SYNOPSYS®

WHITE PAPER

Managing Web Application Security With Coverity

Any application connecting to the internet runs the risk of being targeted by malicious hackers, so securing these applications is critically important. Financial services, healthcare, insurance, and e-commerce are a few of the many industries that rely on web applications to provide services, collect information, communicate, and more. Failing to fix critical vulnerabilities can result not just in financial damages and legal liabilities, it can also ruin an organization's reputation.

A recent example of this is the 2017 Equifax data breach, in which hackers utilized a known vulnerability in the Apache Struts framework that Equifax had failed to fix, even after a warning from security researchers. For more than two and a half months, hackers stole the sensitive data of more than 147 million users from Equifax servers. This hack resulted in hundreds of millions of dollars in losses, and the company's reputation continues to suffer today.

The COVID-19 pandemic has only accelerated this peril. Since the beginning of the pandemic, the FBI has reported a 300% increase in cyber crimes. Traditionally, cyber security spending was focused on securing the network layer to prevent or deter such malicious attacks. However, organizations are realizing that application security is equally important.

Understanding how static analysis can help

It's important to understand the major factors in securing web applications. Specifically, who is responsible for ensuring security, where in the software development life cycle (SDLC) security testing is performed, and what kinds of security testing can be useful.

A recent industry report highlighted how the responsibility for security is shared across teams. For a DevSecOps strategy to be successful, security managers must ensure that application security policies and solutions don't impede developers. Developers are under constant pressure to deliver applications faster, and they will resist any security testing solution that slows them down or causes tool fatigue. Security testing solutions must empower developers to write secure applications and fix vulnerabilities before submitting their code to the production environment, without getting in their way.

Static application security testing (SAST) or static analysis solutions inspect static code automatically by analyzing data flow and control flow paths, and identifying quality issues and security vulnerabilities. A SAST solution that can find defects accurately, quickly, and in the developer's environment helps ensure developer adoption while helping to achieve the organization's security objectives.

Today's web applications are developed at scale, and in highly agile environments. With the speed at which applications are produced today, it's no longer economically feasible to employ security testing only at the production stage. To help organizations build security into their workflows, SAST tools must fit seamlessly into the stages of the software development life cycle. They should also integrate seamlessly into developer IDEs or SCMs and display findings and remediation advice directly in those environments. This allows developers to find and fix the vulnerabilities as they write the code, and before submitting it to production environments.

For security managers, a dashboard that compiles the findings produced by SAST tools can provide continuous visibility into the risks associated with the applications. It also helps them assess compliance with various application security standards. The Open Web Application Security Project (OWASP) provides tools and resources to help secure web applications. The OWASP Top 10 and CWE Top 25 are industry standards comprised of lists of application security risks that can lead to data breaches. Similarly, there are security and data handling standards for specific industries, such as PCI DSS for the financial services industry. A SAST solution that can identify these security risks and help ensure compliance to industry standards can help development and security teams minimize risks in their web applications.

Providing what developers and security managers need

Coverity® empowers developers by providing actionable findings, relevant training resources, and remediation advice in their IDE, via the Code Sight™ IDE plugin. This enables developers to fix security issues in their code as they work. For security managers, Coverity provides a high-level view into application risks and exploitable vulnerabilities through compliance reports for key industry and security standards. For DevOps managers, Coverity provides flexible deployment options, either on premises or in the cloud, as well as integrations into various stages of the SDLC. In addition to the customizations available for Coverity installation, the Coverity CLI provides a very simple way to onboard applications and see results as well as diagnostics of the scan.

Security practitioners can utilize the simplified Coverity CLI to initiate scans by just pointing to the source code, without needing to specify build and configuration details. With this unique analysis technique, Coverity can automatically determine if a build is

required and initiate it based on the environment. The diagnostics information also provides metrics about how successful the file capture and analysis have been, so users can have confidence in the analysis results.

Once analyses are complete, security teams can easily generate reports on the critical vulnerabilities specified by security standards such as OWASP Top 10 and CWE Top 25, or industry standards such as PCI DSS and SEI CERT. Coverity can help security teams demonstrate security and compliance by providing:

- **Reporting aligned to security and industry standards.** Dashboards and reporting that cover the entire application portfolio, issue trends, and more provide auditors, executives, and heads of development with high-level visibility into application risk and compliance to security and industry standards.
- **Automated vulnerability prioritization.** Prioritizing vulnerabilities according to compliance standards, criticality, and custom rulesets helps focus development resources on the most important security vulnerabilities to be remediated.
- **Policy management via Intelligent Orchestration.** Used in conjunction with Synopsys Intelligent Orchestration, Coverity can automatically initiate SAST testing on your application, based on user-defined policies, risk profiles, and severity/context-specific code changes.
- **Comprehensive security coverage.** A wide range of coverage across industry and security standards help organizations assess and ensure compliance.

