Il processo consiste in pratiche di sicurezza, raggruppate in sette fasi distinte: formazione, requisitazione, progettazione, implementazione, verifica, rilascio e monitoraggio/manutenzione. Uno degli aspetti chiave dell'SDL è l'introduzione del Threat Modeling nella fase di progettazione, che promuove l'individuazione preventiva delle vulnerabilità presenti nelle applicazioni e alcune volte persino i potenziali difetti di progettazione. Queste informazioni vengono poi utilizzate per attuare eventuali piani di mitigazione o modifiche progettuali.

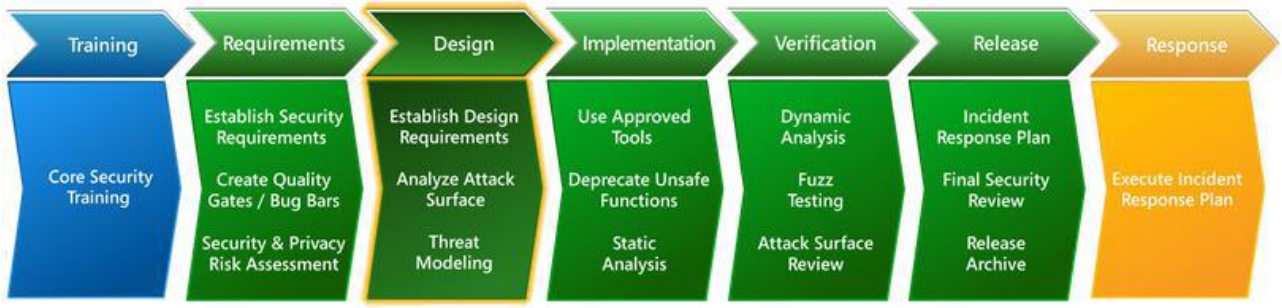

Figura 1 - Processo del ciclo di sviluppo sicuro di Microsoft

Sono disponibili diversi strumenti, non solo per il Threat Modeling ma per ciascun aspetto dell'SDL, tutorial online, documentazione, forum e blog di supporto. Il processo può essere utilizzato anche con le metodologie di sviluppo Waterfall e Agile e può essere applicato a qualsiasi piattaforma e implementato da qualsiasi organizzazione indipendentemente dalla sua dimensione.
L'obiettivo che tutte le metodologie di modellazione delle minacce condividono è lo sviluppo di un processo a passi iterativi che un team di sviluppo può facilmente seguire durante la valutazione di un sistema software.
Microsoft ha sviluppato e pubblicato una propria metodologia di modellazione delle minacce denominata STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) e diversi approcci per l'analisi dei rischi, tra cui la DREAD[11] (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability). Hussain, Erwin e Dunne hanno indicato la STRIDE[12] come la metodologia di Threat modeling più ampiamente utilizzata [1].
Al termine dell'attività STRIDE, viene prodotto un elenco di vulnerabilità. Tali vulnerabilità vengono poi classificate secondo un indice di priorità (basso/medio/alto) utilizzando una analisi qualitativa del rischio come la DREAD che a sua volta consente di definire la priorità delle opportune contromisure . Il prodotto finale dell'analisi STRIDE/DREAD può inoltre indirizzare in una fase successiva un eventuale Penetration Test (sulla base delle vulnerabilità riscontrate è possibile delimitare il perimetro che sarà poi oggetto di PT).
La Figura che segue illustra le fasi principali nella preparazione e nell'esecuzione di una modellazione delle minacce.

[11] https://resources.infosecinstitute.com/qualitative-risk-analysis-dread-model/

[12] https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx