minacce. È possibile aggiungere al modello delle minacce gli opportuni controlli di mitigazione al fine di guidare il progettista nella gestione di particolari minacce. A livello di organizzazione, definire quali azioni devono essere innescate durante la fase di modellazione. Ad esempio, un cambiamento di architettura o la distribuzione di un'applicazione in un nuovo ambiente. Allo stesso tempo, riflettere su come attuare e supportare in modo scalabile il processo di modellazione delle minacce in tutta l'organizzazione. Notificare i risultati dell'attività di modellazione delle minacce al processo di gestione dei difetti del software per dare seguito ad un adeguato follow-up. Adottare un sistema di valutazione per misurare e confrontare la rilevanza delle diverse minacce riscontrate. Considerare l'utilizzo di uno strumento per la gestione dei modelli di minacce delle distinte applicazioni. Istruire gli addetti ai lavori a concentrarsi sulle minacce maggiormente significative, poiché una dei principali problemi nella modellazione delle minacce è quello di individuare un numero elevato di minacce poco significative. Gli strumenti offrono un notevole supporto nell' identificare le potenziali minacce ma, alla fine, la modellazione delle minacce richiede un'intelligenza umana che difficilmente può essere automatizzata.

- Livello di maturità 3
  - Benefici: aggiornamento tempestivo e gestione qualitativa delle minacce applicative
  - Attività: nell'ambito di un processo maturo di modellazione delle minacce, revisionare regolarmente (ad esempio, annualmente) i modelli di minacce esistenti al fine di verificare un eventuale presenza di nuove minacce rilevanti per le applicazioni analizzate. Utilizzare un processo di analisi automatizzato per valutare la qualità e individuare eventuali difettosità nei modelli delle minacce. Revisionare le categorie di minacce maggiormente rilevanti per l'organizzazione. Quando si identificano nuove categorie di minacce, informare tempestivamente l'organizzazione al fine di garantirne una appropriata gestione.

5.5 Modellazione e Individuazione delle minacce: Threat Modeling

I processi di sviluppo sicuro del software, analizzati nel capitolo precedente, prevedono la modellazione delle minacce e suggeriscono l'inclusione dell'attività di Threat modeling nella metodologia, al fine di migliorare la pratica di identificazione delle vulnerabilità in materia di sicurezza del Software.
La tecnica di modellazione e individuazione delle minacce si rivolge alle seguenti figure professionali:

- Progettisti e Architetti del software;
- Threat Modeling SME o Security Assessors, responsabili dell'analisi della sicurezza di tutti i componenti dell'intera applicazione.

Le informazioni adoperate per stabilire i requisiti di sicurezza necessari devono includere i principi di progettazione sicura, descritti a seguire, e valutati da un programma prestabilito di gestione delle vulnerabilità, che può anche richiedere l'intervento di terze parti interessate, come un team di conformità (ad esempio, se l'applicazione deve essere conforme a standard quali HIPAA, PCI, GDPR, ecc.) o un team di gestione e distribuzione, in quanto dove e come viene utilizzata l'applicazione può incidere sulle reali esigenze di sicurezza. Pertanto, prima di iniziare il processo di modellazione delle minacce, è importante identificare gli obiettivi di business delle applicazioni e identificare i requisiti di sicurezza e conformità. Ciò è molto importante da definire in anticipo al