

# COALA SUITE

## Log management e GDPR

### GDPR E LOG MANAGEMENT

Nel contesto del Regolamento Europeo sulla privacy (679/2016) i Log assumono un'importanza strategica. I principi Privacy by Design e Privacy by Default impongono l'uso di metodologie di analisi del rischio e di verifica della necessità dei dati trattati in relazione alle finalità, rendendo indispensabile un sistema evoluto di log management per la loro attuazione.

### COALA SUITE

Coala Suite è una soluzione completa di log management per la gestione e la sicurezza di tutto il ciclo di vita dei log: acquisizione, trasmissione, centralizzazione, archiviazione ed analisi.

Coala Suite permette di gestire grandi quantità di log garantendo la completezza, l'integrità e l'inalterabilità dei dati raccolti e minimizzando i costi di gestione.

Coala Suite è una soluzione modulare che consente di raggiungere elevati livelli di performance e di essere al tempo stesso estremamente scalabile e versatile, grazie anche alla possibilità di personalizzazione in base alle esigenze specifiche del cliente.



### COALA COLLECTOR

Il modulo Coala Collector consente di centralizzare i log in modalità cifrata e con robusti controlli di affidabilità ed integrità del dato, utilizzando appositi collettori software e protocolli sicuri; è anche possibile l'acquisizione dei dati attraverso protocolli di trasmissione standard senza la necessità di installare alcun componente software aggiuntivo sugli host che producono log.

Per ottimizzare la centralizzazione dei log, sono disponibili funzionalità di filtraggio dei log già in fase di acquisizione.

I log sono conservati su filesystem cifrato e cancellati automaticamente in base a tempi di retention configurabili per ogni singola sorgente di log.

### COALA ANALYSIS

Analizzare grandi moli di dati non strutturati ed eterogenei nella forma è stato per molti anni un obiettivo impegnativo a causa dell'impossibilità di gestire efficacemente grandi volumi di dati testuali in tempi compatibili con i bisogni informativi degli utenti. Coala Analysis rende possibili analisi e ricerche full text anche in tempo reale sul contenuto dei log e dei metadati ad essi associati; dashboard di monitoraggio, report e allarmi completano le funzionalità di analisi e consentono di disporre di molteplici strumenti per la consultazione e l'utilizzo dei risultati.



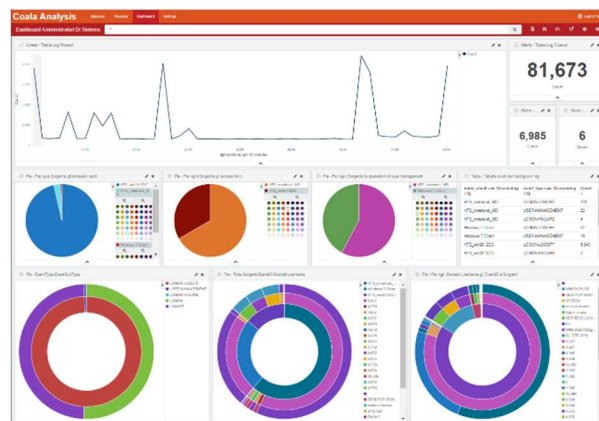
Avere una base dati affidabile su cui svolgere le analisi è il requisito indispensabile per l'attendibilità dei risultati di qualunque analisi, in particolar modo se finalizzata all'adeguamento normativo; questo è ciò che Coala Suite garantisce grazie ai moduli Collector e Analysis.

## TEMPLATE DI ANALISI

I template di analisi consentono di interpretare i log ed il loro contenuto in modo evoluto rendendo possibile il riconoscimento della tipologia di log, l'interpretazione dei singoli campi all'interno dei log, l'aggregazione per significato dei campi tra log eterogenei.

I template di analisi sono disponibili da un ricco catalogo esistente oppure possono essere sviluppati su specifiche esigenze del cliente relative sia al riconoscimento e all'interpretazione di proprie tipologie di log e sia all'aggregazione e presentazione dei risultati in base alle proprie finalità.

L'utilizzo dei template di analisi rende le funzioni del modulo Coala Analysis ancora più evolute e adatte a soddisfare sia le esigenze di conformità normativa e sia le esigenze di controllo e monitoraggio aziendali.



## GDPR: COMPLIANCE E LOG MANAGEMENT

ESIGENZA GDPR	AZIONI	COALA: FUNZIONI PRINCIPALI
Controllo accessi ai sistemi	Registrazione e conservazione log di accesso e verifiche periodiche	Ricerca real time Dashboard Report
Monitoraggio Amministratori di sistema	Registrazione e conservazione sicura log di accesso e di operazioni tipiche degli amministratori di sistema; verifiche periodiche	Ricerca real time Dashboard Report
Controllo accesso a risorse riservate	Monitoraggio accesso a file e cartelle	Dashboard Report Allarmi
Verifiche periodiche e audit	Report periodici, verifiche a campione e verifiche a posteriori	Ricerca real time On demand Report
Monitoraggio incidenti di sicurezza e Data Breach	Monitoraggio sistemi ed eventuali analisi e verifiche a posteriori e comunicazioni alle autorità	Ricerca real time Dashboard On demand Allarmi
Privacy by Design e Privacy by Default	Valutazione rischi e proporzionalità dati trattati rispetto alle finalità e verifiche periodiche	Ricerca real time On demand Filtri Collector