devoteam

Security **Enhancement**

Visit us here: devoteam.se

The purpose of a security enhancement initiative is to assess and improve the security of your software products and services. The goal is to help ensure digital products and services are resilient against cyber-attacks and data breaches.

To achieve this, we will work with experts and stakeholders to identify potential vulnerabilities and co-create recommendations for improving security measures.

Activities

Context and scope: To begin with, we will need to clarify the context and scope of the initiative; e.g. is it a general overview for the whole organization or do we focus on a specific product.

Threat modeling: The next activity is to walk through the existing software product from a security perspective. Threat modeling is a structured and highly collaborative apporach that will help us to identify and prioritize potential security threats and vulnearbilities.

Third-party suppliers: If the product or service relies on third-party components or services (e.g. APIs or cloud services), we will include an assessment of the security risks associated with these components.

Penetration testing: If the product is exposed to the outside, penetration testing, i.e. simulated cyber-attacks, is a useful tool to help to idenitfy vulnerabilities.

Code review: Security code reviews involve manual code walkthroughs and when applicable, automated tools to identify weaknesses in the code.

Policies: Compliance requirements may also be important to consider. Since this is very domain-specific we usually recommend a separate activity if needed.

Closing workshop: The activities will conclude with a workshop to discuss our findings and observations. This is to ensure that our recommendations will be to the point and relevant.

Outcome

A highly important outcome of the activities is an increased and shared understanding of the importance of security, the ambitions and what will be required to achieve the security objectives. We will deliver the *Security Memorandum* which is a comprehensive report including:

- *Executive summary:* A high-level summary of findings and recommendations
- *Key findings:* We will present our most important findings and highlight potential security risks
- *Recommendations:* We will provide specific recommendations for improving the security of the software. This will typically include both technical, organizational and managerial aspects.
- *Roadmap:* The memorandum will propose a prioritized roadmap for implementing the recommendations over time, including resource requirements

Contact us at:
se.advisory@devoteam.com