Buyer’s Checklist: Secure Development Learning Platforms
# Buyer’s Checklist: Secure Development Learning Platforms

## Table of Contents

1. Summary
2. Secure Development Learning Platforms Primer
3. Assessment Criteria
4. About Jon Collins
5. About GigaOm
6. Copyright
1. Summary

Secure development learning platforms (SDLPs) help developers improve software security skills as they work, no matter what their individual security knowledge is. They offer integrated guidance and access to learning materials based on the security needs of developer teams, the software concerned, and its known vulnerabilities and flaws. Leading SDLPs support multiple languages, programming frameworks, and architectures, cover a broad and up-to-date catalog of vulnerabilities, and provide benefits-based, actionable reporting to CISOs and CIOs.

This short paper is aimed at decision makers and technology buyers looking to evaluate security development learning platforms.
2. Secure Development Learning Platforms Primer

Software security is best dealt with as early as possible in the development process. A security flaw costs less to solve the earlier it is discovered and treated, and the cheapest option, of course, is that it never exists at all. This means creating code that is secure from the outset or at least avoids common traps, such as leaving the (back) door open for, say, database injections or buffer overflow vulnerabilities.

While this is great in theory, the practice of “shifting security left” during development can create quite a burden for a number of reasons. First, development does not take place in isolation. The likelihood is that developers will be working on multiple things at once, in a large application, and any security scan could reveal a long list of potential vulnerabilities, not all of which are high priority.

Moreover, not all development teams are created equal. Some engineers are more tuned into the need for good security than others. Skill sets vary across teams, and pressures to deliver will depend on project priorities as well as management competencies. And all of this needs to be considered against a complex, changing background, as teams look to harness a broad set of programming languages and evolving target architectures.

So, what to do? If the problem is one of linking hard data (from scanning software) with softer skills and disciplines, SDLPs may be the answer. They look to address the gap between aspiration—that software is delivered with minimal security risk—and the realities faced by organizations today. SDLPs aim to meet developers where they are, with the knowledge that security is a journey based on building both skills and discipline.

Bringing together training and developmental tools with context-driven knowledge, SDLPs offer a number of benefits across stakeholder groups:

- Developers grow their software security knowledge and skills without hindering innovation and delivery through language- and framework-specific guidance based on their ongoing needs.
- Managers benefit from a learning environment that is embedded within existing practice, which ensures that it fits the need, and gain the ability to track progress over time.
- Application security (AppSec) teams become facilitators and mentors, helping developers prioritize and focus on key areas on an ongoing basis, rather than having to address challenges as they emerge.

Overall, SDLPs enable organizations to reduce code-related security risks and save money by addressing issues found through scanning, enabling developers to focus on innovation rather than fault resolution and rework. At the same time, they enable cross-team interaction and development, helping the organization as a whole. By linking immediate feedback with contextually relevant knowledge and skills, shift-left security becomes something that can happen by default, rather than as a bolt-on.
While SDLPs are applicable to any development scenario, they are particularly useful where organizations are looking to “level up” in some way; for example, to address compliance issues, or where software security has been mandated as an area of strategic focus.

Solution Approaches

**Figure 1** shows how an SDLP brings together training capabilities and context-driven tooling to deliver advisory guidance into the development pipeline. While it can deliver this information preemptively, it can also work with the outputs from vulnerability testing platforms such as SCA and DAST, to create advisory guidance as well as offer and automate fixes.

![Figure 1. SDLPs Combine Training Capabilities and Context-Driven Tooling to Deliver Advisory Guidance into the Development Pipeline.](sourceimage)

As you might imagine, SDLPs are not a one-size-fits-all solution, but need to flex to fit the target organization. Thus, from experience, we have learned to take the following deployment considerations into account:

- **Adopt a “now and next” deployment strategy.** Determine what problem(s) you are looking to address now, then address them while considering how you can build on your progress to enhance maturity.
• **Use measurement as a progress indicator.** Note that progress should be considered in terms of risk reduction—for example, how many high-priority vulnerabilities have been identified and dealt with, rather than training hours undertaken. Time to resolution is also a good metric as it shows skills improvement.

• **Lead secure development from the front.** Successful organizations are those that recognize the importance of good, proactive security practice at all levels. Define who “owns” the challenge of security improvement, and bring in champions who can help teams improve.

• **Understand team structures and roles.** Keep in mind that different teams have different needs. For example, mobile applications teams may face different challenges from those building cloud-native back-end services. Deploying SDLP is an opportunity to understand points of alignment among teams and enhance understanding as a result.

• **Fit with existing working practices.** For example, if an organization has a peer review stage prior to commit, incorporate the creation of a report; if weekly improvement meetings are held, add an agenda item to work on the highest-priority findings.

