5 ANALISI DELLE INIZIATIVE E DEGLI STANDARD

5.1 Iniziative Internazionali

5.1.1 Open Web Application Security Project (OWASP)

L'Open Web Application Security Project (chiamato semplicemente OWASP) è un progetto open-source per la sicurezza delle applicazioni Web. L'OWASP offre guide con consigli sulla creazione di applicazioni Internet sicure, e indicazioni per i test cui andrebbero sottoposte. È stato, inoltre, pubblicato WebGoat, utile ad apprendere, attraverso esempi concreti, le minacce più diffuse per la sicurezza delle applicazioni web. Nel 2004 è stata istituita una fondazione no-profit che supporta l'OWASP e che persegue l'obiettivo di aumentare la sicurezza delle applicazioni consentendo di prendere le decisioni in base ai rischi. In Europa è un'organizzazione no-profit registrata da giugno 2011 ed è presente anche in Italia.

La filosofia cui si ispira OWASP si può riassumere nei seguenti punti:

- **Apertura**. Tutto in OWASP è aperto e trasparente, dal codice sorgente ai bilanci societari.
- **Innovazione**. OWASP incoraggia e supporta l'innovazione e la sperimentazione per trovare nuove e sempre più efficaci soluzioni alle sfide della sicurezza del software.
- **Universalità**. Chiunque è incoraggiato a partecipare alla comunità OWASP.
- **Integrità**. OWASP è una comunità globale, che si basa sull'onestà e sull'indipendenza.

URL	**https://www.owasp.org/**
Country of HQ location	**US**
Geographic Scope	**International**
Type	**Various Industry (not for profit)**

L'iniziativa è organizzata come una comunità collaborativa che produce tool e documenti nelle seguenti tre aree principali:

- Protection,
- Detection,
- Life-cycle security.

Relativamente a queste tre aree, OWASP ha prodotto:

- un insieme di guide sulle buone pratiche quali: OWASP Testing Guide, OWASP Code Review e Software Assurance Maturity Model;
- il Report' OWASP Top 10' sui rischi per le applicazioni web.

Da considerare inoltre, come attività rilevanti svolte da OWASP, quanto segue:

Good Practice	[Protection Area] OWASP Secure Coding Practices - Quick Reference Guide v2.0 - Un insieme indipendente dalla tecnologia di pratiche di codifica della sicurezza generale del software, in formato checklist, che può essere integrata nel ciclo di vita dello sviluppo del software. [Protection Area] OWASP Developers Guide v2.0 (2005) - Un documento completo che copre tutti gli aspetti della sicurezza delle applicazioni e dei servizi web. [Detection Area] OWASP Code Review Guide v2.0 - Una guida che raccoglie le

	migliori pratiche per la revisione del codice. [Detection Area] OWASP Testing Guide v4.0 - Una guida sulle procedure e checklist di test di sicurezza dell'applicazione. [Detection Area] OWASP Mobile Security Testing Guide (MSTG). Un manuale completo per il test di sicurezza delle applicazioni "mobile" e il reverse engineering per il security testing delle piattaforme iOS e Android.
Standards	[Detection Area] Application Security Verification Standard (ASVS). L'ASVS definisce uno standard internazionale per la valutazione della sicurezza delle applicazioni e copre sia la verifica delle applicazioni automatizzata che quella manuale, utilizzando tecniche di test di sicurezza e di revisione del codice. [Detection Area] OWASP Mobile Application Security Verification Standard (MASVS). Uno standard per la sicurezza delle applicazioni mobili.
Tools (Projects)	[Detection Area] Progetto OWASP Web Testing Environment (WTE). Una raccolta di strumenti di sicurezza delle applicazioni e di documentazione disponibile in diversi formati come VM, pacchetti di distribuzione Linux, installazioni basate su cloud e immagini ISO. Il progetto OWASP WTE è un miglioramento dell'originale OWASP Live CD Project. [Detection Area] Progetto Zed Attack Proxy (ZAP) - Questo progetto di punta di OWASP è tecnicamente uno strumento proxy per intercettare, attraverso il traffico di rete, le vulnerabilità nelle applicazioni web. È stato progettato per essere utilizzato da persone con un'esperienza consolidata in materia di sicurezza e, come tale, è ideale per gli sviluppatori e tester funzionali chiamati a svolgere il penetration testing. Include le caratteristiche dei vecchi progetti WebScarab e DirBuster. [Detection Area] Progetto SWFIntruder. È uno strumento per analizzare e testare la sicurezza delle applicazioni flash in fase di esecuzione. [Life cycle security Area] Progetto OWASP WebGoat. Un'applicazione web insicura per insegnare la sicurezza delle applicazioni web attraverso lezioni pratiche interattive. [Life cycle security Area] Piattaforma OWASP O2. Una raccolta di moduli Open Source a supporto dei professionisti della sicurezza delle applicazioni web per massimizzare i loro sforzi e ottenere rapidamente una significativa conoscenza del profilo di sicurezza di un'applicazione. [Protection Area] OWASP OWASP OWTF. Un altro strumento di punta di OWASP per i pen-test. [Detection Area] OWASP Dependency Check. Strumento per controllare e verificare la vulnerabilità delle librerie di terze parti utilizzate nei progetti di sviluppo software. [Protection Area] OWASP Security Shepherd. Strumento destinato a migliorare la capacità di pen-test del personale di sicurezza. [Protection Area] OWASP DefectDojo. Uno strumento open source di gestione delle vulnerabilità che semplifica il processo di testing, fornendo template, report, metriche e strumenti di base. [Life cycle security Area] OWASP Juice Shop. Un'applicazione web volutamente insicura per i corsi di sicurezza scritta interamente in JavaScript che comprende l'intera Top Ten di OWASP e altri gravi difetti di sicurezza. [Protection Area] OWASP Security Knowledge Framework. Uno strumento che viene utilizzato come guida per la creazione e la verifica di software sicuro; può essere utilizzato anche per formare gli sviluppatori sulla sicurezza delle applicazioni. [Detection Area] OWASP Dependency Track. Una piattaforma di analisi della

	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

- EAL1. Functionally tested
- EAL2. Structurally tested
- EAL3. Methodically tested and checked
- EAL4. Methodically designed, tested and reviewed
- EAL5. Semi-formally designed and tested
- EAL6. Semi-formally verified design and tested
- EAL7. Formally verified design and tested.

I seguenti paesi hanno firmato l'accordo Common Criteria Recognition Agreement (CCRA) che si applica da EAL1 to EAL4:

- Paesi EU/EFTA: Austria, Repubblica Ceca, Danimarca, Finlandia, Francia, Germania, Grecia, Ungheria, Italia, Paesi Bassi, Norvegia, Spagna, Svezia e Regno Unito;
- Paesi Non-EU/EFTA: Australia, Canada, India, Israele, Giappone, Corea, Malesia, Nuova Zelanda, Pakistan, Singapore, Turchia e Stati Uniti.

L'European Mutual Recognition Agreement of IT Security Evaluation Certificates o 'SOGIS-agreement' è un accordo tra alcune nazioni europee con l'adesione dell'UE o dell'EFTA relativo al mutuo riconoscimento dei certificati di valutazione secondo gli standard CC per tutti i livelli di valutazione (EAL1 EAL7).

URL	**https://www.commoncriteriaportal.org**
Country of HQ location **Geographic Scope**	International
Type	Government

I criteri comuni per la valutazione della sicurezza informatica e la metodologia comune per la sicurezza delle tecnologie di valutazione sono stati pubblicati come standard ISO.

Risultati più rilevanti:

Standard	Common Methodology for Information Technology Security Evaluation and Common Criteria for Information Technology Security Evaluation Queste costituiscono la base tecnica di un accordo internazionale (CCRA). La versione 2.3 è stata pubblicata anche come ISO/IEC 15408:2009 e ISO/IEC 18045:2008.
Future Related Standard	JTC 1/SC 27 ISO/IEC NP 20004 Tecnologie dell'informazione, tecniche di sicurezza, sviluppo di software sicuro e valutazione secondo le norme ISO/IEC 15408 e ISO/IEC 18405.

