# 6 LA SICUREZZA IN TUTTE LE FASI DEL CICLO DI SVILUPPO DEL SOFTWARE

## 6.1 Secure SDLC

Generalmente gli aspetti di sicurezza sono sottovalutati fin dalle prime fasi del ciclo di vita dello sviluppo software e di conseguenza sono molte le vulnerabilità che vengono introdotte e trasmesse negli stadi successivi. È stato stimato, ad esempio, che un errore introdotto nella fase di specifica dei requisiti, può costare fino a 200 volte, se lo si corregge nelle successive fasi di sviluppo, rispetto a quanto sarebbe costata la sua immediata rimozione. L'attuazione corretta e completa delle **attività di sicurezza** nelle prime fasi consente di incrementare sensibilmente il livello di sicurezza di ogni singola fase successiva con un beneficio di ritorno importante:

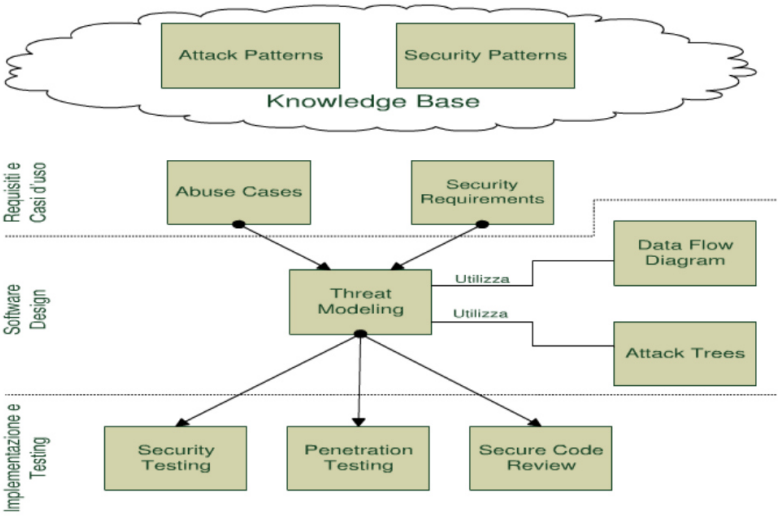


*Figura 8 - Secure development activities*

Un **Secure Software Development Life Cycle (SSDLC)** considera e implementa opportune attività di sicurezza nel corso di tutte le fasi del processo SDLC, come illustrato nella figura che segue:

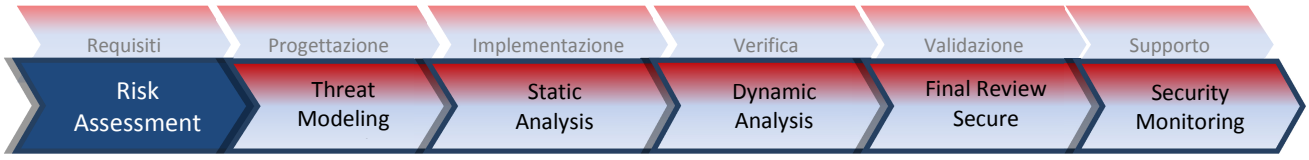


*Figura 9 - Modello fasi SSDLC*

**Requisiti**: in questa fase vengono effettuate, tramite rappresentazione UML, le analisi dei requisiti di sicurezza, dei rischi, delle probabilità di impatto delle minacce, dei casi di abuso. E' importante sottolineare che in questa fase si devono adottare le best practices di carattere generale nella definizione dei requisiti di sicurezza.

**Progettazione**: in questa fase si esamina il sistema in divenire con l'ausilio di tecniche di analisi e modellazione delle minacce. Requisiti di sicurezza di maggior dettaglio si aggiungono quindi a quelli prodotti nella precedente fase.

**Implementazione**: in questa fase si realizza il sistema attraverso la stesura di codice sicuro. Seguono l'esecuzione di test di sicurezza basati sull'analisi delle minacce e l'analisi statica del codice sorgente. Quest'ultima può produrre nuovi requisiti di sicurezza, che possono portare alla revisione del codice.

**Verifica**: in questa fase si analizzano gli aspetti di sicurezza del sistema in esecuzione in un ambiente controllato impiegando tecniche e strumenti di analisi dinamica;

**Validazione**: è la fase immediatamente prima del rilascio, nella quale viene effettuata una final security review per la verifica del rispetto dei requisiti.

**Supporto**: in questa fase si esamina il sistema in essere con l'ausilio di tecniche di: analisi e modellazione delle minacce e/o verifica statica/dinamica del codice applicativo, al fine di produrre nuovi requisiti di sicurezza di dettaglio per indirizzare un'eventuale fase di reingegnerizzazione e/o di patching del sistema in oggetto.

## 6.2 Risk Assessment

L'obiettivo dell'analisi del rischio è da una parte identificare, valutare e misurare la probabilità e la gravità dei rischi (ciò che viene generalmente indicato con il nome di *Risk Assessment*) nei diversi processi dell'organizzazione e, dall'altra decidere come comportarsi a fronte dei rischi identificati (ciò che viene generalmente indicato con il nome di *Risk Management*) al fine di minimizzarli o eliminarli.

Si fornisce di seguito, una classificazione dei principali rischi:

- Rischio strategico, derivante dall'incompatibilità tra due o più dei seguenti fattori:
  - obiettivi strategici,
  - strategie di business,
  - mezzi utilizzati per raggiungere gli obiettivi,
  - quadro macroeconomico nel quale opera l'organizzazione.
- Rischio reputazionale, che può manifestarsi in molteplici situazioni, per esempio in caso di mancato soddisfacimento della clientela.
- Rischio finanziario, derivante dall'incapacità di assolvere gli oneri finanziari assunti.
- Rischio operativo, che è connesso ai processi utilizzati per definire le strategie.
- Rischi di compliance, derivanti da inadempienze legislative (normative e regolamenti).
- Rischi di gestione delle informazioni, derivanti da un insufficiente livello di sicurezza dei sistemi informatici.
- Rischi emergenti e/o potenziali che potrebbero danneggiare il business dell'organizzazione e/o le persone che vi operano.

La gestione del rischio comprende tre attività principali:

- Risk Assessment che include l'identificazione e la valutazione dei rischi e degli impatti; le raccomandazioni e le misure per la riduzione del rischio;
- Mitigazione del rischio, che si riferisce alla prioritizzazione, implementazione e mantenimento delle misure appropriate per la riduzione del rischio raccomandate dal processo di Risk Assessment;
- Valutazione e analisi dei processi e delle misure per l'implementazione di un programma di gestione del rischio di successo (vedi paragrafo 6.2.1).

**Una metodologia di gestione del rischio ben strutturata, se utilizzata in modo efficace, può aiutare l'organizzazione a identificare i controlli adeguati per garantire le capacità di sicurezza essenziali.**

**Ridurre al minimo l'impatto dei rischi sull'organizzazione e fornire solide basi nel processo decisionale sono i motivi fondamentali per cui le organizzazioni sono chiamate a implementare un processo di gestione dei rischi per i loro sistemi IT.**

Il Risk Assessment è uno strumento di analisi, semplice e accurato, che studia i rischi dell'organizzazione (operativi, strategici, finanziari ed esterni) al fine d'individuare successivamente le soluzioni e le misure più adeguate. I passi fondamentali del Risk Assessment possono riassumersi come segue:

- Identificazione dei rischi. Devono essere individuati i fattori di pericolo per l'organizzazione, evidenziando chi o cosa può essere danneggiato e in quale modo. Per ogni fattore di pericolo identificato, bisogna definire ciò che è esposto maggiormente al pericolo.
- Valutazione dei rischi e definizione delle le azioni di mitigazione. E' necessario valutare le azioni e le tecniche per ridurre il pericolo e portarlo a livelli accettabili.
- Annotazione dei risultati e attuazione del piano di mitigazione del rischio. La valutazione precedentemente effettuata va trasformata in un piano operativo, per ottenere una gestione consapevole dei rischi dell'organizzazione.
- Revisione periodica della valutazione e aggiornamenti. E' necessario rivedere periodicamente ciò che si sta facendo. Viene identificato il profilo di rischio e viene proposto un modello di gestione integrato dei pericoli, che evidenzia i singoli fattori di rischio. In seguito vengono valutate le varie misure preventive, agevolando la protezione del valore dell'ente.

