CORA
C - SIEM

Log & asset management.
Security information and event management.

CORA C-SIEM fa parte della soluzione **GRC CORA**, una piattaforma software multi compliance che consente di gestire, in un unico sistema sinergico, più normative, cogenti e non, ottimizzando i tempi di messa in opera e gestione. I moduli sono attivabili in modo indipendente. All'attivazione, il nuovo modulo erediterà le informazioni che questo ha in comune con gli altri elementi già operativi.
GRC CORA è disponibile in modalità **SaaS** e **OnPremise** per accogliere meglio le esigenze di ogni cliente.

Il contesto normativo

Con **CORA C-SIEM** si ha una soluzione di **Log Management** e **SIEM** (quindi con analisi, gestione, monitoraggio, correlazione di eventi derivanti dalla gestione simultanea e veloce di milioni di log per rilevare anomalie, e, se opportuno, intraprendere contromisure) in grado di gestire log e monitorare, real time, tutti i sistemi aziendali, con un'interfaccia web based, user friendly.
CORA C-SIEM gestisce la raccolta log per essere compliant alle seguenti normative:

- **GDPR** (quindi compressi, cifrati e con marcatura temporale). Traccia anche in modalità automatizzata l'accesso ai sistemi degli amministratori di sistema (**ADS**) come previsto dal **Garante Privacy** e, successivo **GDPR**, con retention di almeno **6 mesi.**
- Si rispetta anche lo standard di protezione dei dati **PCI** (**PCI DSS, Payment Card Industry Data Security Standards**), il quale definisce i requisiti minimi di sicurezza dei dati.
- **ISO 27001**, una norma internazionale che contiene i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni.

La soluzione

CORA C-SIEM è la soluzione modulare e scalabile in grado di:

- Gestire i **Log&Asset Management** in maniera compliant a quanto previsto dal GDPR in materia di Log e Amministratori di Sistema;
- Monitorare l'infrastruttura informatica in modo automatico e proattivo grazie agli alert configurati in base alla correlazione degli eventi legati alla sicurezza tracciati dal sistema;
- Gestire e tracciare le attività legate alla **Vulnerability Management**

CORA C-SIEM

Log & asset management.
Security information and event management.

Principali funzionalità

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

In breve

LOG MANAGEMENT

Raccogliere qualsiasi formato di log da qualsiasi tipo di fonte dati. I Log raccolti sono firmati e crittografati al fine di garantire l'integrità dei dati memorizzati.

WINDOWS AUDITOR

Rilevare attacchi esterni sui dati sensibili che riguardano aspetti finanziari, proprietà intellettuale, risorse umane, supporto ai prodotti, assistenza

UBA

Tracciamento, raccolta e valutazione dei dati e delle attività degli utenti mediante sistemi di monitoraggio

POLICIES READY

Indirizzamento alle normative Garante Privacy, GDPR, e alle certificazioni quali ISO 27001, PCI-DSS, ecc.

ARCHIVIAZIONE DEI LOG

Tracciamento sicuro degli accessi al sistema interno logistico

MONITORING

Fornisce informazioni in tempo reale, analizzando le prestazioni e lo stato dei componenti di rete.

VULNERABILITY MANAGEMENT

Scansioni di vulnerabilità per avere una fotografia sullo stato di salute dell'infrastruttura

GDPR READY

Proteggere i segreti commerciali - consapevolezza delle informazioni. Tracciamento sulla cancellazione, modifica, spostamento file/cartelle

La suite per la compliance
semplice, completa, scalabile.

GRC CORA

CORA C-SIEM è parte della soluzione GRC CORA.

GRC CORA è una soluzione personalizzabile e modulabile in base alle specifiche esigenze di ogni realtà.

AGID Cloud Marketplace

Ci trovi sul Marketplace AgID
Catalogo dei servizi Cloud
per la PA qualificat