

# **SGBOX BUNDLE**

## **Next Generation SIEM & SOAR**

SGBox is an all-in-one platform for ICT security management. Its modular architecture enables it to adapt to different business security needs.

www.sgbox.eu



## **SGBOX OVERVIEW**

#### What is SGBox

SGBox is a **Next Generation Modular SIEM & SOAR platform** developed for **ICT security management** and compliance with current regulations, such as Privacy Guarantor, GDPR, nLPD, ISO 27001.

Available in **Cloud, On Premise or Saas mode**. Each module has its own specific functionality and can be added to collaborate with other modules and share the information collected, facilitating and ensuring compliance with the requirements imposed.

#### **The Platform**



## LICENSES PROGRESSIVE LICENSES PLAN

Licenses are based on the number of modules chosen and the number of data sources that send logs, allowing a linear and predictable cost.



#### Access

The Access plan allows the collection and management of logs, ensuring full compliance with the directive of the Data Protection Authority, with the possibility of extending its functions (even retrospectively) through a simple license upgrade.

#### Basic

The Basic plan allows the collection and management of all logs, ensuring full compliance with the relevant national directives, with the possibility of extending its functions (even after the event) through a simple license upgrade.

#### Advanced

The Advanced plan includes almost all the functions of the platform, and in addition to gathering, analyzing and monitoring security information, it includes modules for the correlation and proactive detection of the most complex threats.

#### Premium

The Premium plan alows you to take advatage of all the features, from the collection and analysis of logs, the correlation of information to the orchestration and automation of countermeasures to be taken, for a complete management of ICT security activities.

#### Advantages

Modular solution: you can choose between
different bundles and upgrade at any time.

 The SGBox license is based on the total number of devices that send logs and not the number of events per second (EPS).

The archiving process allows for secure data
storage through protection, encryption, digital signature application and time stamping.

30 % Annual growth 150 + Partners worldwide

## INTUITIVE DASHBOARD REAL TIME VIEWS OF SECURITY STATUS





#### **Compliance with regulations**

The collection of information takes place in compliance with privacy regulations.

#### Scalability

Choose the features you need in a progressive and scalable way.

#### **Predictable price**

The price is commensurate with the actual use of the platform.

# 95 %

Renewals

1500 Customers worldwide



#### ADVANCED LOG MANAGEMENT

The Log Management module is able to manage the event logs related to the security of any type of data source.

- √ Easy and intuitive dashboards with multiple widgets. Multiple ready-touse, pre-defined dashboards. Possibility to create new ones easily.
- Clear and simple analysis panels that allow investigations at various levels.



Ability to generate and query data for deeper searches.



#### SYSTEM MONITOR

The System Monitoring (SM) module allows, through the execution of different scripts, the collection of information from different hosts.

The monitoring feature is designed to complement the SIEM SGBox platform, to prevent malfunctions and allow the support team to analyze an issue and reach its root cause.

1
Ŧ

#### **INCIDENT MANAGEMENT**

The Incident Management module provides a unified platform for the management of incidents or anomalies encountered by other SGBox modules.

This module also allows to correlate more similar incidents, thus reducing the number and false positives, allowing a more filtered and more correct analysis.

Report System functionality allows the generation and consultation of reports in a completely new, safe and interactive format.

<	at. 194					
L CTT				14161'040 🛌 - MOR'R I	• • • • • • • • • •	
- 1a	E ULINE	in Connelfaces Di	20 Words - 1	A Carace	0 D.S.+ Dopper	D
		0	0	0	0	
	nes (1 105) (w. (4) ver				in Second	
		Later Contraction Contract	an the second			
<b>0</b> 1 - Sa.		C Second Room	an 2 n 2 t igur an tartrait			
😷 🖓 🖏		7 7030104 610. 1921	an Ara Ar Indyna Na tarrana			
Carlos ve		Const. 353-69-45534 Total 2003 Local	an ta ta sa			
C 🗠 🛀		Las of Scott Col	6 da tatawa € 0, s.			
C		Land and a second se	αιει Φ λει μει			
<b>CP</b> 136		Land and the second second	a territoria.			
😷 - Car		/ 305 R & C R 1997 - Albert 1997	e for a for by the second s			



#### THREAT INTELLIGENCE FEED MANAGEMENT

The Threat Intelligence feature allows the identification of anomalous activities by collecting information from multiple open source or commercial intelligence feeds.

