CAST ITALIA

Analisi applicativa per la technical due diligence in processi di acquisizione

Il Caso di Successo del gruppo RGI

Descrizione della problematica o del bisogno nell'azienda o pubblica amministrazione utente.

Analisi degli asset tecnologici di aziende target

Il gruppo **RGI** è un'azienda focalizzata sulla realizzazione di soluzioni end to end per supportare la digitalizzazione dei processi core dei player del mercato assicurativo. Il gruppo è composto da più di mille dipendenti, su 19 uffici con clienti privati e del settore pubblico nei maggiori paesi europei.

La crescita del **gruppo RGI** ha avuto una accelerazione coincidente con la spinta alla digitalizzazione accelerata del periodo 2020-2021. In questo contesto il gruppo si è trovato a volere ampliare il proprio portfolio tecnologico acquisendo aziende specializzate, detentrici di asset software proprietari, che presidiavano determinati sottomercati.

Le decisioni a livello strategico andavano confermate e/o mitigate a livello tecnico, senza richiedere al target la disclosure dei sorgenti.

Come ottenere trasparenza ed oggettivazione dei rischi applicativi

I rischi che possono nascondersi in applicazioni apparentemente valide riguardano: l'obsolescenza, le licenze per componenti di terze parti e in primis le vulnerabilità di sicurezza che caratterizzano proprio i componenti necessari al funzionamento e alla evoluzione della applicazione.

Descrizione della soluzione tecnologica (tecnologie usate, architettura, ecc.).

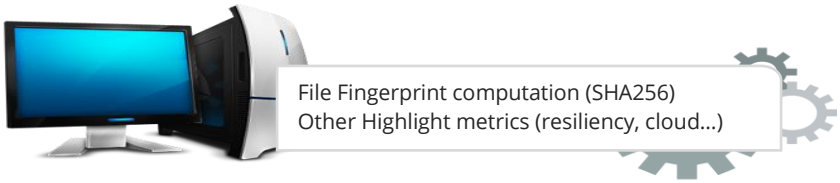
Soluzione di analisi distribuita delle applicazioni e verifica delle fingerprint

- CAST SOFTWARE ha utilizzato la propria applicazione CAST HIGHLIGHT
- CAST HIGHLIGHT ha un componente di scansione che può essere azionato all'interno della azienda target per l'analisi del codice
- Il risultato dell'analisi può essere ispezionato, ed in seguito trasmetto alla piattaforma di visualizzazione e reportistica CAST HIGHLIGHT SAAS:

Analisi dei fingerprint, recupero delle identificazioni, aggregazione dei risultati:

Tutte le risultanze veicolate al sistema di reportistica CAST HIGHLIGHT CLOUD permettono di valutare le applicazioni oggetto di technical due diligence sotto una pluralità di aspetti, a partire dai rischi di sicurezza, di licenze e di obsolescenza:

Il processo prevede quindi una fase di elaborazione locale dei dati, seguita dal confronto con l'upload dei soli dati di sintesi senza alcuna "esposizione" della proprietà intellettuale relativa:

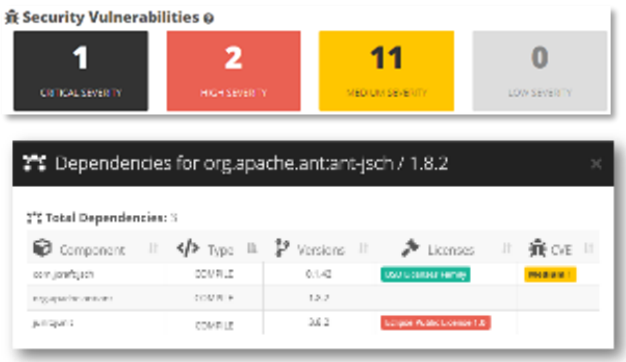


I fingerprints così ottenuti vengono caricati sul servizio HIGHLIGHT SAAS e confrontati con il database, in modo da avere i riscontri che ci informano sulla eventuale provenienza di ciascun file:

Grazie a questa metodologia i confronti vengono effettuati con estrema rapidità, in quanto il database e le operazioni di confronto sono su un infrastruttura cloud scalabile ed estremamente performance (per ragioni precauzionali i server sono situati in un datacenter all'interno della comunità europea).

Ineguagliate capacità di matching:
La collaborazione tra CAST e SOFTWARE HERITAGE, un'iniziativa open supportata da molteplici istituzioni, in collaborazione con UNESCO, permette la rilevazione puntuale dei fingerprints di 178 milioni di progetti open source, sia a livello di sorgenti che di binari.

Efficacia del riconoscimento:
Dalle operazioni di confronto con i fingerprint vengono individuate le versioni esatte dei componenti a cui appartengono i files, siano essi pacchetti binari, che file in codice sorgente (come ormai accade per molti framework open source), con l'ulteriore beneficio di permettere l'individuazione di componenti open source "mixati" con il codice proprietario.



Dal riconoscimento della versione, grazie alla continua alimentazione e d arricchimento che operiamo sul database di CAST HIGHLIGHT, vengono restituiti:

- Termini di licenza
- Vulnerabilità note
- Data di release e gap relativo
- Timeline del pacchetto

Individuazione di possibili vulnerabilità non note:
Caratteristica ulteriore è quella di potere attingere al crescente **database OSSDIB**, elaborato da CAST tramite le proprie capacità di SAST, per l'individuazione delle potenziali vulnerabilità non note (CWE) presenti nei codici sorgenti dei più diffusi pacchetti open source. Questo permette di completare la valutazione della robustezza e dei rischi inerenti ai software del parco applicativo.

In ottica di acquisizione questa capacità ha permesso di completare la valutazione degli asset applicativi target incorporando la valutazione di eventuali vulnerabilità latenti presenti nel software di terze parti.

Valore del contributo dell'uso di CAST HIGHLIGHT per i processi di M&A:

La possibilità di accedere a tutte queste informazioni, per il **gruppo RGI**, ha permesso di valutare le aziende target anche in merito alla maturità di gestione del codice, individuando delle richieste esplicite che sono state poi fatte (per tutti i casi in cui le trattative sono giunte a positiva conclusione):

- Rimozione di determinate vulnerabilità (CVE) tramite patching
- Ottemperamento a licenze che non erano esclusivamente open source (vi sono licenze che in contesti commerciali obbligano l'acquisizione di licenze commerciali),
- Rimozione di componenti duplicati ed obsoleti

Oltre a queste indicazioni puntuali che sono state incorporate nel processo di trattativa, anche considerazioni riguardo al profilo di obsolescenza relativa delle applicazioni (inferito dall'età delle versioni dei pacchetti incorporati), permettendo la mitigazione di tutti quei rischi che non sono altrimenti visibili durante la parte iniziale di un processo di acquisizione.