Prioritizing resources with centralized dashboards

For a CISO, a dashboard that provides a high-level overview of risks across the application portfolio is vital to prioritizing resources and fixing critical vulnerabilities. For example, a web application that utilizes a SQL database in the back end to respond to user queries must be protected against any injection-related vulnerability, so fixing those types of vulnerabilities will be a high priority before the application is deployed. A dashboard with a high-level overview across applications can help quickly find the applications reporting SQL injection vulnerabilities, so security teams can focus development resources to fix them.

Such a dashboard can also help security teams focus on factors such as assessing compliance to important security and industry standards. To help with this, Coverity provides:

- **Scan health and diagnostics.** Scan diagnostics help clarify how successful the scans have been, and identify any anomalies that may lead to an inaccurate risk assessment of the application.
- **In-depth reports with comprehensive risk analysis.** Detailed security reports help organizations assess and address a variety of business priorities, such as responding to auditors, gaining customer confidence, analyzing business impact for technical debt, and more.
- **Defect reports based on standards or other industry-recognized priority lists**. Industry-recognized priority lists such as OWASP Top 10 and CWE Top 25 help organizations filter critical vulnerabilities in the application for a more focused remediation effort.
- **Issue trends.** Trend charts measure progress over time and provide a high-level view into improvements in achieving application security goals. Trend charts can also be used to clarify metrics around time to resolution and age of outstanding issues.
- **Comparative risk profile analysis.** Configurable application risk profile scores provide benchmarks to compare applications with each other for prioritization.

Organizations including OWASP and MITRE (which created and maintain the OWASP Top 10 and CWE Top 25, respectively) provide guidance that helps ensure web application security. Many industry standards, such as PCI DSS and DISA Application Security and Development STIG, reference these lists directly or name the same vulnerabilities.

Figures 1, 2, and 3 on the following pages illustrate how Coverity can generate reports against these industry standards to help organizations and security teams measure their applications' compliance and assess the risk associated with the defects Coverity finds. These reports can be accessed either via Coverity Connect® dashboard or the Polaris Software Integrity Platform® dashboard, with some differences in the way reports are displayed. The issues found can be filtered based on criticality to focus on what matters most to the business.

