SGBOX NEXT GENERATION SIEM

PIATTAFORMA ALL IN ONE

DISPONIBILE ON-PREMISE
MULTITENANT E CLOUD

SGBOX

SIEM AS YOU NEED

SGBox è una piattaforma software che effettuando un monitoraggio di sicurezza, fornisce completa visibilità sull'infrastruttura di rete raccogliendo e aggregando informazioni da qualsiasi componente IT. SGBox esegue l'analisi dei dati in tempo reale correlando le informazioni raccolte per individuare potenziali minacce e ridurre i rischi legati alla sicurezza dei dati. La soluzione offre anche un servizio di scansione di vulnerabilità per ridurre il rischio di violazione dei dati, supportando lo staff IT nelle attività di remediation. SGBox è uno strumento intuitivo e di facile utilizzo che permette di ridurre i costi di gestione.

SECURITY CONTROL MANAGEMENT

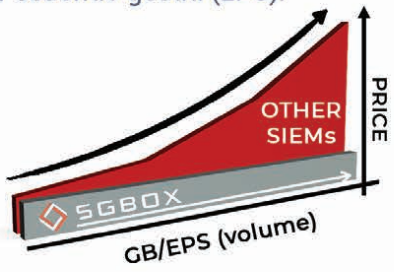
Oltre a gestire tutte le funzionalità di SGBox e i collettori remoti, la console di SGBox offre importanti funzioni condivise con i vari moduli. La console gestisce dashboard inerenti alla raccolta dei dati, monitoraggio dei dispositivi, scansioni di vulnerabilità sia locali che geograficamente distribuite. Gli utenti sono autenticati su directory esterne come LDAP o Active Directory, assegnando loro profili utente e autorizzazioni per ogni singola funzionalità.

MONITORAGGIO DELL'ATTIVITÀ DELL'UTENTE

Monitoraggio costante delle attività degli utenti per individuare un potenziale comportamento anomalo.

PREZZO PREDICIBILE

Il primo SIEM a un prezzo predicibile e un modello di licenza trasparente. Il costo della licenza si basa sul numero totale dei dispositivi che inviano log senza limitazioni sulla quantità di dati raccolti o eventi per secondo gestiti (EPS).



MULTI-TENANT PER MSSP

SGBox è disponibile anche in versione multi-tenant. Utilizzando sonde remote geograficamente distribuite, i dati vengono raccolti e inviati al tenant di riferimento. Le informazioni collezionate vengono mantenute in modalità cifrata per garantire l'inalterabilità del dato e distinte tra i vari tenant. Le sonde remote garantiscono la continuità di servizio anche in assenza di collegamento verso il service provider.

IL VALORE DELLA NOSTRA AZIENDA

In SGBox lavoriamo con passione e supportiamo tutti i clienti con la stessa attenzione, riteniamo che un cliente soddisfatto sia il modo migliore per portare avanti la nostra filosofia. Ci impegniamo nella ricerca e nell'innovazione per offrire ai nostri clienti soluzioni semplici ed efficaci.

COSTI DI GESTIONE CONTENUTI

Rispetto ad altre soluzioni concorrenti, il costo totale di gestione (TCO) di SGBox è vantaggioso. L'interfaccia utente moderna e intuitiva ottimizza la curva di apprendimento; la semplicità del prodotto riduce drasticamente i costi di start-up e i successivi servizi di consulenza.

SERVIZI DI GESTIONE REMOTA

Per garantire l'efficacia del SIEM è indispensabile attuare specifiche personalizzazioni sulle esigenze di ogni singolo cliente. Il team di supporto di SGBox, insieme allo staff tecnico del partner, aiutano gli utenti nella gestione evolutiva della piattaforma.

ARCHITETTURA DISTRIBUITA

L'architettura di SGBox consente di utilizzare collettori remoti per la gestione di infrastrutture complesse geograficamente distribuite o reti segmentate. L'utilizzo di sonde aumenta esponenzialmente la capacità di raccolta delle informazioni garantendo la scalabilità del prodotto.

TECNOLOGIE DI TERZE PARTI

SGBox sviluppa integrazioni con tecnologie di terze parti attivabili dalla console di gestione. Le app implementano diverse funzionalità, dai backup alle contromisure automatiche tramite l'utilizzo delle API garantendo l'interoperabilità con soluzioni esterne.

