Increasing Usage of a Secure Development Lifecycle

P2P3-W12: Increasing Usage of a Secure Development Lifecycle

Cassie Crossley, Director, Product Security Office, Schneider Electric

Increasing Usage of a Secure Development Lifecycle

At the RSA Conference I led a peer-to-peer (P2P) session on the topic of embedding the secure development lifecycle (SDL) into organizations. In my own organization I have the responsibility for deploying our updated SDL (based on IEC 62443) to our global R&D and I.T. development teams. We are mature in the usage of SDL, but my ambition is to expand it beyond the technical team to all roles involved in the development lifecycle. This intimate P2P session provided an excellent forum to brainstorm and hear best practices from 30 conference attendees.

As people entered the room, I asked them if they were positioned in an I.T. or R&D organization. It was nearly a balance of 50/50 which I found extremely refreshing because software development in I.T. organizations is often overlooked. I was also pleased to find diversity of gender and ethnicity in the room, something that I noticed throughout the Conference in the sessions I attended.

Some attendees had mature SDL practices and others were just starting the journey. I described the intent of the session and that my goal was to see at least half participate in the conversation. (We met that goal.) To begin the conversation, I asked directed questions such as “how do you expand SDL to include product owners and leadership?”, “what encouragement, if any, do you provide?”, and “has anyone gamified their SDL?” The discussion was interactive, lively, and we used every minute.

Here are 14 ideas we discussed to further embed SDL into our organizations:

1. When onboarding new employees and contractors, explain SDL and provide training where needed.
2. Introduce SDL into other communities such as project management, offer management, marketing, and of course executive leadership. Focus the topics for the audience.
3. For awareness, have a special ‘Security Week’ or days that bring secure development practices to the organization.
4. Build a ‘Security Champions’ community made of deputies, volunteers, and security experts. Provide content in seminars, lunch and learns, and special events. Have team members present topics and bring in special guests such as researchers or vendors.
5. Send people to security conferences and local events such as OWASP meetings.
6. Create skill levels and targets for your employees to reach. Make it goal-driven by awarding belts (yellow, green, brown, etc.) or some other sequence (bronze, silver, gold; Padawan, Jedi knight, Jedi master).
7. Upskill employees with special projects, training, and funding certifications such as CISSP (Certified Information Systems Security Professional) and CSSLP (Certified Secure Software Lifecycle Professional). Award employees when they achieve certifications.
8. Gamify things such as ‘Capture the Flag’ which should include managers. One company created a game out of Threat Modeling and another company had a ‘Bug Bash’ event focused on closing vulnerabilities.
9. When vulnerabilities are found, offer just-in-time training focused on the specific vulnerability.
10. Rotate people between teams, specifically into teams where the SDL is mature. Have teams perform peer-to-peer reviews of SDL practices.

11. Perform security initiative assessments using BSIMM (Building Security In Maturity Model).
12. Include cyber initiatives and roadmaps into products. Incorporate compliance such as IEC/ISA. Set certification goals, targets, and KPIs.
13. Update processes to include SDL throughout the software development lifecycle in places such as change release and stage gate reviews.
14. Utilize tools and techniques such as static and dynamic code analysis, IDE coaching, software BOMs (bill of materials), and CI/CD (continuous integration / continuous delivery).

The best practices shared during the session exceed my expectations. With the incredible ideas mentioned, I have a large ambition to increase awareness, adoption, and excitement for secure development into my organization. I encourage you to take at least three of the ideas above into your company this year!