

SIX SOLUTION · CYBER SECURITY & DATA PROTECTION

SIX CTI Suite

Dalla raccolta dei segnali di minaccia alla riduzione concreta del rischio: la suite che unifica intelligence, monitoraggio, valutazione e reporting.

[CTI Dashboard](#)

[CTI Monitor](#)

[Pulse Dashboard](#)

[Pulse Daily Report](#)

[Pulse Weekly Report](#)



Dalla conoscenza della minaccia alla riduzione del rischio

Ogni prodotto risponde a un'esigenza operativa diversa, con una copertura progressiva e integrabile.

01



Raccolta

Aggregazione di fonti CTI, feed di vulnerabilità, IoC e campagne ransomware.

SIX CTI Dashboard

02



Monitoraggio

Presidio continuativo su minacce emergenti, data breach e campagne malevole.

SIX CTI Monitor

03



Valutazione

Punteggio di rischio personalizzato, finding per gravità e workflow operativi.

SIX Pulse Dashboard

04



Reporting

Bollettini giornalieri e settimanali per operativi, management e direzione.

SIX Pulse Daily / Weekly

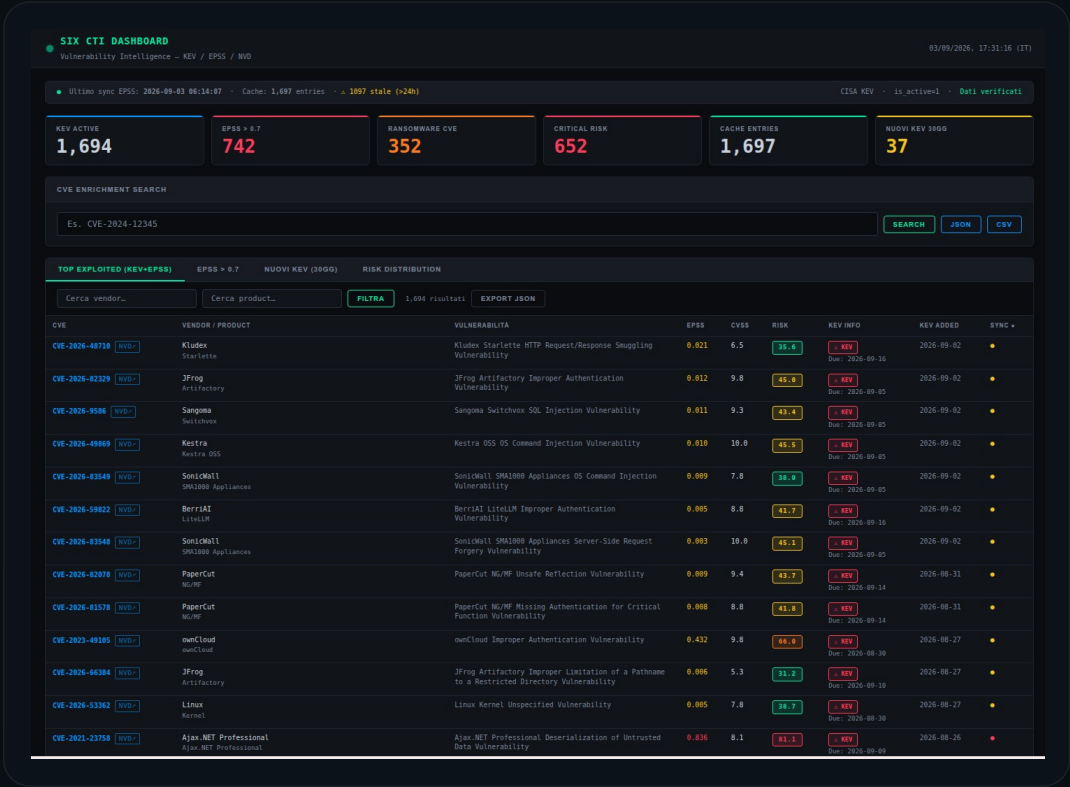
SIX CTI Dashboard

La Cyber Threat Intelligence in un'unica piattaforma operativa: raccoglie e rende consultabili feed di vulnerabilità, campagne ransomware attive, IoC e notizie di sicurezza globali.

