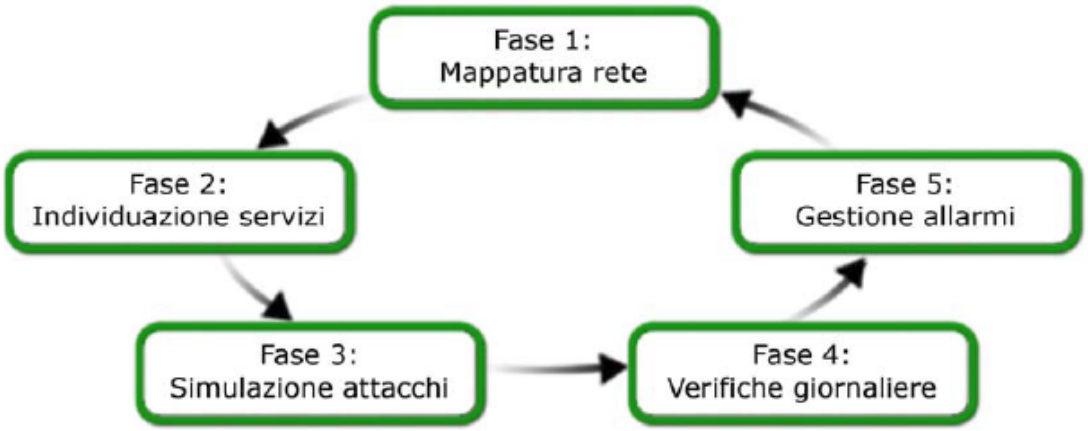
HYPERSafe

HyperGrid ha strutturato il servizio HyperSAFE dopo un attento studio dei metodi utilizzati dagli hackers e delle contromisure impiegate a difesa.



HyperSAFE riesce a garantire l'impenetrabilità dei sistemi informatici, monitorando le risorse di rete e anticipando qualsiasi tentativo di manomissione, controllando le funzionalità, la configurazione e gli aggiornamenti sia dei servers che dei dispositivi di sicurezza. Tutto ciò è possibile grazie ad una serie di verifiche, eseguite in modalità sia automatica che manuale su tutte le informazioni presenti nella rete del Cliente. Questi controlli riescono a valutare l'effettiva conformità delle misure di protezione utilizzate.

Il nostro personale specializzato analizza ogni tentativo di intrusione nella rete, approntando adeguate soluzioni, intervenendo a correggere le configurazioni del sistema. HyperSAFE è un servizio elastico, in grado di adattarsi alle necessità di ogni Cliente. Il servizio si presenta quindi strutturato; offre ad esempio la possibilità di scelta sui tempi di monitoraggio, oppure lascia scegliere attraverso quali modalità conviene avviare i controlli.

Al sistema di verifica di base per le aziende che hanno pochi contatti in rete, si affiancano in progressione altre opzioni aggiuntive: test di intrusione, test manuali, information gathering esteso, audit remoto per siti web, tentativi di Denial of Service.

Prima fase: mappatura della rete.
Realizza una mappa dettagliata sulla costituzione e sull'organizzazione della rete, evidenziando gli eventuali punti deboli dai quali potrebbero passare agenti esterni e verificando i normali sistemi di sicurezza già presenti.

Seconda fase: individuazione dei servizi.
In questa fase si verificano i protocolli attivi sulla rete del Cliente. Trovate le porte e i relativi protocolli si procede alla verifica di vulnerabilità delle stesse.

Terza fase: simulazione degli attacchi.
In questa fase, la più importante, vengono realizzati dei test di verifica sul tipo di connessione Internet e sui tempi di risposta dei sistemi. Vengono inoltre eseguiti altri test, tra cui prove manuali o automatizzate, che servono ai tecnici per analizzare i risultati.

Quarta fase: esecuzione di verifiche giornaliere e installazione di sensori IDS sulla rete del cliente.
Vengono effettuati controlli supplementari a quelli di base. Tali controlli possono essere: test di intrusione, test di interruzione di fornitura servizi, test per siti web, monitoraggio del traffico e attivazione di regole di allarme in funzione della configurazione della rete del Cliente.

Quinta fase: gestione degli allarmi.
Dopo aver analizzato i problemi riscontrati sulla rete, il nostro personale segnalerà le correzioni e le configurazioni adeguate da effettuare.

La procedura esposta è ciclica e il protocollo può essere iterato più volte.