VERACODE

Communicating Application Security Success to Your Executive Leadership

A working group made up of members of the Veracode Customer Advisory Board (CAB) set out to define a set of metrics that CISOs and application security program managers can use to establish, drive adoption, and operationalize an application security program. These data points should help inform decisions at different stages of program maturity while answering the basic question: **is the application security program effective or not?**

1 → Metrics to **Establish the Need for AppSec**

AppSec managers need a justifiable AppSec approach and dataset that set parameters around the program, give a starting point, and set up how the program will grow over time. That approach starts with providing evidence that an application security program is necessary and that it will reduce risk.

Evidence that AppSec is needed

Contain a security flaw on initial scan[1]

3.86 million

The average total cost of a data breach[3]

Contain a security flaw in an open source library on initial scan[1]

↑ 34%

Cyberattack increase since the start of the pandemic[2]

Evidence that AppSec programs reduce risk

11.5x faster

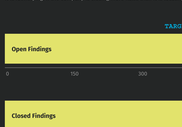
Organizations scanning for security the most (more than 300 times per year) fix flaws 11.5x faster than organizations scanning the least.[2]

2 → Metrics to **Prove Adoption**

AppSec success hinges on development buy-in and engagement. Therefore, proving that your AppSec program is effective requires evidence of developer adoption.

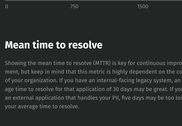
Use of integrations

The most effective AppSec programs integrate seamlessly into developers processes and tools. So, an important metric to highlight application security success is the rate at which development teams are taking advantage of APIs to integrate security into their processes.



Fix rate

Finding vulnerabilities is not the end goal; fixing flaws is. Use the fix rate to understand where training or resourcing investment is needed.



Number of findings closed
÷
Number of findings open
=
Fix rate

3 → Metrics to **Prove Success**

Rather than a one-off initiative, effective application security is ultimately a component of the software development process, just like QA, and the measures of success need to reflect that.

Correlation of early security testing to number of security findings

The "early testing vs. later flaws" metric illustrates how changes in the development process are having a downstream effect that is reducing the costly exercise of fixing security flaws in production.

Findings open to close ratio

The open to close ratio illustrates whether the organization is resolving more security findings than it is identifying. If the company is closing more flaws than it is locating, it is truly reducing risk.

Mean time to resolve

Showing the mean time to resolve (MTTR) is key for continuous improvement, but keep in mind that this metric is highly dependent on the context of your organization. If you have an internal-facing legacy system, an average time to resolve for that application of 30 days may be great. If you have an external application that handles your PII, five days may be too long for your average time to resolve.

Corrective maintenance time
÷
Total number of corrective maintenance actions
=
Mean time to resolve (MTTR)

Policy compliance

The percent of applications in your AppSec program that are in compliance with your AppSec policy is a clear and concise way to prove AppSec success. However, the success of this metric depends on whether you have established the right policy for your organization. Begin with achievable policy standards.

Vulnerabilities identified by pen test

early scanning vs. pen testing

You can illustrate AppSec success by comparing the number of early security tests with the types of flaws identified by pen testers. You should see that you're no longer wasting expensive pen testing dollars on flaws that automated scans picked up.

Benchmarking against your peers

Communicate AppSec success to executives with peer benchmarking. Provide executives with a frame of reference using the state of software security among peers and the comparison to the current state.

For example, use Veracode's annual State of Software Security report to compare your numbers to others in your industry and all other Veracode customers.

For more information on using metrics to justify and confirm the effectiveness of your application security program:

Check out our recent CAB report, *Communicating Application Security Success to Your Executive Leadership*

1 State of Software Security: Volume 11
2 SC Media: COVID-19 accounts for most 2020 cyberattacks
3 Ponemon Institute: 2020 Cost of a Data Breach report
4 State of Software Security: Open Source Edition
5 State of Software Security: Volume 9

VERACODE