PARASOFT
Automated Software Testing

DevSecOps

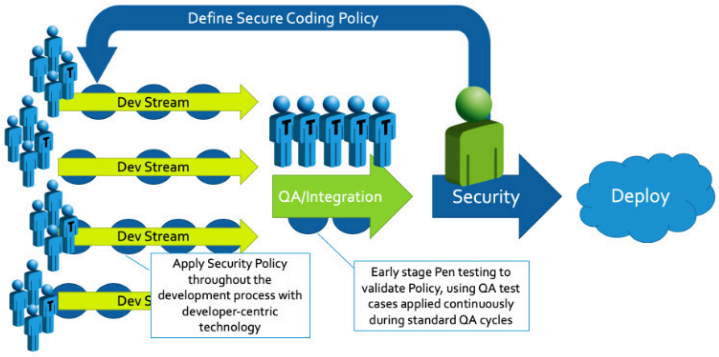
DEVELOPMENT & DEVOPS INFRASTRUCTURE

CREATE SECURE APPLICATIONS WITHOUT DISRUPTING THE DEVELOPMENT PROCESS

Parasoft makes DevSecOps possible with API and functional testing, service virtualization, and the most complete support for important security standards like CWE, OWASP, and CERT in the industry.

BENEFIT FROM THE PARASOFT APPROACH

- ✓ Leverage your existing test efforts for security
- ✓ Combine quality and security to fully understand your software
- ✓ Harden the code – don't just look for bugs/vulnerabilities/or weaknesses
- ✓ Reduce audit costs with ready-to-audit reports for each secure coding standard



PARASOFT

www.parasoft.com

PARASOFT'S APPROACH - BUILD SECURITY IN

Parasoft provides tools that help teams begin their security efforts as soon as the code is written, starting with static application security testing (SAST) via static code analysis, continuing through testing as part of the CI/CD system via dynamic application security testing (DAST) such as functional testing, penetration testing, API testing, and supporting infrastructure like service virtualization that enables security testing before the complete application is fully available.

IMPLEMENT A SECURE CODING LIFECYCLE

Relying on security specialists alone prevents the entire DevSecOps team from securing software and systems. Parasoft tooling enables the team with security knowledge and training to reduce dependence on security specialists alone. With a centralized SAST policy based on industry standards, teams can leverage Parasoft's comprehensive docs, examples, and embedded training while the code is being developed. Then, leverage existing functional/API tests to enhance the creation of security tests – meaning less upfront cost, as well as less maintenance along the way.

HARDEN THE CODE ("BUILD SECURITY IN")

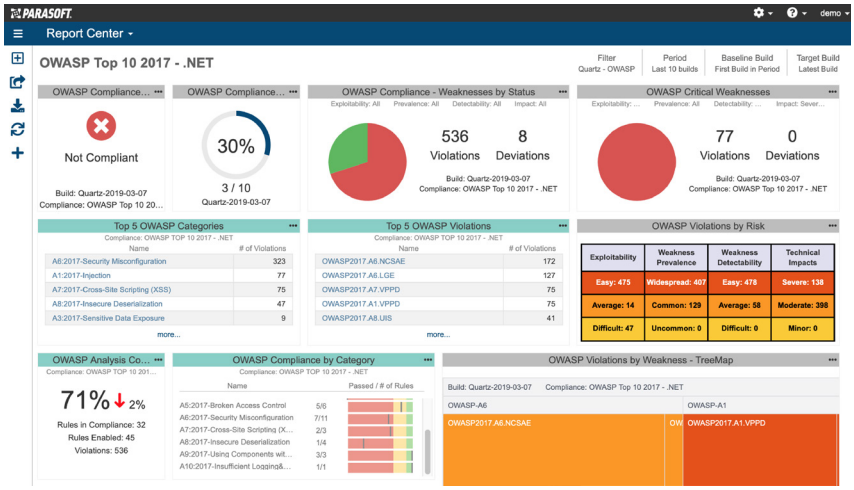
Getting ahead of application security means moving beyond just testing into building secure software in the first place. Best practices for secure software are encapsulated in secure coding standards like CWE, OWASP, and CERT. Parasoft provides complete coverage of these standards, in the IDE and the CI/CD pipeline, to ensure secure engineering standards in SAST. To streamline secure coding compliance, Parasoft provides a standards-centric configuration and reporting dashboards that include "mapless" checkers to guidelines. And everything is integrated with your build and CI plugins so it works with your unique processes and workflows.

START SECURITY TESTING BEFORE THE APPLICATION IS EVEN FINISHED

To keep up with today's short release cycles and agile development, it's necessary to start testing your code not just before deployment, but even before integration. With Parasoft, SAST can run right inside the IDE so that it checks the code before the developers ever check it in. Functional testers can leverage functional/API tests to perform security testing, making it quicker and less intrusive (not to mention a lower cost of maintaining separate tests), and ser-vice virtualization enables teams to decouple from expensive dependencies, as well as versions of services that don't yet exist.

PARASOFT DASHBOARDS AND REPORTS MAKE IT EASIER TO UNDERSTAND RISK

Security is still being left as a gate at the end of the pipeline, where it's difficult to fix security issues when the product is halfway out the door. A bigger cultural shift needs to occur, shifting security testing to as early in the software delivery process as possible. This requires security best practices to be integrated into the developer's daily activities to ensure that vulnerabilities are not discovered at the last moment and releases aren't delayed or shipped with known vulnerabilities.



Parasoft provides not just audit reports and histograms, but modern analytics that help you understand whether it's safe to deploy your software and what the impact of security violations found in your code are based on industry standards for risk, technical impact, likelihood and more. A wide array of dashboards, widgets, and reports let you know which code is risky, what level of risk you have, and where you need to concentrate your efforts.

SUPPORTED STANDARDS

CWE (Including 2019)
- Top 25
- On the Cusp
- + more

OWASP Top 10

CERT C, CERT C++

(rules & recommendaations)

PCI-DSS

UL-2900

SUPPORTED INFRASTRUCTURE

Azure
AWS
Jenkins

PARASOFT'S AUDIT-READY REPORTS

Today's regulatory environment means that software security has moved from a "nice-to-have" feature to an auditable requirement. You need a system that organically keeps track of your security efforts, to make it easier to produce any and all materials necessary for expected audits against required standards like CWE and OWASP.

With Parasoft, reports include status, history, deviations, compliance plans, and other necessary materials to submit for audits. Dashboards and reports use naming conventions from the standards, to ensure that users don't have to map rules or massage reports for audit requirements.

Parasoft makes it easy to prove that you've implemented the complete standard, you know which checkers go with which guidelines, ou know what you ran and what the outcome was, and you know which deviations were permitted, when, and by whom. With all this information at your fingertips, you can prove that you've done all the right things to secure your code with confidence.

PARASOFT CUSTOMERS

U.S. NAVAL RESEARCH LABORATORY
NAVSEA NAVAL SEA SYSTEMS COMMAND
LOCKHEED MARTIN
L3HARRIS
Raytheon

PARASOFT®
Automated Software Testing

Parasoft Corporation
101 E Huntington Drive Monrovia, CA 91016 USA
Sales: 1-888-305-0041 | International Sales: +1-626-256-3680
www.parasoft.com