



Application Security Program Strategy and Planning

Transform your application security program with
the help of industry-leading experts





We've all heard the famous 2011 Marc Andreessen quote, "software is eating the world." A decade later, innumerable companies in a rapidly growing number of industries are developing software. An example from the automotive industry: "The F-22 Raptor fighter jet uses about 1.7 million lines of software code, while a modern luxury vehicle contains close to 100 million lines of software code."1 Billions of lines of code are being written every day, and that means an increased reliance on open source code. Testing all that code—both proprietary and open source—for security issues and vulnerabilities is more important than ever. But the significantly greater velocity and frequency of builds required by DevOps makes testing an ongoing challenge.


Friction-free security testing in the DevOps era is a challenge in itself. What further aggravates the problem is the increased frequency, methods, and avenues of malicious attacks on software. A decade ago, attacks were limited to applications and infrastructure, but now attacks target the environments, containers, the entire software development life cycle (SDLC) including the build stage, and more. Modern AppSec demands a mature, well-rounded software security program (SSP) to manage risk throughout the application life cycle. Every journey begins with a single step, and the first step to transforming your security program is setting your AppSec program strategy.

Developing a software security program based on industry best practices

Change is the only constant, especially in the software security realm. With the increasing complexity of software, attack patterns, and targets; continuous integration / continuous delivery (CI/CD) processes; new open source vulnerabilities; emerging insider threats; supply chain changes; industry-specific regulations; and more, it's always appropriate to re-evaluate your software security program periodically to ensure risk readiness. This is especially important if you're embarking on a new security initiative. In either case, a fresh perspective on your business goals, holistic security strategy, potential gaps, tooling updates, development processes, software /applications, deployment environment, and network is imperative.

The U.S. Department of Homeland Security published a report in 2006 that observed, "The most critical difference between secure software and insecure software lies in the nature of the processes and practices used to specify, design, and develop the software... correcting potential vulnerabilities as early as possible in the software development life cycle, mainly through the adoption of security-enhanced process and practices, is far more cost-effective than the currently pervasive approach of developing and releasing frequent patches to operational software."² This is as relevant today as it was then. The earlier you build security into your software, the easier and cheaper it is to maintain over the long run.

To ensure that your software security program is built on a solid foundation and in line with industry best practices, it often helps to have third-party experts come in and lay the groundwork for plan development. With all the variables in play, it's virtually impossible for an already-time-constrained in-house security team to stay updated on all the new AppSec developments. And nothing beats the experience gained from tackling the security problems of hundreds of organizations over decades.



The most critical difference between secure software and insecure software lies in the nature of the processes and practices used to specify, design, and develop the software

The Black Duck AppSec program strategy

Some organizations have software security programs that consist of a few disparate activities—some code scanning, a bit of training for a part of the development team, and so on. But it's simply not possible to find and fix the vast majority of software security defects with such a haphazard approach to security. The attackers, meanwhile, are getting more sophisticated with their attacks. Modern software security dictates a more comprehensive approach, led by a software security group and in conjunction with a deep-rooted security culture across the organization. This entails measuring, managing, and evolving software security activities in a consistent, coordinated fashion.

With over 400 AppSec focused consultants, more than three decades of experience, and market-leading solutions, Black Duck can be your partner on the journey to transform your software security program. Read on to learn how you can get visibility into your current software security program, identify gaps, prioritize change, and determine how and where to apply resources for immediate improvement.



A foundation built on decades of real-world experience

You can't build a strong SSP on a weak foundation—especially one that isn't validated and backed real-world experience and data. There's too much at stake to take that risk. The processes, methodologies, and training that the Black Duck consulting team provides are derived from decades of software security and consulting experience across hundreds of organizations. Our real-world data is painstakingly calibrated and collected by trained assessors to ensure that the quality is maintained at the highest standards. As a partner throughout your software security journey, a team of dedicated Black Duck consultants helps you define and enact a long-term software security strategy.

Let's look deeper into the methodologies that are essential for evaluating and establishing the foundation of a well-rounded SSP.

