fondamentale importanza individuare le vulnerabilità (e porvi rimedio) sin dalle prime fasi del ciclo di vita dello sviluppo, quando è ancora poco costoso e poco rischioso intervenire.

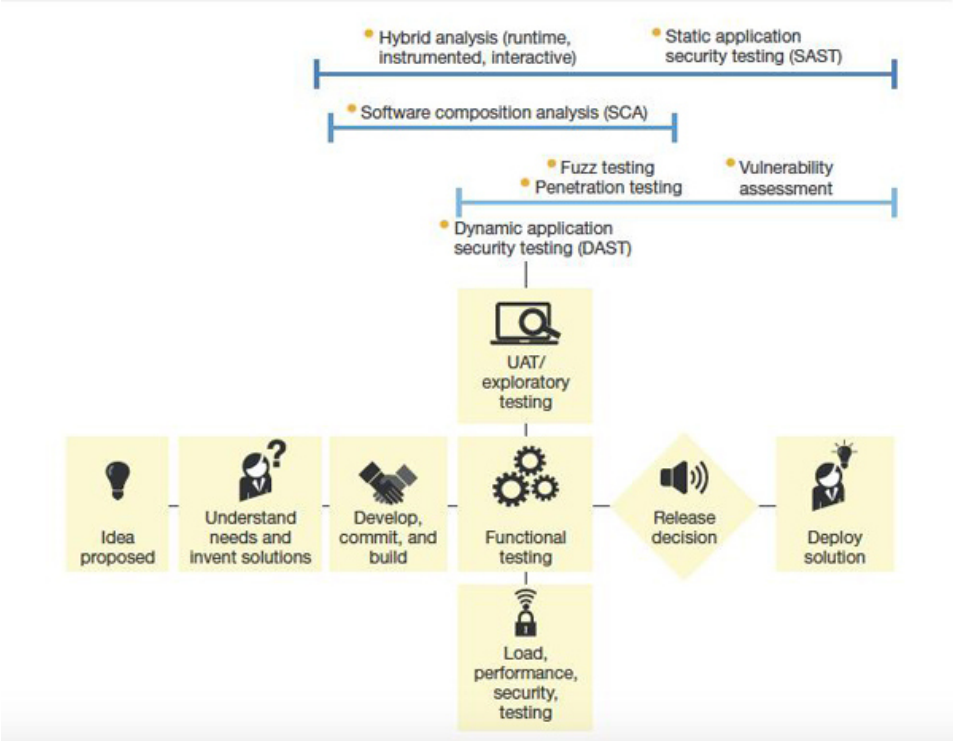

Figura 5 - Augment the life cycle with security tools

[Fonte: Forrester, Five Steps To Reinforce And Harden Application Security]

Per comporre lo stack, queste le tecnologie cui gli I&O professional dovrebbero porre attenzione:

- **Static Application Security Testing (SAST)**, tool che esaminano il codice binario e il codice di programmazione delle applicazioni senza 'mandare in esecuzione' l'applicazione (ossia senza la necessità di farla girare sui sistemi nei processi di testing);

- **Software composition analysis (SCA) tool**, tecnologie che consentono di analizzare le building block applicative per scovare vulnerabilità all'interno, per esempio, delle librerie, dei componenti open source o dei vari 'blocchi' di software che compongono l'applicazione.

- **Dynamic Application Security Testing (DAST)**, sistemi che permettono di osservare in dettaglio come si comporta l'applicazione quando è in funzione per scovarne imperfezioni o vulnerabilità prima che si prosegua con lo step di sviluppo successivo;

- **Fuzz testing tool**, sistemi che analizzano le vulnerabilità sul fronte di protocolli network, application data e input location (sempre durante i cicli di testing applicativo);

- **Hybrid analysis tool**, si tratta di tecnologie di testing per la sicurezza delle applicazioni che integrano funzionalità di Instrumented application security testing (LAST) e Runtime application security testing (RASP) utili per ridurre i falsi positivi e i falsi negativi generalmente evidenziati dai sistemi DAST;

- **Vulnerability assessment tool**, sistemi utili a rendere visibili eventuali criticità a livello di sistema operativo, configurazione dei sistemi, micro-configurazioni dei server e delle altre architetture con cui l'applicazione in sviluppo dovrà interagire una volta messa in produzione;

- **Penetration testing tool**, tecnologie utili a 'validare' l'assessment delle vulnerabilità perché mostrano come potrebbero avvenire gli attacchi simulando la penetrazione nei sistemi e nelle applicazioni.