, interfacce, regole, minacce, IP bloccati, traffico, flussi di rete, riepilogo policy	creazione ed eliminazione regole, blocco e sblocco IP, chiusura minacce
CyberShepherd	target, metriche, allerte, correlazioni, scansioni di compliance, modelli di hardening	presa in carico delle allerte, esecuzione dell'hardening

Integrazione tra i tool

Collegamento, scambio di eventi e regole di ricezione: come i tool si riconoscono e si parlano

Da soli vedono un pezzo. Insieme vedono il caso.

Integrare significa collegare i tool tra loro in fase di configurazione, scambiando le chiavi con cui si riconoscono a vicenda. Una volta collegati si inviano eventi, si chiedono informazioni e reagiscono secondo regole, i **playbook**, abilitate una per una. Senza questa configurazione ogni tool lavora da solo.

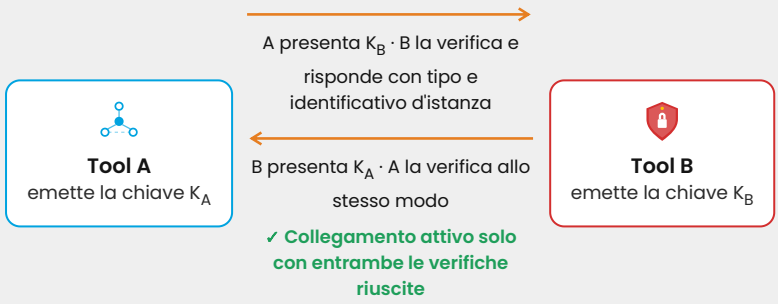
Eventi
«Ho rilevato questo.» Un fatto osservato, con i soli dati di chi lo emette.

Domande
«Questo IP è nel tuo inventario?» Ogni tool risponde sui propri dati.

Playbook
Evento, domande, condizioni, risposta. Si attivano singolarmente.

1 · PAIRING

Due tool sono collegati solo quando ciascuno ha verificato la chiave dell'altro



L'amministratore inserisce in ciascun tool l'URL e la chiave dell'altro, nella scheda Settings › Tool collegati. Una sola direzione non chiude l'handshake.

STATI DEL COLLEGAMENTO

Non configurato	URL o chiave assenti
In attesa	verificata una sola direzione
Attivo	eventi abilitati
Errore	chiave rifiutata, pari irraggiungibile o certificato cambiato
Revocato	chiave cancellata da uno dei lati

Chiavi emesse: salvate solo come hash.

Chiavi ricevute: cifrate a riposo, fuori dal database.

Una chiave, un pari: non vale se la presenta un altro tool.

HTTPS obbligatorio. Le chiavi non concedono permessi.

2 · CONTRATTO DEGLI EVENTI

Una sola busta per tutti, e regole di ricezione che non si fidano di nessuno

evento — la busta comune

```
schema_version  versione; sconosciuta = rifiutata
event_id  UUID; i duplicati sono scartati
event_type  es. threat.detected
source_tool  il tool mittente
timestamp  istante in UTC
case_id  il caso a cui appartiene (opzionale)
payload  dati validati sullo schema
```

Mittente dalla chiave, non dalla busta
Conta la chiave presentata. Se `source_tool` non coincide, l'evento è scartato.

Ogni tool emette solo i propri tipi
Asset e vulnerabilità, rete e minacce, hardening e detection. Il resto è scartato e registrato.

Fatti, non ordini
Anche una richiesta di blocco è una proposta: chi la riceve la sottopone alla propria policy.

Dati esterni mai fidati
Hostname, user-agent e contenuto dei pcap sono marcati come non fidati prima di arrivare a un agente AI.

Consegna e carico sotto controllo. Se un pari è irraggiungibile l'evento resta in una coda limitata, con tentativi a intervalli crescenti; le scritture nate da dati esterni hanno un limite di frequenza. In PRO ogni evento arriva in copia a CyberShepherd, che lo conserva per la consultazione e la simulazione dei playbook.

Risposte automatiche, sotto controllo

Policy delle capacità, agente AI, pipeline di promozione, playbook e audit

3 · POLICY DELLE CAPACITÀ

Per ogni combinazione evento → azione → tool, tre stati possibili

Spenta
L'evento viene mostrato. Nessuna risposta automatica.

