

Penetration Test automatizzati continuativi

Dovrebbe essere una pratica ricorrente, testare le debolezze del sistema e assicurarsi che non ci siano possibili breccie nel perimetro.

I **penetration test automatizzati continuativi** assicurano questi controlli lungo tutto il perimetro.

Simulazione verosimile

L'attacco di prova, effettuato in ambiente controllato e quindi a rischio zero, viene eseguito come avverrebbe nel mondo reale: **direttamente dalla rete, senza credenziali conosciute, proprio come farebbe un hacker.**

Nessuna interruzione di servizio

Lo scopo è quello di non farsi notare, per questo assicuriamo che il processo non interromperà il servizio, simulando le tecniche che userebbe un malintenzionato. **L'attaccante cercherebbe di non essere notato, così faremo anche noi.**

Reporting e correzione errori

Il servizio fornisce un rapporto dettagliato di ogni passaggio del vettore di attacco. Da questo, **stiliamo una lista delle vulnerabilità con relativa mitigazione da mettere in pratica secondo le priorità di rischio.**



A cosa serve un Penetration Test

Un *Penetration Test*, o *Pentest*, è uno strumento di sicurezza atto a testare la solidità e la sicurezza di una rete. L'idea è quella di simulare il comportamento di malintenzionati e cercare di violare in vari modi il sistema.

Consigliamo di eseguire regolarmente un *Pentest*, soprattutto in seguito a importanti cambiamenti nell'infrastruttura. Tuttavia, un *Penetration Test* classico non è sufficiente per assicurarsi che le operazioni quotidiane non mettano a rischio l'intera infrastruttura.

Per questo è nato il servizio di Pentest automatizzato continuativo. Potendo far eseguire in modo automatico degli exploit diretti alla rete, è possibile verificare costantemente che l'infrastruttura sia al sicuro e non esposta a rischi.

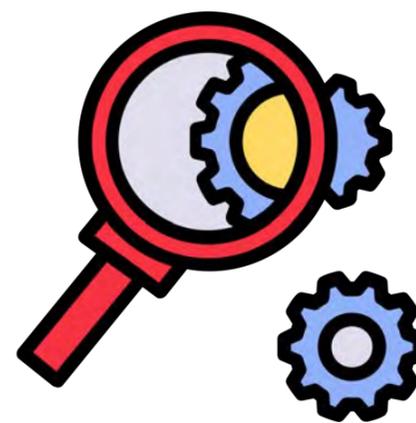


I nostri Penetration Test



Uso di tecniche aggiornate

Il sistema utilizzerà sempre le tecniche di penetrazione più aggiornate, per il migliore controllo possibile.



Frequenza del test variabile

La frequenza di test continuativo può arrivare a una cadenza quotidiana, per verificare in continuazione lo stato dell'infrastruttura.



Non interferisce con altri servizi

Il *pentest* automatico continuativo non influenza eventuali altri servizi che SOD offre per la sicurezza aziendale.

Confronto tra Pentest manuale e continuativo

Pentest	Manuale	Automatizzato
Durata	Pochi giorni	Continuato nel tempo
Tecniche usate	Limitate alla conoscenza del tester	Sempre aggiornate. Non sono implementati scenari inverosimili
Copertura	Parziale, circostanziale	Completa
Abilità di esecuzione	Fluttuante	Coerente
Rischi	Potrebbe causare downtime	Nessun rischio

Attenzione: Il pentest continuativo non esclude quello manuale, che invece è buona norma pianificare regolarmente. **I due servizi non si escludono ma si completano vicendevolmente.**

Il nostro approccio

Il nostro consiglio è quello di eseguire un *Penetration Test* manuale e approfondito una volta all'anno (o dopo cambiamenti significativi nell'infrastruttura) e di eseguire *pentest* automatici continuativamente.

Altri servizi che possono essere abbinati al pentest continuativo: **Web Application Test, Cyber Thrat Intelligence, SOCaas.**



Dal 2011 ci occupiamo di tecnologia Cloud e di sicurezza, affidati a professionisti esperti!



Scegli la
sicurezza per la
tua azienda

Scopri il servizio sul sito



Per ulteriori informazioni, i nostri contatti sono:

Via Statuto 3 c/o Impact Hub,

42121 Reggio nell'Emilia (RE)

www.secure-od.com

Tel. +39 0522 1685330

Fax. +39 0522 015371

E-mail: info@secure-od.com

Pec: secure-od@pec.it

