SGBOX

SGBOX BUNDLE

Next Generation SIEM & SOAR

SGBox è una piattaforma all-in-one per la gestione della sicurezza ICT. La sua architettura modulare la rende in grado di adattarsi alle diverse esigenze di sicurezza aziendale.

www.sgbox.eu

SECUREGATE

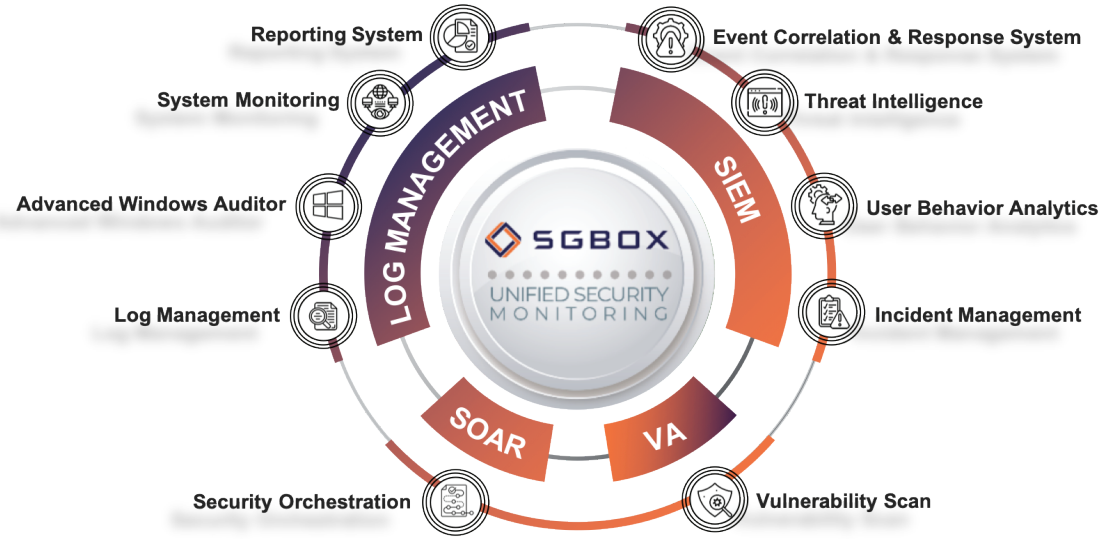
PRESENTAZIONE SGBOX

Cos'è SGBox

SGBox è una piattaforma **Next Generation SIEM & SOAR** modulare sviluppata per la **gestione della sicurezza ICT** e per rispondere alle normative in vigore, come Garante della Privacy, GDPR, nLPD, ISO 27001.

Proposta in modalità **Cloud, On Premise o SaaS**. Ogni modulo ha una sua specifica funzionalità e può essere aggiunto per cooperare con gli altri moduli e per condividere le informazioni raccolte, facilitando e garantendo la conformità con i requisiti imposti.

La Piattaforma



LICENZE

PIANO DI LICENZE PROGRESSIVO

Le licenze sono basate sul numero di moduli scelti e sul numero di data sources che inviano i log, permettendo un costo lineare e deducibile.

Access

Il piano Access permette la raccolta e gestione dei log di accesso, garantendo una piena conformità alla direttiva del Garante della Privacy, con la possibilità di estendere le sue funzioni (anche a posteriori) tramite un semplice upgrade di licenza.

Basic

Il piano Basic permette la raccolta e gestione di tutti i log, garantendo la piena conformità alle direttive nazionali in materia, con la possibilità di estendere le sue funzioni (anche a posteriori) tramite un semplice upgrade di licenza.

Advanced

Il piano Advanced comprende quasi tutte le funzioni della piattaforma, ed oltre alle attività di raccolta, analisi e monitoraggio delle informazioni di sicurezza, comprende i moduli per la correlazione e l'individuazione proattiva delle minacce più complesse.

Premium

Il piano Premium consente di usufruire di tutte le funzionalità, dalla raccolta e analisi dei log, alla correlazione delle informazioni fino all'orchestrazione e automazione delle contromisure da adottare, per una gestione completa delle attività di sicurezza ICT.