Safe
Il tool esegue da solo un'azione deterministica, per lo più di monitoraggio: una regola iptables di osservazione, una regola auditd, un rate limit. Nessun agente AI coinvolto.

Action SOLO PRO
L'azione è intrusiva e passa da un agente AI tramite MCP, con la modalità di avanzamento scelta. Un'action non può essere declassata a safe.

Nell'edizione PRO la policy si definisce nella pagina Integrazioni di CyberShepherd (schede Eventi, Playbook, Approvazioni, Audit), viene distribuita ai tool collegati con un numero di versione crescente e ognuno la applica in locale. Se CyberShepherd è irraggiungibile resta valida l'ultima policy ricevuta. Per gli **asset critici** nessuna action parte senza l'approvazione di una persona.

4 · ACTION E AGENTE AI

Solo strumenti tipizzati, mai comandi liberi: cinque controlli su ogni chiamata

Abilitazione
Lo strumento esiste solo se la capacità è in stato Action.

Validazione
Parametri fuori schema: chiamata rifiutata.

Ambito
Solo gli host dell'evento e i loro cloni dichiarati.

Dati non fidati
I campi dell'evento sono separati dalle istruzioni.

Tracciabilità
Evento d'origine, agente ed esito per ogni chiamata.

5 · PIPELINE DI PROMOZIONE

Prima sui cloni, poi in produzione: tre fasi, tre cancelli

G1 **Test** — la correzione si prova sul clone di test

G2 **Preproduzione** — conferma su un ambiente allineato

G3 **Produzione** — applicata solo dopo due esiti positivi

Modalità	G1 · avvio	G2 · test → preprod	G3 · preprod → produzione
Supervisionata	Persona	Persona	Persona
Semi-automatica	Persona	Agente AI	Persona
Automatica	Automatico	Agente AI	Agente AI, persona notificata

Rollback dichiarato
Prima di partire. Se una fase fallisce si torna indietro e la pipeline si ferma.

Timeout per fase
Dove decide l'agente AI, la scadenza vale come esito negativo.

Controlli di veto
Heartbeat dell'agente e servizi critici: possono solo bloccare, mai approvare.

Asset critici
Il cancello verso la produzione resta sempre in mano a una persona.

6 · PLAYBOOK

Dichiarativi, mai codice

Trigger · Domande · Condizioni · Risposta

Si creano con un builder guidato a menu, ciascuno filtrato dal precedente. Un playbook combina blocchi esistenti e non aggiunge capacità. In PRO si può **simulare** sugli eventi salvati prima di attivarlo.

7 · AMBIENTI E CLONI

Dichiarati dal cliente

Ogni host di produzione può avere un clone di test e uno di preproduzione. Li crea e li mantiene allineati il cliente; la suite non clona nulla. Un host che non dichiara l'ambiente è trattato come **produzione**, cioè con la massima cautela.

8 · AUDIT

Chi può fare cosa, e cosa è stato fatto

Ogni tool registra in un log non modificabile da interfaccia: pairing e revoche, versioni della policy, chiamate MCP, promozioni, rollback, approvatori, eventi scartati e ogni disattivazione della validazione umana, con autore e data.

Gli scenari: quando i tool lavorano insieme

Da «risolto» a «chiuso»: la threat intelligence cambia il peso di una vulnerabilità

SCENARIO 1

Dall'indicatore di compromissione alla remediation coordinata

IntelliDog
THREAT INTELLIGENCE

Una CVE presente sui tuoi server è ora sfruttata in una **campagna attiva**, e alcuni host hanno già contattato i suoi **server di comando e controllo**.

- **SentinelCore** — Alza il rischio, notifica i team responsabili, prova la correzione sui cloni di test e preproduzione.
- **FireDog** — Blocca gli indirizzi coinvolti in base a confidenza ed età dell'indicatore, e da quel momento ne salva il traffico.
- **CyberShepherd** — Verifica il profilo AppArmor del servizio esposto e attiva regole di audit sugli host a rischio.