SYSTEM MONITORING (SM)

Per semplificare l'architettura tecnologica e la complessità gestionale, SGBox rende disponibile anche un modulo per il monitoraggio dei sistemi, servizi e applicazioni. Utilizzando il protocollo SNMP e controlli proprietari integrati, è possibile ottenere una vista d'insieme sulla disponibilità e performance delle risorse. Inoltre, impostando delle soglie di allarme, vengono generate delle notifiche e alert per prevenire potenziali danni causati dal malfunzionamento e indisponibilità delle risorse. SGBox permette di rappresentare graficamente e in modalità geografica, tramite l'utilizzo di dashboard personalizzabili, lo stato attuale dei sistemi.

LOG MANAGEMENT (LM)

Un potente motore di elaborazione permette di semplificare il processo di raccolta, centralizzazione, monitoraggio e analisi dei log. SGBox Log Management è in grado di gestire eventi raccolti da qualsiasi tipo di fonte dati come sistemi operativi, applicazioni, dispositivi di rete, sensori IoT, componenti di sicurezza, ecc. Il modulo accelera i processi di risoluzione dei problemi grazie ai dati raccolti dall'intera infrastruttura IT utilizzando politiche di indicizzazione dinamiche che lo rendono uno strumento indispensabile per raccogliere, ispezionare e archiviare tutti i log. SGBox consente inoltre agli amministratori di fornire report dettagliati sugli eventi di sicurezza e adottare in modo automatico contromisure per intercettare potenziali minacce.

RICERCHE DINAMICHE

Possibilità di "drill-down" degli eventi. Partendo da una vista d'insieme su dati storici è possible entrare nel dettaglio per analizzare il singolo evento. La selezione di un parametro nel flusso di eventi ne condiziona la visualizzazione e permette una ricerca guidata.

RETI E RILEVAZIONE DI MINACCE

SGBox è in grado di rilevare minacce quali accessi dell'utente senza privilegi, attacchi di applicazioni Web, trojan di rete, attacchi DOS, potenziali violazioni della privacy aziendale, monitoraggio dell'integrità dei file, rootkit ecc.

CONFORMITÀ

SGBox aiuta i clienti nel processo di compliance alle principali normative quali GDPR, ISO27001, PCI-DSS, ecc. Il modulo dispone di reportistica in diversi formati, specifica per la compliance e di un tool di Gap Analysis applicata ai principali regolamenti.

NESSUN LIMITE SUL TIPO DI LOG

SGBox è in grado di raccogliere qualsiasi tipo di log, senza alcuna limitazione. I lab SGBox supportano l'utente nel riconoscimento di log provenienti da apparati e applicativi custom fornendo tutti gli strumenti necessari per consentire al cliente o al partner di creare in autonomia il processo di interpretazione.

DATA BASE E CIFRATURA DEI DATI

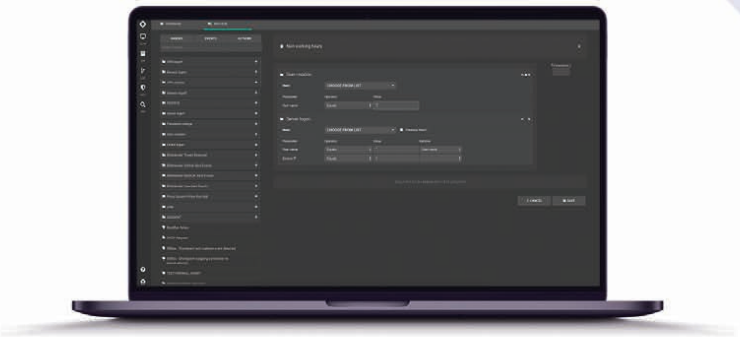
SGBox dispone di un database proprietario progettato per la raccolta e la gestione di grandi quantità di log. La firma e la cifratura asimmetrica dei log garantisce l'integrità e l'inalterabilità dei dati archiviati mentre un elevato fattore di compressione permette l'ottimizzazione dello spazio di archiviazione.

LOG CORRELATION ENGINE (LCE)

L'infrastruttuta IT genera numerosi eventi, molti dei quali significativi e utili a rilevare la presenza di minacce. L'utilizzo del motore di correlazione risulta indispensabile per descrivere e individuare gli scenari di rischio. Ogni evento raccolto contiene informazioni, spesso rilevanti, su quanto accaduto nel dominio di interesse. Il motore di correlazione, attraverso la definizione di regole appositamente strutturate rileva la presenza di anomalie riconducubili a scenari di rischio, valorizzando le informazioni raccolte e applicando una capacità di analisi evoluta e complessa. SGBox propone un motore di correlazione avanzato per descrivere scenari anomali, rilevare e attivare risposte automatiche alle minacce.

REGOLE DI CORRELAZIONE PER EVENTI

Il modulo è in grado di correlare tutti gli eventi, insieme a informazioni contestuali come identità, ruoli, vulnerabilità, allarmi di monitoraggio dei dispositivi e altro, per rilevare scenari che identificano una minaccia.



