CAST
Software Intelligence for Digital Leaders

Il valore di CAST nella realizzazione della Vendor Governance

La governance dei fornitori è una strategia di gestione che consente alle organizzazioni di accrescere il valore generato dai propri fornitori controllando i costi, aumentando l'affidabilità e mitigando il rischio. Inoltre, garantisce che il fornitore diventi parte attiva del successo dell'organizzazione creando una relazione a lungo termine e abilitando il proprio contributo verso l'eccellenza attraverso la condivisione di metriche e obiettivi comuni.

CAST
Software Intelligence for Digital Leaders

CAST Italia
Via San Vittore 49 – 20123 Milano
It.marketing@castsoftware.com

castsoftware.it

Obiettivi

Attraverso l'introduzione della Software intelligence all'interno del Ciclo di Vita di Sviluppo del Software (SDLC), si ottiene:

- Aumento della sicurezza applicativa in conformità agli standard internazionali (tra i quali: ISO 5055, ISO 5230, OWASP, CWE, STIG, CISQ, NIST);
- Indicazioni puntuali delle violazioni rilevate e dei conseguenti meccanismi di mitigazione;
- Creazione di action plan automatici;
- Valutazione dei rischi software che hanno impatto diretto sul business e sui costi di esercizio;
- Introduzione di Risk Gate di controllo sulle forniture ADM e gestione del processo di Continuous Improvement sui rischi;
- Ottimizzazione delle attività di manutenzione correttiva con impatto diretto sui costi operativi;
- Analisi di qualità e sicurezza comune per tutti gli sviluppi e per tutte le aree;
- Misurazione oggettiva della qualità delle forniture tramite calcolo di KPI e SLA basati su standard formali e standard non ambigui;
- Agevolazione nella risoluzione degli errori e divulgazione efficace di best practice tra i fornitori;
- Linee guida per un piano di rimedio massivo inerente alle violazioni pregresse.

Software development life cycle (SDLC)

In una relazione di Vendor Governance il flusso di processo del ciclo di vita del software viene condiviso con tutti gli stakeholder, garantendo uniformità di qualità e di risultati e consentendo la preventiva identificazione di eventuali problemi che potrebbero verificarsi durante la fase di esecuzione, con conseguente minimizzazione delle attività correttive.

Questo garantisce una migliore interazione con i fornitori, basata su evidenze e misuratori definiti durante l'intero ciclo di vita del software, anche grazie a una reportistica facilitata e ai cruscotti automatici.

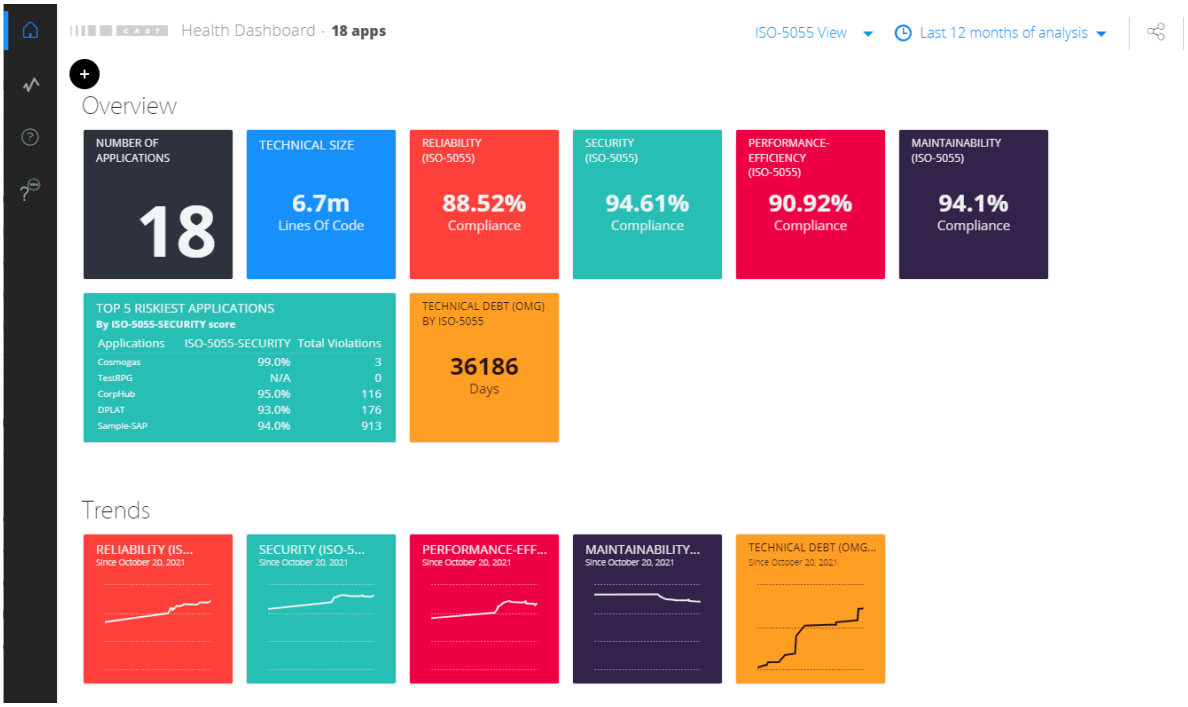
Quando viene automatizzato il processo, implementando ad esempio la metodologia DevSecOps, vi è la possibilità di automatizzare una serie di processi ripetitivi e di effettuare test di controllo automatici a favore di una maggiore sicurezza, scalabilità e collaborazione.

