



Presentazione gruppo Ricerca di ISACA Roma

- Questa è la richiesta di volontari per contribuire alla definizione dello stato dell'arte e delle prospettive in un particolare ambito di sicurezza informatica
- Sono anche gradite le proposte di ricerca in altri ambiti

(a cura di Glauco Bertocchi CISM)

INDICE DELLA PRESENTAZIONE :

1. La proposta di ricerca
2. Quali potrebbero essere gli obiettivi
3. Come potrebbe essere organizzata
4. Varie – Q&A

La proposta di ricerca

Uno degli argomenti attualmente di “moda” è

L'intrusion prevention.

Il mondo IT ci ha abituato al sorgere di “parole d'ordine” che definivano argomenti o tecnologie di cui sembrava impossibile ignorare “l'esistenza e l'assoluta necessità” per lo sviluppo delle umane attività.

Alcune di queste (poche in verità) si sono rivelate vere evoluzioni che hanno superato positivamente la sfida del tempo.

Un “serio” professionista deve andare oltre le mode e cercare, per quanto possibile, di superare l'entusiasmo dettato dalla “moda” o dagli interessi commerciali per analizzare, realisticamente e “scientificamente”, il contenuto innovativo ed i possibili sviluppi di quanto proposto



Quali potrebbero essere gli obiettivi

Gli obiettivi di una ricerca sull'intrusion prevention potrebbero essere:

- Cosa si intende quando si parla di intrusion prevention
 - Stato dell'arte dell'evoluzione da intrusion detection a intrusion prevention
 - Intrusion prevention come proposta di nuova tecnologia o piuttosto come "assemblaggio" di tecnologie esistenti
 - Chi ha bisogno dell'intrusion prevention?
 - Etc., etc.,
-
- Ed infine la produzione di un rapporto da presentare all'Isaca



Come potrebbe essere organizzata

- Un piccolo gruppo, sperando che non sia troppo piccolo, potrebbe iniziare una prima fase dedicata ad una survey iniziale dello stato dell'arte in materia di intrusion prevention.
- Successivamente si avvierebbero, possibilmente in parallelo, le attività necessarie al raggiungimento degli obiettivi (che sarà opportuno sottoporre a revisione critica dopo la conclusione di ogni fase)
- Il gruppo valuterà quale deve essere lo stadio di approfondimento ed quando le attività saranno concluse

Slide 4.1



Bibliografia e sitografia :

Un solo riferimento, tanto per iniziare:

Standard ISO/IEC 15947 IT Intrusion Detection Framework



Varie Q&A

- Se questo argomento vi interessa , per ragioni professionali o per curiosità, aderite....
- Se non vi interessa, ditelo ad un collega od amico
- Se non avete un collega od un amico, ma avete una proposta diversa, proponetela Il mondo IT è vasto e pieno di cose da esplorare....

Grazie dell'attenzione

Sono gradite le domande

Bertocchi Glauco

Tel 3357470900

Bertocchi_g@camera.it