Si riporta di seguito uno schema per il *Risk Assessment*:

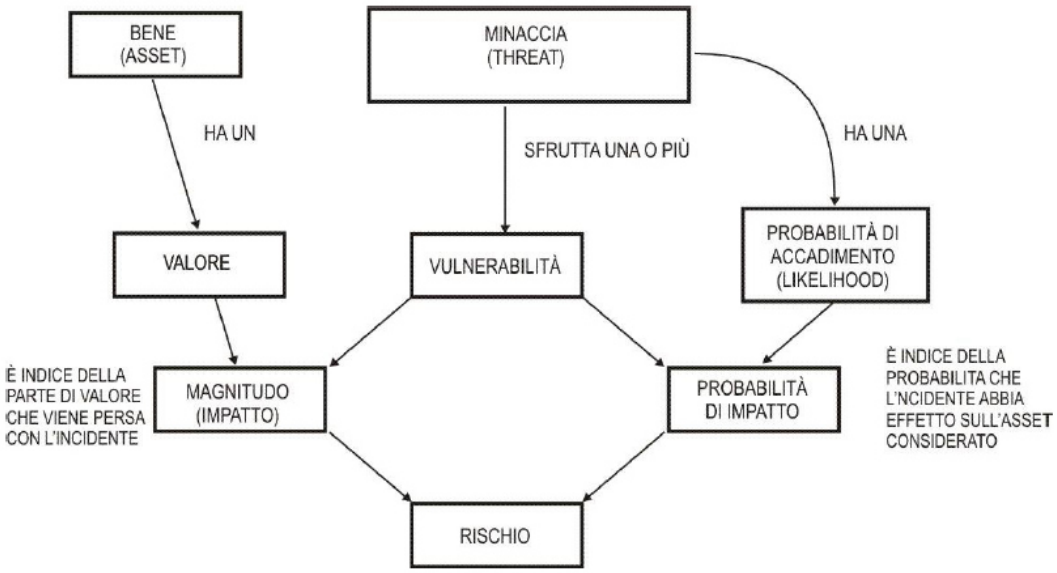


*Figura 10 - Esempio di Schema di Risk Assessment*

La gestione dei rischi per essere effettivamente efficace, deve essere totalmente integrata nell'SDLC:

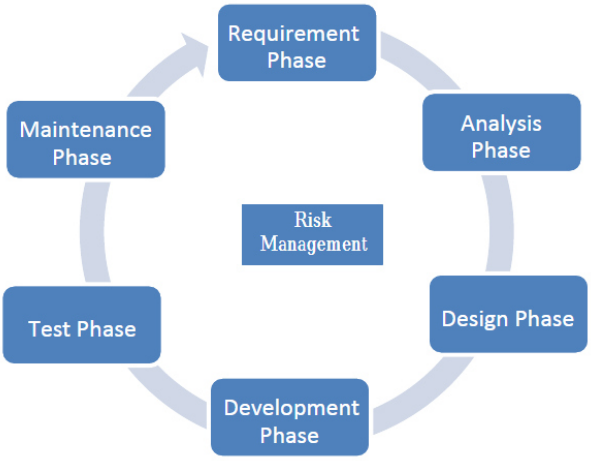


*Figura 11 - Gestione del rischio nel ciclo di vita del Software*

- Avvio del progetto/Requisiti. La valutazione preliminare del rischio è volta a definire l'ambiente di minaccia in cui opererà il prodotto o il sistema. Questa valutazione è seguita da una prima identificazione dei controlli di sicurezza richiesti che devono essere soddisfatti per proteggere il sistema nell'ambiente operativo previsto.
- Disegno. I requisiti di sicurezza del sistema vengono identificati attraverso un processo formale di Risk Assessment. L'analisi parte dalla valutazione del rischio effettuata nella fase precedente di avvio/inizializzazione e viene approfondita per il contesto specifico. Durante questa fase vengono rivisti attentamente i requisiti e le aspettative di sicurezza e privacy al fine di identificare problemi di sicurezza e rischi per la privacy. In questo passaggio vengono identificate le vulnerabilità presenti nell'ambiente software o derivanti dall'interazione con altri sistemi (Security Assessment). Una volta identificati i rischi, devono essere valutati in merito alla loro potenziale gravità dell'impatto e alla probabilità che si verifichino (Risk Assessment). Nel processo di valutazione è necessario definire le priorità per l'attuazione del piano di gestione dei rischi. La mitigazione del rischio (Risk Mitigation) è il piano delle azioni volte a ridurre o eliminare le priorità più alte. Lo scopo è di valutare la progettazione del sistema, i requisiti dichiarati e i requisiti minimi di sicurezza derivanti dal processo di categorizzazione della sicurezza al fine di determinarne l'efficacia delle azioni di mitigazione per i rischi previsti. I risultati dovrebbero mostrare come i controlli di sicurezza specifici forniscono la protezione appropriata o evidenziare le aree in cui è necessaria un'ulteriore pianificazione. La valutazione del rischio deve essere eseguita prima dell'approvazione delle specifiche progettuali (design specifications) poiché potrebbe fornire specifiche aggiuntive o ulteriori elementi da valutare per le specifiche identificate (ad esempio si dovrebbe considerare come il sistema potrebbe influenzare altri sistemi a cui sarà direttamente o indirettamente collegato; ciò implica che ci potrebbero essere controlli comuni che devono essere ereditati dall'applicazione in oggetto o ulteriori rischi che devono necessariamente essere mitigati).
- Implementazione. In questa fase è necessario determinare i rischi residui accettabili (le specifiche possono imporre oneri e costi eccessivi se i rischi residui accettabili non sono conosciuti). L'obiettivo del processo di valutazione della sicurezza è verificare che il sistema sia conforme ai requisiti funzionali e di sicurezza e operi all'interno di un livello accettabile di rischio residuo per la sicurezza.
- Monitoraggio continuo. L'obiettivo finale del monitoraggio continuo è determinare se i controlli di sicurezza continuano a essere efficaci nel tempo alla luce degli inevitabili cambiamenti che si potrebbero verificare nel sistema e nell'ambiente in cui opera. La valutazione del potenziale

impatto di tali modifiche sulla sicurezza del sistema è un'attività essenziale per assicurare un monitoraggio continuo e prevenire l'abbassamento del livello di sicurezza del sistema.

### 6.2.1 Tool per l'analisi del rischio

#### *6.2.1.1 AGID Cyber Risk Management*

Cyber Risk Management[16] di AgID è lo strumento nazionale per la valutazione e il trattamento del rischio cyber. Per la protezione dei dati in formato digitale, a garanzia della loro riservatezza, integrità e disponibilità, il tool AgID di Cyber Risk Management identifica le situazioni e i vari ambiti nei quali le informazioni possono venirsi a trovare, consentendo di valutare i rischi per la loro sicurezza.

Lo strumento è stato realizzato per consentire alle pubbliche amministrazioni di analizzare l'esposizione al rischio dei servizi erogati dalle amministrazioni stesse ed in caso predisporre i "Piani di Trattamento del Rischio". AgID, dal canto suo, fornisce supporto alle amministrazioni che ne hanno necessità sia in fase di analisi che nella fase d'implementazione di tali piani, pianificati e realizzati in base ai risultati forniti attraverso la fase di Risk Treatment.

La Pubblica Amministrazione ha la peculiarità di erogare servizi verso i cittadini, verso i propri dipendenti, verso le imprese e verso altre amministrazioni.

L'analisi del rischio può essere svolta sulle singole entità (cioè sulla pubblica amministrazione come entità unica) ed anche su parti di esse, ad esempio sui dipartimenti ritenuti più critici. A essere esaminati sono i servizi erogati dalla pubblica amministrazione in correlazione con i servizi trasversali, cioè quelli utilizzati dalle pubbliche amministrazioni ma forniti da terzi, siano essi appartenenti a una PA oppure no.

Il quadro normativo sul quale AgID ha costruito il processo di Risk Management si basa sulle linee guida e sui principi dettati dallo standard ISO 31000 [DR-3] e sull'Information Risk Assessment Methodology 2 (IRAM2) dell'Information Security Forum (ISF).