Vantaggi

- Soluzione modulare: possibilità di scegliere tra diversi bundle ed effettuare l'upgrade in qualsiasi momento.
- La licenza SGBox è basata sul numero totale di device che inviano log e non sul numero di eventi per secondo (EPS).
- Il processo di archiviazione permette il salvataggio sicuro dei dati, tramite protezione, cifratura, applicazione della firma digitale e marcatura temporale.

30 %

Crescita annuale

150 +

Partner nel mondo

DASHBOARD INTUTIVA
VISIONE IN TEMPO REALE SULLO STATO DI SICUREZZA

Conformità alle normative

La raccolta delle informazioni avviene nel rispetto delle normative sulla privacy.

Scalabilità

Scegli le funzionalità che ti servono in modo progressivo e scalabile.

Prezzo predicibile

Il prezzo è commisurato all'effettivo utilizzo della piattaforma.

95 %

Rinnovi

1500

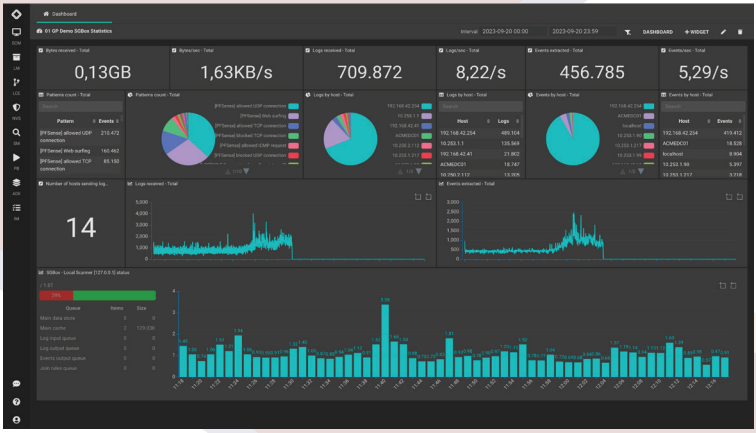
Clienti nel mondo

FUNZIONALITA’

ADVANCED LOG MANAGEMENT

Il modulo di Log Management è in grado di gestire i log degli eventi relativi alla sicurezza di qualsiasi tipo di fonte dati.

√ Dashboard facili ed intuitive, caratterizzate da diversi widget. Molteplici dashboard già predefinite e pronte all’uso. Possibilità di crearne di nuove in modo facilitato.
√ Pannelli di analisi chiari e semplici che permettono investigazioni a vari livelli.
√ Possibilità di generare ed eseguire query sui dati per ricerche più in profondità.



SYSTEM MONITOR

Il modulo di System Monitoring (SM) permette, tramite l’esecuzione di diversi script, la raccolta di informazioni dai diversi host.

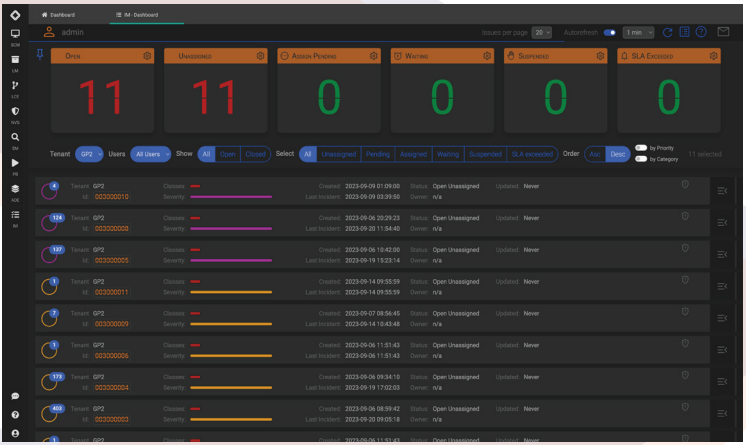
La funzionalità di monitoraggio è stata progettata per completare la piattaforma SGBox SIEM, per evitare malfunzionamenti e consentire al team di supporto di analizzare un problema arrivando alla sua causa principale.