CAST Italia
Via San Vittore 49 – 20123 Milano
It.marketing@castsoftware.com

SLA, Governance e Contract Management

Qualora un'organizzazione appalti ad un fornitore esterno gli sviluppi e le manutenzioni (correttive o evolutive) del software applicativo, è necessario inserire contrattualmente dei *Service Level Agreement* (SLA) che vadano a regolamentare il rapporto che si va ad instaurare tra gli attori.
Al fine di garantire una relazione *win-win* tra cliente e fornitore è necessario che gli SLA siano misurabili oggettivamente e siano raggiungibili dal fornitore nell'ambito del contesto contrattuale: ad esempio, devono essere previsti i tempi e gli *effort* necessari affinché lo SLA possa essere garantito, senza dimenticare il "costo" della misura stessa.

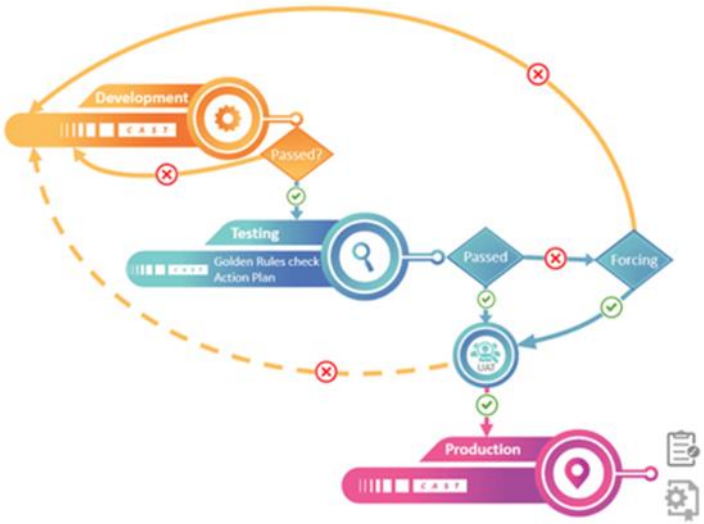
La suite CAST misura una serie di indicatori, relativi al rischio delle applicazioni, declinati secondo una serie di *Business Criteria* (Sicurezza, Manutenibilità, Efficienza, Scalabilità, Robustezza) riconducibili alle più note normative internazionali in materia di qualità e di sicurezza.



CAST Italia
Via San Vittore 49 – 20123 Milano
It.marketing@castsoftware.com

I Risk Gate di CAST

I punti di applicazione della piattaforma CAST, all'interno della catena di sviluppo, vengono convenzionalmente indicati come GATE. È infatti buona norma implementare un processo iterativo basato su azioni di rimedio, a seguito dell'identificazione di violazioni, tale che - ad ogni GATE - la criticità delle violazioni identificate sia sempre più bassa e il rischio che ne venga impattato il servizio in produzione sia via via minore.



Quello di sanare le violazioni non appena se ne ha evidenza nell'ambiente di sviluppo, è quindi un approccio assolutamente vantaggioso, in quanto presuppone che il passaggio allo stadio successivo, tipicamente quello di test/collaudo, sia condizionato alla risoluzione delle violazioni critiche già identificate (approccio shift-left). Il processo, che vede la realizzazione di azioni di rimedio prima del passaggio allo stadio successivo, va implementato su ognuno di quelli che tipicamente sono gli ambienti principali: Sviluppo, Collaudo e Produzione. Questa metodologia consente un'analisi uniforme e comune ai vari ambienti, a livello di criterio e metodologia di valutazione e garantisce il mantenimento di tali caratteristiche anche in situazioni cross-servizio e cross-tecnologia.

Inoltre, tale approccio permette un'interazione migliore con i fornitori, basata su criteri oggettivi, permettendo l'implementazione di interventi mirati e tempestivi e una diffusione ampia delle *best practice* e chiarezza circa i livelli minimi di servizio richiesti. Per essere veramente efficace ed applicabile, questo tipo di soluzione impone naturalmente un criterio di prioritizzazione delle violazioni e l'implementazione di automatismi di analisi oltre ad un meccanismo automatico di notifica verso il team di sviluppo delle violazioni identificate.

Gold, Silver e Bronze Rules

Il meta modello CAST prevede la categorizzazione delle violazioni in base al livello di criticità stilato sulla base del contesto applicativo, il tipo di business in cui il servizio si inserisce, gli aspetti che il cliente ritiene più rilevanti, la qualità di erogazione del servizio e gli standard di

CAST Italia
Via San Vittore 49 – 20123 Milano
It.marketing@castsoftware.com

sicurezza. Tale ulteriore categorizzazione consente di concentrare le attività iniziali di risoluzione fornendo benefici effettivi su un altro parametro centrale: il time to market.

