VERACODE

VOLUME 11

The State of Software Security
Regional Snapshot: Europe

Veracode's State of Software Security (SOSS) Volume 11 focused on how developer actions influence software security. It also looked at the impact attributes about the application and the development environment can have on how quickly flaws are fixed. This infosheet provides a summary of the factors that shape software security for European firms compared to their global brethren.

Figure 1 describes how applications compare across different regions in finding and fixing flaws. From left to right, the columns rank each major geographic region by the proportion of applications with flaws, the proportion of applications with high-severity flaws, the percentage of flaws that are fixed, and the median speed at which flaws are fixed. In this figure, European firms are tied with Asia Pacific for having the largest percentage of applications with any flaws and at the very bottom for having applications with high-severity flaws. When it comes to the remediation rate and the amount of time spent fixing flaws, European firms have a brief highlight with the second highest overall fix rate, but again struggle when it comes to the typical time to fix vulnerabilities, coming in at close to nine months. It appears that European firms are struggling with their overall security fix effectiveness. While these firms are able to get issues corrected eventually, the time it takes them to accomplish that goal is not sufficient given the rate of discovery.

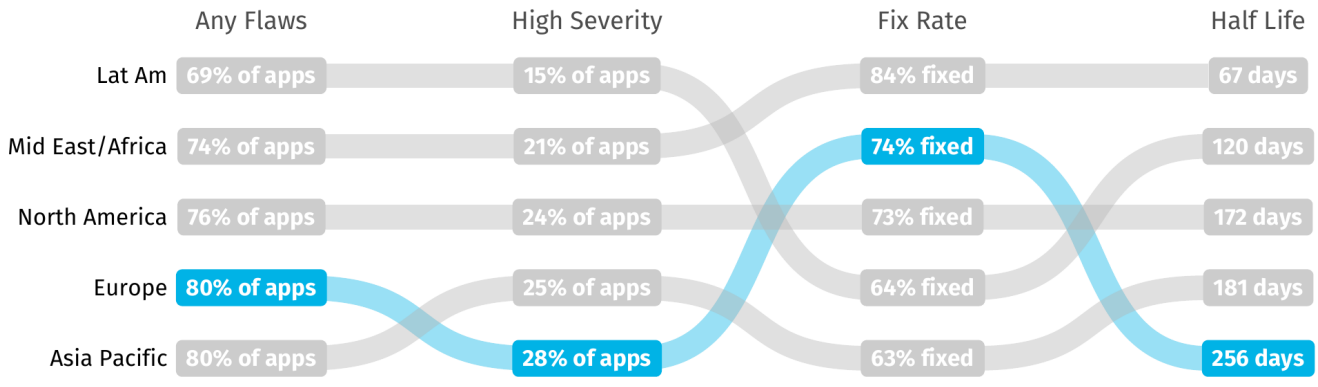

Figure 1: Values and rankings for key software security metrics by region.

In Figure 2, we show a more detailed view of the flaw types discovered in applications. The left axis shows the overall prevalence of each flaw category across all regions, and the right axis shows the prevalence of each category for European firms. This figure shows that the prevalence of several common flaw types are different compared to the overall global rates. The data suggests that European developers most frequently encounter issues related to CRLF infection and code quality, with time and state issues being found much more often in European applications than typically discovered, though this last category is still one of the least commonly found in applications from this region.

In this year's SOSS, we see strong evidence that certain developer behaviors associated with DevSecOps yield substantial benefits to software security. In Volume 10, we discovered that teams scanning applications most frequently carry five times less security debt than infrequent scanners. In this year's volume of the SOSS, we uncover additional developer actions that make a difference in fixing security flaws in software.

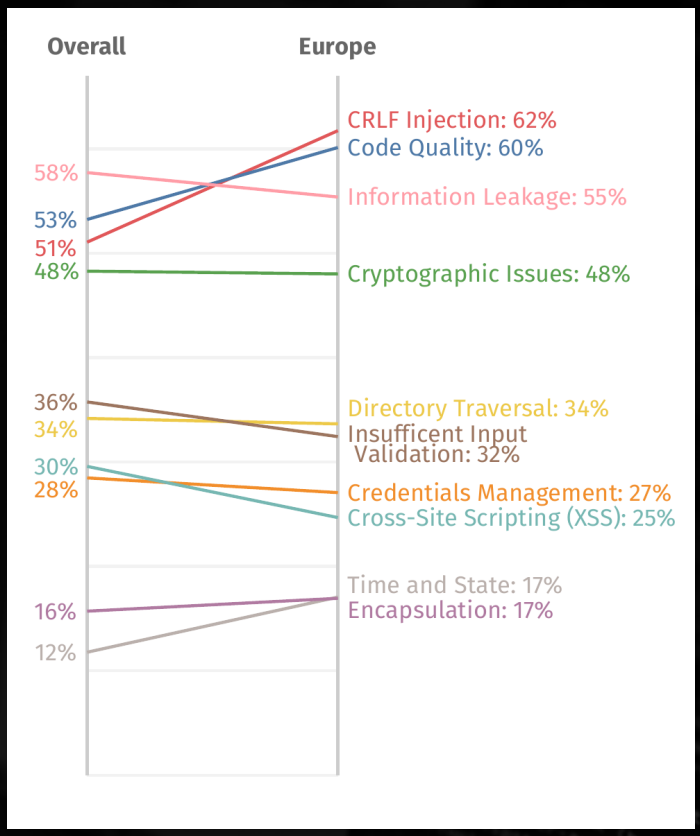

Figure 2: Prevalence of flaw categories in European firms.

In SOSS Volume 11, we looked at the impact attributes about the application and the development environment can have on how quickly flaws are fixed in software. There are some attributes that developers have no control over and others, such as best practices, that developers can influence.

