# LOG MANAGEMENT

La soluzione di LOG MANAGEMENT & CORRELATION di Fastweb è dotata di piattaforme leader di mercato, in grado di raccogliere, archiviare e analizzare file di log generati dai sistemi e apparati di rete aziendali in modo integrato e automatizzato, riducendo notevolmente i costi di gestione e garantendo integrità, confidenzialità e inalterabilità dei dati raccolti.

## A cosa serve

La gestione e correlazione dei LOG generati, garantisce la conformità alle normative vigenti, la raccolta dei dati rilevanti, la presentazione delle informazioni sulle reali minacce che gravano su sistemi e reti aziendali e l'indirizzamento delle relative contromisure.

## Benefici per i clienti

**Time to market e bassi investimenti**: il servizio consente l'accesso a un'infrastruttura di raccolta log senza la necessità di investire tempo e risorse nella realizzazione, delegando tali attività a Fastweb in qualità di Managed Security Service Provider.

**Security Operations Center (SOC)**: è il team di professionisti di Fastweb dedicato all'identificazione delle soluzioni che meglio si adattano alla realtà tecnologica dell'azienda per la raccolta e archiviazione dei log e per l'individuazione di attività informatiche illecite sui sistemi aziendali.

**La garanzia sui dati raccolti**: il sistema di Log Management garantisce l'immutabilità e la non modificabilità dei dati secondo quanto previsto dalla normativa italiana, grazie a protocolli cifrati per la trasmissione e la memorizzazione.

## Il servizio

Le principali caratteristiche del servizio sono:

- **Conformità alle normative** in materia di log retention sia a livello nazionale che internazionale.
- **Controllo persistente** degli eventi di sicurezza di tutti i dispositivi analizzati.
- **Individuazione tempestiva delle minacce** attraverso attività di correlazione e rilevazione anomalie.
- **Produzione di reportistica periodica** con informazioni di sintesi dettagliate e ad alto livello degli eventi occorsi.

Al fine di adattarsi al meglio alle esigenze di ogni azienda, le soluzioni proposte possono essere implementate in due modi:

- **Deployment Cloud**: non è prevista alcuna installazione di appliance hardware nella rete aziendale, ma la sola configurazione dei sistemi da cui raccogliere i log trasferiti direttamente nel Data Center di Fastweb e memorizzati in modo da garantire confidenzialità, integrità e disponibilità.
- **Deployment On Premise**: prevede l'installazione di un appliance dedicato in alta affidabilità per la raccolta dei log direttamente nella rete aziendale. In orari pianificati ne è prevista l'archiviazione sicura nel Data Center di Fastweb.
  Ideale in presenza di sistemi che generano un numero di eventi per secondo molto elevato.

I servizi Cloud di Fastweb sono erogati su DATA CENTER TIER III e TIER IV.