5.1.3 IEEE Computer Society

L'Iniziativa IEEE Computer Society è un'organizzazione senza fini di lucro, i principali progetti sono finalizzati alla pubblicazione di standard su tecnologie IT.

URL	https://www.computer.org
Country of HQ location	US
Geographic Scope	International
Type	Academic (not for profit)

Risultati di questa iniziativa sono libri, conferenze, pubblicazioni relative a conferenze, riviste, corsi on-line, certificazioni di sviluppo software, standard e riviste tecniche.

Risultati più rilevanti:

Good Practice	Guide to the Software Engineering Body of Knowledge (SWEBOK), la guida descrive le conoscenze generalmente accettate in materia di ingegneria del software. Le sue 15 aree di conoscenza (knowledge areas) riassumono i concetti di base e includono un elenco di riferimento per informazioni più dettagliate. Enterprise Information Technology Body of Knowledge (EITBOK) Guide. Un compendio di descrizioni di alto livello delle aree di conoscenza (knowledge areas) che sono generalmente necessarie per il buon funzionamento della tecnologia dell'informazione (IT).
Standard	Software & Systems Engineering Standards Committee (S2ESC) Formal Liaisons with ISO/IEC JTC1/SC7.

5.1.4 International Organisation for Standardization (ISO)

ISO è il più grande sviluppatore e editore al mondo di standard internazionali. Industrie ed esperti del settore generalmente contribuiscono come membri dei comitati tecnici ISO proponendo nuove normative che devono essere approvate almeno dal 70% dei membri ISO.

Il comitato tecnico che opera nell'ambito degli standard IT è il JTC 1 che, a sua volta, è organizzato in 22 sottocomitati che coprono aree specifiche. Si riporta di seguito un sottoinsieme significativo:

- ISO / IEC JTC 1 / SC 7: Ingegneria del software e dei sistemi;
- ISO / IEC JTC 1 / SC 22: Linguaggi di programmazione, compresi ambienti e interfacce software di sistema;
- ISO / IEC JTC 1 / SC 27: Sicurezza delle informazioni, sicurezza informatica e protezione della privacy;
- ISO / IEC JTC 1 / SC 38: Cloud Computing e piattaforme distribuite;
- ISO / IEC JTC 1 / SC 41: Internet of Things e tecnologie correlate;
- ISO / IEC JTC 1 / SC 42: Intelligenza artificiale.

Relativamente agli ambiti SSE troviamo:

- pubblicazione di rapporti tecnici e standard:
  - ISO / IEC TR 15026-1: 2013, ISO / IEC TR 24731-1: 2007, ISO / IEC TR 24772: 2013, ISO / IEC 15408 e ISO / IEC 18405
- 2 progetti in corso.

URL	https://www.iso.org
Geographic Scope	International
Type	Network of national standards institutes

Risultati più rilevanti:

ISO/IEC JTC 1/SC 7	ISO/IEC 15026-1:2019 Systems and software engineering -- Systems and software assurance -- Part 1: Concepts and vocabulary
ISO/IEC JTC 1/SC 22	ISO/IEC TR 24731-1:2007 Information technology - Programming languages, their environments and system software interfaces - Extensions to the C library - Part 1: Bounds-checking interfaces. Specifica una serie di estensioni del linguaggio di programmazione C, specificato dalla norma internazionale ISO/IEC 9899: 1999. Queste estensioni possono essere utili nella mitigazione delle vulnerabilità di sicurezza nei programmi. ISO/IEC TR 24731-2:2010 Information technology — Programming languages, their environments and system software interfaces — Extensions to the C library — Part 2: Dynamic Allocation Functions. Fornisce funzioni alternative per la libreria C che favoriscono la programmazione sicura. ISO/IEC TR 24772:2013 Information technology - Programming languages - Guidance on avoiding vulnerabilities in programming languages through language selection and use. Specifica le vulnerabilità del linguaggio di programmazione software da evitare nello sviluppo di sistemi in cui è richiesto un comportamento sicuro ai fini security/safety, mission critical e software business-critical. In generale, questa guida è applicabile al software sviluppato, rivisto, o mantenuto per qualsiasi applicazione. Le vulnerabilità sono descritte in modo generico, applicabili a una vasta gamma di linguaggi di programmazione. Questa guida può essere anche utilizzata dagli sviluppatori per produrre o selezionare gli strumenti di valutazione del codice sorgente capaci di scoprire ed eliminare alcuni costrutti che potrebbero portare alla vulnerabilità del software o per selezionare un linguaggio di programmazione che consenta di evitare i problemi attesi.

Progetti in corso:

ISO/IEC JTC 1/SC 7	ISO/IEC 15026-2:2011 - Systems and software engineering - Systems and software assurance -- Part 2: Assurance case. Specifica i requisiti minimi per la struttura e il contenuto di un Assurance Case per migliorare la coerenza e la comparabilità degli Assurance Case e per facilitare le comunicazioni delle parti interessate, le decisioni d'ingegneria e altri Assurance Case. Secondo questo documento ISO "*An assurance case includes a top-level claim for a property of a system or product (or set of claims), systematic argumentation regarding this claim, and the evidence and explicit assumptions that underly this argumentation. Arguing through multiple levels of subordinate claims, this structured argumentation connects the top-level claim to the evidence and assumptions*". ISO/IEC CD 15026-3 Systems and software engineering -- Systems and software assurance -- Part 3:2015 System Integrity levels. Si riferisce ai livelli d'integrità dell'Assurance Case e include i requisiti relativi al loro utilizzo con e senza un Assurance Case. Secondo questo documento ISO "*A software integrity level denotes a range of values of a software property necessary to maintain system risks within tolerable limits*".
ISO/IEC JTC 1/SC 27	ISO/IEC 27021:2017 Information technology -- Security techniques -- Competence requirements for information security management systems professionals ISO/IEC/IEE 15026-1:2019: Systems and software engineering -- Systems and software assurance -- Part 1: Concepts and vocabulary ISO/IEC 15026-2:2011 Systems and software engineering — Systems and software assurance — Part 2: Assurance case ISO/IEC NP 20004: Information technology - Security techniques - Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405. Si riferisce a un problema differente e più urgente associato all'uso pratico dei Common Criteria, ossia la relazione tra i processi di sviluppo e di valutazione con l'analisi dei potenziali attacchi. E' legato all'iniziativa CAPEC. ISO/IEC TS 19608: 2018 Guidance for developing security and privacy functional requirements based on ISO/IEC 15408 ISO/IEC TS 19249: 2017 Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls

5.1.5 International Society of Automation (ISA)

ISA è un'organizzazione globale no-profit che sviluppa standard per l'industria, certifica i professionisti di settore, offre istruzione e formazione, pubblica libri e articoli tecnici, ospita convegni e fiere per i professionisti dell'automazione.
La cybersecurity per l'industria è diversa dalle altre aree. Nell'automazione industriale la priorità è mantenere l'impianto in funzione garantendo, laddove possibile, integrità e riservatezza (AIC - availability,

integrity and confidentiality) mentre nelle altre aree la priorità è la protezione dei dati (CIA - confidentiality, integrity, availability).

URL	https://www.isa.org/
Country of HQ location **Geographic Scope**	US International
Type	Industry (not for profit)

I membri ISA pagano una tassa regolare (annuale o biennale), in base al loro tipo di appartenenza, al fine di ottenere i benefici ISA come l'accesso alle informazioni tecniche e alle risorse per lo sviluppo professionale.

