**System Development Life Cycle:**Threat modeling becomes a very integral component for SDLC as it can help identify early potential threats early on. As during the plan phase threat modeling helps with gathering the required fields for a security focus approach. As this gives a way to help with decisions that will mitigate risks. During the developmental phase threat models will enable the tools for developers to follow secure coding practices for areas with vulnerabilities. During the testing phase there will be outputs of threat modeling which will help establish security testing by prioritizing their efforts and target areas that will be identified as “high-risk.” After the post-deployment phase threat modeling will continue to be a useful tool as it will then establish maintenance. This will help teams in establishing a way to continue the processes and how the teams move forward will continue to update and provide the regular routine maintenance on the system.   
 **Software Development Life Cycle:**With the topic of threat modeling in the software development life cycle we can ensure the focus is specifically to the software side of things. By doing this we will ensure that the security is integrated into the application from conception through the release, this will then involve the maintenance as well. Unlike a system-level threat modeling this will solely focus on the software architecture, code, and processes. During the requirement phase we can ensure that threat modeling will have a security requirement defined with a functional use for addressing how the software will handle data, communication in a secure manner, and authentication. In the design phase a developer will be able to analyze data, flows, and pinpoint where attackers might exploit the application. This will influence the decision for what is encryption sensitive data and what will require securing APIs, as well as what we should limit user privileges.   
 **Security Maturity:**Threat modeling holds an important place in a company’s security maturity as it will be utilized to be proactive in risk management and fostering a culture of secure developments. An organization that has a high degree of security maturity will have threat modeling throughout their projects, software development, and infrastructure. This will help with addressing early phases of product and system lifecycles leading to fewer vulnerabilities in production. As part of the threat modeling will promote continuous improvement. An organization will gain a deeper insight into emerging risks and vulnerabilities with each update that they end up implementing into their security maturity. As the higher ends and further the more it continues to mature it will become more of an automated and integrated into agile workflows. Providing the team with a real time insight into the issues at hand. Organizations will be more likely to train their teams into making their Security Maturity the most effective and efficient they can.  
 **Security Plan and Policies:**While discussing security plan and policies the threat modeling will be an essential tool for crafting and effective policy and plan. This should align them with theoretical frameworks with real world risks. Typically, the security plan will define how well an organization is at protecting their assets. The policy will help with establishing rules and guidelines for maintaining security. By utilizing threat modeling we will be able to bridge the gap between strategies and operational realities. When we look to develop a security plan we want to identify the most critical assets, threats, and potential attack points. By doing this we will allow the organization to prioritize its resources into effective uses for security measures. By utilizing the threat model, we can ensure we work on the proper controls and clarifications. To know which areas, require access restrictions, encryption requirements, and incident response protocols. These policies typically will align with actual threat landscapes making them relevant and enforceable. As new threats emerge the models will be updated prompting for policy revisions and plan adjustments in order to stay effective.