[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