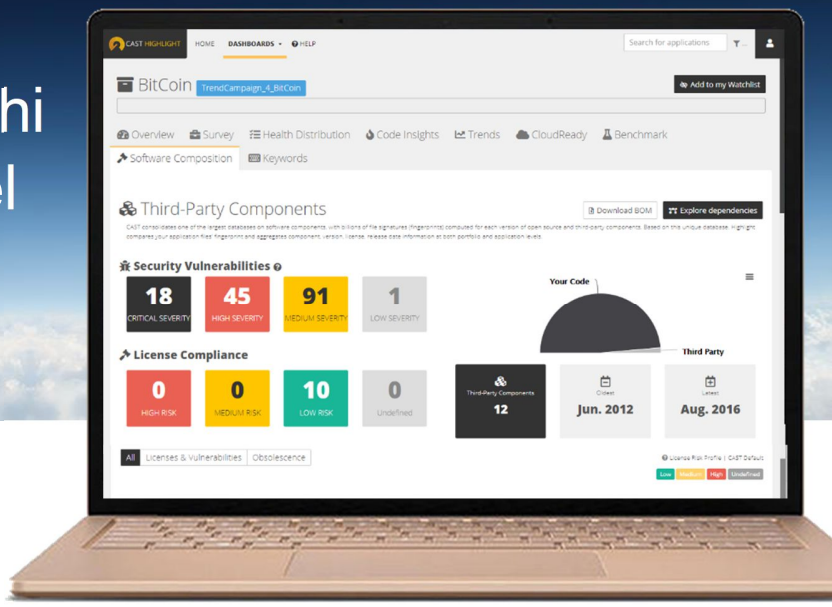
CAST
Software Intelligence for Digital Leaders

Prendi il controllo dei rischi Open Source nascosti nel tuo portfolio applicativo



Identifica ed elimina i rischi che insidiano i tuoi servizi critici a causa di un uso incontrollato di librerie Open Source nelle tue applicazioni digitali

La piattaforma CAST Highlight, basata su analisi statica predittiva, permette in pochi giorni di analizzare un intero portfolio applicativo e incorpora un meccanismo in grado di identificare ogni occorrenza di componenti Open Source negli asset software.

- **Identifica librerie, componenti e sottocomponenti attraverso l'uso dei repository** Software Heritage
- **Mappa ogni vulnerabilità di sicurezza indotta**
- **Misura obsolescenza e ridondanza del portfolio**
- **Evidenzia i rischi di licensing indotti dall'uso scorretto degli Open Source**

Riduci rischi di sicurezza

Scopri ed elimina le CVE (Common Vulnerabilities & Exposures)

Individua i componenti ridondanti ed obsoleti

Gestisci rischi di licensing

Licensing e proprietà intellettuale

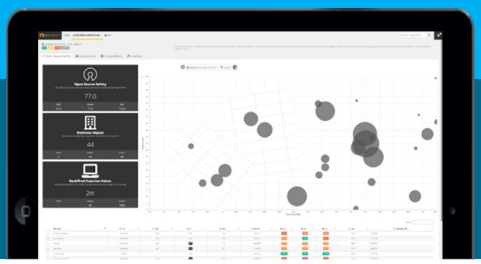
Individua le dipendenze transitive

Genera la Distinta Base del portfolio

Prendi decisioni informate

Oggettività sull'intero portfolio

Metriche complete: Business Impact, Cloud Readiness, Reliability, Agility, Elegance



castsoftware.com

CAST Highlight per l'analisi dei rischi delle librerie Open Source

La piattaforma di Rapid Portfolio Assessment permette di analizzare in tempi estremamente rapidi l'intero portfolio applicativo individuando tutte le occorrenze di utilizzo di librerie Open Source, che siano linkate o incluse nei sorgenti, sia nella loro interezza che per componenti parziali, file, classi o oggetti. Alla base di tale capacità c'è l'integrazione stretta con il più grande repository mondiale di software Open Source, *Software Heritage*, che garantisce tracciabilità storica di qualsiasi componente di pubblico dominio, fornendo quindi la possibilità di riconoscerne la presenza all'interno di qualsiasi applicativo. È così possibile tracciare accuratamente l'utilizzo di componenti di terze parti, sia diretto che attraverso alberi di dipendenze tra librerie. Ciò permette di valutare accuratamente la ridondanza, l'obsolescenza e soprattutto la rischiosità in termini di sicurezza, individuando le vulnerabilità note (*CVE*). La catalogazione accurata dei componenti Open Source permette quindi di comporre la Distinta Base del portfolio individuando tutti i potenziali rischi legati all'uso non informato di licenze di pubblico dominio che prevedono comunque stringenti clausole di proprietà intellettuale, *disclosure* e ricondivisione.

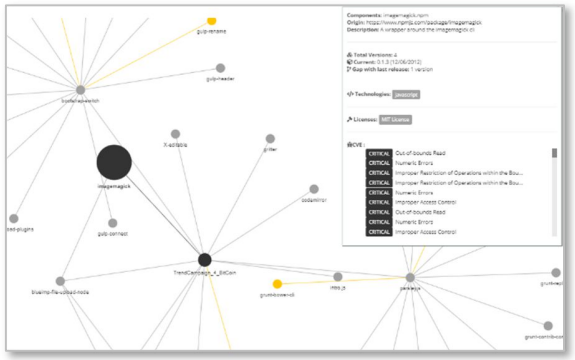
Un caso pratico

La sfida: Un cliente banking desiderava identificare le violazioni e, quindi, i punti critici di sicurezza presenti nel proprio portfolio applicativo al fine di ridurne i rischi verso i dati delle proprie *operation* e verso i dati dei propri clienti al fine di evitare eventuali furti o manipolazioni di dati. Il portfolio applicativo è composto da più di 200 applicazioni distinte.

La soluzione: Il cliente ha eseguito uno scan massivo del codice delle proprie applicazioni in portfolio. Data la quantità elevata di applicazioni in perimetro, è stata data priorità alle prime 53 applicazioni identificate come business critical, mentre la fase due si concentrerà sulle restanti 155.

I risultati:

- La fase 1 si è conclusa in 2 settimane di analisi e ha evidenziato più di 100 vulnerabilità CVE di grado CRITICAL o HIGH (basti pensare che 1 vulnerabilità CRITICAL ha generato il databreach Equifax), su componenti su cui sono stati effettuati upgrade o patch, potendo scegliere grazie a CAST quelli a minore costo.
- La fase 2 è in esecuzione e sta già portando evidenze della presenza di ulteriori CVE e di problematiche relative alla obsolescenza delle versioni attualmente utilizzate in produzione.



CAST Highlight permette di valutare i driver di Open Source Safety contestualmente ad altri parametri di valutazione dei rischi di portfolio quali: *Cloud Readiness, Resiliency, Agility, Elegance e Technical Debt, CoCoMo II*

Software Heritage (www.softwareheritage.org) ha costruito un'infrastruttura pubblica e aperta, che raccoglie tutti i sorgenti di pubblico dominio mai prodotti garantendo:

- **disponibilità**: il codice è archiviato, conservato e reso accessibile a lungo termine
- **tracciabilità**: ogni componente software ha un identificatore univoco su cui fare affidamento con profondità storica
- **uniformità**: nonostante la grande varietà di origini, è possibile accedere al codice sorgente tramite API

CAST Italia
via San Vittore, 49 20123 Milano
it.marketing@castsoftware.com