**Initial Post**

**The Importance of Secure Software Development Practices**

In cybersecurity, building secure software is essential to protect sensitive information and maintain user trust. Two key practices that help achieve this are Threat Modelling and Code Review.

**Threat Modelling** is all about spotting potential security threats right from the start. Think of it as getting into the mindset of a hacker to predict and prevent their moves. For example, using the STRIDE model (which stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) helps developers identify and address these threats early on (Howard & LeBlanc, 2003). The big plus here is catching security issues early, which is cheaper and easier than fixing them later. But, it does take time and expertise to do it right.

**Code Review** involves having other developers check your code to find any security flaws. It’s like having a fresh pair of eyes to spot mistakes you might miss. Regular code reviews can uncover problems like SQL injection vulnerabilities or buffer overflows that automated tools might overlook (Anderson, 2008). The strength of code reviews lies in the combined knowledge of the team, leading to stronger, more secure code. However, they do require time and good collaboration.

By making Threat Modelling and Code Review a regular part of the software development process, organisations can greatly improve their security. These practices ensure that security is built into every step, resulting in safer and more reliable software.

**References**

Anderson, R. (2008) *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3rd ed. Indiana: Wiley & Sons.

Howard, M. & LeBlanc, D. (2003) *Writing Secure Code*. 2nd ed. Microsoft Press.

McGraw, G. (2006) *Software Security: Building Security In*. Boston: Addison-Wesley Professional.

Shostack, A. (2014) *Threat Modeling: Designing for Security*. Indianapolis: Wiley.