CHECKMARX

ROI of Shifting Left

Defining the ROI of AST

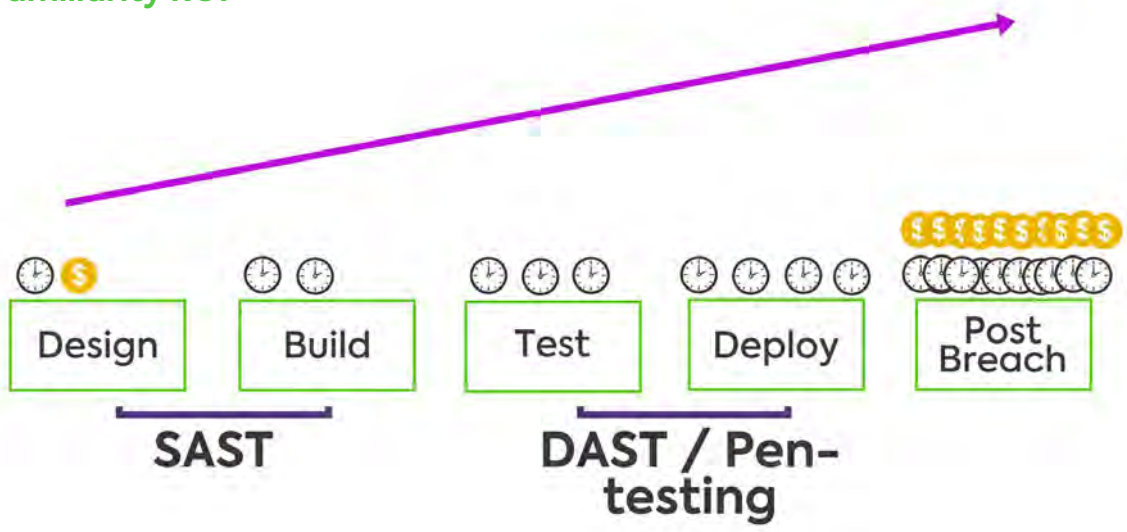
A key differentiator for application security testing solutions (AST) is the ROI that each method brings to the organization. AST ROI can be measured in terms of **cost** of company resources in dollars, personnel and **time** needed to remediate detected vulnerabilities.

Proximity to Code

For developers writing 50 of the lines of production code (LoC) per day, the price for "boltingon" security at the end of the development cycle is critical. For a two week turnaround time from when the code was written to when it is sent back to developers for mitigation, that time can feel like eternity. By this time, the developer may be 500 LoC away from when they started.

When organizations discover code flaws that need to be mitigated, regardless of whether it is a quality or security related flaw, remediation needs to be done ASAP in order to minimize the the time needed to fix the flaw. By scanning code in its raw source code format, Checkmarx is able to push security to the left, and hook into the development process as soon as the code is created, thus significantly minimizing the delays.

Code Familiarity ROI



Shifting Security Left Frees Up Company Resources

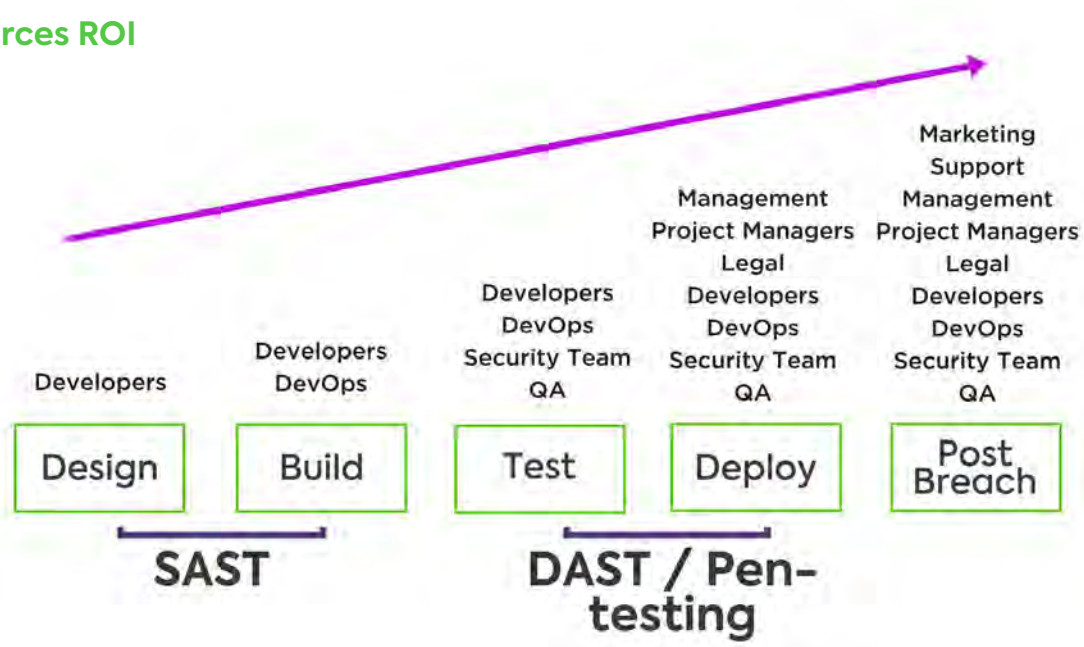
In addition to ensuring that developers are able to remediate vulnerabilities on code that they're familiar with, shifting security left also lessens the amount of personnel needed to help mitigate the damage (or potential damage) of the flaw.