Cosa offre

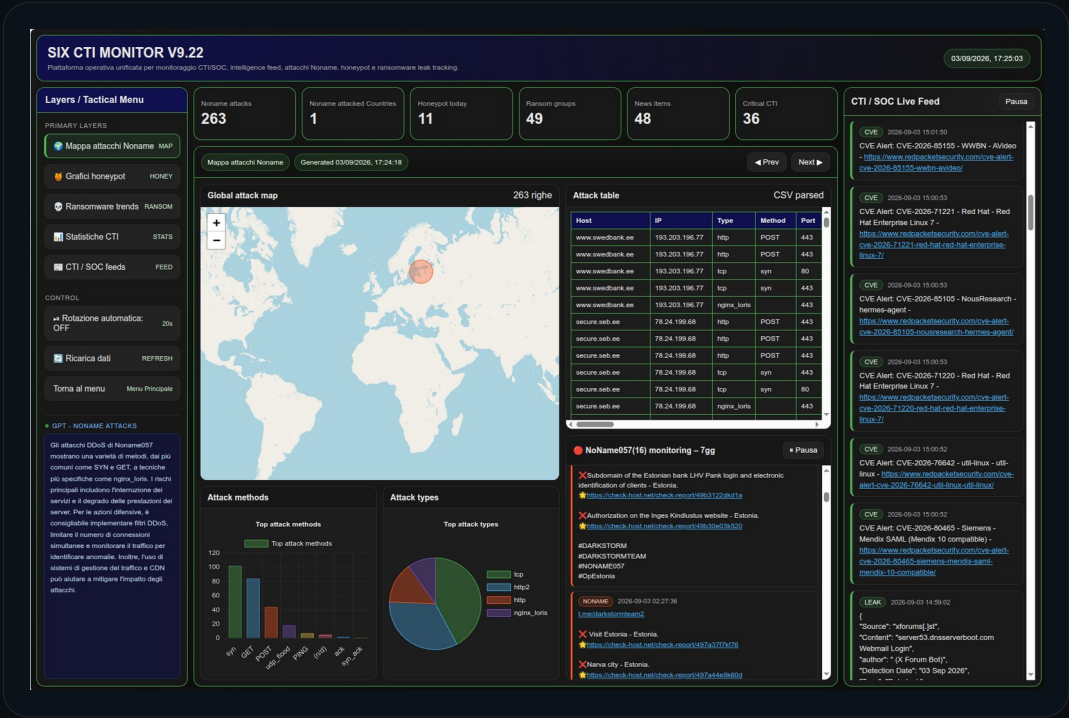
- Visione centralizzata dello scenario cyber in tempo reale
- Ricerca su campagne, attori di minaccia e vulnerabilità
- Riduzione del rumore tramite aggregazione intelligente

Ideale per: SOC · MSSP · consulenti di sicurezza · team IT



SIX CTI Dashboard · Vulnerability Intelligence — KEV / EPSS / NVD

SIX CTI Monitor



SIX CTI Monitor · Mappa attacchi globali e feed CTI/SOC live

Il presidio continuo sulle minacce che possono interessare l'organizzazione: fonti specializzate, canali underground e surface web, zero-day, ransomware e data breach.

Filtro intelligente — informazioni classificate per rilevanza: nessun rumore, solo segnale.

Anticipazione del rischio — intercetta le minacce prima che si concretizzino.

Senza team CTI interno — estende in modo efficace la sicurezza esistente.

