5.1.3 Building Security in Maturity Model (BSIMM)

L'iniziativa di sicurezza BSIMM[8] è stata progettata per aiutare i team di sviluppo software a comprendere e pianificare la sicurezza in un ciclo di vita di sviluppo delle applicazioni, studiando le pratiche di cinquantuno importanti iniziative di sicurezza software. Aziende come Google, Adobe, Intel, Visa, Nokia, Sony e Microsoft hanno partecipato alla ricerca guidata da Gary McGraw (leader esperto di settore nella sicurezza del software, vicepresidente della Security Technology presso la Synopsys Inc. SNPS, autorità riconosciuta a livello mondiale per la sicurezza del software e autore di otto libri tra i più venduti su questa tematica). La metodologia risultante ha unito le migliori pratiche (parere del team BSIMM) in un'unica iniziativa. Si tratta di dodici pratiche raggruppate in quattro domini, Governance, Intelligence, SSDL Touchpoint (pratiche associate all'analisi e alla garanzia di particolari manufatti e processi di sviluppo del software. Tutte le metodologie di sicurezza del software includono l'analisi dell'architettura, la revisione del codice e i test di sicurezza) e Deployment, utilizzate per organizzare le attività del framework di sicurezza del software. La prima pratica all'interno del dominio "Intelligence" è costituita dai modelli di attacco. Il Threat modeling viene utilizzato durante questa fase per modellare gli attacchi e per creare una base di conoscenza relativa all'applicazione.
BSIMM non è un approccio innovativo per lo sviluppo sicuro del software. Questo framework ha raccolto dati su attività effettivamente svolte dai leader dell'industria promuovendo poi quelle migliori e più utilizzate, anche se per tradizione, le società di software erano riluttanti a divulgare informazioni riguardo le loro pratiche interne. L'impiego della metodologia BSIMM risulterebbe vantaggiosa per un'organizzazione che intende adottare un'iniziativa di sicurezza o migliorare/maturare le pratiche esistenti. Tuttavia, tale framework non fornisce sufficienti informazioni di dettaglio riguardo il Threat Modeling.

5.1.4 Comprehensive, Light-weight Application Security Process (CLASP)

Il CLASP[9], è un framework di sicurezza supportato dall'OWASP che contiene best practices formalizzate per attuare la sicurezza, in modo strutturato e ripetibile, nei cicli di vita di sviluppo di software in essere o in divenire. Il framework esiste dal 2005, ma non sono stati registrati recenti aggiornamenti del progetto. È stato originariamente sviluppato dalla Secure Software Inc. e successivamente donato a OWASP che lo ha rilasciato come soluzione completa di sicurezza a favore di quelle organizzazioni che intendono adottarlo. Insieme all'SDL di Microsoft, CLASP è stato riconosciuto come uno dei processi originali di alto profilo per lo sviluppo di software sicuro. CLASP, si basa su sette best practices che sono alla base di tutte le attività connesse alla sicurezza. La valutazione dell'applicazione è una di queste pratiche, che promuove un'analisi dei requisiti di sicurezza e la progettazione del sistema basata su l'utilizzo del Threat Modeling.
Il CLASP non è legato ad alcun metodo di modellizzazione specifico e non ha sviluppato un proprio approccio. Al fine di proporre un'iniziativa di sicurezza, a causa di una mancata evoluzione di questo progetto, è preferibile prendere in considerazione un framework maggiormente innovativo.

5.1.5 Microsoft's Security Development Lifecycle (SDL)

Il ciclo di vita di sviluppo sicuro (SDL[10]) è una metodologia introdotta dall'iniziativa "Trustworthy Computing" di Microsoft. SDL mira a ridurre i costi di manutenzione del software e ad aumentare l'affidabilità implementando la sicurezza in ciascuna fase del ciclo di vita dello sviluppo.

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

[9] https://www.owasp.org/index.php/CLASP_Concepts

[10] https://www.microsoft.com/en-us/sdl/default.aspx