Progetto Log Management
(conformità provvedimento garante)

Secure Store Box (SSB) di Balabit è un appliance che colleziona, elabora, monitora e gestisce messaggi di log. È un log server appliance centralizzato che può ricevere messaggi di log (syslog ed evento) e messaggi snmp dall'infrasturttura IT in esercizio, memorizzarli in uno storage (interno o esterno) sicuro, gestirne automaticamente il backup-restore e le policy di memorizzazione.

Le funzionalità di SSB più importanti sono :

- Sicurizzazione del canale di trasmissione dei log tramite TLS o Archiviazione crittografata, firmata e con marcatura temporale (timestamp)
- Possibilità dei log da un ampio gamma di piattaforme che include
  - Linux, UNIX, BSD, Sun Solaris, HP-UX, IBM AIX, IBM system-i, Microsoft Windows XP, serve 2003, Vista server 2008.
- Inoltro dei messaggi verso motori di correlazione SIEM (Security incident event management).
- Classificazione dei messaggi tramite pattern personalizzabili
- Eventuale alta affidabilità, per garantire un servizio in ambiente mission critical
- Real time log monitoring e alerting
- Gestione utenti centralizzata (sia su database interno che su repository esterno ldap).
- Auditing di tutte le operazioni svolte sulla piattaforma SSB.

SSB non è un engine di correlazione, ma è piuttosto in grado di memorizzare i messaggi di log lasciandone inalterato il contenuto. È possibile definire dall'interfaccia amministrativa dei filtri in grado di garantire la memorizzazione dei soli messaggi di interesse rispetto alla totalità. Per una eventuale analisi forensica, il sistema è in grado di inoltrare i log ricevuto verso sistemi esterni di terzi parti in grado di svolgere l'attività di correlazione (SIEM).

Conquist Srl · Via Calefati, 6 · 70121 Bari
Tel. 080 9755801 pbx · Fax 080 9644801 · info@conquist.it · www.conquist.it
Reg. Imp. Bari, C.F e P.Iva 05525400726

I messaggi di log contengono informazioni che riguardano eventi che accadono nell'infrastruttura IT. Il monitoraggio di questi messaggi è essenziale per garantire la sicurezza ed il corretto funzionamento dei sistemi. Una soluzione di log management efficace consente numerosi benefici, dal monitoraggio degli accessi, ad eventuali usi non consentiti dei servizi di rete. Un analisi continuativa dei log permette di identificare eventuali di sicurezza, violazione delle policy aziendali o eventuali altre anomalie.

Inoltre vi sono numerose normative che richiedono esplicitamente la centralizzazione, l'archiviazione a lungo termine e l'analisi periodica dei log (Es. SOX, Basilea 2, HIPAA, PCI-DSS, ed in Italia in provvedimento del garante della privacy).

SSB colleziona nativamente i log provenienti da flussi syslog, in tutte le sue versioni, dalla storica versione con protocollo UDP a syslog-ng, per finire con syslog-tls.

Per tutti gli ambienti che non sono in grado di inviare gli eventi via syslog, SSB permette il recupero di questi log via agent che supporta le piattaforme sopra citate.

Tutti i dati ricevuti da SSB vengono immediatamente cifrati, firmati e marcati temporalmente prima di essere memorizzato sullo storage.

Quest'ultimo può essere un file (o più) interno alla macchina o un database relazionale esterno (Oracle, microsoft SQL, MySQL e PostGres).

Per ambienti particolarmente estesi è sconsigliato l'uso di database relazionali esterni i quali potrebbero degradate le prestazioni del sistema. Il log store su file interno invece è prestazionalmente piu' efficiente (non essendo effettuata analisi forensica, non vi è la necessità di avere dati relazionati) e trattandosi di dati di sistema, tipicamente dati testo è ipotizzabile anche l'utilizzo di compressione che permette la memorizzazione di molti più eventi.