SGBox collects the safety information in Indicators of Compromise (IoC) and is able to correlate the data to produce reports and alarms.



#### **ADVANCED EVENT SEARCH**

The Advanced Event Search module exploits the information collected by the other modules of the platform and allows you to create specially structured rules in order to detect the presence of anomalies attributable to risk scenarios.

- √ Intuitive Drag & Drop interface
- $\sqrt{}$  Correlation rules applicable to real-time and historical data.
- ✓ The correlation engine aggregates data from different sources and gives the ability to create custom rules to activate automatic countermeasures.



#### **USER BEHAVIOR ANALYTICS**

The module of User Behavior Analytics (UBA), allows to analyze data related to user activities identifying potentially abnormal behaviors.

By automatically creating a user-specific behavioral baseline, the solution allows you to identify any abnormalities or deviations from normal behavior.

٥	🖨 Dashboard 🛛 🧮 Class/Patters analy	Multi-class analysis Milling Historical search						
ě	GP 07 User behavior analytics - User anomalies					<b>T</b> 04598	 + where	
				E1010 202		1, UASHE	THISLE	
	widert top user hisk esp title	📥 widget pop jouer risk jesp tile	According					
10								
P								
		70.800						
		SS 831						
0		Icinali@securecite.ft	18-03-2021 01:40:26	number of times (15 times)	event of type information on ma ( to other users (2)	all server flow on he		
					event of type information on ma	all server flow on he		
Q.								
			18-03-2021	times) in 12 minutes compa				
					: Information on mail server fi			
	200.000							
	20,000							
	200,000							
	0123456789			times (15 times) in 12 minu	type information on mail server sets (2)			
				times (15 times) in 13 minu				
	There risk trend - last 24 hours		I Defails		Net N 121			
		전 🗶 🗶 🔸 🛧 💆 💆 💆						
		· · · · · · · · · · · · · · · · · · ·						
		+6510 12						
		-132 14 🍈 🍈 🔹 🖌 🍈 🍈						
		- 18 - 19 - 🕘 - 🕘 - 🔸 - 🌢 - 🎍 - 🗶 -						
		- as 👌 👤 🗣 🔭 🖢 👤 👘						
0								
		-140 Bibliot						
0	and the Party of State	-4441 O Rick level						

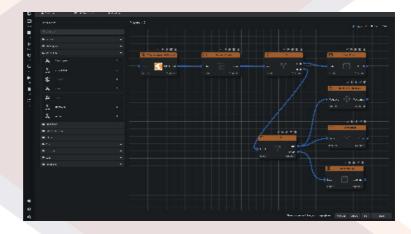




#### SOAR (Security Orchestration, Automation & Response)

The Security Orchestration, Automation, and Response (SOAR) system focuses primarily on threat management, security operations automation, and security incident responses.

The SOAR module can immediately evaluate, detect, intervene or perform investigation of accidents and processes without the need for human interaction.





#### FIM (File Integrity Monitor)

The solution allows the collection of multiple information from Windows systems, both client and server.

Through the proprietary agent of SGBox for Windows, it is possible to collect logs and information generated by Windows devices, from login and logout activities, up to the operations that took place within the file servers.

This functionality also permeates the monitoring of the integrity of files, to detect in real time any alterations and unwanted accesses of the corporate users and send timely alerts.

Δ=	ר
-	<b>~</b>
	$\overline{}$

#### **ACTIVE DIRECTORY AUDITOR**

ADA is a tool designed to constantly monitor the status of Active Directories, determine the risk and warn when the set KPI thresholds are exceeded.

This module is perfectly integrated with all other SGBox features, in fact it is able to generate lists that can be used by other modules to perform specific tasks such as event correlation, filtered reports, etc.

