Due Diligence Tecnologica

Input

1. Descrizione del software, delle funzionalità e delle modalità di utilizzo lato utente e lato backend
2. Descrizione dell'architettura del software
3. Audit di terze parti (vulnerability assessment/ penetrations test/ code review)
4. Sono implementati standard di sicurezza quali ad esempio PCI, HIPAA, etc…
5. Standard utilizzati nello sviluppo del software
6. Certificazioni ottenute dal software
7. Roadmap di sviluppo sia software che tecnologica
8. Descrizione dei miglioramenti e delle modifiche più significative degli ultimi due anni
9. Schema e caratteristiche delle piattaforme tecnologiche, data centers, localizzazione, cloud, backup, piani di disaster recovery e business continuity, RPO e RTO
10. Documentazione relativa all'analisi del rischio, censimento dei dati e DPIA svolte
11. Report relativo ai problemi tecnici degli ultimi 3 anni
12. Report relative a incidenti informatici, data breach, indagini interne, degli ultimi 5 anni
13. Documentazione per l'utente finale, manuali e brochure
14. Che tipo di log vengono raccolti? Come e con che retention?
15. Vengono raccolte log relativamente alle azioni degli utenti?
16. …

Output: Interviste al venditore, supporto all'acquirente. Parere sulle tecnologie adottate e su eventuali criticità da approfondire

Fattibilità e congruità del budget: avere almeno le info del punto 1,2,3.

Due Diligence Licenze Software

Input

1. Elencazione dei framework, software di terze parti o software open source utilizzati
2. Numero di righe di codice
3. Linguaggio con cui sono scritti
4. Fornitura degli eseguibili
5. Fornitura del codice sorgente

Output: Documento. Verifica della completezza e veridicità di quanto dichiarato. Elencazione dei software di terze parti e open source rilevati.

Fattibilità e congruità del budget: avere almeno le info del punto 1,2,3.

Vulnerability Assessment Applicazione Web

Input

1. Numerosità di url esposti sul web
2. elencazione delle diverse tipologie di profili utenti che si possono autenticare
3. fornitura di credenziali di autenticazione per ogni profilo da testare

Output: Documento. Relazione tecnica contenente le vulnerabilità presenti e le possibili remediation.

Quotazione: avere almeno le info del punto 1,2.

Vulnerability Assessment Server

Input

1. Numero di server da testare (in datacenter, in locale, in cloud come ad esempio azure, aws…)
2. Elenco degli IP esposti su internet per ogni server
3. fornitura di credenziali di autenticazione per l'accesso ad ogni server da testare

*Attenzione che i test su alcuni servizi in cloud potrebbero richiedere una autorizzazione:
https://aws.amazon.com/it/security/penetration-testing/
https://portal.msrc.microsoft.com/en-us/engage/pentest

Output: Documento. Relazione tecnica contenente le vulnerabilità presenti e le possibili remediation.

Quotazione: avere almeno le info del punto 1,2.

Penetration test

Input

- Da valutare in relazione a quanto emerso nei punti precedenti

* In tale servizio è inclusa la verifica di eventuali interdipendenze di sicurezza tra le applicazioni

Output: Verifica della completezza e veridicità di quanto dichiarato

Quotazione: solo dopo aver svolto Vulnerability Assessment