Tipicamente si arriva a definire come **Golden Rules**, quel sottoinsieme di regole la cui risoluzione è ritenuta imprescindibile affinché un componente applicativo raggiunga l'ambiente di produzione, o - in generale - venga trasferito nell'ambiente successivo.

Vengono definite **Silver Rules**, quelle regole non bloccanti, ma che hanno impatto rilevante sul codice in termini di rischio, e che meritano un'attenzione particolare e un processo di rimedio specifico.

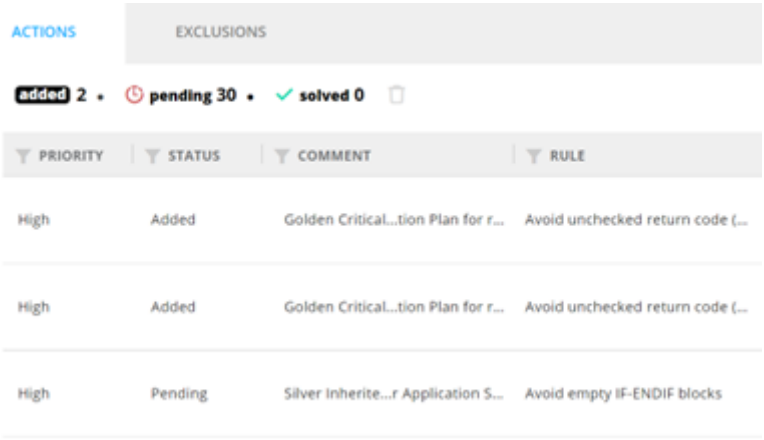
Il resto delle violazioni, di tipo critico e non critico secondo il meta modello CAST, che non siano state identificate nei passaggi precedenti, vengono inserite in una terza categoria: le regole minori o **Bronze Rules**.

Risulta logico che per garantire un'analisi puntuale e fruibile ad ogni nuova release, si renda necessario automatizzare i processi di estrazione del codice, scansione e pubblicare i risultati, integrando tali azioni con il processo di SCM (Software Control Management) aziendale.

Una volta completata l'implementazione, saranno tempestivamente disponibili gli Action Plan di rimedio, tramite i quali potranno essere pianificate le eventuali necessarie azioni di modifica e correzione e riciclo dell'analisi, oppure viene sancita la promozione del codice allo stadio successivo.

CAST Italia
Via San Vittore 49 – 20123 Milano
It.marketing@castsoftware.com

Action Plan/Project Plan



L'Action Plan è un piano di rimedio per le violazioni che vengono individuate durante l'analisi delle applicazioni ed è definito su un set di regole considerate fondamentali per la qualità e la sicurezza dell'applicazione.
Una volta elaborato, viene fornito al team di sviluppo e contiene le informazioni necessarie per individuare la violazione nel codice sorgente e per risolverla comprendendone le motivazioni e ricevendo indicazioni puntuali sulle linee guida per implementare la soluzione.

Automated Function Points

Al fine di introdurre un importante elemento di valutazione dei prodotti forniti dai Vendor, CAST ha implementato un metodo di misura automatica, attraverso l'applicazione di algoritmi di software intelligence, in grado di intercettare nel codice sorgente quelle relazioni di "uso" che tipicamente si utilizzano per accedere a entità di memorizzazione dati.
CAST ha sviluppato tale metodo introducendo la misura automatica del contenuto funzionale di un'applicazione a partire dall'analisi statica del codice sorgente, divenuto successivamente standard ISO 19515 nel 2019.

L'uso degli standard

Lo standard di riferimento al quale afferiscono gli indicatori di qualità proposti da CAST è la ISO/IEC 5055:2021 che integra il precedente standard ISO 25010 che presentava esso stesso un modello di qualità del software, ma definiva un insieme di caratteristiche solo a livello comportamentale.
L'ISO 5055 entra invece nel merito delle aree di business, dando indicazioni precise in termini di KPI misurabili ed è di fatto la norma comunemente usata nei processi di accettazione dei fornitori come garanzia di qualità.

Lo standard definisce le regole in modo da consentire il rilevamento automatico di "gravi" punti deboli contenuti nel codice applicativo esaminato.

CAST Italia
Via San Vittore 49 – 20123 Milano
It.marketing@castsoftware.com

La piattaforma CAST è in grado di trovare, segnalare e misurare i punti deboli indicati dalla ISO 5055 nell'intero stack tecnologico e in tutte le sue interconnessioni, con la sua capacità unica di

comprendere l'architettura e tenere traccia della manipolazione e dell'accesso ai dati lungo i percorsi, dalle interfacce al database. Questa piattaforma esegue l'analisi automatica dell'intero sistema di tutte le strutture di dati e i componenti del codice ed effettua inoltre il *reverse engineering* di tutte le loro interdipendenze.

Inoltre, il suo motore fornisce piani d'azione che descrivono quali punti deboli devono essere affrontati per primi per aiutare le organizzazioni a raggiungere i loro obiettivi di punteggio ISO 5055 con il minimo sforzo seguendo il percorso più breve affinché il software diventi solido, più efficiente e più sicuro