HOST CLASSIFICATI

- CVE + contatto → incidente
- Solo contatto → da investigare
- Solo CVE → remediation prioritaria

1. **Caccia** — Ricerca settimanale sullo storico, o mirata al primo segnale forte.
2. **Rischio** — La CVE «media» diventa urgente: priorità e piano ai team.
3. **Contatti** — Gli indicatori sono incrociati con il traffico osservato.
4. **Contenimento** — Blocco pesato: niente tagli alla cieca su CDN e hosting.
5. **Sorveglianza** — Audit mirato, anche da regole Sigma pubbliche.
6. **Un caso** — Tutto legato alla campagna; a chiusura le regole temporanee scadono.

Risposte di monitoraggio. Non bloccano nulla e possono partire da sole: regole di osservazione, cattura del traffico, audit.

Risposte intrusive. Passano da agenti AI che usano solo strumenti predefiniti, vengono provate sui cloni e, salvo diversa scelta del cliente, richiedono l'approvazione di una persona.

SCENARIO 2

Risolto non vuol dire chiuso

Risolto
La correzione è installata. Si verifica confrontando pacchetti e aggiornamenti dell'host con gli avvisi ufficiali dei vendor, in formato **OVAL** e **CSAF**.

→

TRE CONTROLLI DI CHIUSURA

- **Hardening** ripassa i controlli sull'host
- **Esposizione** il servizio non è più esposto come prima
- **Persistenza** ricerca mirata per escluderla

→

Chiuso
Solo se tutti e tre i controlli sono negativi. L'esito resta registrato con data e fonte, come **evidenza per gli audit**; le regole temporanee scadono.

LA SCALA DI MATURITÀ

1. Scansione e patch in ordine di CVSS
2. Priorità sul rischio reale: KEV, EPSS, asset. **SentinelCore lavora già qui.**
3. Priorità aggiornate dall'intelligence e risposta coordinata tra rete, host e vulnerabilità
4. Chiusura verificata, con evidenze conservate

COSTRUITO SU STANDARD APERTI

STIX · MISP · OVAL · CSAF · Sigma · MITRE ATT&CK

Dati verificabili, interoperabili e non legati a un formato proprietario. Gli scenari portano ai gradini 3 e 4: richiedono processi già solidi, sono opzionali e si attivano playbook per playbook.

In cantiere

Dove sta andando la suite: quello che abbiamo già predisposto di sviluppare

La suite cresce. Ecco in quale direzione.

SentinelSuite è un progetto vivo. Oltre a quanto descritto in questa scheda, abbiamo già messo in programma quattro linee di sviluppo, pensate per chi governa la sicurezza, per chi la installa e per chi la usa ogni giorno.

A · PER CISO E DIREZIONE TECNICA

AlphaSentinel

Un eseguibile standalone per chi deve avere la situazione sotto controllo senza entrare nelle console dei singoli tool.

- **Visuale generale** della situazione, con gli eventi più significativi in primo piano
- **Attività soprattutto in lettura:** si osserva, non si rischia di modificare
- **Allerte mirate** su ciò che conta per chi decide
- **Veto opzionale** sulle azioni che lo richiedono
- E molto altro

B · PER CHI INSTALLA

Tutta la suite in un unico rilascio

Oggi ogni tool ha la propria macchina virtuale. Sarà possibile avere l'intera SentinelSuite in una sola.

- **Un'unica VM Debian 13** con tutti i tool della suite
- Formati **qcow2** e **ova**, come per i rilasci attuali
- Meno macchine da creare, aggiornare e sorvegliare
- La scelta giusta per partire in fretta o per ambienti compatti

C · PER CHI HA GIÀ UN'INFRASTRUTTURA

Sempre più plugin

Maggiore integrazione con le terze parti, per estendere quello che hai già nella tua rete invece di sostituirlo.

- Nuovi connettori verso gli strumenti già presenti in azienda
- I dati che oggi restano chiusi in un prodotto diventano **utilizzabili** da tutta la suite
- E diventano **azionabili**: entrano negli eventi, nei playbook e nelle risposte

D · PER CHI È IN MOVIMENTO

App Android e iOS

La suite a portata di mano, anche lontano dalla postazione di lavoro.

- Applicazione per **Android**
- Applicazione per **iOS**

USI STRUMENTI DI TERZE PARTI NON SUPPORTATI O POCO CONOSCIUTI?