La metodologia adottata è di tipo "Gray Box", poiché l'analisi parte da una situazione nota solo in parte. I servizi, ad esempio, non devono necessariamente essere esaminati in dettaglio: le informazioni fornite formano una matrice di correlazione che viene analizzata con un algoritmo sviluppato ad hoc e che fornisce come risultato l'elenco delle minacce con i relativi dettagli. Parte del report può essere visto nell'immagine seguente:

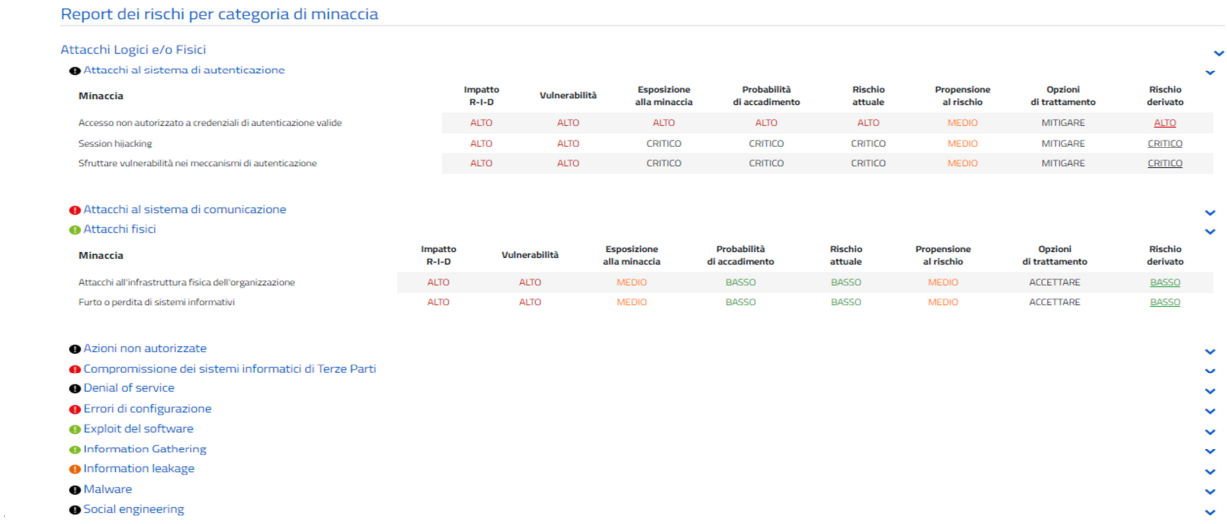


*Figura 12 - Cyber Risk Management di AgID – Report dei rischi per categoria di minaccia*

Ad esempio, per valutare l'impatto in termini di riservatezza, integrità e disponibilità delle informazioni, ci si sofferma sugli aspetti economico/finanziario, operativo, reputazionale e legale (compliance).

Le fasi che costituiscono la gestione del rischio effettuato con Cyber Risk Management di AgID sono le seguenti:

1) Analisi del contesto. Vengono identificati i servizi erogati e i servizi trasversali utilizzati in ambito pubblica amministrazione. Di ogni servizio viene descritto un profilo di criticità.
2) Valutazione di ciascun servizio erogato e da ciascun servizio trasversale in termini d'impatto su riservatezza, integrità e disponibilità delle informazioni trattate.
3) Calcolo del rischio attuale, sulla base dei valori di probabilità di accadimento e d'impatto, per ogni minaccia identificata. La fase di Risk Assessment prevede anche l'identificazione delle contromisure da implementare per un'efficace mitigazione del rischio.
4) Applicazione delle contromisure previste dal piano di trattamento del rischio, volte a mitigare, accettare o trasferire i rischi individuati.
5) Analisi del rischio residuo, cioè la valutazione del rischio che permane, nonostante l'applicazione del piano di trattamento del rischio.
6) Fase di monitoraggio dell'intero processo, con eventuale adeguamento in seguito a modifiche del contesto o in presenza di nuove minacce alla sicurezza delle informazioni.

Il tool AGID di Risk Management è gratuito ed a completa disposizione di tutte le Pubbliche Amministrazioni: www.sicurezzait.gov.it

## 6.3 Requisiti

La fase di analisi e specifica dei requisiti è fondamentale nel ciclo di vita dello sviluppo software.

Di seguito si riportano i linguaggi e gli strumenti utili alla fase di definizione dei requisiti di sicurezza del software.

### 6.3.1 Linguaggi per la specifica dei requisiti

Un linguaggio di specifica in ambito sicurezza può essere considerato:

- un linguaggio di specifica software utilizzato per indicare gli attacchi (AsmL e UML state charts),
- l'estensione di un linguaggio di specifica software utilizzato per rappresentare gli attacchi (Misuse Cases , Abuse Cases, AsmLSec e UMLintr) e i requisiti di sicurezza (UMLsec, SecureUML, Secure Tropos e Misuse Cases),
- un linguaggio per la specifica degli attacchi (*attack specification language), per esempio* STATL e Snort Rules.

**UMLsec**[17] è un'estensione di UML per lo sviluppo di sistemi sicuri e usa stereotype, tag e constraint per specificare i requisiti di sicurezza. Gli stereotype servono come etichette per gli elementi del modello UML allo scopo di introdurre informazioni al modello e specificare i vincoli che devono essere soddisfatti da questo. I tag sono associati con gli stereotype e sono utilizzati per specificare in modo esplicito una

[17] https://en.wikipedia.org/wiki/UMLsec

semplice proprietà di un elemento del modello. UMLsec definisce 21 stereotype da utilizzare per rappresentare i seguenti requisiti di sicurezza:

- fair exchange (la necessità di uno scambio leale),
- non-repudiation (un'azione non si può negare),
- role-based access control,
- secure communication link,
- confidentiality,
- integrity,
- authenticity,
- freshness of a message (ad esempio nonce),
- secure information flow among components,
- guarded access (uso di protezioni per imporre il controllo di accesso).

Sette di questi stereotype hanno dei tag associati e nove hanno vincoli. Gli stereotype possono essere utilizzati per i diagrammi dei casi d'uso, i diagrammi delle classi, diagrammi di stato, diagrammi di attività, diagrammi di sequenza, i diagrammi e le implementazioni per specificare i requisiti di sicurezza in un modello UML (per le specifiche relative sia ai requisiti, sia al design). Un insieme di **tools** sono stati rilasciati per la modellazione attraverso l'impiego di UMLsec e per la verifica dei modelli così realizzati (utilizzando il model checking).

**SecureUML**[18] SecureUML è un'altra estensione di UML che si concentra sulle politiche di controllo degli accessi ad un modello basato sui ruoli. Queste politiche possono essere considerate come requisiti di sicurezza. SecureUML propone nove stereotype che possono essere utilizzati per annotare un diagramma delle classi, con informazioni di controllo di accesso basato sui ruoli. SecureUML utilizza l'oggetto Constraint Language (OCL) per specificare i vincoli, le azioni e le autorizzazioni per le risorse. Contrariamente a UMLsec, questi vincoli possono essere specificati in base alle esigenze del singolo componente software.

**Snort Rules**[19] è un network intrusion detection system (IDS) ampiamente utilizzato. Esso utilizza scenari di attacchi specificati come regole per rilevare gli attacchi attraverso la rete. Una snort rule specifica quale azione deve essere intrapresa se la regola è associata a un pacchetto di rete, gli indirizzi IP di origine e destinazione e le porte, il protocollo della rete osservato, e la direzione del pacchetto di rete. Un certo numero di opzioni possono anche essere specificate. Queste opzioni vanno dalla registrazione di un messaggio alla ricerca di una particolare stringa nel pacchetto.

**Secure Tropos**[20] può essere utilizzato per lo sviluppo di software sicuro ed è un'estensione della metodologia di sviluppo Tropos. Secure Tropos utilizza le nozioni di *actor* (person(s), organization(s), software), *goal* (obiettivi che gli attori vogliono ottenere), *soft goal* (un obiettivo la cui realizzazione non può essere determinata in modo esplicito), *task* (un compito per raggiungere un obiettivo), *resource* (fisica o dati), *security constraint* (specificato come le dichiarazioni di alto livello), *secure goal* (utilizzato per soddisfare un vincolo di sicurezza), *secure task* (un compito per raggiungere un obiettivo di sicurezza), *secure resource* (una risorsa che è connessa a *security constraints*, *secure goal*, *secure task*, oppure a un'altra *secure resource*). Un *actor* può dipendere da un altro *actor* per raggiungere un *goal/soft goal*, per

[18] https://ieeexplore.ieee.org/document/6997358

[19] https://www.snort.org/downloads

[20] http://www.troposproject.eu/node/301

svolgere un *task*, o rilasciare una risorsa. La notazione SecureTropos può essere utilizzato per rappresentare vincoli di sicurezza (requisiti) sulle interazioni tra gli attori durante la fase di specifica dei requisiti.

**Misuse Cases**[21] è una tipologia di Use Case UML utilizzata per descrivere comportamenti indesiderati del software. Un *misuse case* è avviato da un particolare tipo di attore chiamato *mis-actor* (ad esempio, l'attore con intenti malevoli). *Misuse cases* e *mis-actors* possono essere utilizzati per suscitare più casi d'uso per neutralizzare le minacce poste dai casi di uso improprio. *Misuse cases* e *mis-actors* sono rappresentati in colore nero pieno per distinguerli dai casi d'uso e dagli attori UML. Due relazioni speciali chiamati "prevents" e " detects" mettono in relazione *use cases* e *misuse cases*. Il processo può essere utilizzato in modo graduale per sviluppare un diagramma dei casi d'uso (compresi i *misuse cases*) oppure, se necessario, può essere utilizzato anche in modo iterativo. Secondo tale processo, dovrebbero essere specificati prima gli *use cases* e poi i *misuse cases*. Dopo di che, devono essere identificate le relazioni potenziali tra gli *use cases* e i *misuse cases* perché spesso la funzionalità del software viene utilizzata per attaccarlo. Infine, i nuovi *use case* devono essere specificati per individuare o prevenire i *misuse cases*. Questi nuovi use case costituiscono i requisiti di sicurezza di alto livello del software e sono chiamati come " security use cases".