The BSIMM report

For over a decade, the "Building Security In Maturity Model" (BSIMM) report has studied SSPs and gathered data, and that has produced a unique industry model and yardstick. By quantifying the activities of many different types of organizations, the BSIMM describes the common ground they share as well as the variations that make each unique. A BSIMM assessment provides a way to assess the current state of an SSP, identify gaps, prioritize changes, and determine how and where to apply resources for immediate improvement.

Roadmap planning

Once you have identified areas for advancement in your SSP, the next step is to create a plan to achieve those goals. Developing a plan is essential to prioritize funding, streamline resources, and reduce the risk of software vulnerabilities. A Maturity Action Plan (MAP) provides actionable guidance for doing just that. Black Duck consultants will partner with your SSP leaders to establish a multiyear strategy tailored to maximize ROI and reduce risk within your organization. Here are a few examples of MAPs:

- **DevSecOps integration.** Integrating security in DevOps (DevSecOps) establishes a security culture within existing CI/CD pipelines without causing additional friction. A DevSecOps MAP gives you a detailed assessment of the people, processes, and technology that support your environment, with focused recommendations to enhance security across the SDLC.
- **Cloud security.** Most organizations probably already have applications in the cloud or are in the process of migrating applications and infrastructure to the cloud. But security policies vary significantly between on-premises and cloud environments. Enforcing a consistent security policy across all deployments (on premises, cloud/multicloud, hybrid) is the key to successful risk mitigation. A cloud security MAP lays out a proven plan to help your applications become cloud-ready by providing a checklist of attributes specific to your application and cloud environment that ensure reliable security.
- **Security training.** With the ongoing evolution of AppSec, it's important that staff be trained on software security and products. This is especially important for developers as they are often unaware of AppSec best practices, but it's also important for DevOps engineers, especially as many organizations begin to instill the DevSecOps culture. Black Duck offers both software security courses and product education. Software security training ranges from web and mobile application testing to defensive programming. Product training consists of training on software composition analysis, static application security testing, dynamic application security testing, and more. Flexible training options include both instructor-led private classes and self-paced eLearning courses.

Real-world results

Here are a couple case studies that show organizations starting in their security journey with the help of Black Duck program strategy and development consulting.

- **One of the largest medical device companies in the world** discovered a vulnerability in a medical device that could potentially be exploited by hackers to alter medication dosages to patients and even alter device data and displayed readings. The gravity of this vulnerability was enormous and resulted in the creation of a central security function. Building security in the product development process was identified as an important area for improvement. Since the security program was new, the company partnered with Black Duck AppSec consulting to measure the security program with a BSIMM assessment. After the BSIMM identified areas for improvement the company established an achievable roadmap with a CI/CD MAP. Black Duck consultants then helped with a successful and on-time CI/CD implementation. The company also leveraged eLearning to train developers on secure coding best practices. The program was a tremendous success that ultimately led to the promotion of the program sponsor.
- **A top five pharmaceutical company** reached out to Black Duck AppSec consulting services because it was inundated with vendor emails expressing concerns about the NotPetya breach. NotPetya was one of the most devastating attacks in history, and a major U.S. pharmaceutical company had just been breached by a NotPetya malware attack. The pharma company had a lot of open source software deployed across all of its applications, so it also wanted to automate API testing in a DevOps environment. The CI/CD MAP was the preferred option as it covered both open source security and CI/CD automation. The final report delivered a comprehensive plan to help achieve open source security and CI/CD goals. The partnership with the Black Duck consulting team was extended to define and document policies, standards, and workflows, including open source and binary scanning, expert triage of results, and remediation. These security initiatives helped the pharma company achieve its compliance goals.

References

1. Kenneth Hall, [Modern luxury vehicles claimed to feature more software than a fighter jet](#), Motor Authority, 2/5/2009.
2. U.S. Department of Homeland Security, [Security in the Software Lifecycle: Making Software Development Processes—and Software Produced by Them—More Secure](#), Software Engineering Institute, 8/2006.

About Black Duck

Black Duck[®] offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.