| Domain | Section | Stream | Questions |
|---|---|---|---|
| Governance | Education and Guidance | Training & Awareness | Do you require employees involved with application development to take SDLC training? |
| | | | Do your team know who to speak to if they need security guidance from outside the product team? |
| | | Organisation & Culture | Have you identified a Security Champion for each development team? |
| | | | Are roles and responsibilties clearly defined within the development team? |
| Design | Threat Assessment | Threat Modelling | Do you identify and manage architectural design flaws with threat modeling? |
| | | Software Requirements | Do project teams specify security requirements during development? |
| | Security Architecture | Architecture Design | Do teams use security principles during design? |
| | | | Do you use shared security services during design? |
| | | | Do you base your design on available reference architectures? |
| Implementation | Secure Build | Build Process | Is your full build process formally described? |
| | | | Is the build process fully automated? |
| | | | Do you enforce automated security checks in your build processes? |
| | | | Is code being stored securely? |
| | | Software Dependencies | Do you have solid knowledge about dependencies you're relying on? |
| | | | Do you prevent build of software if it's affected by vulnerabilities in dependencies? |
| | | Deployment Process | Do you use repeatable deployment processes? |
| | | | Are deployment processes automated and employing security checks? |
| | | Secrets Management | Do you inject production secrets into configuration files during deployment? |
| | | | Do you practice proper lifecycle management for application secrets? |
| | Defect Management | Defect Tracking | Do you track all known security defects in accessible locations? |
| | | | Do you enforce SLAs for fixing security defects? |
| | | Metrics & Feedback | Do you use basic metrics about recorded security defects to carry out quick win improvement activities? |
| Verification | Architecture Assessment | Architecture Validation | Do you review the application architecture for key security objectives on an ad-hoc basis? |
| | | | Do you regularly evaluate the threats to your architecture? |
| | Requirements Testing | Control Validation | Do you test applications for the correct functioning of standard security controls? |
| | | Misuse/Abuse Testing | Do you test applications using randomization or fuzzing techniques? |
| | | | Do you perform denial of service and security stress testing? |
| | Security Testing | Scalable Baseline | Do you scan applications with automated security testing tools? |
| | | | Do you integrate automated security testing into the build and deploy process? |
| | | Deep Understanding | Do you manually review the security quality of selected high-risk components? |
| | | | Do you perform penetration testing for your applications at regular intervals? |
| Operations | Incident Management | Incident Detection | Do you ensure that newly deployed applications are integrated with the organisation's SIEM solution? |
| | Environment Management | Configuration Hardening | Do you harden configurations for key components of your technology stacks? |
| | | | Do you have hardening baselines for your components? |
| | | Patching and Updating | Do you identify and patch vulnerable components? |
| | Operational Management | Data Protection | Do you operate separate Dev/Test/Production environments? |
| | | | Do you protect web facing applications and API's using a Web Application Firewall? |
| | | | Do you ensure that all devloper workstations are secured adequately? |