Q. Research and Reflect. Explain one of the tactics in plain language.

TACTIC:**DATA ENCRYPTION**

Data encryption involves transforming sensitive data into an unreadable format, which can only be decrypted using a specific key or password. This tactic ensures that even if unauthorized individuals gain access to the data, they will not be able to understand or make use of it.

Purported benefits:

1. **Vulnerability prevention**: Secure methods of coding make sure that software is constructed on a strong basis, minimizing the chance that vulnerabilities may be created during development.
2. Since each component is secure, the likelihood of security vulnerabilities will be reduced,and the system becomes more secure.
3. **Protection from hacking attempts**: By following to secure coding principles, engineers increase the system's overall security by making it difficult for an attacker to exploit code errors.
4. **Long term cost reduction**:Secure coding methods minimize security issues from the start, saving time and money on maintenance and legal costs while protecting resources.
5. **Enhanced reputation**: Using secure coding techniques shows users, users, and stakeholders that a company is committed to data security and privacy.
6. Secure coding techniques, based on best practices and industry standards, lead to higher-quality software by enhancing performance, maintainability, and reliability.

In conclusion, data encryption has many advantages in terms of security by design. It offers additional safety to sensitive data, making it difficult for unauthorized users to access. Encrypted data enables businesses to pay attention to privacy and data protection laws. Encryption also guarantees the security and integrity of data throughout its lifecycle and reduces the danger of data hacking.

Problems solved:

1,Sensitive data is protected.
2.Insecure coding practices are avoided.
3. Elimination of backdoor risks.
4.Maintenance costs are minimized.
5.Supply chain attacks are prevented.
6.Prevents accessing or stealing sensitive information.
7. Protection against data loss from lost or stolen physical devices.

Putting together in a nutshell,Data encryption plays a prominenet role in securityby design which enhances data security and protects against unauthorized access, hacking, tampering, and compliance issues.Integrating encryption into the design process establishes a strong foundation for data protection.It helps organizations safeguard their data assets and build trust with customers.