1. What are the security activities you perform at each step of the SDLC?
2. Do you have dedicated specialists for each phase of the SDLC?
3. Do you have a threat model?
4. What is your incident response plan?
5. How do you monitor for vulnerabilities? What about open source library vulnerabilities?
6. Do you have a coordinated disclosure process?
7. What’s your maintenance release schedule?
8. How do you measure product security posture when its time to release a piece of software?
9. Do you have criteria to gate a release if there’s a vulnerability?
10. How do you communicate risk to customers? Do you have an advisory process?