• **Use integrations to drive behavior.** For example, if a significant problem is not addressed before a commit, you can automatically inform an issue tracking tool so it can be caught prior to deployment.

• **Make it a positive experience.** Rather than subscribing to the notion that security is onerous, make it fun with tournaments, security-themed team-building activities, or by using reports to direct incentives to builders. Consider rewarding success directly.
3. Assessment Criteria

So, what should you consider in a solution? To help you determine how to meet your needs, we have divided the topic into the following areas:

- Table stakes – functionality that should exist in any solution
- Key criteria – further capabilities that may be applicable depending on your needs
- Evaluation metrics – non-functional requirements

You can use the following questions to determine your own needs, by considering whether a certain option is a top priority or a secondary priority for your organization. You may need to consider the needs of different stakeholder groups, in which case you can use this checklist as a workshop tool.

You can then compare your priorities against what a specific vendor provides.
## TABLE STAKES

<table>
<thead>
<tr>
<th>Knowledge sharing</th>
<th>Does the solution enable findings and guidance to be shared within and across teams?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context-specific assessment</td>
<td>Does the solution offer guidance that is applicable to language and architecture concerned?</td>
</tr>
<tr>
<td>Tools integration</td>
<td>Can the solution interface with commonly used CI/CD, static code analysis (SCA), and problem management and collaboration tools?</td>
</tr>
<tr>
<td>IDE seamless integration</td>
<td>Can findings be displayed within IDE editors, similar to a spell checker?</td>
</tr>
<tr>
<td>Management reporting</td>
<td>Does the solution enable dashboards and reports to be generated to fit specific needs, such as progress dashboards and compliance reports?</td>
</tr>
</tbody>
</table>

## KEY CRITERIA

<table>
<thead>
<tr>
<th>Proactive guidance</th>
<th>Does the tool offer guidance that fits the notion of learning pathways? Can these be customized to the organization concerned?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizable automation</td>
<td>Can the solution enable guidance and (automated) responses to be programmed, including reminders and (potentially) external triggers?</td>
</tr>
<tr>
<td>Vertical industry support</td>
<td>Does the solution offer industry- or domain-specific guidance, for example, based on industry vertical, compliance type, and so forth?</td>
</tr>
<tr>
<td>Target setting</td>
<td>Does the tool enable goals to be set, for example, to meet an audit or compliance deadline?</td>
</tr>
<tr>
<td>Gamification and rewards</td>
<td>Are incentives offered for progress and activity, such as leader boards or badges?</td>
</tr>
</tbody>
</table>

## EVALUATION METRICS

<table>
<thead>
<tr>
<th>Flexibility/ubuality</th>
<th>Can the tools be configured to meet the needs of the organization and its maturity level on an ongoing basis?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scale to large teams</td>
<td>Can the tool facilitate working in smaller groups and roll up information and guidance to larger groups?</td>
</tr>
<tr>
<td>Security of reports</td>
<td>Can the insights generated by the solution be stowed and communicated securely?</td>
</tr>
<tr>
<td>Breadth of coverage</td>
<td>How broad is the solution in terms of guidance offered, and languages and architectures supported?</td>
</tr>
<tr>
<td>Licensing</td>
<td>How well does the solution’s licensing model scale to fit increased use?</td>
</tr>
<tr>
<td>Overall ROI/TCO</td>
<td>Overall, what is the measurable benefit of the solution with respect to cost?</td>
</tr>
</tbody>
</table>

Source: GigaOm 2021
4. About Jon Collins

Jon Collins has nearly 20 years of experience in IT. He has worked as an industry analyst for a number of years, and has advised some of the world’s largest technology companies, including Cisco, EMC, IBM, and Microsoft in product and go-to-market strategy. He has acted as an agile software consultant to a variety of enterprise organizations, advised government departments on IT security and network management, led the development of a mobile healthcare app and successfully managed a rapidly expanding enterprise IT environment. Jon is frequently called on to offer direct and practical advice to support IT and digital transformation initiatives, has served on the editorial board for the BearingPoint Institute thought leadership program, and is currently a columnist for IDG Connect.

Jon wrote the British Computer Society’s handbook for security architects and co-authored The Technology Garden, a book offering CIOs clear advice on the principles of sustainable IT delivery.
5. About GigaOm

GigaOm provides technical, operational, and business advice for IT’s strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm’s advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm’s perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.
6. Copyright

© Knowingly, Inc. 2021 "Buyer's Checklist: Secure Development Learning Platforms" is a trademark of Knowingly, Inc. For permission to reproduce this report, please contact sales@gigaom.com.