Adoption of Secure Coding Standards:

Implementing standards like OWASP ensures vulnerabilities are addressed early, not left for later. Practices such as input validation and static code analysis reduce risks and save costs.

Risk Evaluation and Mitigation:

Assess risks using frameworks like CVSS. Address high-risk issues immediately, while weighing the cost-benefit for lower-priority vulnerabilities.

Zero Trust:

No one is trusted by default. Use least privilege access, continuous verification (e.g., MFA), and segment resources to prevent insider threats and breaches.

Security Policies:

Define access control, prepare incident response plans, and enforce regular employee training. Automate policy compliance with tools like SIEM to stay proactive.