RISPOSTA AUTOMATICA ALLE MINACCE

Il motore di correlazione permette di attivare contromisure automatiche in caso di minacce lanciando uno script o interagendo con componenti di sicurezza esterni tramite API.

INTEGRAZIONE SOAR

SGBox può essere integrato con le soluzioni SOAR (Security Operations Automation Response) e alimenta eventi di sicurezza e allarmi che verranno presi in carico per analisi e approfondimenti dal team di incident response.

SGBOX API

SGBox espone le API per consentire agli strumenti esterni di recuperare informazioni su allarmi ed eventi permettendo ulteriori analisi.

CORRELAZIONE IN TEMPO REALE E SULLO STORICO

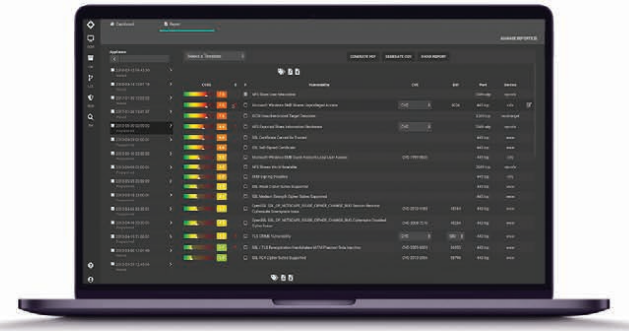
Le regole di correlazione possono essere applicate sia ai dati raccolti in tempo reale sia a quelli storici per investigazioni su anomalie o incidenti avvenuti in un determinato arco temporale.

NETWORK VULNERABILITY SCANNER (NVS)

All'interno della piattaforma SGBox è disponibile un modulo di scansione per evidenziare le vulnerabilità note su qualsiasi host. Inoltre SGBox identifica e rileva le vulnerabilità derivanti da configurazioni errate come ad esempio un firewall, un router, un server web, un server applicativo, ecc. SGBox Network Vulnerability Scanner effettua un'analisi continuativa delle vulnerabilità presentando i risultati sotto forma di report personalizzabili e incrementali. E' possibile schedulare le scansioni e inviare automaticamente i report profilati in base al ruolo dei destinatari per ottimizzare le attività di risoluzione delle vulnerabilità.

REPORT PERSONALIZZABILI

Possibilità di definire report personalizzati in base alle diverse figure aziendali che visionano il dettaglio delle vulnerabilità emerse da un'attività di scansione.



GRUPPI DI ATTIVITÀ

SGBox consente la creazione di un gruppo di risorse per differenziare le politiche di scansione e la pianificazione, associando a ciascun gruppo una o più figure di riferimento che riceveranno automaticamente i report e gli avvisi in base alle impostazioni predefinite.

CVSS & SCANSIONI REMOTE

SGBox Vulnerability Scanner utilizza il sistema di scoring riconosciuto a livello internazionale (CVSS) per attribuire un punteggio individuale per ogni singolo asset, gruppo o l'intera infrastruttura analizzata.

SCANSIONI PER LA COMPLIANCE

SGBox supporta le aziende nel percorso di certificazione e conformità verso le principali normative quali GDPR, PCI-DSS, ISO27001, ecc. SGBox mette a disposizione una serie di report per semplificare le attività di compliance.

REPORT DIFFERENZIALI

È possibile generare report incrementali per evidenziare l'andamento delle vulnerabilità riscontrate. I diversi report indicano le vulnerabilità risolte, le nuove e quelle ancora presenti in un predefinito arco temporale. Il report fornisce importanti indicazioni per la risoluzione delle vulnerabilità.

SYSTEM MONITORING (SM)

Per semplificare l'architettura tecnologica e la complessità gestionale, SGBox rende disponibile anche un modulo per il monitoraggio dei sistemi, servizi e applicazioni. Utilizzando il protocollo SNMP e controlli proprietari integrati, è possibile ottenere una vista d'insieme sulla disponibilità e performance delle risorse. Inoltre, impostando delle soglie di allarme, vengono generate delle notifiche e alert per prevenire potenziali danni causati dal malfunzionamento e indisponibilità delle risorse. SGBox permette di rappresentare graficamente e in modalità geografica, tramite l'utilizzo di dashboard personalizzabili, lo stato attuale dei sistemi.

ARCHITETTURA BASATA INTERAMENTE SU WEB

SGBox System Monitoring non richiede una configurazione specifica sui dispositivi controllati o sul firewall per effettuare i controlli. Poiché utilizza protocolli Web standard (HTTP / HTTPS) per tutte le comunicazioni, SGBox consente il monitoraggio di server distribuiti in una rete privata o nel cloud pubblico.