Risultati più rilevanti:

Standards	**ANSI/ISA 62443** (formerly **ISA-99**) - **Security for industrial automation and control systems** - è una serie di standard, report tecnici e relative informazioni che definiscono le procedure per l'implementazione di sistemi sicuri di automazione e controllo industriale (IACS). La presente guida si applica a tutte le parti interessate che attuano o gestiscono l'IACS. Tutti gli standard ISA-62443 e i report tecnici sono organizzati in quattro categorie generali denominate *General*, *Policies and Procedures*, *System and Component*.
INDUSTRIAL CYBERSECURITY STANDARDS	ANSI/ISA-62443-4-2-2018, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components. ANSI/ISA-62443-4-1-2018, Security for industrial automation and control systems, Part 4-1: Product security development life-cycle requirements. Definisce un **secure development life-cycle (SSDLC)** allo scopo di realizzare e mantenere prodotti software sicuri. Questo ciclo di vita comprende la definizione dei requisiti di sicurezza, la progettazione sicura, l'implementazione sicura (incluse le linee guida di codifica), la verifica e la convalida, la gestione dei difetti di sicurezza, la gestione delle patch e la fine del ciclo di vita del prodotto. Tali requisiti possono essere applicati a processi nuovi o esistenti per sviluppare, mantenere e dismettere hardware, software o firmware per prodotti nuovi o esistenti. Tali requisiti si rivolgono allo sviluppatore e al manutentore del prodotto, ma non agli addetti all'integrazione né all'utente finale del prodotto. ANSI/ISA-62443-2-4-2018 / IEC 62443-2-4:2015+AMD1:2017 CSV, Security for industrial automation and control systems, Part 2-4: Security program requirements for IACS service providers (IEC 62443-2-4:2015+AMD1:2017 CSV, IDT). ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security levels. Questo standard definisce i requisiti di sicurezza che sono raggruppati in sette categorie: 1) Controllo degli accessi, 2) Controllo dell'utilizzo, 3) Integrità dei dati, 4) Riservatezza dei dati, 5) Limitazione dei flussi di dati, 6) Risposta tempestiva a un evento e 7) Disponibilità delle risorse di rete. Ogni categoria comprende una mappatura dei requisiti per garantire un adeguato livello di sicurezza.

	ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program. ANSI/ISA-62443-1-1 (99.01.01)-2007, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models.
INDUSTRIAL CYBERSECURITY CERTIFICATE PROGRAM	Certificate 1: ISA/IEC 62443 Cybersecurity Fundamentals Specialist. Certificate 2: ISA/IEC 62443 Cybersecurity Risk Assessment Specialist. Certificate 3: ISA/IEC 62443 Cybersecurity Design Specialist. Certificate 4: ISA/IEC 62443 Cybersecurity Maintenance Specialist. ISA/IEC 62443 Cybersecurity Expert.
CONFORMITY ASSESSMENT	Cybersecurity Certification to ISA/IEC 62443 Standards – It certifies devices and systems to the ISA/IEC 62443 Industrial Automation and Control Systems (IACS) cybersecurity standards.
TRAINING COURSES	Introduction to Industrial Automation Security and the ANSI/ISA99 Standards (IC32C). Using the ANSI/ISA99 Standard to Secure Your Control System (IC32). Industrial Networking and Security (TS12). Assessing the Cybersecurity of New or Existing IACS Systems (IC33). IACS Cybersecurity Design & Implementation (IC34). IACS Cybersecurity Operations & Maintenance (IC37).

5.1.6 Software Assurance Forum for Excellence in Code (SAFECODE)

SAFECode è un'iniziativa privata creata da sviluppatori software e fornitori. Individuando e promuovendo le migliori pratiche in SSE, questa iniziativa sostiene che l'industria del software potrebbe rilasciare software, hardware e servizi più sicuri e affidabili. Tra le sue uscite principali, ci sono i documenti che raccolgono le migliori pratiche, tenendo conto del ciclo di vita di sviluppo del software.

URL	**https://www.safecode.org**
Country of HQ location	US
Geographic Scope	International
Type	Industry (not for profit)

SAFECode afferma che i suoi obiettivi sono:

1. Identificare e condividere collaudate pratiche di garanzia del software;
2. Promuovere una più ampia adozione di tali pratiche nell'ecosistema informatico;
3. Lavorare con istituzioni e fornitori di infrastrutture critiche per sfruttare le pratiche nella gestione dei rischi aziendali.

Risultati più rilevanti:

Training	**Security Engineering Training** Un quadro di riferimento per i programmi di formazione aziendale sui principi dello sviluppo sicuro del software. Security engineering training by SAFECode è una risorsa della comunità online che offre corsi gratuiti di formazione sulla sicurezza del software erogati

	tramite webcast on-demand.
Good Practice	**Software Integrity Controls** Un approccio impiegato per ridurre al minimo i rischi nella catena di fornitura del software. Sulla base delle pratiche dei membri SAFECode, il rapporto fornisce controlli di integrità per l'approvvigionamento, lo sviluppo, i test, la consegna e la resilienza del software. **The Software Supply Chain Integrity Framework** Documento che definisce i rischi e le responsabilità per rendere sicuro il software nella catena di fornitura globale. Sulla base dell'esperienza dei membri del SAFECode, descrive la catena di fornitura del software (modello a scala dei fornitori di software) e i principi per la progettazione dei controlli di integrità del software. **Fundamental Practices for Secure Software Development** Sulla base delle pratiche dei membri SAFECode, questo documento delinea un insieme di pratiche per lo sviluppo sicuro del software che possono essere applicate nelle diverse fasi del ciclo di vita dello sviluppo del software. **Software Assurance: An Overview of Current Industry Best Practices** Documento che descrive i metodi di sviluppo e i controlli di integrità utilizzati dai membri SAFECode per migliorare la sicurezza del software e la sicurezza nel rilascio. **Practices for Secure Development of Cloud Applications** SAFECode e la Cloud Security Alliance (CSA) rilasciano una guida per lo sviluppo sicuro di applicazioni cloud. Questo documento rappresenta il prodotto di tale collaborazione ed è destinato ad aiutare i lettori a comprendere meglio e implementare le migliori pratiche per lo sviluppo di software cloud sicuro. **Tactical Threat Modeling** Questo documento sfrutta le intuizioni dei membri del SAFECode per offrire modi efficaci per integrare meglio la modellazione delle minacce nei processi di sviluppo. **Managing Security Risks Inherent in the Use of Third-party Components** L'uso di componenti di terze parti (TPC), compresi i componenti software open source (OSS) o commerciali off-the-shelf (COTS), è diventato di fatto uno standard nello sviluppo del software. Questo documento analizza il processo e le procedure di cui gli sviluppatori necessitano per testare, migliorare e quantificare la sicurezza dei componenti di terze parti.

5.1.7 SANS Software Security Institute (SANS SSI)

SANS SSI offre una libreria di iniziative di ricerca e di community per aiutare sviluppatori, architetti, programmatori e responsabili della sicurezza delle applicazioni a proteggere le loro applicazioni software/web.
Questa iniziativa raccoglie e fornisce informazioni tecniche aggiornate, come l'accesso gratuito alle risorse sui più recenti vettori di attacco e sulle vulnerabilità di sicurezza delle applicazioni, tra cui un blog aggiornato, news-letters settimanali, webcast, articoli e documenti in materia di sicurezza del software.

URL	**https://www.sans.org**
Country of HQ location	US
Geographic Scope	International

Type	Academic

SANS pubblica relazioni annuali (Top 25 Software Errors) con l'analisi sugli errori di programmazione più pericolosi: http://www.sans.org/top25-software-errors/.

L'ultima release (**2019 CWE Top 25 Most Dangerous Software Errors**) è fruibile al seguente link: https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html.

Risultati più rilevanti:

Resources	**Application Security Resources:** Whitepapers e webcasts sulla sicurezza della applicazioni. **Security Laboratory:** Il "Security Laboratory" è un insieme informale di articoli e whitepaper sulla sicurezza, l'informatica e l'industria della sicurezza informatica. **Fundamental Practices for Secure Software Internet Storm Center (ISC)** Il ISC fornisce un servizio gratuito di analisi e di allarme agli utenti di Internet e alle organizzazioni. I volontari donano il loro tempo per analizzare difetti e anomalie e pubblicare un diario giornaliero delle loro analisi e riflessioni sul sito web di Storm Center. **Application Security Procurement Language:** Questo è un progetto di contratto software per gli acquirenti di software personalizzato. Il suo obiettivo è quello di rendere gli sviluppatori di codice responsabili del controllo del codice e della correzione dei difetti di sicurezza prima della consegna del software. **Top 25 Software Errors**. Sono elencate in tre categorie: • Interazione non sicura fra componenti • Risky Resource Management • Difesa insufficiente. Ciascun errore include: • La classificazione all'interno della Top 25 • Collegamenti a tutti i riferimenti alla CWE • Frequenza delle CWE e relative conseguenze nei campi dati • Costi di risanamento • Facilità di rilevamento • Esempi di codice • Metodi di rilevamento • Frequenza degli attacchi e consapevolezza degli aggressori • Le relative CWE e i modelli di attacco per questa vulnerabilità. Comprende anche misure di prevenzione e bonifica sufficientemente estese che gli sviluppatori possono adottare per mitigare o eliminare la vulnerabilità.

