	composizione del software (SCA) che tiene traccia di tutti i componenti di terze parti per identificare proattivamente le vulnerabilità dei componenti che mettono a rischio le applicazioni. [Life cycle security Area] OWASP Software Assurance Maturity Model (SAMM). Un framework aperto per aiutare le organizzazioni a formulare e implementare una strategia per la sicurezza del software su misura per i rischi specifici dell'organizzazione.
Code Projects	[Protection Area] Progetto OWASP AntiSamy - Una libreria per la codifica HTML e CSS: API Java e .NET per la convalida degli input HTML/CSS forniti dagli utenti al fine di prevenire gli attacchi di cross-site scripting e phishing. [Life cycle security Area] Progetto OWASP Enterprise Security API (ESAPI) - Una raccolta di librerie di sicurezza gratuite e open source che possono essere utilizzate dagli sviluppatori per costruire applicazioni web sicure. [Protection Area] Progetto OWASP ModSecurity Core Rule Set (CRS). Un insieme di regole di sicurezza per configurare strumenti di firewall come ModSecurity. [Protection Area] Progetto OWASP CSRFGuard. Una libreria da includere nei progetti di sviluppo software per costruire una difesa contro gli attacchi CSRF (Cross-Site Request Forgery). [Detection Area] Progetto OWASP AppSensor. Un quadro concettuale e una metodologia che offre una guida prescrittiva per implementare il rilevamento delle intrusioni e la risposta automatica nelle applicazioni. [Protection Area] Progetto OWASP Top Ten. La pubblicazione OWASP più famosa: le prime 10 minacce per le applicazioni web, classificate per prevalenza, sfruttabilità, rilevabilità e impatto.

5.1.2 Common Criteria (CC)

I Common Criteria sono uno standard pubblicato dall'ISO (ISO/IEC 15408-1:2009[10]), lo standard è costituito da tre parti:

- Introduzione e modello generale
- Requisiti di sicurezza funzionali
- Requisiti di sicurezza di assurance

Con i CC è fornita anche una metodologia per la valutazione, la Common Criteria Evaluation Methodology (CEM), anch'essa standardizzata dall'ISO (ISO/IEC 18405:2008). Il processo di valutazione CC di un prodotto (software o hardware) riguarda diverse fasi del SDLC applicato:

- Requisiti (Protection Profile document - PP)
- Implementazione (Security Target document – ST)
- Test

Le verifiche previste sul sistema/prodotto, nel corso della valutazione da parte dello sviluppatore e del valutatore, mirano ad accertare che siano stati soddisfatti opportuni requisiti di assurance che diventano sempre più severi al crescere del livello di valutazione.

I CC definiscono una scala di sette livelli di valutazione:

[10] https://www.iso.org/standard/50341.html