5.3 Threat Intelligence e Threat Modeling

Se l'obiettivo che ci si prefigge è quello di individuare gli attacchi a cui il software è correntemente esposto, allora il possesso di informazioni sulle minacce possono favorire nel porre l'attenzione sulle precise azioni necessarie che potrebbero essere intraprese nell'immediato. Diversamente, se l'obiettivo è ridurre la superficie di attacco e indirizzare gli investimenti in modo proattivo, allora la modellazione delle minacce può essere sicuramente di maggiore supporto. Quest'ultima non è in grado di fornire una risposta rapida al singolo problema di sicurezza che invece può essere data dalla Threat Intelligence, ma può sicuramente essere di aiuto nel guidare un programma maggiormente strategico che ha come obiettivo quello di elevare il livello di resilienza del software.

	Threat Modeling	**Threat Intelligence**
Finestra temporale	Proattivo	Reattivo
Estensione	Individuazione delle problematiche di sicurezza	Individuazione degli attaccanti
Supporto dal mercato	Consulenza e formazione	Feeds & Tools

Table 1 – Differenze tra Threat Modeling e Threat Intelligence

5.4 Threat Modeling e Threat Assessment

L'attività di Threat Assessment si concentra sull'identificazione delle minacce nelle applicazioni. Tale pratica è orientata all'individuazione e alla accurata comprensione di potenziali attacchi al software per recepire meglio i rischi e facilitarne la gestione. Difatti, la "software assurance" consiste nell'identificare i rischi presenti nelle applicazioni trattandoli quindi di conseguenza.
I rischi per un'applicazione possono essere relativi al business dell'applicazione (si pensi agli attacchi alla logica di business) o alla configurazione tecnica dell'applicazione. Lo stream del profilo di rischio dell'applicazione si occupa del primo, mentre il Threat Modeling si concentra sul secondo. Di seguito una sintesi dei livelli di maturità di un'organizzazione riguardo la valutazione delle minacce in relazione al profilo di rischio applicativo e all'attività di Threat modeling:

	Profilo di rischio applicativo	**Threat Modeling**
Livello di maturità 1 – Identificazione del Best-effort delle minacce di alto livello per l'organizzazione e per i singoli progetti.	Valutazione base del rischio applicativo	Modellazione delle minacce ad hoc del Best-effort
Livello di maturità 2 - Standardizzazione e analisi a livello aziendale delle minacce legate al software all'interno dell'organizzazione.	Comprensione del rischio per tutte le applicazioni dell'organizzazione	Modellazione delle minacce standardizzata
Livello di maturità 3 - Miglioramento proattivo della copertura delle minacce in tutta l'organizzazione	Revisione periodica dei profili di rischio dell'applicazione	Miglioramento della qualità grazie all'automazione del processo di analisi

Table 2 - Threat Assessment Overview

A seguire si descrivono in modo maggiormente dettagliato i singoli livelli di maturità sopra indicati, considerando che il tool di Risk Management di AGID può essere utilizzato per gestire questa tematica a tutti e tre i livelli, in base alla completezza delle informazioni gestite:

1) Profilo di rischio applicativo