5.1.8 Web Application Security Consortium (WASC)

WASC produce best practice per le applicazioni web. WASC riassume la sua missione nella seguente frase "*to develop, adopt, and advocate standards for web application security*".

URL	http://www.webappsec.org/
Country of HQ location Geographic Scope	US International
Type	Industry (not for profit)

Risultati più rilevanti:

Resources	**Web Application Security Scanner Evaluation Criteria (**WASSEC**)** Una serie di linee guida per valutare gli strumenti di scansione delle applicazioni web riguardo la loro efficacia nel testare e identificare le vulnerabilità. **The Web Hacking Incidents Database (WHID)** WHID è un progetto del Web Application Security Consortium dedicato al mantenimento di un elenco di applicazioni web relative agli incidenti di sicurezza. **WASC Script Mapping Project** Elenco delle modalità di esecuzione degli script all'interno di una pagina web senza usare i tag <script>. **Distributed Web Honeypot (DWH) Project** Identificare gli attacchi emergenti contro le applicazioni web e segnalarli alla comunità. **Web Security Glossary** Indice dei termini e della terminologia relativa alla sicurezza delle applicazioni web. **WASC Threat Classification v2.0** È un effort per classificare le debolezze e gli attacchi che possono portare alla compromissione di un sito web, dei suoi dati o dei suoi utenti. **Web Application Firewall Evaluation Criteria** Sviluppo di criteri dettagliati per la valutazione di un firewall di un'applicazione web (WAF). **WASC Web Application Security Statistics** Raccolta di statistiche sulla vulnerabilità delle applicazioni per identificare e mappare i problemi di sicurezza delle applicazioni sui siti web aziendali.

5.1.9 Institute For Software Quality (ifSQ)

L'Istituto per la Qualità del Software, con sede nei Paesi Bassi, è un gruppo di professionisti coinvolti nello sviluppo e nella distribuzione di software. ifSQ persegue un obiettivo comune: aumentare gli standard software (e dello sviluppo software) in tutto il mondo attraverso la promozione del Code Inspection, come prerequisito del Software Testing nel ciclo di produzione e rilascio del software.

URL	http://ifsq.org
Country of HQ location Geographic Scope	The Netherlands International
Type	Industry (non profit)

ifSQ ha analizzato, quantificato e migliorato lo stato dell'arte della ricerca sulla qualità del software, e ha definito un set di indicatori (Defect Indicators) che sono stati raccolti in un insieme coordinato di tre standard, pubblicati sul sito, in forma di opuscolo e sotto forma di corsi e workshop. La maggior parte dei criteri di valutazione, in particolare "major string", "parametri non controllati" e " unexpected state not trapped", sono rilevanti per migliorare la sicurezza del software.

Risultati più rilevanti:

Resources	**Software Quality Standards -** Levels 1 (An Entry-Level Standard for Computer Program Source Code), 2 (A Foundation-Level Standard for Computer Program Source Code) and 3 (Industry Best Practice for Computer Program Source Code - *is not yet complete*) are available.

5.2 Iniziative europee

Questo paragrafo ha l'obiettivo di fornire una vista delle iniziative in ambito Europeo. Le iniziative di seguito presentate sono state classificate sulla base dell'ambito geografico e della tipologia di appartenenza (accademiche, governative, industria).

Analizzando ambiti, obiettivi e risultati di ognuna, emerge che:

- Un insieme di iniziative rappresentano per obiettivi e risultati una categoria isolata. Tra queste iniziative, definiamole 'non raggruppabili', ci sono: NESSI, OWASP Local Chapters, MISRA e Serenity Forum.
- Altre iniziative posso essere 'raggruppate' sulla base di alcuni elementi che li caratterizzano e li accomunano: Events and Periodicals, Certifications, Academic Education. Queste iniziative potrebbero essere classificate con più tag sulla base dei loro risultati rilevanti o attesi in SSE: standardisation, industry platform, vulnerability detection, vulnerability protection, information sharing, specialised workshop, certification and training.

5.2.1 Networked European Software and Services Initiative (NESSI)

NESSI è la piattaforma tecnologica europea dedicata al Software e ai Servizi. L'obiettivo principale di NESSI si indirizza sul potenziamento dei servizi Internet attraverso attività di ricerca, standard e policy, e contributi costruiti attraverso una community industria/università.

I partecipanti NESSI sono divisi in tre gruppi:

- partner NESSI: prevalentemente industriale, ma ci sono anche alcuni profili accademici - coordinano la piattaforma e forniscono il sostegno finanziario per le attività NESSI;
- I membri NESSI: industria, mondo accademico e gli utenti - rappresentano i principali stakeholders del dominio della fornitura di servizi ICT. Non è obbligatorio un contributo finanziario
- abbonati NESSI: usano diversi canali di informazione per tenersi aggiornati sulle attività di NESSI.

URL	http://www.nessi-europe.com
Country of HQ location	Belgium
Geographic Scope	Europe
Type	Industry

Piattaforme tecnologiche nazionali e regionali sono parte della rete NESSI: gestiscono obiettivi NESSI da un punto di vista locale.

I focus NESSI hanno alcune correlazioni SSE:

- Identificare le direzioni della ricerca futura sui servizi;
- costruire contributi formali sui settori chiave;
- investire sulla rete NESSI per migliorare il coordinamento tra i programmi di ricerca europei, nazionali e regionali.

Risultati più rilevanti:

Research Agenda	*NESSI Strategic Research and Innovation Agenda* (NESSI SRIA 2017) *Next Generation Software Technologies Empowering the Digital Transformation of Europe.* Recommendations on Software Technology Research for Horizon Europe.
Working Group related to SSE	*Security and Privacy: From the Perspective of Software, Services, Cloud and Data*. NESSI è la Horizon 2020 European Technology Platform (ETP) per il software, i servizi e i dati. Il presente white paper si concentra sul ruolo crescente della sicurezza e della privacy e mette in evidenza le direzioni di ricerca di una prospettiva NESSI. Software and the Next Generation Internet (2019-05-09). Per sfruttare il potenziale delle NGI sono necessarie ricerca e innovazione per affrontare le sfide poste dalle crescenti minacce derivanti da attacchi informatici, compresa la gestione dei rischi e il contenimento delle intrusioni, nonché le minacce derivanti dalle nuove tecnologie.

5.2.2 Piattaforme Nazionali NESSI

L'obiettivo generale delle Piattaforme NESSI è di promuovere lo sviluppo e l'applicazione di tecnologie e servizi ICT per affrontare le sfide future all'interno dell'industria europea e del governo.

Nella tabella che segue vengono sintetizzate le attività di ciascuna piattaforma nazionale il cui scopo è di gestire gli obiettivi NESSI da un punto di vista locale e di pubblicare le proprie SRA nazionali.

URL	**http://www.nessi-europe.com**
NESSI - Norway	E' la filiale norvegese del NESSI. Il suo obiettivo principale è quello di creare un'arena norvegese per gli stakeholders del settore industria, ricerca/mondo accademico e pubblico e di influenzare la strategia di ricerca ICT del governo norvegese.

URL	**http://www.nessi-europe.com**
NESSI - Slovenia	Alla base di queste attività è che NESSI assumerà la responsabilità del contenuto e dell'attuazione del 7° programma quadro dell'UE per R&D. Essi invitano chiunque sia coinvolto in attività di R&D a partecipare a questo lavoro.