FUNZIONALITA’

INCIDENT MANAGEMENT

Il modulo di Incident Management permette di avere una piattaforma unificata per la gestione degli incidenti o anomalie riscontrate dagli altri moduli di SGBox.

Questo modulo permette inoltre di correlare fra loro più incidenti similari, andando così a ridurne il numero e i falsi positivi, permettendo un’analisi maggiormente filtrata e più corretta.
La funzionalità di Report System permette la generazione e la consultazione dei report in un formato completamente nuovo, sicuro e interattivo.



THREAT INTELLIGENCE FEED MANAGEMENT

La funzionalità di Threat Intelligence permette l’identificazione di attività anomale grazie alla raccolta di informazioni derivanti da molteplici Intelligence Feed open source o commerciali.

SGBox raccoglie le informazioni di sicurezza in Indicatori di Compromissione (IoC) ed è in grado di correlare i dati ai fini di produrre report e allarmi.

FUNZIONALITA’

ADVANCED EVENT SEARCH

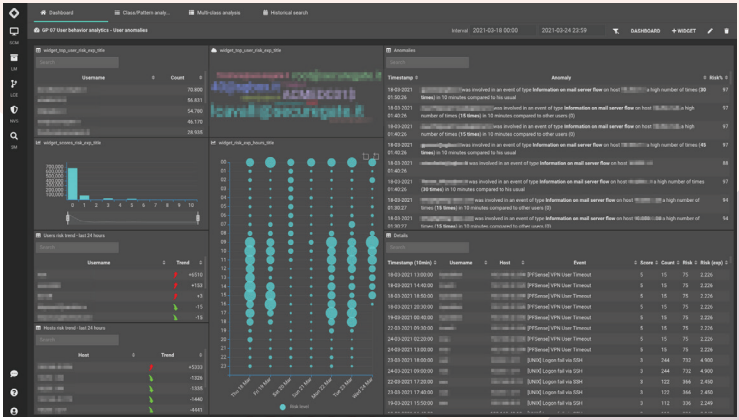
Il modulo di Advanced Event Search sfrutta le informazioni raccolte dagli altri moduli della piattaforma e consente di creare regole appositamente strutturate al fine di rilevare la presenza di anomalie riconducibili a scenari di rischio.

- √ Interfaccia Drag & Drop intuitiva
- √ Regole di correlazione applicabili ai dati in tempo reale e ai dati storici.
- √ Il motore di correlazione aggrega i dati provenienti da diverse fonti e dà la possibilità di creare regole personalizzate per attivare contromisure automatiche.

USER BEHAVIOR ANALYTICS

Il modulo di User Behavior Analytics (UBA), permette di analizzare i dati relativi alle attività degli utenti identificando comportamenti potenzialmente anomali.

Grazie alla creazione automatica di una baseline comportamentale specifica per ogni utente, la soluzione consente di identificare eventuali anomalie o discostamenti dal normale comportamento abituale.

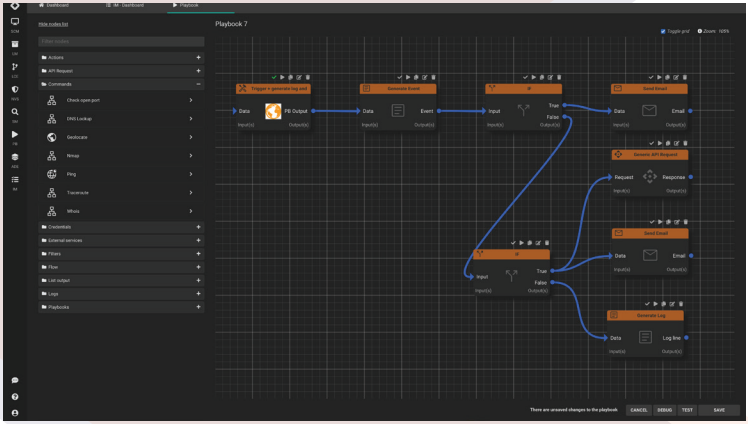


FUNZIONALITA’

SOAR (Security Orchestration, Automation & Response)

Il sistema di orchestrazione, automazione e risposta per la sicurezza (SOAR) si concentra principalmente sulla gestione delle minacce, sull’automazione delle operazioni di sicurezza e sulle risposte agli incidenti di sicurezza.

