Recent attacks against SolarWinds or ASUS show that a secure development lifecycle alone is not sufficient. Development and security management lifecycle that leverages principles and SAFECode’s partnership with CSA to create a comprehensive Crypto Agility strategy. This fourth post in the ongoing SAFECode blog series provides guidance on practices required to establish Crypto Agility. This post focuses on protecting source code and build integrity, and identifying source code changes that were not intended to prevent code from being exploited.

To build security into an organization’s DNA, a company must create a security culture from top to bottom. Many SAFECode members have found software development programs to be of significant value to their software development and security management teams. These programs can be sustained by engaging a Security Champion or setting up a Security Champions program. If you haven’t already, be sure to check out our Security Champions blog series.

In many organizations, use of cryptography is often tightly coupled with critical business processes and functions. Therefore, careful planning, sound prioritization, and informed decision-making based on risk management are necessary to ensure that the business processes and functions utilizing cryptography are not disrupted. SAFECode’s Code Integrity: Best practices for ensuring code integrity during the code development or delivery step provides guidance on preventing code from being exploited. Technology vendors also need to employ best practices to ensure that malicious code is not being inserted in the code they create for their customers. The goal of the working group is to discuss best practices of DevSecOps and best practices of protecting source code and build integrity.

Help Us Change the World!

One of the benefits of being a SAFECode Volunteer is that the work you do can help secure software in the world. As countries continue with their mass vaccination programs, some organizations are considering a mandated “back to office” lifestyle for their employees. The rationale cited is their inability to manage a large remote workforce. Other organizations are planning to let their employees choose whether to work from home or the office. Come and participate in an exploratory discussion on what a hybrid workforce means for secure software development.

The Benefits of Being a SAFECode Volunteer

- Participants today have access to SAFECode’s online courses and training material.
- Access to the world’s best minds in software development and security.
- Opportunity to help the software developer community.
- Access to the largest cyber security community in the world.
- TrueRemove™

If you have any questions, please contact us at helpdesk@safecode.org.