URL	http://www-it.fmi.uni-sofia.bg/nessibg/
NESSI-Bulgaria	NESSI-Bulgaria è stata fondata nel 2005. Si tratta di un forum per lo scambio di conoscenze, lo sviluppo di strategie e la ricerca di nuove potenzialità a livello internazionale IT e servizi industriali. La visione centrale della piattaforma è di consentire nuovi modelli di business orientate ai servizi. I loro obiettivi sono: • Definire una Roadmap bulgara e l'SRA per l'evoluzione del programma di innovazione R&D bulgaro. • Supporto alle attività R&D nei settori del software e dei servizi. •Fornire formazione: nuovi corsi, programmi MSc, programmi PhD e formazione

URL	http://nessi.ik.bme.hu/
NESSI- Hungary	NESSI-Ungheria è stata fondata nel 2007 con lo scopo di evolvere la direzione della ricerca e dello sviluppo strategico nel settore del software e dei servizi, sulla base di un approccio unificato. Gruppi di lavoro di questa piattaforma sono divisi in due sottogruppi: domain-oriented e technological-oriented. La piattaforma è aperta a qualsiasi altra organizzazione ungherese.

URL	http://www.bicc-net.de/
Germany Bicc-Net	BICC-NET, Piattaforma di NESSI tedesca, è il Polo ICT bavarese della Germania. Fondata nel 2007, intende stimolare selettivamente l'innovazione. BICC-NET comprende quanto segue: • sviluppo e distribuzione del software • lo sviluppo e la distribuzione di hardware • telecomunicazioni • sistemi software e hardware embedded nei prodotti • processi basati su software in fase di sviluppo, la produzione, i servizi e della pubblica amministrazione • Servizi nelle aree di cui sopra. BICC-NET viene utilizzato per garantire la crescita ICT in Baviera. Essa è guidata dalla BICC sede ufficiale "cluster", che è stato direttamente commissionato dal Ministero bavarese per gli Affari economici, infrastrutture, trasporti e tecnologia. BICC-NET supporterà i profili di innovazione delle aziende ICT bavaresi e gli sviluppi in corso.

URL	https://www.fi-stockholm.eu/
NESSI- Sweden	NESSI svedese è stata fondata nel 2010. L'obiettivo generale di NESSI Svezia è di promuovere lo sviluppo e l'applicazione di tecnologie e servizi ICT per affrontare le sfide future all'interno dell'industria svedese e del governo

URL	http://www.nessi-europe.com/
NESSI- Romania	NESSI Romania è stata fondata nel 2010. Gli obiettivi a breve termine di NESSI-Romania sono: • istituire gruppi di lavoro nazionali su diversi argomenti definiti in NESSI SRA • Definire un SRA nazionale per l'evoluzione futura del programma nazionale R&D e innovazione relativamente a software e servizi • Diffondere i risultati NESSI dei progetti strategici e compatibili

5.2.3 OWASP Local Chapters

Questa sezione fornisce una vista dei gruppi di lavoro OWASP distribuiti sul territorio Europeo.

URL	https://www.owasp.org/index.php/Belgium
OWASP Belgium Local Chapter	Le principali attività svolte riguardano l'organizzazione di incontri su come difendere le applicazioni web da attacchi.

URL	https://www.owasp.org/index.php/Aarhus
OWASP Denmark Local Chapter	Le principali attività svolte riguardano l'organizzazione di incontri su diversi argomenti di sicurezza delle informazioni legate alle applicazioni web. Le presentazioni sono disponibili sul sito web

URL	https://www.owasp.org/index.php/France
OWASP France Local Chapter	Le principali attività svolte riguardano l'organizzazione di incontri e la traduzione della documentazione OWASP in francese. Questo Chapter fornisce anche la formazione su progetti e risorse OWASP attraverso il programma "OWASP projects and resources you can use today", che ha lo scopo di promuovere progetti OWASP, fornendo una selezione di progetti maturi ed enterprise-ready, insieme con esempi pratici di come usarli.

URL	https://www.owasp.org/index.php/Germany
OWASP Germany Local Chapter	Le principali attività riguardano l'organizzazione di incontri, conosciuti come AppSec Germany Conference, che si svolge ogni anno.

URL	https://www.owasp.org/index.php/Geneva
OWASP Geneva Local Chapter	Le principali attività svolte da questo capitolo riguardano l'organizzazione di incontri legati alle identità digitali e autenticazione nelle applicazioni web.

URL	https://www.owasp.org/index.php/Greece
OWASP Greece Local Chapter	Il gruppo di lavoro OWASP greco è stata fondato nel 2005 con l'obiettivo di informare la comunità greca sui rischi per la sicurezza nelle applicazioni web. Il motivo principale che ha spinto alla sua creazione è il sempre crescente numero di incidenti di sicurezza su Internet, come ad esempio i tentativi di phishing a banche greche. Oggi, il gruppo greco promuove localmente

	l'iniziativa OWASP attraverso il Software Libero/Open e la traduzione in greco della documentazione OWASP. Emettono una newsletter mensile, mantengono una mailing list per gli aggiornamenti e gestiscono dibattiti online su problemi di sicurezza di attualità. La comunità greca OWASP vuole riunire tutti coloro che sono interessati e preoccupati per la sicurezza delle applicazioni web. Allo stesso tempo, accoglie i volontari che sono disposti a lavorare su progetti coordinati dall'OWASP, utilizzando software libero/open source. Invitano a chiunque di condividere le proprie idee, pensieri e riflessioni sugli attacchi, la difesa, i metodi di risposta, strumenti e buone pratiche in materia di sicurezza di Internet.

URL	**https://www.owasp.org/index.php/Category:Ireland**
OWASP Ireland Local Chapter	Questo paese ha quattro gruppi locali: Belfast, Cork, Dublino e Limerick. Il gruppo più attivo è quello di Dublino le cui attività principali riguardano l'organizzazione di eventi e conferenze. Questo gruppo fornisce anche la formazione su progetti e risorse OWASP attraverso il programma " OWASP projects and resources you can use today". Questo ha lo scopo di promuovere i progetti OWASP, fornendo una selezione di progetti maturi ed enterprise-ready con esempi pratici di come usarli.

URL	**https://www.owasp.org/index.php/Italy**
OWASP Italy Local Chapter	Le attività riguardano l'organizzazione di eventi e lo sviluppo di tool. Il gruppo cerca di organizzare almeno 2 conferenze l'anno, uno in primavera e un altro in autunno. Recentemente, hanno lavorato sullo sviluppo di sqlmap, un *automatic SQL injection tool* sviluppato in Python. L'iniziativa è sostenuta da partner come IsecLab, CLUSIT e ISACA Roma.

URL	**https://www.owasp.org/index.php/Latvia%20**
OWASP Latvia Local Chapter	E' stata creata nell'ottobre 2007. Le attività principali riguardano l'organizzazione di eventi. Il gruppo non si è dimostrato molto attivo negli ultimi anni.

URL	**https://www.owasp.org/index.php/London**
OWASP London Local Chapter	Le attività di OWASP Londra si concentrano sulla preparazione e l'organizzazione di eventi, conferenze e presentazioni. Il gruppo ha registrato elevata attività nel corso del 2010. Esso prevede anche la formazione su progetti e risorse OWASP attraverso il programma "OWASP projects and resources you can use today", che mira a promuovere progetti OWASP, fornendo una selezione di progetti maturi ed enterprise-ready con esempi pratici di come usarli.

URL	**https://www.owasp.org/index.php/Luxembourg**
OWASP Luxembourg Local Chapter	Le attività del gruppo riguardano la preparazione e l'organizzazione di eventi e conferenze come il Java User Group (YAJUG) o Chaos Computer Club

	Letzebuerg (C3L). Attualmente sembra che vi sia poca attività in questo gruppo.

URL	**https://www.owasp.org/index.php/Norway**
OWASP Norway Local Chapter	Le attività di OWASP Norvegia riguardano la preparazione e l'organizzazione di eventi e conferenze. Questo gruppo è stato molto attivo negli anni passati, quando ha organizzato 8 conferenze in Norvegia in un anno.

URL	**https://www.owasp.org/index.php/Poland**
OWASP Poland Local Chapter	L'attività principale che questo gruppo è di organizzare eventi. In questo gruppo sembra essere molto attivo, sono stati coinvolti in 11 conferenze nel corso del 2010. L'iniziativa è sostenuta da ISSA.