As code progresses out of the development stage in the software development lifecycle (SDLC) before the application reaches production, an exponential increase in manpower needed as the code gets further away from it's original creator. Once code reaches the build stage, DevOps teams must also get involved in the remediation as delays in release cycles may clog the release pipeline. In the testing stage, where most traditional security solutions are retro-fitted on late in the development cycle, members of the security and QA teams must also join the remediation efforts.

If code with a exploitable vulnerability makes it into production, the crowd needed to prevent a potential crisis grows even larger as management must get involved, legal teams may need to assess any consequences if the flaw is exploited and project managers will need to reschedule any project timelines as employees from a variety of teams may need to stop what they're doing to help with the mitigation efforts.

With AST solutions, such as SAST, that scan in the early stages of development, there is no costly crowd needed for remediation. Here, the developer is able to quickly mitigate flaws in code that they already familiar with.

Resources ROI



Shifting Left with Checkmarx Will Make A Big Impact on Your Organization's Bottom Line

According to the Ponemon Institute, vulnerabilities detected on production cost 100 times more to remediate than those discovered in the design stage of development in the SDLC, where Checkmarx identifies them.

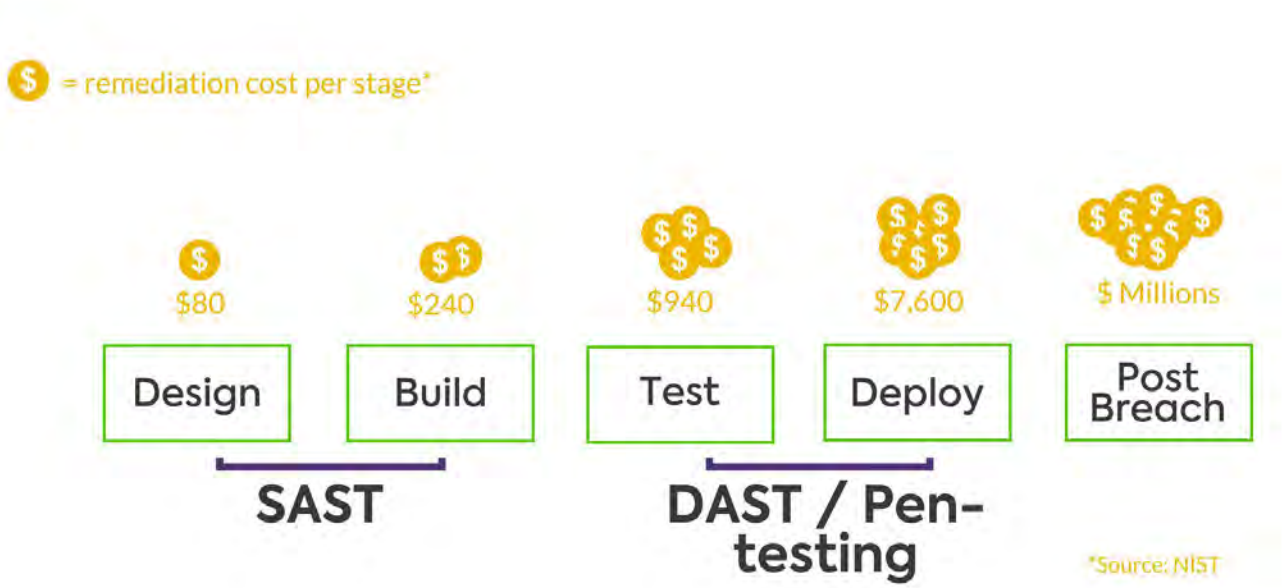
Shifting left with Checkmarx's CxSAST allows automation at every step in the software development stages which translates into savings at every integration point in the SDLC as the costly resources that need to be invested in vulnerability detection are significantly reduced.

Checkmarx includes the ability to incrementally scan only new, or edited, code which also adds savings as scan times are reduced and there is no need to scan tens of thousands of lines of code as needed with other solutions.

Unlike security testing done with DAST or pen-testing tools, Checkmarx's CxSAST has access to the source code which allows it to show developers exactly where code flaws are located, thus saving precious remediation time. Checkmarx's "best fix location" provides a graph view that maps out problematic lines of code which allows developers to remediate multiple vulnerabilities with a single fix which significantly reduces the number of code changes the developer has to go through. The time saved allows applications to make it to production faster and frees up developer time for other projects.

Companies using SAST scanning early in the SDLC enjoy the amount of savings that result in no longer relying on the expensive and lengthy delays from pen-testing.

Cost of Remediation ROI



About Checkmarx

Checkmarx is an Application Security software company whose mission is to provide enterprise organizations with application security testing products and services that empower developers to deliver secure software faster. Amongst the company's 1,400+ customers are five of the world's top ten software vendors and many Fortune 500 and government organizations, including SAP, Samsung, and Salesforce.com.