**Abuse Cases**[22] Un altro modo per specificare il comportamento indesiderato di un pezzo di software utilizzando i diagrammi UML è di sviluppare un *abuse case model*. Un *abuse case model* specifica le interazioni pericolose usando attori e *abuse case*. Non c'è differenza di notazione tra i componenti di un *UML use case diagram* e un *abuse case model*. Si raccomanda l'utilizzo di una struttura ad albero per gli approcci multipli. Questo aggiunge ulteriori dettagli al modello e permette di identificare tutte le possibili misure di sicurezza. Dettagli sugli attori come le loro risorse, le competenze, e l'obiettivo dovrebbero essere inclusi come testo. Gli *abuse case model* possono essere utilizzati nelle fasi di progettazione e collaudo.

**UMLintr**[23] è un'estensione di UML che utilizza stereotype e tag per specificare intrusioni (attacchi) utilizzando use case diagrams, class diagrams, state charts, package diagrams. Gli attacchi vengono divisi in quattro tipologie diverse. Ogni tipo è rappresentato come un pacchetto fornito di stereotype. Ci sono tre stereotype definiti per le classi e dodici per lo use case diagram. Gli stereotype per le classi hanno anche i tag.

**Abstract State Machine Language (AsmL)**[24] ASML è un linguaggio a stati finiti machine-based eseguibile utilizzato anche per specificare scenari di attacco. In generale, in ASML possono essere specificati attacchi con step multipli. Tali scenari di attacco possono essere tradotti automaticamente in *Snort rules* che possono poi essere utilizzati con un'estensione di IDS Snort; sono altresì in grado di catturare più attacchi con step multipli, utilizzando le informazioni di contesto. Le Snort rules, l'input standard di Snort, non possono rappresentare attacchi con step multipli.

**AsmLSec**[25] è un'estensione di ASML sviluppata per specificare scenari di attacco. AsmLSec utilizza stati, eventi e transizioni per rappresentare gli attacchi. Ogni transizione ha un'origine e uno stato di destinazione, una serie di condizioni da soddisfare e le azioni da compiere. Gli scenari di attacco rappresentati in AsmLSec possono essere tradotti automaticamente in ASML attraverso un compilatore appositamente sviluppato. E' stato sviluppato un IDS che prende in input gli scenari di attacco tradotti.

---

[21] https://en.wikipedia.org/wiki/Misuse_case

[22] https://en.wikipedia.org/wiki/Abuse_case

[23] https://ieeexplore.ieee.org/document/1607377

[24] https://www.microsoft.com/en-us/research/project/asml-abstract-state-machine-language/

[25] https://ieeexplore.ieee.org/document/4159874

**UML State Charts for Security**[26] i diagrammi di stato UML (senza alcuna estensione) sono stati utilizzati per specificare gli attacchi, che a loro volta possono essere collegati alle snort rules. Questi diagrammi di stato possono essere tradotti manualmente nelle snort rules, che poi potranno essere utilizzati con un'estensione di IDS Snort. Attraverso l'impiego dei diagrammi di stato, è possibile rappresentare attacchi complessi con step multipli che normalmente non possono essere rappresentati con snort rules ordinarie.

**STATL**[27] sta per "State Transition Analysis Technique Language" e utilizza due costrutti principali per specificare un attacco: stato e transizione. Ogni transizione deve avere un evento associato che, quando si verifica, avvia la transizione. All'avvio le transizioni possono eseguire azioni facoltative. Stato e transizione specifiche possono anche avere del codice eseguibile al loro interno. Un ambiente di sviluppo per STATL è inoltre disponibile e può essere utilizzato, tra le altre cose, per visualizzare scenario di attacco specificati come macchina a stati.

### 6.3.2 Tool per la specifica dei requisiti

Il CATALOGO SECURITY TOOLS 6.9 raccoglie i tool disponibili, divisi per fase del processo SSDLC, che offrono funzionalità applicabili in ambito secure application development.

Si riporta di seguito la tabella 'Software Requirements Tools':

| Prodotto | Categoria | Fase SSE | Tipo Licenza | Sito Web |
|---|---|---|---|---|
| **CaseComplete** | Requirements management | Requirements | Versione trial disponibile su richiesta | https://casecomplete.com/ |
| **IBM Engineering Requirements Management DOORS Next** | Requirements management | Requirements | Versione trial non disponibile | https://www.ibm.com |
| **IBM Rational RequisitePro solution** | Requirements management | Requirements | Versione trial non disponibile | https://www.ibm.com |
| **Microfocus Atlas** | Requirements management | Requirements | Versione trial disponibile | https://www.microfocus.com/ |
| **Objectives** | Requirements management | Requirements | Versione trial disponibile | http://www.objectiver.com |
| **Open Source Requirements Management Tool (OSRMT)** | Requirements management | Requirements | Open Source | http://sourceforge.net/projects/osrmt/ |
| **Reqtify** | Requirements management | Requirements | Demo non disponibile | https://www.3ds.com/it/prodotti-e-servizi/catia/prodotti/reqtify/ |
| **rmtoo** | Requirements management | Requirements | Open Source | http://rmtoo.florath.net/ |

[26] https://ieeexplore.ieee.org/document/7042284

[27] https://pdfs.semanticscholar.org/8e78/63430446f610f5015a484d084cccb7e3c376.pdf

| | | | | |
|---|---|---|---|---|
| **Simulink Requirements** | Requirements management | Requirements | Versione Trial disponibile | https://it.mathworks.com/products/simulink-requirements.html |
| **Teamcenter Systems Engineering Requirements (TcSE)** | Requirements management | Requirements | Versione trial non disponibile | https://www.plm.automation.siemens.com/global/it/products/teamcenter |
| **Telelogic DOORS** | Requirements Management | Requirements | Gratuito | http://telelogic-doors.software.informer.com/ |
| **Visual Trace Spec** | Requirements management | Requirements | Versione trial disponibile | http://visualtracespec.com/# |
| **Visure Requirements Management Tool** | Requirements management | Requirements | Versione trial disponibile su richiesta | https://visuresolutions.com/requirements-management-tool/ |

## 6.4 Progettazione

La fase di progettazione identifica i requisiti generali e individua la struttura più adatta per la realizzazione del software. In questa fase viene definita l'architettura di sicurezza, adottando le linee guida di progettazione; vengono altresì documentati gli elementi che delimitano la superficie d'attacco e vengono modellate le minacce.

### 6.4.1 Secure Design Languages

Molti dei linguaggi per specificare i requisiti di sicurezza sono utilizzati anche per le specifiche di design. Ciò è dovuto al fatto che i requisiti di basso livello sono davvero vicini alla progettazione statica e dinamica. Questi linguaggi (ad esempio, UMLsec, SecureUML, e SecureTropos) sono già stati discussi nella sezione precedente. Due sono i principali punti che dovrebbero essere considerati nella scelta di un linguaggio di design sicuro:

- la varietà di schemi disponibili per rappresentare un disegno, comprensivo dei vari aspetti e livelli di astrazione;
- la disponibilità degli strumenti.

**UMLsec** fornisce una varietà di schemi e ha strumenti disponibili.
**SecureUML** può essere utilizzato anche per la progettazione di software sicuro; tuttavia, si limita a rappresentare solo nozioni di controllo degli accessi basati sui ruoli in un diagramma delle classi UML.
**Secure Tropos** propone di utilizzare gli Agent UML capability diagrams. Questi schemi sono simili ai diagrammi di attività UML (piano e capacità) e diagrammi di sequenza (interazione agente).

### 6.4.2 Software Design Tools

Il CATALOGO SECURITY TOOLS 6.9 raccoglie i tool disponibili, divisi per fase del processo SSDLC, che offrono funzionalità applicabili in ambito secure application development.

Si riporta di seguito la tabella 'Software Design Tools':

| Prodotto | Categoria | Fase SSE | Tipo Licenza | Sito Web |
|---|---|---|---|---|
| **Coras** | Threat Modeling tool/practies | Design | Open Source | http://coras.sourceforge.net/downloads.html |
| **IriusRisk** | Threat Modeling tool | Design | C'è una versione (limitata) open source | https://iriusrisk.com/ |
| **Microsoft Threat Modeling Tool** | Threat Modeling tool | Design | Free | https://www.microsoft.com |
| **ThreatModeler** | Threat Modeling tool | Design | Demo disponibile | https://threatmodeler.com/ |
| **SeaMonster - Security Modeling Software** | Threat Modeling tool | Design | Open Source | https://sourceforge.net/projects/seamonster/ |
| **TRIKE** | Threat Modeling tool/practies | Design | Open Source | http://www.octotrike.org/ |

## 6.5 Implementazione

Durante questa fase il team di sviluppatori mette in atto le contromisure secondo le specifiche della fase precedente ed effettua dei test sul codice sorgente per verificare l'assenza di security flaws.

