Plan	Code	Build	Internal testing	Release/ Deployment	External testing	Monitoring	Run/Operate
• Design security requirement • Privacy requirement • Asset Management • Architecture Security requirement • Secure coding best practices requirement • Threat modelling	• Credentials management • Coding security best practicies • Security test cases generation • Coding software editor security • Manual code review • API security	• Infrastructure configuration security • Data security • Dependency • Database configuration security • Application configuration security	• DAST • SAST • Functional security testing • Internal red teaming • Vulnerability management • Security scanning through open source tools • Purple teaming exercise • Unit testing from security point of view	• Dockers and Kubernetes security • Deployment process security • UAT to production security • Releasing automation security • WAF implementation security & review • IDS/IPS implementation security & review • Secure and monitor the entire physical and virtual environment • Security of transport layer • Vendor (third-party) security • Segregation of duties (process, hardware, software, environment)	• Penetration testing • External red teaming • Bugbounty • Risk assessment	• Security operations monitoring • Security event monitoring • Security incident management and monitoring • Threat intelligence exercises • Threat hunting exercise	• Bug fixes • Patch management • Call support operation security • New release security and automation • Incident management and response • Cross-team security awareness training (Building culture) • Version control and metadata • Compliance • Access control security (for internal team, external vendor, consumers)