Progetto SIEM per il controllo del livello di Sicurezza dei Sistemi Informativi del Gruppo SOGIN

1 SINTESI DEL PROGETTO

Si richiede di realizzare un'infrastruttura SIEM mediante la fornitura di apparati hardware, relativo software di base e d'ambiente, software applicativo e servizi ad esso correlati, compresi i servizi di maintenance. La soluzione proposta, necessariamente on-premise, dovrà garantire il conseguimento dei seguenti obiettivi, che saranno dettagliati in forma di requisiti nella Specifica Tecnica:

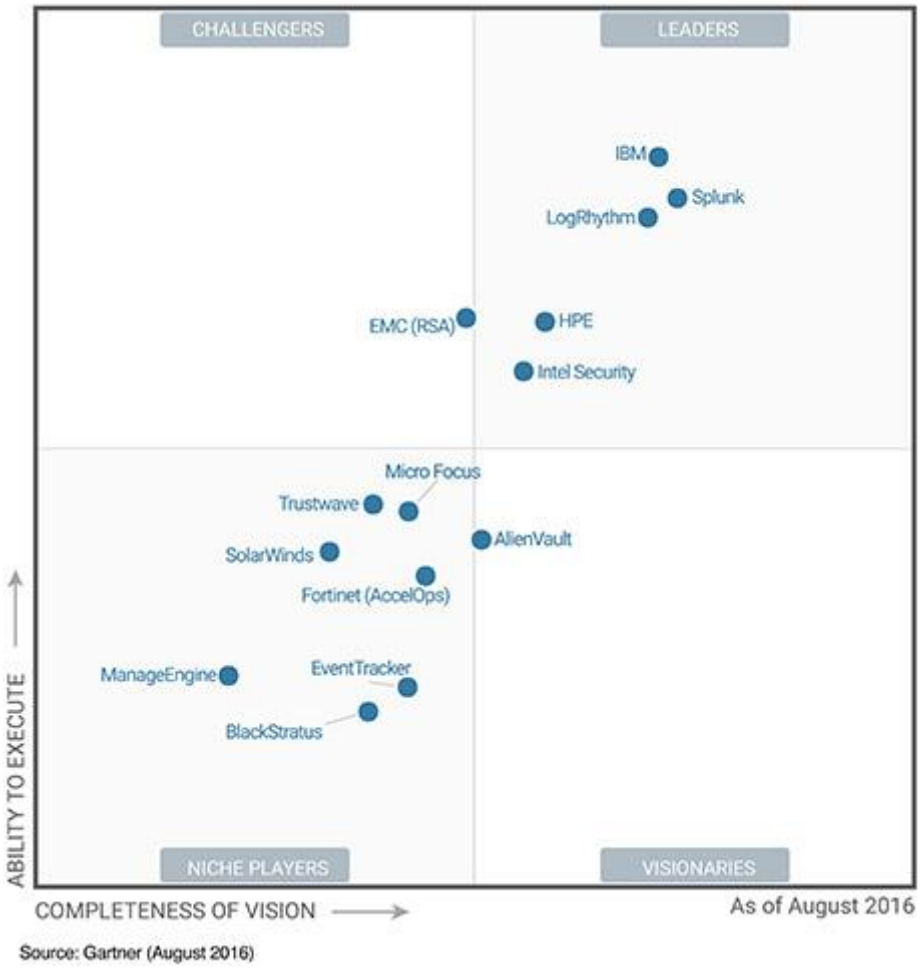
- Ottimizzare il processo di prevenzione e gestione degli incidenti informatici, tramite una nuova piattaforma di Security Information Event Management che automatizzi le fasi di raccolta, normalizzazione, analisi (in tempo reale e su basi storiche) e correlazione di tutti gli eventi rilevanti per la sicurezza dei sistemi gestiti dal Gruppo Sogin.
- Supportare il processo di analisi e rendicontazione della sicurezza, tramite una piattaforma che semplifichi e automatizzi la produzione di report di sicurezza multi-livello.

Ulteriori obiettivi di carattere funzionale sono:

- Supportare in un'ottica multi dominio (multi-tenancy) il processo di gestione incidenti nel Gruppo Sogin, garantendo a ciascuna azienda una vista isolata sugli eventi di sicurezza di propria competenza e mantenendo al contempo la gestione centralizzata della piattaforma di gestione incidenti.
- Supportare gli operatori incaricati in tutte le fasi della gestione degli incidenti di sicurezza informatica, ovvero:
    - assegnazione degli allarmi rilevati ad un incident handler;
    - classificazione degli allarmi;
    - individuazione delle misure di contrasto e contenimento;
    - segnalazione e/o escalation verso strutture all'interno di Sogin.
- Ottimizzare il processo di condivisione delle conoscenze all'interno del gruppo degli operatori incaricati alla gestione incidenti di sicurezza, tramite una knowledge base interna (aggiornabile dagli operatori stessi) in grado di indirizzare tutte le fasi della gestione incidenti.
- Ottimizzare il processo di produzione degli indicatori elementari relativi alla gestione degli incidenti, in conformità con la necessità di Sogin di garantire un'adeguata gestione della Sicurezza del Gruppo.

In particolare, Sogin intende acquisire i servizi di implementazione, tuning e manutenzione correttiva ed evolutiva di un ambiente completo di Security Information Event Management. Tale ambiente dovrà essere basato su soluzioni modulari, scalabili, flessibili ed affidabili, in grado di adattarsi facilmente ai cambiamenti organizzativi di Sogin.
Il Fornitore dovrà fare riferimento alle soluzioni presenti nel Magic Quadrant Gartner 2016 ed in particolare dovrà riferire il progetto ad uno dei prodotti appartenenti ai quadranti "Leaders" e "Challengers" indicati nel grafico.

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (August 2016)

La soluzione si intende complessiva della seguente fornitura con servizi a corredo a completa cura dell'aggiudicatario:

1. Dotazione Hardware su appliance/server dedicato completo di storage DAS opportunamente dimensionato e ridondato.
2. Hight Availibility garantita su altro appliance ovvero macchina virtuale sulla infrastruttura VmWare + storage SAN messa a disposizione da Sogin secondo le indicazioni tecniche indicate.
3. Componenti software e/o moduli e/o appliance dedicati per rispondere ai requisiti tecnici previsti da Sogin.
4. Tutti i moduli e le licenze necessari alla gestione delle fonti alimentanti Sogin (Server, end point vertice, end point critici, Firewall, IPS, Web Gateway, email gateway, network gateway ecc.).
5. Tutto il licensing per garantire l'utilizzo della soluzione dal personale di Sicurezza Industriale, dal SOC, dal personale di ICT Operations ecc.

6. Tutte le attività di installazione, configurazione, tuning, test e rilascio in esercizio della soluzione.
7. Attività di follow up della soluzione dopo periodo significativo di utilizzo con tuning ulteriore del sistema.
8. Maintenance correttivo biennale.
9. Maintenance biennale del sistema che preveda l'aggiornamento con continuità della reputazione di indirizzi IP e URL e li inserisca direttamente nel flusso degli eventi di sicurezza, identificando prontamente le interazioni passate e presenti con elementi notoriamente dannosi.