### 6.5.1 Software Implementation Tools

Il CATALOGO SECURITY TOOLS 6.9 raccoglie i tool disponibili, divisi per fase del processo SSDLC, che offrono funzionalità applicabili in ambito secure application development.

Si riporta di seguito la tabella 'Software Implementation Tools':

| Prodotto | Categoria | Fase SSE | Tipo Licenza | Sito Web |
|---|---|---|---|---|
| **Brakeman** | SAST | Implementation | Open Source | https://brakemanscanner.org/ |
| **Burp Suite by PortSwigger** | SAST, DAST, Penetration Testing | Implementation / Verification | Versione Community liberamente scaricabile | https://portswigger.net |
| **CppCheck** | SAST | Implementation | Open Source | http://cppcheck.sourceforge.net/ |
| **Checkmarx** | SAST, DAST, RASP | Implementation / Verification | Versione trial disponibile a richiesta | https://www.checkmarx.com/ |
| **CodeDx** | SAST, DAST | Implementation / Verification | Versione trial disponibile | https://codedx.com/ |
| **CodeProfiler by Virtual Forge** | SAST per applicazioni SAP | Implementation | Nessuna versione trial disponibile | https://www.virtualforge.com |

| | | | | |
|---|---|---|---|---|
| **Contrast Enterprise** | IAST, RASP | Implementation / Verification | Demo disponibile su richiesta | https://www.contrastsecurity.com |
| **Dependency Check** | Library Inspection | Implementation | Open Source | https://www.owasp.org/index.php/OWASP_Dependency_Check |
| **SpotBugs** | SAST | Implementation | Open Source | https://spotbugs.github.io/ |
| **Gendarme** | SAST | Implementation | Open Source | https://github.com/mono/website/blob/gh-pages/docs/tools+libraries/tools/gendarme/index.md |
| **Microfocus Fortify Static Code Analyzer** | SAST, DAST, IAST, RASP | Implementation / Verification | Demo disponibile su richiesta | https://www.microfocus.com/it-it/products/static-code-analysis-sast/overview |
| **HCL Security AppScan** | SAST, DAST, IAST | Implementation / Verification | Versione trial non disponibile | https://www.hcltech.com |
| **JSHint** | SAST | Implementation | Open Source | https://jshint.com/ |
| **Klocwork** | SAST | Implementation | Versione trial disponibile su richiesta | https://www.perforce.com/products/klocwork |
| **MetaFlows** | Cloud Security Scanning | Implementation | Demo disponibile su richiesta | www.metaflows.com |
| **Microsoft BinScope** | SAST | Implementation | Free | https://www.microsoft.com |
| **Microsoft Code Analysis Tool** | SAST | Implementation | Free | https://www.microsoft.com |
| **Microsoft FxCop** | Library Inspection | Implementation | Free | https://www.microsoft.com |
| **Microsoft SDL Regex Fuzzer** | SAST | Implementation | Free | https://www.microsoft.com |
| **Microsoft SDL MiniFuzz File Fuzzer** | SAST | Implementation | Free | https://www.microsoft.com |
| **ModSecurity** | WAF | Implementation / Verification | Open Source | http://modsecurity.org/ |
| **N-Stalker Cloud Web Scan** | SAST, DAST | Implementation / Verification | Free Tier Available | https://www.nstalker.com |
| **PYLINT** | SAST | Implementation | Open Source | https://www.pylint.org |
| **PMD** | SAST | Implementation | Open Source | https://pmd.github.io |
| **Risk Fabric by Bay Dynamics** | Predictive Security Analytics | Implementation / Verification / Response | Demo disponibile su richiesta | https://baydynamics.com |
| **RSA Advanced Threat** | DAST | Implementation / Verification | Available by Request | https://www.dellemc.com |

| | | | | |
|---|---|---|---|---|
| **Management Solution** | | | | |
| **Website Malware Scanner** | SAST, DAST | Implementation / Verification | Demo non disponibile | https://www.sitelock.com |
| **SonarLint** | SAST | Implementation | Open Source | https://www.sonarlint.org |
| **SonarQube** | SAST | Implementation | Open Source | https://www.sonarqube.org |
| **Symantec Advanced Threat Protection** | IAST, RASP | Implementation / Verification | Versione Trial disponibile su richiesta | https://www.symantec.com |
| **Tanium Endpoint Platform** | Endpoint Security, App Security Scanning | Implementation / Verification | Demo non disponibile | https://www.tanium.com |
| **Trend Micro Deep Security Platform** | SAST, DAST | Implementation / Verification | Versione Trial disponibile | https://www.trendmicro.com |
| **Tripwire Enterprise** | IAST, RASP | Implementation / Verification | Demo disponibile su richiesta | https://www.tripwire.com |
| **Veracode Cloud Platform** | SAST, DAST, Mobile AST, Penetration Testing | Implementation / Verification | Demo disponibile su richiesta | www.veracode.com |
| **WhiteHat Sentinel** | SAST, DAST, MAST | Implementation / Verification | Demo di 30 giorni disponibile su richiesta | https://www.whitehatsec.com/info/security-check/ |

## 6.6 Verifica

Prima della fase di rilascio definitiva del software i team che lavorano in sicurezza effettuano un ulteriore verifica del codice elaborato mediante test di sicurezza. I test di sicurezza mirano a controllare la vulnerabilità delle superficie di attacco, in modo da agire in via preventiva alla correzione di eventuali problemi che potrebbero verificarsi in fase di rilascio.

### 6.6.1 Software Verification Tools

Il CATALOGO SECURITY TOOLS 6.9 raccoglie i tool disponibili, divisi per fase del processo SSDLC, che offrono funzionalità applicabili in ambito secure application development.

Si riporta di seguito la tabella 'Software Verification Tools':

| Prodotto | Categoria | Fase SSE | Tipo Licenza | Sito Web |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **Acunetix Web Vulnerability Scanner** | DAST, IAST | Verification | Versione trial a 14 giorni disponibile | https://www.acunetix.com/ |
| **AppSpider Pro by Rapid7** | DAST | Verification | Versione trial disponibile | https://www.rapid7.com |
| **BeEF** | Penetration Testing | Verification | Open Source | https://beefproject.com/ |
| **BrightCloud Threat Intelligence by Webroot** | DAST | Verification | Nessuna versione trial disponibile | https://www.brightcloud.com |
| **Burp Suite by PortSwigger** | SAST, DAST, Penetration Testing | Implementation / Verification | Versione Community liberamente scaricabile | https://portswigger.net |
| **Checkmarx** | SAST, DAST, RASP | Implementation / Verification | Versione trial disponibile a richiesta | https://www.checkmarx.com/ |
| **Citrix Web App Firewall** | WAF | Verification | Demo disponibile su richiesta | https://www.citrix.com/it-it/products/citrix-web-app-firewall/ |
| **CloudSOC Cloud Access Security Broker (CASB)** | Cloud Security Testing/Scanning | Verification | Nessuna versione trial disponibile | https://www.symantec.com/products/cloud-application-security-cloudsoc |
| **CodeDx** | SAST, DAST | Implementation / Verification | Versione trial disponibile | https://codedx.com/ |
| **Contrast Enterprise** | IAST, RASP | Implementation / Verification | Demo disponibile su richiesta | https://www.contrastsecurity.com |
| **Endpoint Privilege Management** | Endpoint Security | Verification / Response | Demo disponibile su richiesta | https://www.beyondtrust.com/ |
| **Falcon** | Endpoint Security | Verification / Response | Versione trial disponibile | https://www.crowdstrike.com |
| **GrayMatter Platform** | Penetration Testing, App Security Scanning | Verification | Demo disponibile su richiesta | https://www.reliaquest.com/ |
| **HCL Security AppScan** | SAST, DAST, IAST | Implementation / Verification | Versione trial non disponibile | https://www.hcltech.com |
| **Kali Linux** | Penetration Testing | Verification | Open Source | https://www.kali.org/ |
| **LogRhythm Security Intelligence** | Predictive Security Analytics | Verification / Response | Demo disponibile su richiesta | www.logrhythm.com |