URL	**https://www.owasp.org/index.php/Porto**
OWASP Portugal Local Chapter	Le attività di questo gruppo riguardano l'organizzazione di conferenze e pubblicazioni. Ha organizzato uno dei più importanti eventi di OWASP: *Ibero-American Web Application Security Conference IBWAS'2010*.

URL	**https://www.owasp.org/index.php/Scotland**
OWASP Scotland Local Chapter	Le principali attività svolte da questo gruppo, secondo quanto riportato sul loro sito, sono finalizzate a fornire risposte insieme ad altri gruppi britannici locali ai diversi uffici governativi del Regno Unito. Questo gruppo sembra che organizzi anche incontri annuali.

URL	**https://www.owasp.org/index.php/Spain**
OWASP Spain Local Chapter	Questo gruppo svolge due attività principali. Da un lato collabora attivamente con OWASP su un progetto per fornire le specifiche e i requisiti legali per le applicazioni Web. D'altra parte, come la maggior parte degli altri gruppi locali di questa sezione, organizza eventi e conferenze annuali. Ha partecipato anche all'evento IBWAS'2010 [https://www.owasp.org/index.php/IBWAS10] in collaborazione con il gruppo portoghese.

URL	**https://www.owasp.org/index.php/Sweden**
OWASP Sweden Local Chapter	Questo gruppo si concentra sull'organizzazione di meeting ed eventi. Ha organizzato conferenze anche in collaborazione con altri gruppi del nord, come il norvegese e il finlandese.

URL	**https://www.owasp.org/index.php/Switzerland**
OWASP Switzerland Local Chapter	Questo gruppo organizza incontri su base periodica, soprattutto nella parte tedesca della Svizzera. I loro incontri e gli eventi sono principalmente su temi come test di sicurezza, lo sviluppo sicuro, hacking e architetture sicure. Sul loro sito Web sono fruibili diapositive di eventi e conferenze.

URL	https://www.owasp.org/index.php/Ukraine
OWASP Ukraine Local Chapter	E' un gruppo di recente formazione ancora in fase di organizzazione.

5.2.4 Motor Industry Software Reliability Association (MISRA)

MISRA è un *Motor Companies Consortium* all'interno del Regno Unito. I suoi risultati (ricerca, risultati della ricerca e standard de facto, linee guida) sono finalizzati principalmente allo sviluppo di software sicuro e affidabile per sistemi embedded nel settore automobilistico.

MISRA instaura quindi una collaborazione tra costruttori di veicoli, fornitori di componenti e di consulenza ingegneristica. Esso mira a promuovere le migliori pratiche nello sviluppo di sistemi elettronici legati alla sicurezza dei veicoli stradali e di altri sistemi embedded.

La sua documentazione non è accessibile al pubblico, ma può essere acquistata sul sito web del consorzio.

URL	https://www.misra.org.uk
Country of HQ location **Geographic Scope**	UK National
Type	Industry

I lavori in corso MISRA includono:

Model based development and autocode – Incoraggia alle buone pratiche.

- MISRA Autocode (Produzione di best practice di modellazione)
- MISRA C++ (Produzione di una serie di linee guida per l'uso di C ++ in sistemi critici)
- MISRA C3 (3rd review of MISRA C)
- Mira a promuovere le migliori pratiche nello sviluppo di sistemi elettronici legati alla sicurezza nei veicoli stradali e di altri sistemi embedded (è stato adottato e utilizzato in una vasta gamma di settori e applicazioni, tra cui il settore ferroviario, aerospaziale, militare e medico)

MISRA Safety Analysis – Linee Guida che descrivono come il ciclo di vita della sicurezza dei sistemi automotive si inserisce nel ciclo di vita dello sviluppo dei veicoli.

Risultati più rilevanti:

Good Practice	MISRA Compliance 2016: Achieving compliance with MISRA coding guidelines, ISBN 978-906400-13-2 (PDF), April 2016. Guidelines for the Use of the C Language in Vehicle Based Software, ISBN 978-0-9524156-6-5, April 1998, October 2002 Guidelines for the Use of the C Language in Critical Systems, ISBN 0 9524156 2 3 (paperback), ISBN 0 9524156 4 X (PDF), October 2004 Guidelines for safety analysis of vehicle based programmable systems, ISBN 978-0-9524156-5-7 (paperback), ISBN 978-0-9524156-7-1 (PDF), November 2007. Guidelines for the Use of the C++ Language in Critical Systems, ISBN 978-906400-03-3

	(paperback), ISBN 978-906400-04-0 (PDF), June 2008.
Standard	MISRA AC GMG: Generic modeling design and style guidelines, ISBN 978-906400-06-4 (PDF), May 2009. MISRA Compliance: MISRA C, MISRA C++ coding guidelines

5.2.5 European Space Agency (ESA)

Dall'inizio degli anni '90 l'ESA si è occupata di definire la qualità dei prodotti software. La famiglia PSS[11] di standard (poi sostituito da standard ECSS) include un software engineering standard e una serie di guide.

URL	**https://www.esa.int/**
Country of HQ location	Paris
Geographic Scope	European
Type	Collaboration of Several European Countries

Uno degli standard di software ampiamente utilizzato, chiamato "Guide to applying the ESA Software Engineering Standards to small software projects" è disponibile all'indirizzo: http://emits.sso.esa.int/emits-doc/e_support/Bssc962.pdf

Questo standard definisce una serie di criteri di qualità per i requisiti software e di design, che hanno una influenza diretta e indiretta sulla sicurezza del software. Nell'ambito dei *quality criteria requirements* sono rilevanti i seguenti aspetti:

- *Sono menzionate le caratteristiche degli utenti e delle funzionalità del software maggiormente utilizzate? (Non risultano mancanti categorie di utenti)*
- *Sono esplicitamente menzionate tutte le interfacce esterne del software? (Non risultano mancanti interfacce)*
- *E' stata definita una priorità per ciascun requisito? (Il significato dei livelli di priorità è chiaro?)*
- *Ciascun requisito è verificabile (in un test di accettazione provvisoria)? (Misurabile: dove possibile, quantificare; capacità, prestazione e accuratezza).*
- *I requisiti sono consistenti? (Non sono in conflitto)*
- *I requisiti sono sufficientemente accurati e inequivocabili? (Quali interfacce sono coinvolte, chi ha l'iniziativa, chi fornisce quali dati, nessuna voce passiva).*
- *I requisiti sono completi? Tutto ciò che non è esplicitamente vincolato può essere considerato dal punto di vista dello sviluppo libero? Un prodotto che soddisfa tutti i requisiti è davvero accettabile? (Nessun requisito mancante)*
- *I requisiti sono comprensibili per coloro che li dovranno successivamente utilizzare?*
- *I requisiti sono realizzabili all'interno del budget?*
- *La maggior parte dei criteri di qualità di progettazione sono rilevanti per la sicurezza del software.*

[11] http://www.esa.int/TEC/Software_engineering_and_standardisation/TECBUCUXBQE_2.html

Risultati principali:

Good Practice	The PSS [https://www.esa.int/TEC/Software_engineering_and_standardisation/TECBUCUXBQE_2.html] famiglia di standard per la qualità del software. Una guida per l'applicazione degli standard ESA di ingegneria del software ai piccoli progetti è disponibile all'indirizzo: ftp://ftp.estec.esa.nl/pub/wm/wme/bssc/Bssc962.pdf L'Università di Tecnologia di Eindhoven fornisce ulteriori requisiti semplificati e checklists di progettazione. [https://www.win.tue.nl/is/doku.php]

5.3 Iniziative US

In questa sezione viene fornita una panoramica delle iniziative SSE negli Stati Uniti. Tali iniziative sono state classificate in funzione della tipologia: accademiche o governative.

5.3.1 CERT Secure Coding

Il CERT Secure Coding è un'iniziativa di sicurezza del programma Computer Emergency Response Team (CERT). Questo programma fa parte del Software Engineering Institute (SEI) alla Canergie Mellon University[12] (Pennsylvania, USA). Alcuni dei suoi programmi sono finanziati dal governo degli Stati Uniti.

