SecuLens

Panoramica delle funzionalità

La lente sulla tua superficie d'attacco.

Vulnerability Assessment e Penetration Test in un unico strumento desktop per consulenti e team di sicurezza. Ricognizione, valutazione, punteggio e report professionale — in un flusso unico, in sola lettura.

Perimetro & rete interna | Superficie d'attacco | Report PDF | Dati locali cifrati

Che cos'è SecuLens

SecuLens è un'applicazione desktop per Windows che raccoglie in un unico ambiente le attività di **valutazione della sicurezza** di un'organizzazione: ricognizione del perimetro esposto, analisi della rete interna, controllo dei siti web, verifica dell'esposizione di credenziali, monitoraggio delle minacce e supporto al penetration test.

I risultati vengono consolidati in un **punteggio di sicurezza**, in grafici chiari e in un **report PDF professionale** pronto per il cliente. Filosofia del prodotto: **prevedere gli attacchi, non eseguirli** — tutti i controlli sono in sola lettura e non distruttivi.

A chi è rivolto: consulenti di sicurezza, società di servizi IT, MSP e team interni che devono produrre valutazioni ripetibili e documentabili.

I moduli di analisi

Perimetro — superficie esposta su Internet

Individua host, porte e servizi raggiungibili dall'esterno, con rilevamento di versioni, vulnerabilità note (CVE) e vulnerabilità **attivamente sfruttate** (CISA KEV). Evidenzia pannelli di amministrazione esposti, servizi obsoleti e configurazioni rischiose.

Rete interna

Analizza host e servizi della LAN tramite una **sonda** dedicata, per fotografare l'esposizione interna (SMB/RDP, protocolli obsoleti, servizi non necessari).

Siti web

Controlla HTTPS e redirect, header di sicurezza, cookie, versioni esposte, PHP fuori supporto, file sensibili (**.git**, **.env**, backup), WordPress e librerie JavaScript vulnerabili.

Data breach, sniffing e monitoraggio minacce

Verifica l'esposizione delle email in violazioni note (con mascheramento automatico), importa e analizza catture di traffico (pcap), e tiene sotto osservazione l'attività dei **gruppi ransomware** correlando le vulnerabilità sfruttate con gli asset del cliente.

Penetration Test

Raccoglie e approfondisce i rilievi in una vista dedicata, con automatismi di analisi e sempre in sola lettura. Si attiva solo dopo il caricamento della **lettera d'incarico**.

Valutazione e punteggio

SecuLens traduce centinaia di controlli in un **punteggio di sicurezza** immediato, sensibile sia alla **quantità** sia alla **gravità** dei problemi. Ogni area riceve il proprio indicatore a semaforo (critico / da migliorare / ottimale) e l'andamento nel tempo mostra l'efficacia dei rimedi. Ogni rilievo può essere classificato, declassato, giustificato o escluso: il punteggio si aggiorna in modo trasparente.

Superficie d'attacco

Un diagramma dedicato rappresenta la superficie d'attacco come un percorso: il **Cloud/Internet** da un lato, la **rete interna (LAN)** dall'altro e, al centro, il **perimetro/firewall**. I servizi esposti che attraversano il perimetro sono evidenziati come **percorsi d'attacco**, con i cammini critici in risalto. Pensato per comunicare il rischio anche a un pubblico non tecnico; incluso nel report in versione stampabile.

Gestione dei rilievi

- **Selezione multipla** dei findings per operare in blocco.
- **Unione** di rilievi duplicati o correlati.
- **Promozione al Penetration Test** dei rilievi pertinenti, con copie indipendenti tra le sezioni.
- **Eliminazione in blocco** e riorganizzazione rapida.
- **Verifica delle credenziali predefinite** su un singolo asset, come azione separata e guidata.

Report PDF professionale

Con un clic SecuLens genera un **report PDF** completo e curato: sintesi esecutiva, punteggio, esito dei controlli, superficie d'attacco e dettaglio dei rilievi. Sfondo bianco e impaginazione pensata per la stampa e la consegna al cliente. I dati sensibili sono mascherati automaticamente.

Import ed export

- **Import** da nmap (XML), Nessus / OpenVAS (.nessus / XML) e dati di esposizione credenziali.
- **Export del singolo test** in file cifrato **.slx** protetto da password.
- **Backup completo** di test e impostazioni, anch'esso cifrato; al salvataggio l'app chiede **dove** salvare e conferma il percorso.

Sicurezza e responsabilità

- **Dati locali e cifrati.** L'archivio risiede sulla macchina dell'operatore in un database cifrato (AES-256-GCM): nessun dato del cliente viene trasmesso a terzi.
- **Controlli non distruttivi.** L'intero flusso è in sola lettura. La verifica delle credenziali predefinite è l'unica azione attiva: richiede la lettera d'incarico, una conferma esplicita per ogni uso, usa solo coppie predefinite documentate dei produttori, si ferma al primo esito e non effettua attacchi a dizionario o forza bruta.
- **Lettera d'incarico obbligatoria** per abilitare il modulo di Penetration Test.
- **Uso autorizzato.** SecuLens va utilizzato solo su sistemi per i quali si dispone di autorizzazione scritta.

Requisiti tecnici

- **Sistema operativo:** Windows 10 / 11 (64 bit).
- **Interfaccia:** applicazione desktop nativa; il report PDF è generato tramite il motore di Microsoft Edge / Google Chrome già presenti nel sistema.
- **Strumenti opzionali:** nmap e nuclei potenziano l'analisi e si installano su richiesta; SecuLens resta utilizzabile anche senza, grazie allo scanner interno.
- **Connettività:** non necessaria per l'analisi locale; richiesta solo per le fonti online (CVE/KEV, data breach, monitoraggio minacce).

SecuLens — documento commerciale. I dati e i nomi riportati nelle schermate sono di esempio e non si riferiscono ad alcuna organizzazione reale.