Il modulo SOAR può immediatamente valutare, rilevare, intervenire o eseguire ricerche di incidenti e processi senza la necessità di interazione umana.



WINDOWS AUDITOR

La soluzione permette la raccolta di molteplici informazioni dai sistemi Windows, sia client che server.

Tramite l’utilizzo di agenti proprietari, SGBox è in grado di raccogliere tutte le informazioni generate dai dispositivi ws, dalle attività di login e logout, fino alle operazioni avvenute all’interno dei file server.

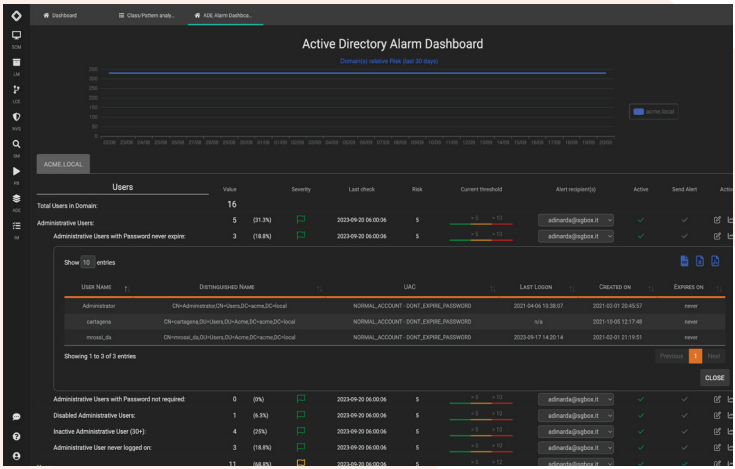
La soluzione permette inoltre la raccolta di informazioni tramite sysmon, legate all’analisi dei processi, le dns query ecc…

FUNZIONALITA’

ACTIVE DIRECTORY AUDITOR

ADA è uno strumento progettato per monitorare costantemente lo stato delle Active Directory, determinare il rischio e avvisare quando vengono superate le soglie KPI impostate.

Questo modulo è perfettamente integrato con tutte le altre funzionalità di SGBox, infatti è in grado di generare elenchi che possono essere utilizzati da altri moduli per eseguire attività specifiche come correlazione di eventi, report filtrati, ecc.



FUNZIONALITA’

NETWORK VULNERABILITY SCANNER

Il modulo di SGBox Network Vulnerability Scanner (NVS) permette di rilevare la presenza di vulnerabilità sulla propria rete.

Il modulo è perfettamente integrato con tutte le altre funzionalità di SGBox ed è in grado di generare elenchi che possono essere utilizzati da altri moduli per eseguire attività specifiche come correlazione di eventi, report filtrati, ecc.

Il modulo NVS integra il motore di scansione basato su tecnologia Qualys, per eseguire scansioni all’avanguardia e approfondite su tutte le vulnerabilità presenti.

MATRICE PRODOTTI SGBOX

- I piani Access e Basic sono conformi alla normativa del Garante della privacy, mentre i piani Basic e Advanced al GDPR.
- La funzione di scansione delle vulnerabilità è indipendente dal numero di Data sources.
- Le licenze sono disponibili sia in modalità “Subscription” (1-3 anni) che in modalità “Perpetual”.

CONTATTACI !

Siamo pronti ad affiancarti nel trovare la soluzione di sicurezza più adatta alle tue esigneze! Richiedi una demo gratuita per scoprire nel dettaglio le funzionalità di SGBox.

Indirizzo
Via Melchiorre Gioia 168- 20125 Milano, Italia

Telefono
+39 02 60830172

Sito Web
www.sgbox.eu

Email
info@sgbox.it