Nel novembre 1988, la Defense Advanced Research Projects Agency (DARPA) incaricò il SEI di creare un centro per coordinare la comunicazione tra gli esperti di sicurezza durante le emergenze e per aiutare a prevenire futuri incidenti, a fronte di ciò, il CERT ha sviluppato il Software Initiative Assurance, che comprende: Secure Coding Standards, Source Code Analysis Lab (SCALe), Vulnerability analysis, Function extraction for malicious code.

Il SEI è un centro di ricerca e sviluppo finanziato dal governo federale, che conduce ricerche di ingegneria del software in acquisizione, architetture e linee di prodotto, miglioramento dei processi e misurazione delle performance, sicurezza e l'interoperabilità del sistema e l'affidabilità.

Il SEI lavora a stretto contatto con le organizzazioni di difesa e di governo, soprattutto l'Ufficio Secretary of Defense/Acquisition, Technology, and Logistics (OSD/AT&L)[13], l'industria e il mondo accademico, con l'obiettivo di migliorare continuamente i sistemi software-intensive.

URL	https://www.sei.cmu.edu
Country of HQ location **Geographic Scope**	US National
Type	Academic

Le aree di lavoro CERT Secure Coding sono:

- **Secure coding standards**

[12] https://www.cmu.edu/

[13] http://www.acq.osd.mil/

[https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards] - Propone standard per migliorare la sicurezza nell'uso dei linguaggi di programmazione (Android, C, C++, Java, Perl).

- **International Standards Development**/- Standard di sviluppo Internazionale.
- **Source Code Analysis Laboratory (SCALe)** [cert.org/secure-coding/products-services/scale.cfm] SCALe consente di valutare il codice sorgente rispetto a una serie di standard di codifica sicura. SCALe rilascia e certifica i test di conformità quando le risultanze dei test sono state indirizzate dagli sviluppatori.
- **Secure Coding Tools** - Tali strumenti sono utilizzati nell'auditing SCALe, ma possono anche essere di supporto agli sviluppatori di software per ridurre il numero di vulnerabilità presenti nel loro codice.

CERT Secure Coding vuole influenzare i fornitori per migliorare la sicurezza base all'interno dei loro prodotti. Al fine di raggiungere questo obiettivo, CERT Secure Coding lavora con sviluppatori di software e organizzazioni di sviluppo software per ridurre le vulnerabilità derivanti da errori di codifica (C, C ++ o linguaggi di programmazione Java) prima di essere distribuiti. Inoltre, gli analisti CERT valutano le cause della vulnerabilità e identificano le pratiche di secure coding.

CERT collabora con ISO per la creazione di diversi standard su secure coding.

Risultati più rilevanti:

Training	**Secure Coding in C and C++** [http://www.sei.cmu.edu/training/p63.cfm] Course of secure coding in C and C++ based on Addison-Wesley's material: "Secure Coding in C and C++" and "The CERT C Secure Coding Standard"
Standards for Software Developers	**SEI CERT C Coding Standard** [https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard] **SEI CERT C++ Coding Standard** [https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88046682] **SEI CERT Oracle Coding Standard for Java** [https://wiki.sei.cmu.edu/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java] **SEI CERT Perl Coding Standard** [https://wiki.sei.cmu.edu/confluence/display/perl/SEI+CERT+Perl+Coding+Standard] **Android TM Secure Coding Standard** [https://wiki.sei.cmu.edu/confluence/display/android/Android+Secure+Coding+Standard]

5.3.2 Software Assurance Metrics and Tool Evaluation (SAMATE)

SAMATE è un'iniziativa US Government software assurance, un progetto inter-agenzie tra gli Stati Uniti e il DHS National Institute of Standards and Technology (NIST).

Obiettivo di SAMATE è migliorare la garanzia software:

- sviluppando metriche e metodologie per valutare i tool di sicurezza del software;
- identificando le vulnerabilità relative alla pratiche di codifica e dei metodi di ingegneria del software.

Il progetto di riferimento di SAMATE sviluppa casi di test al fine di esaminare il codice sorgente di strumenti e applicazioni. Rileva e segnala le debolezze in modo da fornire, agli utenti finali e sviluppatori, tool di garanzia del software con una serie di flaws noti attraverso i quali valutare i propri tool.

L'uscita principale di questa iniziativa è il SAMATE Reference Dataset (SRD), un database online alimentato regolarmente da SAMATE. Questa banca dati online, a disposizione del pubblico, fornisce casi di test per gli sviluppatori e utenti finali, attraverso i quali è possibile effettuare valutazioni di tool di sicurezza.

URL	**https://samate.nist.gov/**
Country of HQ location **Geographic Scope**	US National
Type	Governement

SAMATE è finalizzato al miglioramento del software assurance attraverso lo sviluppo di metodologie che consentano la valutazione software dei tool, misurare l'efficacia dei tool e delle tecniche, individuare le lacune negli strumenti e nei metodi. Il progetto sostiene Tools Software Assurance della US DHS e R&D Requirements Identification Program (in particolare, la Parte 3, tecnologia -strumenti e requisiti-), che affronta l'individuazione, la valorizzazione e lo sviluppo di software assurance tools.

Il progetto SAMATE compone di due parti:

- sviluppo di metriche per l'efficacia dei software security assessment (SSA) tools
- valutazione di metodi e strumenti SSA attuali al fine di individuare le carenze che possono portare a guasti dei prodotti software e vulnerabilità

Infine, SAMATE sta sviluppando anche alcune specifiche rivolte agli sviluppatori di strumenti di garanzia del software, che gli consentano di classificare e valutare questa tipologia di tool.

Risultati più significativi:

Specifications	Source Code Security Analysis [https://samate.nist.gov/index.php/Source_Code_Security_Analysis.html] "Source Code Security Analysis Tool Functional Specification Version 1.1" Specifiche e piani di test per gli strumenti di analisi della sicurezza del codice sorgente. Questo tipo di strumento esamina il codice sorgente al fine di rilevare e segnalare le difettosità che possono portare a vulnerabilità di sicurezza.
	Web Application Scanner [https://samate.nist.gov/index.php/Web_Application_Scanner.html] "Web Application Scanner Functional Specification Version 1.0". Queste specifiche sono raccolte nella pubblicazione NIST Special Publication 500-269 [https://samate.nist.gov/docs/webapp_scanner_spec_sp500-269.pdf].
Test Cases	SAMATE reference datasheet [https://samate.nist.gov/SRD/] Fornisce a utenti, ricercatori e sviluppatori di strumenti di garanzia della sicurezza del software una serie di difetti di sicurezza noti. Questi consentiranno agli utenti finali di valutare tali strumenti e agli sviluppatori degli

	strumenti di testare le loro metodologie applicate.
	SRD database [https://samate.nist.gov/SRD/view.php] Una raccolta di casi di test per individuare le debolezze del codice.

5.3.3 Common Weakness Enumeration (CWE)

CWE è un'iniziativa sostenuta e co-sponsorizzata dalla NCSD della US DHS e dal NIST. Attualmente è mantenuta e guidata da MITRE Corporation.

Il CWE è una lista formale o tassonomia, che classifica le tipologie più comuni di vulnerabilità del software. Gli obiettivi principali di CWE sono:

- Gestire la *common taxonomy* per la classificazione delle vulnerabilità comuni del software relativamente ad architettura, progettazione e codice;
- Fornire una classificazione standard per tool di protezione del software
- Fornire una linea di base da cui partire per aiutare la community SSE a identificare, attenuare e prevenire questo tipo di debolezza software.

URL	**https://cwe.mitre.org** **https://nvd.nist.gov/cwe.cfm**
Country of HQ location **Geographic Scope**	US National
Type	Government

Questo progetto utilizza i risultati del progetto SAMATE per creare l'elenco CWE delle vulnerabilità e la sua tassonomia associata e l'albero di classificazione (vedi figura sotto tratta dal NIST).