Chiedici l'integrazione.

Se vuoi usare SentinelSuite e vuoi, o devi, continuare a utilizzare gli strumenti che hai già adottato nella tua rete, ma mancano i connettori o i plugin adatti, chiedici di svilupparli.

Dognet Technologies è prima di tutto un fornitore di servizi, che ha deciso di rilasciare strumenti per chi, come noi, fa security. Sappiamo che adattamento, flessibilità e integrazione sono fondamentali: sviluppare un componente su richiesta, per noi, non è un problema.

Raccontaci cosa usi

info@dognet.tech
Tel. 352 068 1747

Questa pagina descrive le direzioni di sviluppo già pianificate. Funzionalità e modalità di rilascio potranno evolvere.

Edizioni, conformità e distribuzione

Community aperta, PRO completa: dalla tecnologia alle evidenze

EDIZIONI

Cosa include	Community	PRO
SentinelCore · FireDog · dog-agent	✓ **open source**	✓
Server MCP su ogni tool	✓	✓
CyberShepherd	—	✓
IntelliDog (modulo di espansione)	—	✓
Tool collegabili tra loro	SentinelCore ↔ FireDog	tutti
Risposte automatiche safe	✓	✓
Risposte action con agente AI e pipeline	—	✓
Chi definisce la policy	ogni tool, in locale	CyberShepherd
Simulazione dei playbook · stato «chiuso»	—	✓ **opzionale**

DISTRIBUZIONE

.ova · .qcow2 · .tar.gz · .deb · .rpm · sorgenti git

Artefatti firmati **GPG** con checksum **SHA256**: si verifica prima di installare. Deploy self-hosted, anche senza accesso a Internet.

Community: SentinelCore e FireDog sono disponibili, gratuiti e open source, dal sito e da GitHub.
PRO: le licenze di SentinelCore PRO e di CyberShepherd + IntelliDog si acquistano e si rinnovano dal portale clienti www.sentinelsuite.online, con accesso riservato.

In arrivo. La prossima release di FireDog e dog-agent porta il supporto a Windows, Oracle Linux e Arch Linux e le integrazioni tra i tool. CyberShepherd è in fase avanzata di sviluppo: al rilascio includerà server MCP in lettura e scrittura e le integrazioni PRO.

CONFORMITÀ

Come la suite supporta NIS2, ISO/IEC 27001 e NIST CSF

SentinelCore

- Inventario degli asset — **A.5.9**
- Gestione delle vulnerabilità tecniche — **A.8.8**
- Valutazione del rischio per asset — **ISO 6.1 / NIS2**

FireDog

- Sicurezza e segmentazione delle reti — **A.8.20–8.22**
- Monitoraggio del traffico — **A.8.16**
- Protezione perimetrale — **NIS2 All. 1**

CyberShepherd

- Configurazione sicura — **A.8.9**
- Logging e correlazione eventi — **A.8.15–8.16**
- Telemetria endpoint con dog-agent — **NIS2 All. 1**

IntelliDog

- Threat intelligence — **A.5.7**
- Intelligence nell'analisi — NIST CSF **ID.RA-02**, **DE.AE-07**

Con le integrazioni PRO: NIS2 art. 21(2) lettere b, e, f · ISO/IEC 27001:2022 A.5.7, A.8.8, A.8.16 · NIST CSF 2.0 ID.RA-01, ID.RA-02, ID.RA-05, ID.RA-06, DE.AE-07, RS.MI. Uno strumento da solo non rende conformi: fornisce il processo e le evidenze su cui la conformità si dimostra.



PARLIAMONE

Costruiamo il vostro perimetro di sicurezza.

Dalla valutazione del perimetro alla conformità, con la combinazione di tool e licenze più adatta alla vostra organizzazione.

info@dognet.tech
Tel. 352 068 1747
Portale clienti: www.sentinelsuite.online
sentinelsuite.dognet-technologies.online
github.com/Dognet-Technologies

Dognet Technologies S.r.l. · Via XXV Aprile 47, 24055 Cologno al Serio (BG) · P.IVA 04867480164 · REA BG-495176 · SentinelSuite è un prodotto di Dognet Technologies.