OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1-Injection
A2 – Broken Authentication and Session Management	→	A2-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10-Insufficient Logging&Monitoring [NEW,Comm.]

Figura 4 - OWASP Top 10 - 2017

L'adozione di un Secure Software Development Life Cycle (SSDLC) atto a considerare e implementare opportune attività di sicurezza, nel corso di tutte le sue fasi del ciclo di vita del SW (dall'analisi fino alla manutenzione), è una necessità inderogabile per rispondere in modo efficace alle problematiche di sicurezza e per ridurre i costi che comportano trascurarla.

Ripensare alla sicurezza tra responsabilità e consapevolezza, oltre ad essere una buona pratica, è anche un obbligo di legge (Regolamento UE 679/2016).

4.3 Security Tools

Nell'ambito della cybersecurity, Forrester[8], nel suo report "**Five steps to reinforce and harden application security**"[9], rileva la necessità di cooperazione tra i team Security & Risk (S&R) e gli IT manager (I&O), ribadendo più volte come i primi non siano in grado, da soli, di coprire tutte le vulnerabilità scaturite dalle nuove esigenze in ambiti IT e digital business. Dal punto di vista dell'analista, infatti, l'IT team deve adottare, attraverso opportuni meccanismi di automazione e integrazione, le **security practices** all'interno di una '**continuous delivery pipeline**'. Questo garantisce una maggiore visibilità nelle interazioni tra hardware, software, servizi web e customer data. I professionisti I&O hanno, quindi, l'obiettivo di creare un ambiente di sicurezza 'responsive'.

A tal fine, Forrester propone cinque steps per costruire un **responsive security environment**:

Step 1: rimuovere le 'inconsistenze' e creare un 'conto' dei materiali

Innanzitutto è necessario eliminare tutte le problematiche di sicurezza spesso derivanti da vulnerabilità riconducibili a servizi non più utilizzati e non più mantenuti o una cattiva gestione degli accessi e delle autorizzazioni. Tale attività deve essere svolta attraverso la collaborazione tra i team dedicati (I&O e S&R).

[8] https://www.forrester.com/

[9] https://www.forrester.com/report/Five+Steps+To+Reinforce+And+Harden+Application+Security/-/E-RES127875

In aggiunta, il censimento delle componenti applicative (attraverso un approccio 'application modeling') consente di ottenere ulteriori benefici in termini di: riduzione del mean-time-to-repair (attraverso l'impiego di strumenti di gestione della configurazione a sostegno del processo di monitoraggio delle modifiche applicative e dell'infrastruttura a supporto); utilizzo limitato di software per l'analisi delle vulnerabilità di terze parti (la visione completa dell'applicazione e di come interagisce con gli altri sistemi esistenti consente di limitare l'uso di ulteriori strumenti); rapida rimozione dei 'difetti' che possono generare vulnerabilità.

Step 2: limitare e rinforzare l'accesso ai sistemi e ai network device, monitorare i cambiamenti

Generalmente l'accesso intenzionale, non autorizzato, ai dati presenti all'interno della propria organizzazione, consegue, essenzialmente, da vulnerabilità derivanti da un hardening non adeguato, da problematiche di sicurezza nel software/hardware e/o da una cattiva progettazione del sistema stesso. E' necessario lavorare a livello infrastrutturale per bloccare tutti gli accessi non autorizzati monitorando costantemente network e traffico sui sistemi. I team di gestione dell'infrastruttura e quelli della sicurezza dovrebbero cooperare nel processo di identificazione delle policy e dei tool per il monitoraggio, delle applicazioni in particolare, per verificare in tempo reale eventuali cambiamenti prima che questi si traducano in vulnerabilità.

Step 3: assistere i team di Security&Risk sul fronte intrusion detection & response

E' richiesto l'impiego di sistemi infrastrutturali e tool tecnologici a supporto delle politiche di sicurezza. Questi svolgono un ruolo determinante nella prevenzione (e nella risposta) delle intrusioni in quanto, a fronte di anomalie (legate ad esempio all'utilizzo delle Cpu o al numero delle transazioni di sistema), avendo il controllo di tutto lo stack tecnologico, riescono a fornire in tempo utile alert e informazioni al team di sicurezza. Un sistema di controllo di questo tipo accelera il mean-time-to-detection (il tempo di localizzazione di una vulnerabilità o di un attacco) e il tempo di risposta. Inoltre, cosa molto importante, riduce il range dei falsi allarmi di sicurezza (grazie ai controlli incrociati tra i team di infrastruttura e i team della sicurezza).

Step 4: 'loggare' quanto più possibile

E' estremamente importante l'attività di tracciamento e di monitoraggio in tutte le fasi del ciclo di vita di sviluppo dell'applicazione. L'obiettivo è di analizzare tutte le fonti dati nonché il materiale di ciascuna applicazione, e monitorarne ogni minimo cambiamento. A tal fine, dal punto di vista tecnologico, Forrester suggerisce:

i) l'integrazione degli Application Release Automation tool nei processi di auditing;

ii) l'adozione di sistemi di Automate Change Tracking e dashboard a supporto dai team di I&O e S&R.

Step 5: creare uno stack di application security tool

Gli step precedenti concorrono alla creazione di un vero e proprio stack tecnologico incentrato sulla sicurezza applicativa. Al fine di indirizzare correttamente una protezione efficace delle applicazioni, è di