CORA
C - SIEM

Log & asset management.
Security information and event management.

CORA C-SIEM is part of the **GRC CORA** solution, a multi-compliance software platform that allows you to manage, in a single synergistic system, more regulations, mandatory and non-binding, optimizing the time of implementation and management. The modules can be activated **independently**. Upon activation, the new module will inherit the information it has in common with the other elements already operational. **GRC CORA** is available in **Saas** and **OnPremise** mode to better accommodate the needs of each customer.

The regulatory environment

With **CORA C-SIEM** you have a solution of **Log Management** and **SIEM** (therefore with analysis, management, monitoring, correlation of events resulting from the simultaneous and fast management of millions of logs to detect anomalies, and, if appropriate, take countermeasures) can manage **logs** and **monitor**, **real time**, **all business systems**, with a **web-based interface**, **user friendly**.
CORA C-SIEM manages the log collection to be compliant with the following regulations:

- **GDPR** (then compressed, encrypted and time-stamped). It also tracks in automated mode the access to the systems of system administrators (**ADS**) as provided by the **Privacy Guarantor** and, subsequent to **GDPR**, with retention of at least **6 months**;
- It also complies with the **PCI DSS** (**Payment Card Industry Data Security Standards**), which defines the minimum data security requirements;
- **ISO 27001**, an international standard that contains the requirements to set up and manage an **information security management system**.

The solution

CORA C-SIEM is the modular and scalable solution capable of:

- Manage **Log&Asset Management** in a manner compliant with the provisions of the **GDPR** regarding **Log and System Administrators**;
- Monitor the **IT infrastructure** automatically and proactively thanks to alerts configured according to the correlation of security events tracked by the system;
- Manage and track **Vulnerability Management activities**.

CORA C-SIEM

Log & asset management.
Security information and event management.

The main features

- Log Management
- User Behavior Analytics (UBA)
- System Monitoring
- Threat Intelligence Feed Support
- Event Correlation
- Windows Auditor
- Vulnerability management

In short

LOG MANAGEMENT

Collect any log format from any type of data source. The collected Logs are signed and encrypted in order to ensure the integrity of the stored data.

WINDOWS AUDITOR

Detect external attacks on sensitive data involving financial aspects, intellectual property, human resources, product support, support.

UBA

Tracking, collection and evaluation of user data and activities through monitoring systems.

POLICIES READY

Address to the Italian Data Protection Authority, GDPR, and certifications such as ISO 27001, PCI-DSS, etc.

STORAGE OF THE LOGS

Secure access tracking to the internal logistics system.

MONITORING

It provides real-time information, analyzing the performance and status of network components.

VULNERABILITY MANAGEMENT

Vulnerability scans to get a snapshot of the infrastructure health status.

GDPR READY

Protect trade secrets - awareness of information. Tracking on deletion, modification, file/folder movement.

A simple, complete, scalable compliance suite.

GRC CORA

CORA C-SIEM is part of the GRC CORA solution.

GRC CORA is a customizable and modular solution according to the specific needs of each reality.

AGID Cloud Marketplace

You can find us on Marketplace AgID Cloud Services Catalog for Qualified PA