immersive

DevSecOps Culture Maturity

Benchmark Assessment Worksheet

May 2025

Prove

Security Culture Benchmark Assessment Worksheet

Instructions:

For each item, check the box if it has been completed or is in progress. Answer the questions thoughtfully and add notes as needed.

1. Security Culture Baseline Assessment

Use the categories to understand your current DevSecOps Security Culture maturity. Remember to capture key findings and highlight your most significant security concerns or gap.

□ Evaluate security awareness & training.

□ **Assessed developer understanding of secure coding principles**

Questions:

What are the perceived knowledge gaps among developers? How practical is our current training?

Notes:

□ Evaluate existing security processes.

□ **Assessed integration of security reviews into development workflows**

Questions:

At what stage of the development lifecycle are security reviews conducted? How can we shift them "left"?

Notes:

□ Evaluate tooling & automation.

- □ Captured a complete list of existing, relevant security tools and costs
- □ Conducted survey to understand current user knowledge and use of existing, relevant security tools

Questions:

Are developers knowledgeable about and effectively using the available tools? What new tools might be needed?

Notes:

□ Evaluate inter-team collaboration.

- □ Conducted survey to understand current communication tools, processes, and alignment between security and development teams

Questions:

What are the current communication barriers between security and development? Is anything working, which might be replicable or scalable? If not, how can we foster better collaboration?

Notes:

□ List utilized tools (e.g. internal security audits or maturity models, like OWASP).

- □ Tool:
- □ Tool:
- □ Tool:

Questions:

What key insights did the chosen tool provide? How will these insights be used?

Notes:

2. Understanding The Human Element

Now, learn what motivates and deters DevSecOps personas when it comes to participating in security initiatives.

□ Document any disconnect between security professionals and developers.

Questions:

What specific examples illustrate a disconnect? Are any internal practices or culture norms undermining efforts? How can we bridge gaps?

Notes:

□ Evaluate developer motivations (speed, functionality, rewards, etc.).

Questions:

How can we align security goals with developer motivations? What incentives can we offer?

Notes:

□ Evaluate security professional motivations (holistic protection).

Questions:

How can we communicate the importance of holistic security to developers?

Notes:

□ Analyze the "Why" behind security mindsets.

Questions:

What are key pain points—such as the hassle of debugging after a security breach—that help make security a priority? How can we use these insights to promote secure coding practices?

Notes:

□ Establish team to lead-forward, planning how to bridge the gap between different groups.

Questions:

Who should be involved to support cross-team alignment? What are the deliverables and associated timelines? How can we improve collaboration and communication?

Notes:

3. Defining Initial Metrics

□ **Document current metrics used to hold developers accountable (e.g. velocity, output).**

Questions:

How do these metrics influence developer behavior?
What adjustments might be needed to promote security outcomes achievements?

Notes:

□ **Document current metrics used to hold security professionals accountable (e.g. incident response).**

Questions:

How effectively do these metrics measure security performance?
Are there opportunities to promote cross-team collaboration or otherwise support desired outcomes?

Notes:

□ **Discuss how to add security metrics to developer metrics.**

Questions:

What specific security metrics could be added or adjusted?
How will metrics be tracked and measured?

Notes:

immersive

Be Ready

Immersive is trusted by the world's largest organizations and governments, including Citi, Pfizer, Humana, HSBC, the UK Ministry of Defence, and the UK National Health Service. We are backed by Goldman Sachs Asset Management, Ten Eleven Ventures, Menlo Ventures, Summit Partners, Insight Partners and Citi Ventures.

www.**immersivelabs**.com | sales@immersivelabs.com