

Gathering Security Requirements



- 1 **Eliciting** software security requirements takes different approaches



- 2 Security Requirements should be **enumerated** separately from the functional requirement so that they can be separately **reviewed** and **tested**

- 3 Mixing the **security requirement** with the **functional requirement** can make the security requirement gathering process more **complicated** and **less accurate**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Why We Need Different Approaches for Security Requirement Gathering



- 1 Functional requirements are **positive requirements** specifying what the software should do

- 2 Security requirements are **negative requirements** specifying what the software should not do

- 3 It is the **natural tendency** of people to be clear about what they want but to find it difficult to understand things they don't want

- 4 Software needs to be viewed in a more **negative, critical, and destructive** way to reveal its non-intended use and its associated security requirements

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Notes: _____

Key Benefits of Addressing Security at the Requirement Phase



- Addressing security at the requirement phase can save **billions of dollars** compared to addressing security at a later phase of software development
- It also specifies the **security mechanisms** that need to be implemented in order to comply with regulations, standards or requirements for the secure application development and attack protection
- Security requirements give the developer an overview about the **key security controls** required to build a secure application
- Correctly understood security requirements can help in implementing security in the **design, development, and testing** stages

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Secure Application Design and Architecture



- A security negligence in the **design and architecture** phase may lead to vulnerabilities that are difficult to detect and expensive to fix in production
- Security vigilance in the design phase enables the detection of potential **security flaws** early in the software development lifecycle
- Secure design of an application is based on the **security requirements** identified in the previous phase of the SDLC
- Secure design is a **challenging process** as designing required security controls may obstruct business functionality requirements

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Notes: _____

