Keeping Your Security Cool in a DevOps and Agile World

P2P4-W12: Keeping Your Security Cool in a DevOps and Agile World

Jenny Menna, Senior Vice President, US Bank
We had a full room on Wednesday at RSA Conference to talk about strategies for implementing security in DevOps and Agile environments. While we had a quite a few financial institutions in the room, we had a good diversity of industries represented as well. With a show of hands, most of the attendees were either just beginning or early in the DevSecOps journey. That meant that the few people with a lot of lessons learned got a ton of questions; many thanks to them for their patience and willingness to share. Discussion topics of interest very quickly coalesced into a few main areas: how to use automation, tools, measurement/metrics and training/people issues. Unfortunately, we didn’t get much past the first two.

It was no surprise that all attendees agreed that automation and effective use of tools was imperative to being able to achieve security risk reduction goals at the speed of DevOps. A number of specific tools were discussed in the room to support various functions. The issue of tracking open source software was briefly discussed. Many teams use a lot of open source software in their products and ensuring that these are secure is important. In addition, some of the more mature implementers talked about actively training every developer to code securely (“Security Savvy” was the phrase everyone took note of) and turning a few key folks on the team into security ninjas – those with the aptitude and interest to get a little more depth. Training the product team on the importance of security and their role is a key lesson. A number of participants noted that dedicated security staff could then participate as needed rather than being co-located at all times, participating in weekly story reviews. One company mentioned that their security team participated in “Risk Pods” for the DevOps projects, firewalled from other business as usual duties.

A key metric discussed was the lowering of technical debt. We also discussed tracking and addressing vulnerabilities identified in scans, with some debate about risks associated with those medium rated items after they were allowed to age. One participant noted they had good luck given the collaborative, fast fail fast fix environment, letting any less than critical bug go forward with the developers gladly fixing in the next release. The group noted that in some environments, such as industrial control systems, this type of approach might not ever be appropriate, where in areas like mobile apps it made good sense. A number of participants cited the ING transformation as a valuable case study to reference.

The group could easily have filled an extra 45 minutes on this topic. With the discussion primarily focusing on secure coding practices and continuous vulnerability scanning, we did not get to dive into privileged and administrative access management and identity management, which were important topics for some of our attendees. We look forward to a continued community discussion.