MONITORAGGIO IN TEMPO REALE

Grazie a numerosi check presenti, è possibile monitorare in tempo reale lo stato dei servizi e potenziali criticità come perdita di pacchetti, latenze, errori e analisi delle prestazioni anche per la verifica di SLA di servizio.

SOGLIE DI ALLARMI

Le soglie possono essere definite per ogni tipo di allarme con parametri e livelli personalizzabili al fine di ottenere avvisi in caso di criticità.

COLLETTORI DI MONITORAGGIO

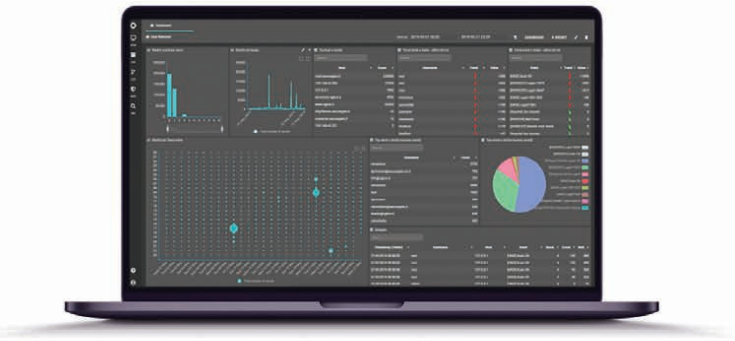
Il modulo System Monitoring utilizza collettori esterni per eseguire controlli di monitoraggio su reti complesse e geograficamente distribuite.

SETUP FACILE E COSTI TRASPARENTI

Il monitoraggio di SGBox è veloce e facile da configurare, eliminando costi ricorsivi per servizi di consulenza professionale. Come tutte le soluzioni SGBox, anche il costo del modulo di monitoraggio si basa su un modello di prezzo per dispositivo al fine di garantire un costo predicibile e trasparente.

USER BEHAVIOR ANALYTICS (UBA)

L'applicazione UBA di SGBox è progettata per raccogliere dati relativi all'attività degli utenti, individuando una "baseline" delle attività considerate standard e identificando comportamenti anomali. Ogni evento viene valutato grazie ad uno storico di informazioni raccolte e tiene conto di una serie di parametri quali l'ambiente, la frequenza, la quantità, il comportamento di altri utenti appartenenti allo stesso gruppo e ulteriori altri fattori rilevanti. UBA rileva la regolarità di una certa situazione, e se non è statisticamente accettabile, associa un fattore di rischio a ciascuna azione evidenziando l'anomalia.



INTEGRAZIONE PERFETTA

La funzionalità non richiede particolari configurazioni dal momento che UBA verifica automaticamente i fattori di rischio. Tutte le anomalie rilevate generano eventi che innescano regole nel motore correlazione più o meno complesse, con la possibilità di intraprendere contromisure, inviare allarmi o interagire con strumenti esterni attraverso le API.

VISUALIZZAZIONE TRAMITE DASHBOARD

Attraverso la console di SGBox vengono visualizzate le informazione provenienti da UBA. Abilitando l'app, l'utente sarà in grado di aggiungere una serie di nuovi widget che consentono di visualizzare informazioni relative al comportamento degli utenti in diverse modalità.

RISCHIO ASSOCIATO ALL'UTENTE

Il comportamento degli utenti viene associato alle categorie di rischio per definire delle priorità, basate sul significato di un particolare evento e non solo sul volume. Una serie di widget dedicati mostrano, insieme ad altri indicatori strategici, il rischio associato per eventi e host correlati all'attività dell'utente.

ALLARMI FACILMENTE INTERPRETABILI

UBA consente di individuare facilmente e automaticamente comportamenti anomali, ad esempio, che: *"L'utente John è coinvolto in un evento di escalation di privilegi, attività mai rilevata in precedenza. Ciò normalmente non succede alle 3 del mattino. Questo ci porta a pensare che questa sia una grave anomalia da investigare"*.

FILTRI PER RICERCA

L'utente può applicare filtri su qualsiasi oggetto nel set di widget semplicemente selezionando l'host o l'evento o l'utente che sta cercando. La dashboard presenterà automaticamente le selezioni delle utenze e metterà in evidenza le informazioni significative per consentire una rapida evidenza di anomalie.

CONTATTI

Uffici
Via Melchiorre Gioia 168, Milano, 20125 - Italia

sales@sgbox.it
www.sgbox.it