Ideale per: PMI · enti pubblici · infrastrutture critiche

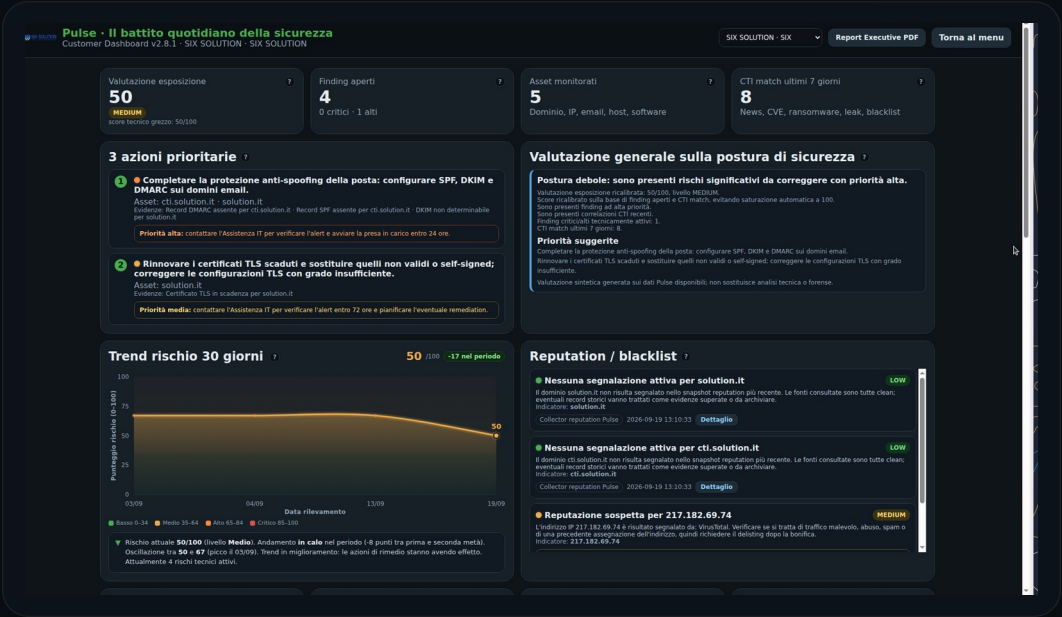
DALLA CONOSCENZA ALLA DECISIONE

Conoscere lo scenario cyber non basta: serve trasformarlo in azioni misurabili di riduzione del rischio.

CTI Dashboard + CTI Monitor → Pulse Dashboard → Daily / Weekly Report

SIX Pulse Dashboard

Trasforma dati tecnici e CTI in una valutazione chiara e personalizzata del rischio aziendale.



SIX Pulse Dashboard · Panoramica del rischio in tempo reale

- Punteggio di rischio live
- Azioni prioritarie proposte
- Workflow dei finding
- Trend & report executive

VISIBILITÀ OPERATIVA COMPLETA

Cosa monitora SIX Pulse

Una mappa completa dell'esposizione tecnica e reputazionale, aggiornata in continuo.



Domini e IP

Sottodomini esposti, IP pubblici e presenza in blacklist internazionali.



Email e configurazioni

SPF, DKIM e DMARC: individua configurazioni che espongono a spoofing e phishing.



Vulnerabilità e CVE

Correlazione con CVE/NVD, KEV ed EPSS su software e appliance esposte.



Certificati

Validità, scadenza e configurazione TLS, con alert preventivi.



Leak e credential exposure

Credenziali ed email aziendali in dump pubblici, dark web e breach noti.

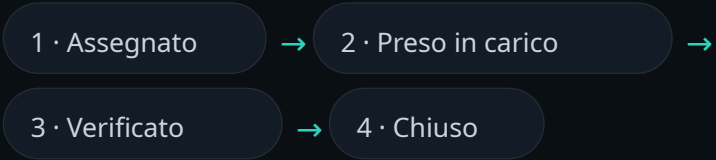


Ransomware

Campagne attive e riferimenti all'organizzazione nei canali dei threat actor.

SIX Pulse in azione: dalla segnalazione alla chiusura

Ogni segnalazione può essere assegnata, presa in carico, verificata e chiusa — con traccia completa di ogni decisione, incluso rischio accettato o falso positivo.