		Acti	ve Directory A	larm Da	shboard			
ACMELOCAL								
Users					Current threshold			
fotal Users in Domain:								
Idministrative Users:								
Administrative Users with Password never expir					⊨ 5 ⇒ 10			
								B 🛙
Show 10 entries								🗳 🖾
	Distinguished Name	f i. Hocal	NORMAL ACCOU			T LOSON 11 CREATER 4-05 10:38:07 2021-02-01		EXPIRES OF
Administrator CN			NORMAL ACCOU	IT - DONT, EXPIRE	E,PASSWORD 2021 4		20.45.57	
Administrator CN- cartagena CN-car	-Administrator,CN+Usera,DC+acme,DC+			(T - DONT, EXPIRE	E.PASSWORD 2021 6	406103807 2021-02-01	20.45.57 12:17:48	never
Administrator CN- cartagena CN-car	+Administrator,CN+Users,DC+acme,DC+ rtagena,OU+Users,OU+Acme,DC+acme,			(T - DONT, EXPIRE	E.PASSWORD 2021 6	406 19:38:07 2021-02:01 n/a 2021-10:05	20.45.57 12:17:48 21:19:51	never
Administrator CN certagona CN-cor mrossi,da CN-mre	+Administrator,CN+Users,DC+acme,DC+ rtagena,OU+Users,OU+Acme,DC+acme,			(T - DONT, EXPIRE	E.PASSWORD 2021 6	406 19:38:07 2021-02:01 n/a 2021-10:05	20.45.57 12:17:48 21:19:51	rever rever rever
Administrator CNv cartogene ONvoa moost.da ONvea Showing 1 to 3 of 3 entities	-Administrator, CN-Ubers, DC-acme, DC- tagenz, OU-Ubers, OU-Acme, DC-acme, ossi, da, DU-Ubers, OU-Acme, DC-acme,			(T - DONT, EXPINE (T - DONT, EXPINE (T - DONT_EXPINE	LPASSWORD 2021-0 LPASSWORD 2023-0 LPASSWORD 2023-0	4-05 15 38:07 2021-02:01 n/a 2023-15:05 5-17 14:20:14 2023-02:01	20.45.57 12:17.48 21:19.51	rever rever rever Previcus
Administrative ON cartagens Ohima mostilution Ohima Shewing 1 to 3 of 3 entries Administrative Users with Passend not require	-Administrator, ON-Osena, DC-acona, DC- tragena, OSH-Usena, OSH-Acona, DC-acona, DC-ac		NORMAL_ACCOU NORMAL_ACCOU 2023-09-20 06:00:06	(T - DONT_EXPIRE (T - DONT_EXPIRE (T - DONT_EXPIRE (T - DONT_EXPIRE 5		adinarda@sgbox.it	20.45.57 12.17.48 21.19.51	never never Previcus 1
Administrator CNv cartogene ONvoa moost_de ONvera Showing 1 to 3 of 3 entries	-Administrator, CN-Ubers, DC-acme, DC- tagenz, OU-Ubers, OU-Acme, DC-acme, ossi, da, DU-Ubers, OU-Acme, DC-acme,			(T - DONT, EXPINE (T - DONT, EXPINE (T - DONT_EXPINE	LPASSWORD 2021-0 LPASSWORD 2023-0 LPASSWORD 2023-0	4-05 15 38:07 2021-02:01 n/a 2023-15:05 5-17 14:20:14 2023-02:01	20.45.57 12:17.48 21:19.51	rever rever rever Previcus



#### NETWORK VULNERABILITY SCANNER

The SGBox Network Vulnerability Scanner (NVS) module allows you to detect vulnerabilities on your network.

The module is seamlessly integrated with all other SGBox features and is capable of generating lists that can be used by other modules to perform specific tasks such as event correlation, filtered reports, etc.

The NVS module integrates the Qualys-based scanning engine to perform state-of-the-art and in-depth scans of all vulnerabilities.



## SGBOX PRODUCT MATRIX

	SGBox Product Matrix								
Features	ACCESS	BASIC	ADVANCED	PREMIUM					
Access Log	0	ø	ø	9					
System Monitor	×	ø	ø	0					
Advanced Log Management	×	ø	0	•					
Advanced Event Correlation	×	×	9	•					
Windows Auditor	×	ø	ø	0					
Threat Intelligence Feed	×	×	•	ø					
User Behavior Analytics	×	×	9	0					
Vulnerability Scanner*	о	ο	0	0					
SOAR	×	×	×	ø					
Incident Management	×	×	•	•					
*Optional feature									

 The Access and Basic plans comply with
the regulations of the Data Protection Authority, while the Basic and Advanced

The vulnerability scan function is independent of the number of Data sources.

 $\triangleright$ 

Licenses are available both in "Subscription" mode (1-3 years) and in "Perpetual" mode.



# CONTACT US!

We are ready to support you in finding the security solution that best suits your needs! Request a free demo to learn more about the features of SGBox.

#### Website

www.sgbox.eu

Email info@sgbox.it

#### Address

Via Melchiorre Gioia 168- 20125 Milano, Italy

**Telephone** +39 02 60830172