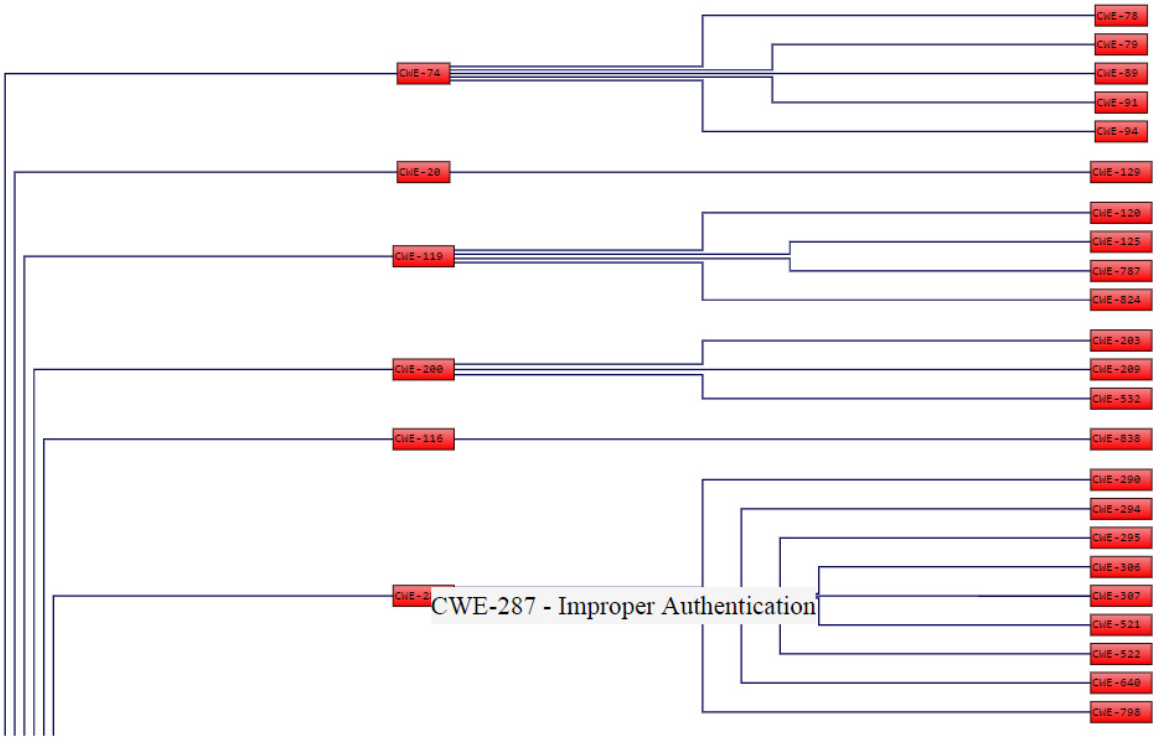

Figura 6 - Una porzione dell'albero di classificazione CWE

*[Fonte: **https://nvd.nist.gov/vuln/categories/cwe-layout**]*

La Figura 6 mostra la classificazione gerarchica delle CWE, come proposto nella pagina del National Vulnerability Database[14] (NVD) della NIST. Il grafico presenta le varie CWE raggruppate in categorie. Ogni CWE può essere in relazione con una CWE di livello superiore (più generica).

Va inoltre sottolineato che CWE è una community-developed, l'elenco formale delle vulnerabilità comuni del software coinvolgono il mondo accademico, il settore commerciale e il governo degli Stati Uniti.

Risultati più rilevanti:

- **CWE List** (Version 3.4): https://cwe.mitre.org/data/index.html

  Le definizioni e le descrizioni di CWE supportano la scoperta delle tipologie di flaw di sicurezza software nel codice, prima di rilasciarlo. Ciò significa che sia gli utilizzatori che gli sviluppatori dei tool e dei servizi di sicurezza software possono utilizzare CWE come un meccanismo per descrivere i flaw di sicurezza del software.

  L'elenco CWE è disponibile in tre diversi formati:

  - Research Concepts [https://cwe.mitre.org/data/definitions/1000.html];
  - Development Concepts [https://cwe.mitre.org/data/definitions/699.html];
  - Architectural Concepts [https://cwe.mitre.org/data/definitions/1008.html].

- **CWE Top 25 Most Dangerous Software Errors.** Di seguito è riportato un l'elenco pubblicato nel 2019:

[14] https://nvd.nist.gov/vuln/categories

Rank	ID	Name	Score
[1]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	75.56
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.69
[3]	CWE-20	Improper Input Validation	43.61
[4]	CWE-200	Information Exposure	32.12
[5]	CWE-125	Out-of-bounds Read	26.53
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24.54
[7]	CWE-416	Use After Free	17.94
[8]	CWE-190	Integer Overflow or Wraparound	17.35
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	15.54
[10]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.10
[11]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11.47
[12]	CWE-787	Out-of-bounds Write	11.08
[13]	CWE-287	Improper Authentication	10.78
[14]	CWE-476	NULL Pointer Dereference	9.74
[15]	CWE-732	Incorrect Permission Assignment for Critical Resource	6.33
[16]	CWE-434	Unrestricted Upload of File with Dangerous Type	5.50
[17]	CWE-611	Improper Restriction of XML External Entity Reference	5.48
[18]	CWE-94	Improper Control of Generation of Code ('Code Injection')	5.36
[19]	CWE-798	Use of Hard-coded Credentials	5.12
[20]	CWE-400	Uncontrolled Resource Consumption	5.04
[21]	CWE-772	Missing Release of Resource after Effective Lifetime	5.04
[22]	CWE-426	Untrusted Search Path	4.40
[23]	CWE-502	Deserialization of Untrusted Data	4.30
[24]	CWE-269	Improper Privilege Management	4.23
[25]	CWE-295	Improper Certificate Validation	4.06

Figura 7- CWE Top 25 [Fonte: https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html]

5.3.4 Common Attack Pattern Enumeration and Classification (CAPEC)

CAPEC è un'iniziativa co-sponsorizzata dal NCSD dell'US DHS e guidata dalla Cigital[15]. Costruttori di software sicuro devono proteggersi da importanti vulnerabilità potenziali. Per identificare e mitigare le vulnerabilità relative al software, la community di sviluppo ha bisogno di capire la prospettiva dell'attaccante e gli approcci utilizzati per sfruttare il software.

Gli schemi di attacco sono le descrizioni di metodi comuni per lo sfruttamento del software, fornendo sia la prospettiva che la guida dell'attaccante sui modi per mitigare il loro effetto. Essi derivano dal concetto di pattern design applicato in un distruttivo, piuttosto che costruttivo, contesto e sono generati da un'analisi approfondita di specifici esempi di casi del mondo reale.

Questa iniziativa mira a fornire un catalogo a disposizione del pubblico di schemi di attacco, insieme ad uno schema di classificazione e tassonomia completo. La filosofia è di evolvere il catalogo con la partecipazione e i contributi pubblici e così consolidare un meccanismo standard per l'identificazione, la raccolta, la raffinazione, e la condivisione di modelli di attacco nella community software.

URL	**https://capec.mitre.org**
Country of HQ location **Geographic Scope**	US National
Type	Government

[15] https://www.synopsys.com/software-integrity.html

Secondo questa iniziativa, le informazioni sugli schemi di attacco, se catturati in modo formale, possono portare un notevole valore per considerazioni di sicurezza del software attraverso tutte le fasi del SDLC e le altre attività relative alla sicurezza, tra cui:

- Raccolta dei requisiti: Identificazione dei requisiti di sicurezza pertinenti, dei misuse e abuse cases.
- Architettura e design: Fornisce il contesto per l'analisi dei rischi architetturali e le linee guida per la sicurezza nelle architetture del software.
- Implementazione e codifica: Prioritizzazione e guida delle attività di revisione sicura del codice.
- Test del software e controllo qualità: Fornisce il contesto per una appropriata analisi del rischio e test di penetrazione.
- Operatività dei sistemi: Sfruttare le esperienze apprese dagli incidenti di sicurezza per fornire una guida preventiva.
- Politiche e generazione di standard: Guida all'identificazione di adeguate politiche e standard organizzativi prescrittivi.

Risultati più rilevanti:

- **List of Attack Patterns** [http://capec.mitre.org/]. L'elenco è disponibile in due diversi formati:
  - View by Mechanisms of Attack [http://capec.mitre.org/data/definitions/1000.html].
  - View by Domains of Attack [http://capec.mitre.org/data/definitions/3000.html].