| | | | | |
|---|---|---|---|---|
| **Platform** | | | | |
| **Malwarebytes Endpoint Security** | Endpoint Security | Verification | Versione trial disponibile | https://www.malwarebytes.com/business/endpointsecurity/ |
| **MetaDefender** | Predictive Security Analytics | Verification / Response | Available by Request | https://metadefender.opswat.com/ |
| **Metasploit by Rapid7** | Penetration Testing | Verification | Open Source | https://www.metasploit.com/ |
| **Microfocus Fortify Static Code Analyzer** | SAST, DAST, IAST, RASP | Implementation / Verification | Demo disponibile su richiesta | https://www.microfocus.com/it-it/products/static-code-analysis-sast/overview |
| **Microsoft Application Verifier** | DAST | Verification | Free | https://www.microsoft.com |
| **Microsoft Attack Surface Analyzer** | Intrusion Prevention | Verification | Free | https://www.microsoft.com |
| **Microsoft Cloud App Security (MCAS)** | Cloud Access Security Broker | Verification | Versione trial disponibile | https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/cloud-app-security |
| **ModSecurity** | WAF | Implementation / Verification | Open Source | http://modsecurity.org/ |
| **Network Security Monitoring and Management** | CDN, App Security Scanning | Verification | Demo non disponibile | https://enterprise.verizon.com/products/security/ |
| **NEVIS Security Suite** | WAF, Authentication, Identity mngt | Verification | Available by Request | https://www.nevis-security.ch/en/ |
| **Next-Generation Firewalls (NGFW)** | | Verification | | |
| **Nikto2** | Web Server Scanner | Verification | Open Source | https://www.cirt.net/Nikto2 |
| **Nmap** | Penetration Testing and Network Mapping | Verification / Response | Open Source | https://nmap.org/ |
| **NSFOCUS Web Application Firewall** | DAST, WAF | Verification | Demo non disponibile | https://nsfocusglobal.com/web-application-firewall-waf/ |

| | | | | |
|---|---|---|---|---|
| **N-Stalker Cloud Web Scan** | SAST, DAST | Implementation / Verification | Free Tier Available | https://www.nstalker.com |
| **OWASP Zed Attack Proxy (ZAP)** | Penetration Testing | Verification / Response | Open Source | www.owasp.org |
| **Paloalto Next-Generation Firewall** | WAF | Verification | Demo disponibile su richiesta | https://www.paloaltonetworks.com |
| **Peach Fuzzer** | Penetration Testing | Verification / Response | Demo disponibile su richiesta | https://www.peach.tech/ |
| **Pradeo Security** | Mobile AST | Verification | Nessuna versione trial disponibile | https://www.pradeo.com/it-IT/protezione-flotta-mobile |
| **Qualys Security & Compliance Suite** | DAST, WAF | Verification / Response | Versione trial disponibile | https://www.qualys.com |
| **Risk Fabric by Bay Dynamics** | Predictive Security Analytics | Implementation / Verification / Response | Demo disponibile su richiesta | https://baydynamics.com |
| **RSA Advanced Threat Management Solution** | DAST | Implementation / Verification | Available by Request | https://www.dellemc.com |
| **Runtime Application Self-Protection** | RASP | Verification / Response | Demo disponibile su richiesta | https://www.imperva.com/products/runtime-application-self-protection-rasp/ |
| **Samurai Web Testing Framework** | DAST, Penetration testing | Verification | Open Source | http://www.samurai-wtf.org/ |
| **SRX Series Firewall by Juniper Networks** | WAF | Verification | Versione Trial disponibile | https://www.juniper.net/us/en/products-services/security/srx-series/ |
| **Sucuri Website Application Firewall** | WAF | Verification | Demo non disponibile | https://sucuri.net/website-firewall/ |
| **Symantec Advanced Threat Protection** | IAST, RASP | Implementation / Verification | Versione Trial disponibile su richiesta | https://www.symantec.com |
| **Synopsys Black Duck Hub** | Library Inspection | Verification | Demo disponibile su richiesta | https://www.blackducksoftware.com/ |
| **Tanium Endpoint Platform** | Endpoint Security, App Security | Implementation / Verification | Demo non disponibile | https://www.tanium.com |

| | | | | |
|---|---|---|---|---|
| | Scanning | | | |
| **Thunder TPS by A10 Networks** | DDoS Protection | Verification / Response | Versione Trial disponibile | https://www.a10networks.com/products/thunder-tps/ |
| **Trend Micro Deep Security Platform** | SAST, DAST | Implementation / Verification | Versione Trial disponibile | https://www.trendmicro.com |
| **Tripwire Enterprise** | IAST, RASP | Implementation / Verification | Demo disponibile su richiesta | https://www.tripwire.com |
| **Trustwave Secure Web Gateway** | CDN, DAST | Verification | Demo non disponibile | https://www.trustwave.com/en-us/services/technology/secure-web-gateway/ |
| **Trustwave Web Application Firewall** | WAF, Penetration Testing | Verification | Demo non disponibile | https://www.trustwave.com |
| **Veracode Cloud Platform** | SAST, DAST, Mobile AST, Penetration Testing | Implementation / Verification | Demo disponibile su richiesta | www.veracode.com |
| **VMWare Carbon Black** | Endpoint Security | Verification / Response | Demo disponibile su richiesta | https://www.carbonblack.com/ |
| **vSentry by Bromium** | Endpoint Security | Verification / Response | Demo disponibile su richiesta | www.bromium.com |
| **Website Malware Scanner** | SAST, DAST | Implementation / Verification | Demo non disponibile | https://www.sitelock.com |
| **WhiteHat Sentinel** | SAST, DAST, MAST | Implementation / Verification | Demo di 30 giorni disponibile su richiesta | https://www.whitehatsec.com/info/security-check/ |
| **Wireshark** | Penetration Testing and Packet-level Monitoring | Verification | Open Source | https://www.wireshark.org/ |
| **Yottaa** | CDN, DDoS Protection, WAF | Verification | Demo disponibile su richiesta | https://www.yottaa.com |

## 6.7 Validazione

Durante questa fase il software è oggetto di una Final Security Review finalizzata a stabilire se il software soddisfa tutti i requisiti di sicurezza individuati nella fase iniziale del progetto.

In questa fase ci si accerta, inoltre, che i bug di sicurezza precedentemente identificati siano stati corretti e che il SW sia sufficientemente robusto di fronte a nuove vulnerabilità.

Le azioni di sicurezza di questa fase possono essere così sintetizzate:

- **Software Remediation dopo un'analisi statica (SAST)**
  - Analisi della reportistica e classificazione degli errori, rilevati nella fase di analisi statica del codice;
  - Rimozione degli errori di sicurezza legati all'uso di librerie esterne vulnerabili, sostituendo queste ultime con le versioni sicure;
  - Ristrutturazione delle classi e funzioni identificate come vulnerabili alle varie injection, al cross site scripting, etc.
  - Applicazione delle modifiche ai costrutti sintattici che rendono il software vulnerabile;
  - Correzione del software in base ai warning sulla qualità del codice;
- **Software Remediation dopo un'analisi dinamica (DAST)**
  - Analisi della reportistica e classificazione degli errori per rilevanza e quindi per priorità e urgenza della loro correzione.
  - Rimozione degli errori messi in evidenza dal fuzzy testing, ad esempio aumentando i controlli applicativi.
  - Correzioni degli errori, eventualmente tramite implementazione di nuove funzioni, per esempio aggiungendo meccanismi di autenticazione o rivedendo la struttura delle classi e funzioni.
  - Adozione di attributi del protocollo per innalzare la sicurezza di cookie e sessioni.
- Definizione di un **Incident Response Plan** cioè la documentazione contenente le istruzioni per rispondere e limitare gli effetti di un incidente di sicurezza.
- Produzione di un documento di Security Review un processo collaborativo che identifica i problemi relativi alla sicurezza, il livello di rischio associato a tali problemi e le decisioni da prendere per ridurre o accettare tale rischio.
- Aggiornamento delle procedure di sicurezza, certificazione del rilascio del software, testing e archiviazione.


*Figura 13 - Input e Output della fase Final Review - Secure Release*

### 6.7.1 Software Release Tools

Il CATALOGO SECURITY TOOLS (vedi paragrafo 6.9) raccoglie i tool disponibili, divisi per fase del processo SSDLC, che offrono funzionalità applicabili in ambito secure application development.

Si riporta di seguito la tabella 'Software Release Tools':

| Prodotto | Categoria | Fase SSE | Tipo Licenza | Sito Web |
|---|---|---|---|---|
| **Armor Complete** | Cloud Security Platform | Release | Available by Request | https://www.armor.com |

### 6.8 Supporto

La fase di supporto riguarda la manutenzione e l'assistenza post rilascio. Questa fase nasce per seguire tutte le novità in materia di sicurezza, imposte dal dinamico mercato informatico, per adeguarsi all'evoluzione delle vulnerabilità del software.

