VERACODE

Software Security Checklist:

10 Elements of an Effective AppSec Program

Most organizations recognize the positive effects of their application security (AppSec) programs, but struggle to find a baseline for gauging effectiveness and maturity.

Use this checklist as a starting point to see how well your AppSec program measures up to the most effective programs. The more boxes you check off, the more effective your program.

- [ ] **Application security controls are highly integrated into the CI/CD toolchain**

- [ ] **Application security training is included as part of your ongoing development security training program.**

  Offer at-leisure training opportunities such as *Veracode Security Labs*.

- [ ] **Ongoing developer security training includes formal training programs, and a high percentage of developers participate.**

  Implement formal security training with a set completion date and a skills assessment to ensure that developers are acquiring the skills they need to write secure code and remediate vulnerabilities.

- [ ] **Development managers communicate best practices to developers.**

- [ ] **Security issues are traced back to the individual development teams.**

  When you track the security issues, you can target efforts to improve those teams and individuals who introduce the most issues.

- [ ] **You track your AppSec program using formal processes and metrics to ensure that it's continuously improving.**

  You should have a formal process in place to regularly measure your AppSec program using metrics. With *the right metrics*, you can pinpoint areas where your AppSec program is performing well and areas that could use improvement. The data can also be used to show senior management or stakeholders the return on their AppSec investment.

- [ ] **You track individual development teams using metrics to ensure that they are continuously improving.**

- [ ] **You track security issues during the code development process.**

  If you are not assessing code for security issues in the development phase, and a vulnerability is identified later in the software development lifecycle (SDLC), it can be costly and time consuming to fix the flaws. You can assess code early in the development process with a tool like *Veracode's IDE Scan*.

- [ ] **Automated risk aggregation tools roll-up risk to keep senior development leaders informed.**

  Senior development leaders should be fully aware of the risks and vulnerabilities in applications.

To learn more about building an effective AppSec program and for more information on the ESG survey, download the full report:

Modern Application Development Security

Learn More

Veracode is the leading AppSec partner for creating secure software, reducing the risk of security breach and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of automation, integrations, process, and speed, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.

Learn more at www.veracode.com, on the Veracode blog and on Twitter.