Trend del rischio nel tempo e report executive per il confronto con il management

Certificati server · Ultimo controllo: 2026-09-19 13:01:52 · [Dettagli](#)

Open relay: non rilevato (configurazione corretta) · [Dettagli](#)

Finding attivi e in verifica · [Vista](#) · Attivi e in verifica

Gravità	Finding	Stato	Data aggiornamento	In carico a	Aggiornato da
HIGH	Record DMARC assente per cti.solution.it EMAIL_DMARC_MISSING - cti.solution.it	Da risolvere / da prendere in carico	19/09/2026 13:02	—	system
MEDIUM	Record SPF assente per cti.solution.it EMAIL_SPF_MISSING - cti.solution.it	Da risolvere / da prendere in carico	19/09/2026 13:02	—	system
LOW	DKIM non determinabile per solution.it EMAIL_DKIM_UNKNOWN - solution.it	Da risolvere / da prendere in carico	19/09/2026 13:02	—	system
MEDIUM	Certificato TLS in scadenza per solution.it TLS_CERTIFICATE_EXPIRING - solution.it	Da risolvere / da prendere in carico	13/09/2026 10:55	—	system

Finding · [Vista](#) · Attivi e in verifica

Tipo

Gravità

Stato

Cerca

Tutti

Tutte

Attivi da gestire

Titolo, asset, assegnatario

[Applica](#)

[Azzerà](#)

Tipo	Gravità	Finding	Asset	Stato	Data aggiornamento	In carico a	Azione
EMAIL_DMARC_MISSING	HIGH	Record DMARC assente per cti.solution.it Il dominio non pubblica un record DMARC: il rischio di spoofing e abuso del dominio in campagne phishing è più elevato.	cti.solution.it	Da risolvere / da prendere in carico	19/09/2026 13:02	—	Gestisci
TLS_CERTIFICATE_EXPIRING	MEDIUM	Certificato TLS in scadenza per solution.it Il certificato TLS del dominio scade entro 30 giorni (giorni residui: 0). Serve pianificare il rinnovo per evitare interruzioni o avvisi browser.	solution.it	Da risolvere / da prendere in carico	13/09/2026 10:55	—	Gestisci
EMAIL_SPF_MISSING	MEDIUM	Record SPF assente per cti.solution.it Il dominio non pubblica un record SPF. Un attaccante potrebbe tentare invii email non autorizzati usando il dominio aziendale.	cti.solution.it	Da risolvere / da prendere in carico	19/09/2026 13:02	—	Gestisci
EMAIL_DKIM_UNKNOWN	LOW	DKIM non determinabile per solution.it Non è stato possibile determinare la presenza di DKIM: nessun record è stato trovato sui selector verificati. Il dominio potrebbe firmare con un selector non incluso nella lista. N	solution.it	Da risolvere / da prendere in carico	19/09/2026 13:02	—	Gestisci

Visualizzati 1-4 di 4 finding

[Precedenti](#)

[Successivi](#)

SIX Pulse Dashboard · Finding attivi e in verifica

BOLLETTINO QUOTIDIANO

SIX Pulse Daily Report

Ogni giorno, solo le informazioni cyber che meritano attenzione: sintetizzate in pochi minuti, anche nelle riunioni mattutine del SOC.

- Vulnerabilità critiche del giorno: CVE, score, patch
- Campagne ransomware: attori e settori colpiti
- Incidenti e breach, con analisi dell'impatto
- Indicazioni operative e priorità di intervento

Ideale per: SOC · IT · riunioni operative quotidiane



SIX Pulse Daily Report · Copertina

SIX Pulse Weekly Report

La settimana cyber in una sintesi pensata per decidere: contesto, tendenze e priorità, in un linguaggio accessibile anche alla direzione.



Contesto e tendenze

Evoluzione dei fenomeni e delle tecniche degli attori più attivi nella settimana.



Priorità per la settimana

Pianificazione più efficace di remediation, aggiornamento e mitigazione.



Linguaggio direzionale

Pensato per direzione, CDA e responsabili di governance, senza rielaborazione.