Le azioni di sicurezza di questa fase possono essere così sintetizzate:

- **Vulnerability assessment**:
  - esecuzione di test che consentano di individuare le vulnerabilità dell'applicazione;
  - valutazione della priorità/severità dei problemi riscontrati;
  - definizione del Remediation Plan;
  - produzione di reportistica di sintesi e di dettaglio;
- **Data Loss/Leak Prevention**:
  - rilevazione, analisi e classificazione dei dati che transitano nell'organizzazione, ovunque siano archiviati;
  - creazione di regole predefinite per la protezione dei dati, per assicurarsi che siano usati in conformità con le politiche di privacy e sicurezza;
  - generazione automatica di alert nel caso in cui vengano violate le policy di sicurezza definite;
- **Database Security**:
  - analisi dei database e valutazione dei rischi mediante l'accertamento di nuove vulnerabilità;
  - individuazione delle alterazioni dei dati, degli utenti e dei profili di accesso;
  - arresto in tempo reale delle sessioni che violano le policy, evitando che i dati vengano compromessi;
  - applicazione delle ultime patch di sicurezza disponibili;
- **Web Application Firewall Management e Secure Web Gateway**:
  - funzionalità di standard firewall (policy enforcement, stateful inspection, packet filtering, NAT, VPN client-to-site e site-to-site);
  - anti-malware e anti-spam;
  - Intrusion Prevention (IPS) per il blocco delle minacce;
- **Patching Update:** notifica, installazione e test di nuovi security improvement packages.

#### 6.8.1 Software Response Tools

Il CATALOGO SECURITY TOOLS 6.9 raccoglie i tool disponibili, divisi per fase del processo SSDLC, che offrono funzionalità applicabili in ambito secure application development.

Si riporta di seguito la tabella 'Software Response Tools':

| Prodotto | Categoria | Fase SSE | Tipo Licenza | Sito Web |
|---|---|---|---|---|
| **Airlock Suite by Ergon Informatik** | WAF, Authentication, Identity | Response | Versione trial disponibile | https://www.airlock.com |
| **Akamai** | CDN, DDoS Protection, WAF | Response | Prova gratuita disponibile | https://www.akamai.com/it/it/ |
| **Alert Logic SIEMless Threat Management** | Intrusion Prevention System, Cloud Access Security Broker, WAF, Container Security | Response | Versione trial disponibile | https://www.alertlogic.com/ |
| **AWS WAF** | WAF | Response | Nessuna trial disponibile | https://aws.amazon.com/it/waf/ |
| **Potection Center** | Mobile AST | Response | Nessuna demo disponibile | https://appmobi.com |
| **AppWall by Radware** | WAF, DDoS Protection | Response | Nessuna versione trial disponibile | https://www.radware.com/ |
| **Arbor DDoS Protection** | DDoS Protection | Response | Nessuna versione trial disponibile | https://www.netscout.com/arbor-ddos |
| **Arxan Application Protection** | Mobile AST | Response | Nessuna versione trial disponibile | https://www.arxan.com/application-protection |
| **Barracuda Web Application Firewal** | WAF | Response | Versione trial disponibile su richiesta | https://www.barracuda.com/products/webapplicationfirewall |
| **Lookout Mobile Endpoint Security** | Mobile Access Security Broker | Response | Demo disponibile su richiesta | https://www.lookout.com/products/mobile-endpoint-security |
| **CD Protection by CD Networks** | CDN, WAF, DDoS Protection | Response | Nessuna versione trial disponibile | https://www.cdnetworks.com |
| **CipherCloud** | Cloud Access Security Broker | Response | Versione trial disponibile | https://www.ciphercloud.com |
| **CloudFlare** | CDN, DDoS Protection, WAF | Response | Nessuna versione trial disponibile | www.cloudflare.com |

| | | | | |
|---|---|---|---|---|
| **CloudFront by Amazon** | CDN, DDoS Protection | Response | Nessuna versione trial disponibile | https://aws.amazon.com/it/cloudfront/ |
| **Cloud Access Security Broker (CASB)** | Cloud Access Security Broker | Response | Demo gratuita a richiesta | https://umbrella.cisco.com/products/casb |
| **CloudPassage Halo** | Cloud Access Security Broker | Response | Versione trial disponibile | https://www.cloudpassage.com |
| **DDoS Strike by Security Compass** | DDoS Protection | Response | Demo disponibile su richiesta | https://www.securitycompass.com |
| **R&S®Web Application Firewall** | WAF | Response | Demo disponibile su richiesta | www.denyall.com |
| **F5 Big-IP** | WAF, DDoS Protection | Response | Demo disponibile su richiesta | https://f5.com |
| **FireEye NX** | Web Server Scanner, WAF | Response | Versione trial non disponibile | https://www.fireeye.com |
| **FortiWeb: Web Application Firewall and API Protection** | WAF | Response | Demo disponibile su richiesta | https://www.fortinet.com/products/web-application-firewall/fortiweb.html |
| **FortiGate NGFW** | WAF | Response | Demo disponibile su richiesta | https://www.fortinet.com/it/products/next-generation-firewall/models-specs.html |
| **Imperva FlexProtect** | WAF, DDoS Protection | Response | Demo disponibile su richiesta | https://www.imperva.com/products/flexprotect-plans/ |
| **BloxOne Threat Defense** | WAF | Response | Versione trial disponibile su richiesta | https://www.infoblox.com/products/bloxone-threat-defense/ |
| **Hillstone E-Series** | WAF | Response | Demo non disponibile | https://www.hillstonenet.com |
| **Kona Site Defender by Akamai** | WAF, DDoS Protection | Response | Demo disponibile su richiesta | https://www.akamai.com/it/it/products/security/kona-site-defender.jsp |
| **CenturyLink DDoS and Web Application Security** | CDN, DDoS Protection | Response | Demo non disponibile | https://www.centurylink.com/business/security/ddos-and-web-application.html |

| | | | | |
|---|---|---|---|---|
| **Netsparker Web Application Security Scanner** | DAST | Response | Demo disponibile su richiesta | https://www.netsparker.com/ |
| **Neustar** | DDoS Protection, WAF | Response | Demo disponibile su richiesta | https://www.home.neustar/ |
| **Palo Alto Threat Prevention Services** | RASP WAF | Response | Demo disponibile su richiesta | https://www.paloaltonetworks.com |
| **Network Threat Detection** | Intrusion Prevention System | Response | Demo disponibile su richiesta | https://www.bricata.com |
| **Sophos Next-Gen Firewall** | WAF | Response | Versione Trial a 30 giorni disponibile | https://www.sophos.com/en-us/products/next-gen-firewall.aspx |
| **Sucuri Website Security Solutions** | WAF, DDoS Protection, App Security Scanning | Response | Demo non disponibile | https://sucuri.net/website-security-platform/signup/ |
| **Ziften** | Endpoint Security | Response | Demo disponibile su richiesta | https://ziften.com/ |

## 6.9 Catalogo Security Tools

Il CATALOGO SECURITY TOOLS raccoglie i tool disponibili che offrono funzionalità applicabili in ambito secure application development.

In Appendice 1 viene riportato il Catalogo Security Tools con il seguente formato:

| Prodotto | Categoria | Fase SSE | Tipo Licenza | Sito Web |
|---|---|---|---|---|
| *nome commerciale del tool* | *indica la macro-funzione: per es. DAST, SAST, WAF ecc.* | *la fase del sw life-cycle coperta dal tool* | *tipo licenza* | *indirizzo web per approfondimenti* |

*Tabella 4 - Struttura del Catalogo Security Tool*

## 6.10 Training e formazione

***Le organizzazioni inoltre dovrebbero investire di più anche nello sviluppo di competenze interne sulla base anche del fatto che molti degli attuali problemi di sicurezza derivano da errori di progettazione o di implementazione, risolvibili solo disponendo di personale qualificato. Alcuni analisti affermano che il 64% degli sviluppatori non sono confidenti di poter scrivere applicazioni sicure*** [fonte: Microsoft Developer Research].

Questa sezione fornisce un elenco di riferimento dei corsi disponibili in ambito secure software development.

### 6.10.1 Secure Coding in C and C++

Il corso è basato su material di Addison-Wesley: "Secure Coding in C and C++" and "The CERT C Secure Coding Standard". Il training SEI può essere offerto anche fuori dall'area statunitense.

| | |
|---|---|
| **URL** | http://www.sei.cmu.edu/training/p63.cfm |
| **Country of HQ location** | US |
| **Geographic Scope** | International |
| **Type** | Academic (SEI) |

Questo corso fornisce una spiegazione dettagliata di errori di programmazione comuni in C e C ++ e descrive come questi errori possono portare a codice vulnerabile. Il corso si concentra sulle questioni di sicurezza intrinseche dei linguaggi di programmazione C e C ++ e delle librerie associate.

