Application Security Management – Sicurezza DevOps attraverso l'automazione

Nell'epoca in cui le app sono protagoniste incontrastate dei servizi digitali, la loro sicurezza rappresenta un'istanza fondamentale. Tra le priorità di aziende e professionisti della cybersecurity, oggi spicca il bisogno di visibilità e controllo in merito all'**affidabilità delle applicazioni** impiegate nei loro differenti campi di attività; non a caso recenti ricerche evidenziano come, in media, un'organizzazione utilizzi tra gli 11 e i 20 *tools* a tale scopo.



I vari strumenti di *Application Security Testing* **(AST)** disponibili sul mercato sono senz'altro utili. Ma il rischio, in un mercato ipertrofico soggetto a continue novità – la sola Facebook mette quotidianamente in circolazione tra le 50 e le 60000 *build* per Android, mentre Amazon consegna un nuovo software al secondo e Netflix distribuisce oltre 100 *release* al giorno – è disperdere tempo ed energie in continue procedure di analisi scarsamente coordinate fra loro.

L'enorme quantità di dati emergente da tali controlli dev'essere infatti processata "a mano" per trasformarsi in conoscenze concretamente spendibili nella prevenzione dei rischi presenti o futuri. Per evitare di appesantire il lavoro degli sviluppatori, rallentando i tempi e l'efficienza della produzione, è allora necessario prevedere un costante coordinamento con i *security team* e organizzare i test nel giusto ordine di urgenza, così da consentire una gestione tempestiva delle eventuali minacce riscontrate.

L'acronimo **ASOC**, ideato dalla piattaforma Gartner per indicare

le procedure di *Application Security Orchestration and Correlation*, ben sintetizza il concetto: oggi la richiesta va nella direzione di integrare gli attuali strumenti di rappresentazione dei rischi con la loro analisi immediata, in un lavoro "corale" il più possibile automatizzato affinché tali necessarie procedure (spesso rallentate da analisi ridondanti o falsi positivi) non finiscano per impattare negativamente sui flussi di lavoro.

Simili esigenze sono alle origini di Synopsys Code Dx, nata per offrire alle organizzazioni una gestione centralizzata delle operazioni di *Application Security Testing* condotte con qualsivoglia strumento, sia esso commerciale od *open source*. L'impiego del *Triage Assistant*, applicando strumenti di *Machine Learning* per un'analisi predittiva sul potenziale impatto delle vulnerabilità scoperte, fa inoltre sì che le successive azioni vengano implementate nel giusto ordine di priorità (anche in considerazione degli obblighi di *compliance* vigenti) e che sia sempre garantita la tracciabilità dei vari compiti assegnati ai diversi gruppi di lavoro.

Forte delle oltre 4000 realtà che in tutto il mondo si affidano ai suoi servizi, Synopsis propone una **soluzione unitaria, flessibile, altamente customizzabile** per ampliare e centralizzare la visibilità dei rischi veicolati dalle app – incluse le componenti di terze parti – e ridurre drasticamente le possibilità di attacco, garantendo massima rapidità ed efficienza anche nelle attività di *remediation* che risultino necessarie in seguito all'esame e alla correlazione dei risultati.

Grazie alla minimizzazione delle operazioni manuali Code DX permette ai professionisti del mondo DevSecOps di concentrarsi sul proprio lavoro senza distrazioni, superando l'attuale parcellizzazione dei controlli in favore di una più organica e funzionale visione d'insieme.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/application-security-management-sicurezza-devops-attraverso-lautomazione/