Secure Techniques

Baseline -> Security standards and configurations that an organization establishes to protect data and systems with the industry best practices, regulatory requirements and organization's needs

1. Establish
    a. Assessment -> Understanding the specific needs
    b. Define Standards -> Set configuration and controls
    c. Documentation -> Create polices and procedures to implement these baselines
2. Deploy
    a. Implementation -> Make sure the configurations are implemented in every device/software
    b. Automate (if possible)
    c. Verification -> Compliance check if the baseline it's well implemented
3. Maintain
    a. Monitoring -> Audit logs
    b. Updating -> Well patched
    c. Training and Awareness -> Users trained how to work with the device/software

MDM (Mobile Device management) -> Software application that allow it administrators to control, secure and enforce polices on mobile devices (EDR for mobile)

BYOD (Bring your own device) -> Use personal device for work purpose
COPE (Corporate-Owned, Personally Enabled) -> Corporate device but the organization allow for some personal use
CYOD (Choose your own device) -> Employee choose from a selection of devices provided by the organization, it is the balance between personal preference and corporate control

AppSec -> Ensure that software applications are secure

- Input Validation -> Validate the input text are validated so you cannot put characters to explore XSS or SQLi
- Secure Cookies -> Key attributes include Secure (indicating that the cookie should only be sent over HTTPS connection)
- SAST/DAST -> Scans that review the code to find possible vulnerabilities, code flaws and ensure compliance
- Code Signing -> Use certificate
- Sandboxing -> Isolate application, processes or programs to simulate the end-user