Collaborating with my colleagues and learning about their perspectives and experiences on this subject. To summarise this discussion, it can be fairly claimed that the key to developing a strong security architecture is layering a number of security measures on top of one another. To understand how to construct such an architecture and to substantiate this assertion, threat modelling is the suitable methodology.

Threat modelling is a continuous process that begins with the creation of a scalable representation of a system and ends with the identification of possible threats against it. It is a strategy used in engineering to discover countermeasures to risks that may impact a system/software/application, and so on. Threat modelling is used to develop the architecture of an application, ensure that security goals are met, and finally, to mitigate risk exposure to threat actors.

Threat modelling enables businesses to identify security risks to a particular architecture and make informed choices about how to handle them. It identifies flaws early in the software development life cycle, even before the first line of code is written. It not only aids in identifying design defects that conventional security testing techniques may miss, but also in analysing attack avenues that would have been overlooked otherwise. Additionally, threat modelling drives an organisation to go beyond traditional threats and emphasises concerns unique to the current scenario. It shines a light on essential assets, possible threat actors, and lacking controls, highlighting components that might be targeted by potential threat actors.

It paves the way for building a layered approach to cyber security by coming efforts of both offensive capabilities like penetration testing, red teaming, vulnerability assessment and analysis as well as defensive capabilities like SIEMs, EDRs, etc. leading to a clear “line of sight” across a project that justifies security efforts.

**References**

* Drake, V. (2019). Threat Modeling | OWASP. owasp.org. Available from: https://owasp.org/www-community/Threat\_Modeling [Accessed 26 Apr. 2022].
* Microsoft (2018). Microsoft Security Development Lifecycle Threat Modelling. Microsoft.com. Available from: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling [Accessed 26 Apr. 2022].
* Amazon Web Services. (2021). How to approach threat modeling. Available from: https://aws.amazon.com/blogs/security/how-to-approach-threat-modeling/ [Accessed 26 Apr. 2022].