Fortify Prospect Questions 1/24/2023

Question	Response
CISO	
How does your organization define software security?	
Where does AppSec rank in your overall risk environment?	
How do you manage overall application security risk?	
What percent of applications are covered with your current AppSec program? Do you have plans to secure and ensure compliance of every release of every application in the future?	
How do you measure success of your AppSec program?	
AppSec Director	
What is your process for identifying security vulnerabilities in your applications?	
Are you testing for vulnerabilities with every release of every application? Can you walk me through this process?	
Who is or would be expected to conduct applications security testing? The Application Security team, developers, or both?	
How confident are you that your security testing processes can adapt and scale to keep up with the increasing demand for speed and volume?	
How do you address application security testing tool integration into the Dev tool chains?	
How much time is spent triaging scan results for one application? Can you provide results in the timeframes developers are demanding vs. the need for depth and accuracy?	
Do you have a centralized way to manage, prioritize, and monitor application vulnerabilities?	
Are you leveraging machine learning to reduce the false positive rate of your scans?	
Are you able to scan the majority of the applications you have with the security tools you are using today? (language coverage)	
Do you prefer to have testing conducted on-prem or would you consider a secure, managed service that's offsite? Both are options, and many customers take a hybrid approach given resource constraints.	
Which SAST, DAST, RASP tools are you using today?	
Development Team Director/Managers	
What types of applications are you building/managing?	

Do you do in-house development, and if so, what's a ballpark number of custom applications that you have in your inventory?	
How often do you deploy applications on average how many updates or new releases are there per year to those applications?	
Which software development models are being used (Waterfall, Agile, DevOps)?	
Is security testing applied across the SDLC?	
What build environments are being used by developers? Is there a single paid-path of dev tools, or a variety of dev tool chains being used by the different dev teams?	
Have you had success integrating security testing in the IDEs, tool chains, and build processes?	
Which programming languages do your developers use?	
How much time is spent remediating security vulnerabilities?	
How is security changing to address new application development trends? (i.e. DevOps)	
What's the level of awareness do your developers have of secure coding best practices? Are you training your developers in these practices? If so, how often and what forms of education?	