SGBOX

SGBOX AND GENERAL DATA PROTECTION REGULATION

SGBOX AND COMPLIANCE WITH GDPR

SGBOX AND COMPLIANCE WITH GDPR

EU Regulation 679/2016

The entry into force of the EU Regulation 679/2016 - General Data Protection Regulation - that obliges companies to protect personal data of people in EU, had have an immediate impact on information systems.
In particular, accountability principle (Article 5, paragraph 2) imposes data controllers to demonstrate compliance with the legislation assessing adequacy of technological solutions adopted and their effectiveness in protecting personal data. Regulation violation can cause administrative charges (by control authorities, article 58) that are explained in the Article 83 as well as the criminal ones (Articles 197,168 and 169).

Here, log generated by IT devices becomes one of the main tools to trace data management activities.
Security information and event management platforms (SIEMs) have gained an important value also considering possibilities to gather information about accesses orderly.
SGBox is a next generation modular SIEM platform for a smart data management in cloud, virtual or physical appliances. Each module can be activated separately and has its own specific feature. It works together with other modules to share gathered information, facilitating the compliance with GDPR requirements.

GDPR requires to define data-destruction policy (retention period) that respects the right to obey data of the concerned party. SGBox allows not only registering all users' accesses to company's files via server audit and NAS but also to prove that secure personal data cancellation procedures are respected.

ARTICLE 17
("right to erasure/right to be forgotten")

- Monitoring of users access to resources (authentication systems, VPN accesses, file server, NAS, email server, etc);
- monitoring of system administrators accesses to resources (access log, details of operations made in the system);
- monitoring of traffic logs of perimeter firewalls (information about network connections from internal systems, communication with Command and Control systems, possible actions of data exfiltration identification);
- monitoring of generated logs from Endpoint Protection platforms (EPP) and Endpoint Detection and Response (EDR) allowing malware identification or possible attacks aimed to avoid company data;
- monitoring of logs generated by Host Intrusion Prevention and Detection (IPS, IDS) tools, also Host-based intrusion detection system (HIDS);
- monitoring of logs generated by File Integrity Monitoring (FIM) and Data Leakage Protection (DLP) solutions aimed to protect company data;
- decrease attack surface with vulnerability management activities (NVS module), identification of data asset vulnerabilities caused by updates lack or by incorrect configuration (hardening); threats classification;
- collection of Open Source Threat Intelligence Feed of third parties (LM and LCE modules) to reduce number of false positive and provide accurate information to technical staff;
- advanced features of data analysis and presentation to facilitate the IT incidents management process.

Taking advantage of collected data, Log Correlation Engine module (LCE) allows to identify risk scenarios with correlation rules that can apply automatic countermeasures.

ARTICLE 24
("responsibility of the controller")

ARTICLE 25
("data protection by design and by default")

ARTICLE 28
("right to erasure/right to be forgotten")

SGBox allows to demonstrate adequacy of technical and informative measures via security system data centralization (firewall, IDS / IPS, EOO, EDR, DLP, FIM, VPN, directory service, etc).

A powerful log recognition and normalization engine with a simple and intuitive interface allows users to aggregate logs produced by different platforms in the company. The collected data can be centrally analyzed and managed in real time. It can be done in logs history as well. The analyzed data can be presented with graphs and detailed personalized reports (dashboards).
When it is necessary to take advantage of a strong authentication, it is possible to use authentication mechanisms of an external directory server to connect to SGBox web console.

ARTICLE 32
("Security of processing")
In particular in reference to the need to adopt adeguate technical and organizational measures

---

SGBox encourages the detection of system violation (Articles 33 and 34) using automatic features based on behavioral models of User Behavior analytics (UBA).
The platform offers a complete visibility (24x7) of security events (dashboard, views, etc.) to identify an attack and accelerate response time in case of an IT incident.
Information centralization (with a possibility to set up a personalized retention time to respect the security system needs and proportion principle) encourages investigations and allows to set up root cause of a data breach.

ARTICLE 33
("notification of a personal data breach to the supervisory authority")

ARTICLE 34
("communication of a personal data breach to the data subject and by default")

SGBox offers a possibility to differentiate the access to logs information according to least privilege and need to know principles.
On request, SGBox allows to disguise information about navigation of users from proxy servers logs in visualization (via parser), in order to allow access only to authorized users (data obfuscation).
With SGBox, it is possible to correctly apply role-based access control technics to limit access to data of logs included in SIEM platform.
The platform offers asset discovery features as well as those related to definition of dynamic groups of host related to specific company functions (perimeter systems ISO 27001, human personnel systems, etc).

ARTICLE 35
("data protection impact assessment")

SGBOX

NEXT GENERATION SIEM

CONTACT US

168 Melchiorre Gioia str.
Milan, Italy 20153

+ 39 02 60830172

sales@sgbox.it

www.sgbox.it