I partecipanti acquisiscono conoscenza sugli errori comuni di programmazione che portano a vulnerabilità del software, come questi errori possono essere sfruttati, e le strategie di mitigazione efficaci per impedire l'introduzione di tali errori. In particolare, i partecipanti acquisiscono competenze in merito a:

- migliorare la sicurezza complessiva di ogni tipo applicazione C o C ++
- contrastare attacchi buffer overflow e stack-smashing che sfruttano la manipolazione logica di stringhe insicure
- evitare vulnerabilità e security flaws derivanti dal non corretto utilizzo delle funzioni di gestione della memoria dinamica
- eliminare i problemi integer-related: integer overflows, sign errors, truncation errors
- usare correttamente le funzioni di output formattato senza introdurre vulnerabilità format-string
- evitare le vulnerabilità di I/O, tra cui condizioni *race conditions*
- evitare I/O vulnerabilities, including race conditions

### 6.10.2 Writing Secure Code - C++

Questo corso di formazione computer-based spiega quali sono le funzioni di sicurezza principali del linguaggio C ++, come evitare che gli sviluppatori cadano nelle trappole di sicurezza comuni e come costruire applicazioni aziendali sicure e affidabili utilizzando C ++. Gli studenti sono guidati attraverso esempi di codice hands-on che evidenziano i problemi e le soluzioni prescritte.

Il corso ha i seguenti moduli:

- Introduction to Software Security
- Data Protection – in Storage and in Transit
- Authentication
- Authorisation
- Data Validation

- Process Handling
- Error Handling and Exception Management
- Logging and Auditing
- Memory Management

### 6.10.3 Writing Secure Code - Java (J2EE)

Questo corso di formazione computer-based illustra le caratteristiche chiave di sicurezza della piattaforma J2EE, come evitare che gli sviluppatori cadano nelle trappole di sicurezza comuni e come creare applicazioni web sicure e affidabili utilizzando Java. Gli studenti sono guidati attraverso esempi di codice hands-on che evidenziano i problemi e le soluzioni prescritte.

Il corso ha i seguenti moduli:

- Introduction to Software Security
- Data Protection – in Storage and in Transit
- Authentication
- Authorisation
- Data Validation
- Process Handling
- Error Handling and Exception Management
- Logging and Auditing
- Memory Management

### 6.10.4 Foundstone (Mcafee) Courses

Foundstone offre un programma di formazione di sicurezza di rete per la creazione di professionisti della sicurezza qualificati.

| | |
|---|---|
| **URL** | http://www.foundstone.com |
| **Contact Method** | http://www.mcafee.com/us/about/contact-us.aspx<br>Email, web form, phone and address |
| **Country of HQ location** | US |
| **Geographic Scope** | International |
| **Type** | Industry (McAfee) |

### 6.10.5 Threat Modeling

Questo corso di formazione computer-based spiega i processi e i concetti di creazione di software sicuro al fine di designare un quadro di sicurezza, identificando quindi minacce e contromisure. Gli studenti possono apprendere come utilizzare la modellazione delle minacce per migliorare il SDLC.

Il corso ha i seguenti moduli:

- Introduction to Threat Modeling and Hacme Books
- Identify Security Requirements
- Understand the System and the Application
- Identify Threats and Countermeasures
- Post-Threat Modeling Activities

### 6.10.6 Writing Secure Code - ASP.NET (C#)

Questo corso di formazione computer-based spiega le caratteristiche chiave di sicurezza della piattaforma .NET, come evitare che gli sviluppatori web cadano nelle trappole di sicurezza comuni e quindi come creare applicazioni web sicure e affidabili utilizzando ASP.NET. Gli studenti sono guidati attraverso esempi di codice hands-on che evidenziano i problemi e le soluzioni più idonee.

Il corso ha i seguenti moduli:

- Introduction to Software Security
- Data Protection – in Storage and in Transit
- Authentication
- Authorization
- Data Validation
- Process Handling
- Error Handling and Exception Management
- Logging and Auditing
- Memory Management

### 6.10.7 Oracle Courses

Oracle University è il principale fornitore di formazione per le tecnologie e i prodotti Oracle. Offre corsi class-based, on-site, virtuali e su CD-ROM, molti dei quali si concentrano sulla programmazione Java o sui prodotti Oracle.

| | |
|---|---|
| **URL** | http://education.oracle.com |
| **Contact Method** | Education Contact<br>Email and phone |
| **Country of HQ location** | US |
| **Geographic Scope** | International |
| **Type** | Industry (Oracle) |

### 6.10.8 Developing Secure Java Web Services, Java EE 6

Il corso Developing Secure Java Web Services fornisce le informazioni necessarie per progettare, implementare, distribuire e gestire secure web services e web service client utilizzando componenti di tecnologia Java e Java Platform, Enterprise Edition 6 (Java EE 6 della piattaforma).

Gli studenti vengono guidati sulla necessità di garantire servizi web sicuri e sulle sfide associate alla sicurezza dei servizi Web. Gli studenti vengono formati anche sui principali standard di settore e sulle iniziative sviluppate per fornire soluzioni di sicurezza complete per i servizi web; nonchè come applicarli per garantire servizi web sicuri. In particolare, gli studenti imparano come proteggere i servizi Web utilizzando tecnologie application-layer security, transport-layer security e message-layer security, come ad esempio come quelle specificate dalle estensioni di sicurezza WS- *.

Questo corso introduce anche i concetti di gestione delle identità, i driver che stanno dietro le soluzioni di gestione delle identità e le funzioni di Sun Java System Access Manager.

Gli obiettivi del corso sono i seguenti:

- Identify the need to secure web services
- List and explain the primary elements and concepts of application security
- Outline the factors that must be considered when designing a web service security solution
- Describe the issues and concerns related to securing web service interactions
- Analyse the security requirements of web services
- Identify the security challenges and threats in a web service application
- Evaluate the tools and technologies available for securing a Java web service
- Secure web services by using application-layer security, transport-layer security and message-layer security
- Describe the concept of identity and the drivers behind identity management solutions
- Explain the role of Sun Java System Access Manager in securing web services
- Secure web services by using UserName token profile
- Secure web services by relying on Sun Java System Access Manager

Il corso tratta i seguenti argomenti:

- Encapsulating the Basics of Security
- Examining Web Services Security Threats and Countermeasures
- Securing Java Web Services Using JavaEE
- Introduction to Web Services Security
- Web Services Security with JAX-WS and Project Metro
- Authentication in JAX-WS
- Identity Management and OpenSSO

### 6.10.9 MySQL and PHP - Developing Dynamic Web Applications

Il corso MySQL and PHP - Developing Dynamic Web Applications spiega come sviluppare applicazioni in PHP e come usare MySQL in modo efficiente per le applicazioni. Con un approccio hands-on, questo corso con istruttore migliorerà le capacità di PHP e di come combinarle con collaudate tecniche di gestione di database per creare applicazioni web best-of-breed che siano efficienti, solide e sicure.

Gli obiettivi del corso sono:

- Design web-based applications
- Design schemas based on MySQL
- Use „include files" to make code easier to maintain
- Use PHP 5 and take advantage of its advanced features
- Build applications, following a precise flow
- Authenticate users in a secure way against a database
- Handle errors in your PHP applications efficiently and elegantly
- Write composite queries using JOINs and subqueries
- Use indexing in order to manipulate large amounts of data efficiently
- Use JOINS to extract data from multiple tables
- Use GROUP BY clauses and aggregate functions
- Write applications whose components can be scaled to meet increased demand
- Build a complete application that includes authentication and session management
- Understand how PHP, MySQL and the Apache web server work together to deliver dynamic web content

Il corso tratta i seguenti argomenti:

- PHP Foundations
- MySQL Foundations
- Manage Databases
- Manage Tables
- SQL SELECT Commands
- SQL Expressions
- SQL DML Commands
- SQL JOINS
- MySQL Database-Driven Web-Based Forms
- Session Handling
- Object-Oriented Programming
- Authentication
- Securing PHP and MySQL

### 6.10.10 Google Gruyere

Google Code University fornisce un ambiente di laboratorio gratuito chiamato Gruyère[28], dove gli studenti possono provare ad hackerare applicazioni web. Gli studenti hanno l'opportunità di fare qualche prova reale di penetrazione, sfruttando esempi reali con complessità crescente. In particolare, gli studenti possono imparare:

- come un'applicazione web può essere attaccata utilizzando vulnerabilità di sicurezza comune, come le vulnerabilità cross-site scripting (XSS) e cross-site request forgery (XSRF)
- come trovare, correggere ed evitare queste vulnerabilità comuni, e altri bug che hanno impattano sulla sicurezza, come ad esempio denial-of-service, la divulgazione di informazioni o l'esecuzione di codice remoto.

### 6.10.11 OWASP Training Courses

OWASP offre materiali di formazione gratuiti, video e presentazioni, e fornisce opportunità di formazione presso le sue conferenze sulla sicurezza delle applicazioni.

[28] http://google-gruyere.appspot.com/