* What is your role in conquering security concerns as a developer? What might that involve?
  + As a developer, my role is of course to be educated on the methods in which to build secure applications, of course, but the responsibility goes deeper than that as well. For example, pushing to an incorrect branch can be a security risk. It would also be in my best interest to understand and be present for the planning stage of the application. Should a security risk be found it will be important for me to engage with the reporters and the security team to understand the problem.
* Where does security fall within the software stack and development life cycle?
  + We find that considerations for security should be apparent in the planning, coding, building, testing, releasing, deploying, and operating stages of the SLDC. In other words, all stages.
* How might you add security measures to transform a DevOps pipeline into a DevSecOps pipeline?
  + The idea is to add security at each stage. Depending on the stage, this can look different. For example, during the planning stage we may determine that 2FA would be best for securing our application. This is practicing good security planning techniques. During the coding stage we may practice security by conducting regular code reviews or ensuring unit tests are being created.
* The article suggests creating and following a plan to secure the entire DevOps life cycle. What is included in the suggested plan and would you recommend following it?
  + The plan provided is a great boilerplate for security considerations. The considerations listed are very general and will add value to almost any application so I would recommend using it. However, every application will have different requirements. It is important to customize your solutions for your specific application and still think critically about what an application may or may not need.