Aspetto	Daily Report	Weekly Report
Frequenza	Ogni giorno	Ogni settimana
Focus	Operativo, azione immediata	Strategico, tendenze e contesto
Destinatari	SOC, IT	Direzione, CDA, governance

Confronto tra i prodotti

Adottabili singolarmente o come percorso integrato e progressivo.

Prodotto	Funzione principale	Destinatari	Modalità
SIX CTI Dashboard	Ricerca e analisi centralizzata di campagne, Indicatori di compromissione (IoC) e vulnerabilità	Analisti CTI, SOC, MSSP	Piattaforma SaaS consultabile su richiesta
SIX CTI Monitor	Monitoraggio continuativo delle fonti CTI e selezione delle segnalazioni rilevanti	Responsabili IT e sicurezza e Organizzazioni prive dipresidio dedicato	Monitoraggio informativo continuativo delle fonti CTI
SIX Pulse Dashboard	Valutazione dell'esposizione cyber e strumenti per la gestione delle criticità e il tracciamento degli interventi correttivi	IT, sicurezza, responsabili della conformità e management	Dashboard dedicata al cliente
SIX Pulse Daily Report	Sintesi operativa quotidiana su minacce e vulnerabilità	Responsabili IT, team di sicurezza e SOC	Bollettino giornaliero
SIX Pulse Weekly Report	Sintesi settimanale delle minacce e delle priorità di attenzione a supporto delle decisioni	Direzione, CdA e responsabili della sicurezza e governance	Bollettino settimanale

Nota: I prodotti della SIX CTI SUITE offrono strumenti software e contenuti di Cyber Threat Intelligence a supporto degli adempimenti NIS2 previsti dal D.Lgs. 138/2024. La fornitura non comprende la gestione operativa dei sistemi del cliente né l'esecuzione degli interventi correttivi. Le decisioni e l'attuazione delle misure di sicurezza restano di competenza dell'organizzazione cliente.

Il percorso in quattro passi

01 

Conoscere il panorama

Base informativa su attori e tecniche d'attacco (CTI Dashboard + Monitor).

02 

Misurare l'esposizione

Pulse Dashboard traduce l'intelligence in un rischio personalizzato.

03 

Informare e decidere

Daily e Weekly Report allineano operativi e direzione, ogni giorno e ogni settimana.

04 

Ridurre il rischio

L'integrazione progressiva porta a una mitigazione concreta.

Risk Exposure Report

Analisi AI on-demand per singolo dominio o indirizzo IP.

Oltre al monitoraggio continuo, la suite genera su richiesta un report di approfondimento: rischio complessivo, motivazione e azioni raccomandate, correlando in automatico decine di fonti OSINT.

[Scarica report PDF](#)

[PDF + allegato tecnico](#)

DOMAIN – example.com

Durata analisi: 301.4 s - modello: gpt-5.4-mini

Tool non eseguiti perché la chiave API non è configurata: safebrowsing (chiave google_safebrowsing), exposed_documents (chiave google_cse_key)

Rischio complessivo: Medio

Motivazione:

example.com è un dominio storico e generalmente benigno, con DNSSEC attivo e reputazione positiva. Tuttavia emergono elementi di rischio non trascurabili: postura email debole/inefficace nel monitoraggio, certificato con scadenza ravvicinata e configurazione TLS migliorabile, assenza di CAA, e soprattutto una superficie di typosquatting molto ampia con diversi domini registrati e alcuni sospetti/malicious. Non risultano evidenze di compromissione diretta del dominio.

Azioni raccomandate:

- Rafforzare la gestione TLS: eliminare protocolli legacy, correggere il finding sul key usage del certificato e monitorare la scadenza

Fonti correlate: VirusTotal · WHOIS/RDAP · crt.sh · Shodan InternetDB · SecurityTrails · AbuseIPDB

INIZIA CON SIX

Dalla conoscenza della minaccia alla riduzione concreta del rischio.

Per maggiori informazioni sulla suite SIX CTI o per richiedere una demo personalizzata, contatta il team SIX Solution — Cyber Security & Data Protection.