In Figure 3, we look at how European companies compare with firms across the world in their development attributes (nature) and their adoption of helpful developer behaviors (nurture). The data shows European firms have a mix of leading and trailing attributes. Going from left to right for the developer attributes, European firms in the SOSS have the oldest applications, make up the largest of organizations, and have application sizes that are close to the largest worldwide, yet the density of flaws in applications are relatively good. It appears that the environment for most European developers consists of larger, more established firms with legacy codebases. In contrast, European firms tend to be strong adopters of DevSecOps behaviors, with scan cadence, software composition analysis, and dynamic analysis being world leaders (or second place at worst). On integrating security testing into the development process (using the API), European developers show middle-of-the-pack in performance. The only developer behavior European firms seem to struggle with compared to other regions is in the overall frequency of scanning – while their cadence, or regularity, of scanning is excellent, European developers aren't scanning very often.

In the most recent SOSS, we see that certain factors are likely to lead to flaws getting fixed faster, and others lead to slower fixes. Region is something developers don't have control over, so how does the local geography affect the time to remediate flaws?

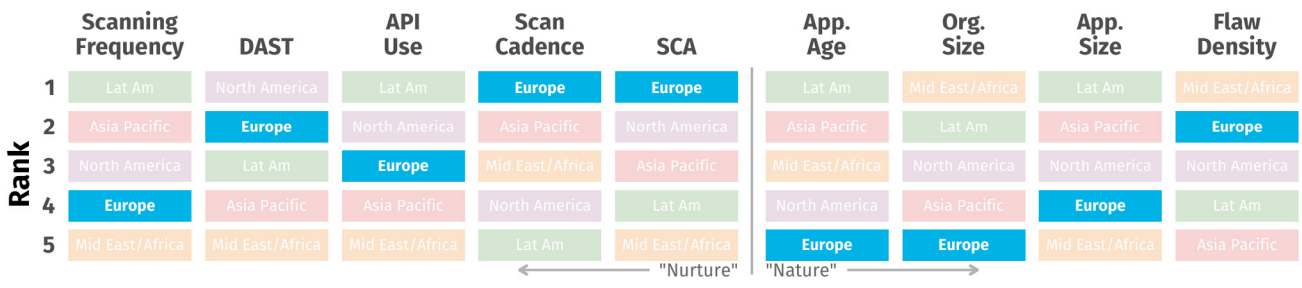

Figure 3: Relative ranking of European firms for attributes and actions associated with application security performance

Figure 4 shows that being based in Europe means the firm is more likely to remediate flaws over 31 days slower than other parts of the world. We saw in Figure 3 that European developers firms utilize several DevSecOps behaviors, despite typically working in environments with negative attributes. We clearly see the impact of that combination in Figure 4 as the data trends towards slower flaw remediation. It goes to show that developers' actions have a long road to overcome an organizational legacy of security and technical debt. Actions can matter, but it takes concerted and sustained effort.

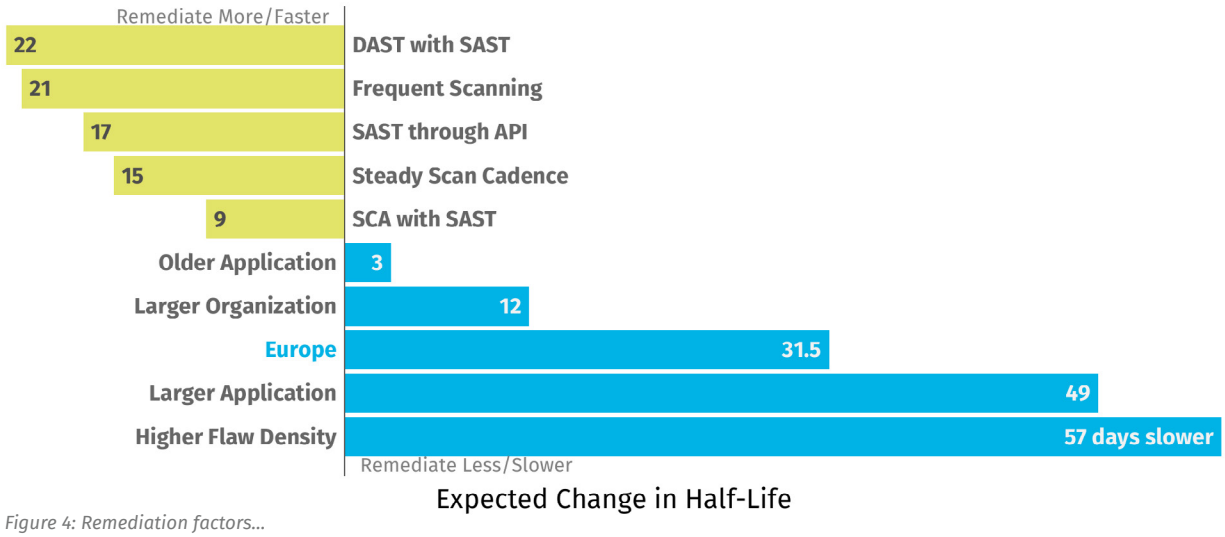

Figure 4: Remediation factors...

VERACODE

Veracode is the leading AppSec partner for creating secure software, reducing the risk of security breach and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of automation, integrations, process, and speed, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities. Veracode serves more than 2,500 customers worldwide across a wide range of industries. The Veracode cloud platform has assessed more than 14 trillion lines of code and helped companies fix more than 46 million security flaws.

www.veracode.com Veracode Blog Twitter

Read the Full Report

TO LEARN MORE ABOUT SOFTWARE SECURITY, CONTACT US.