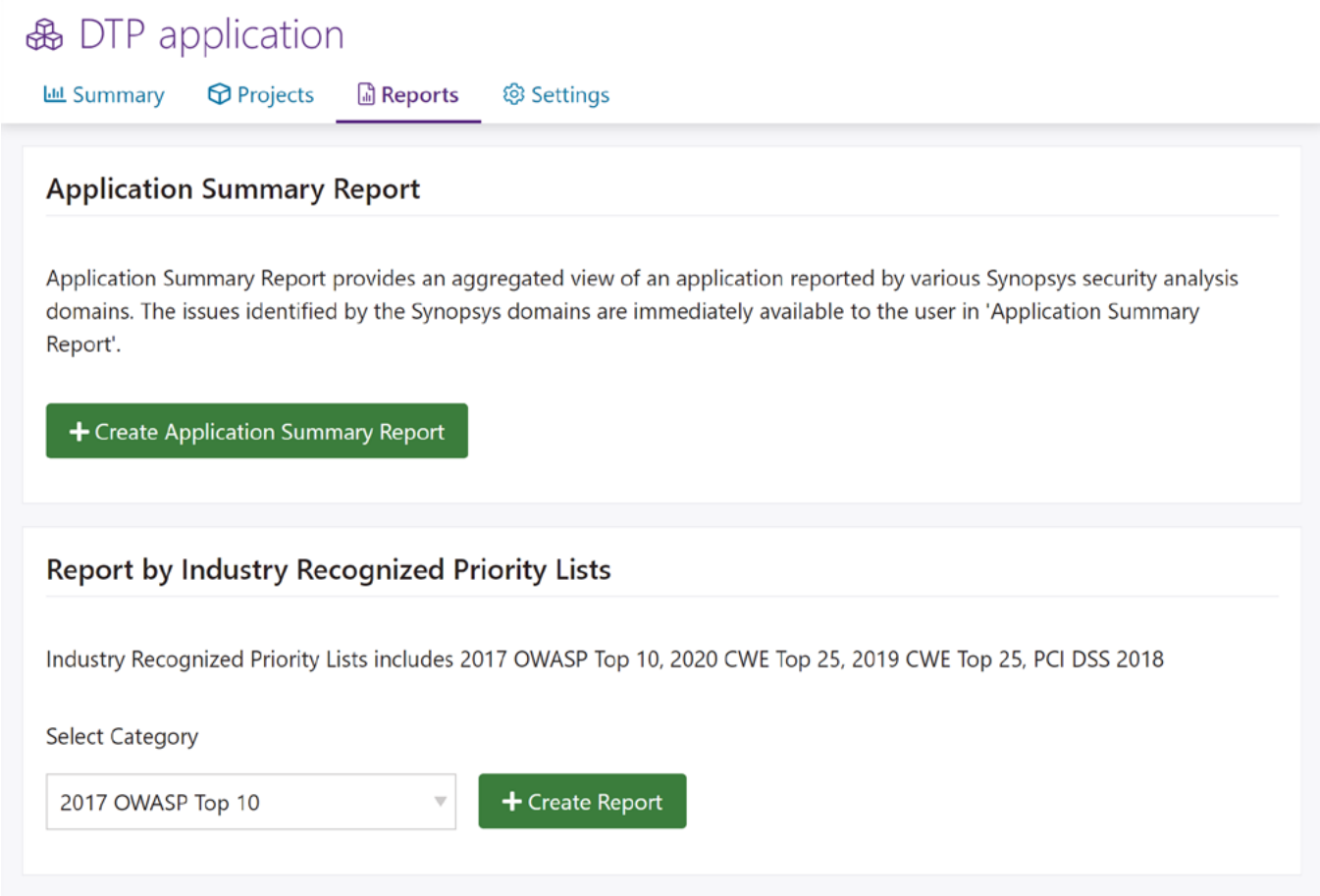

Figure 1: Comprehensive report generation in Polaris Software Integrity Platform

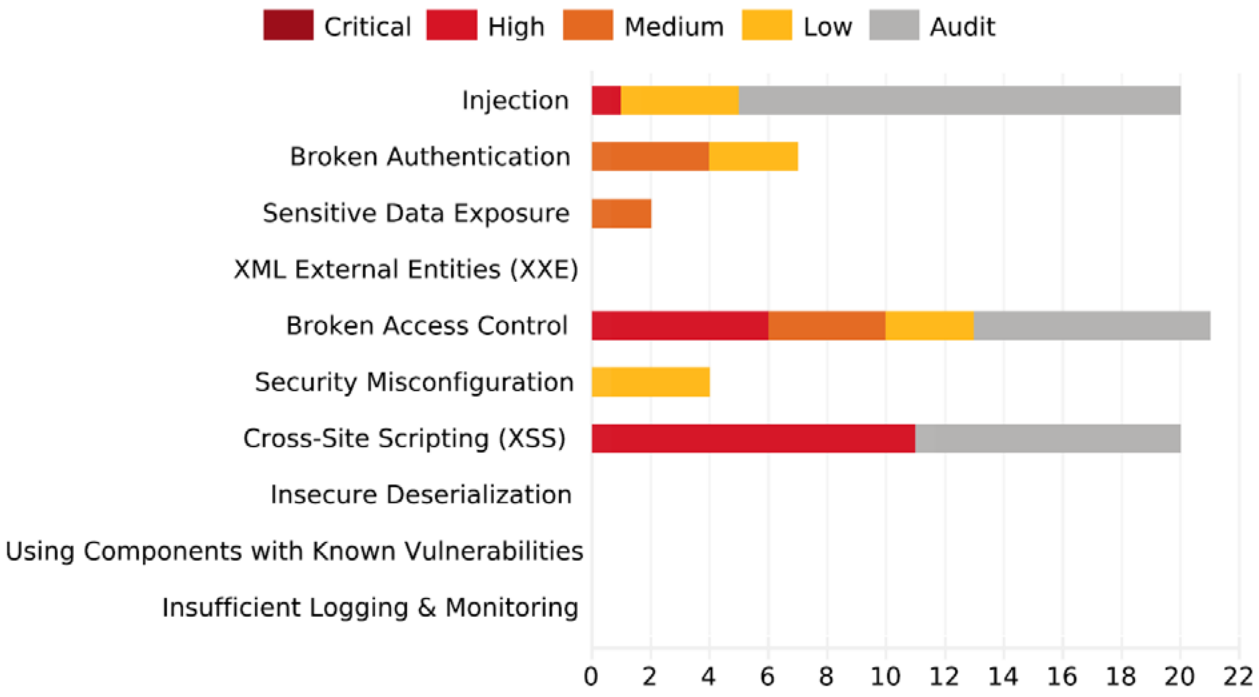

Figure 2: The OWASP Top 10 issues by category as listed in the PDF report, in the order of the Top 10 web application security risks

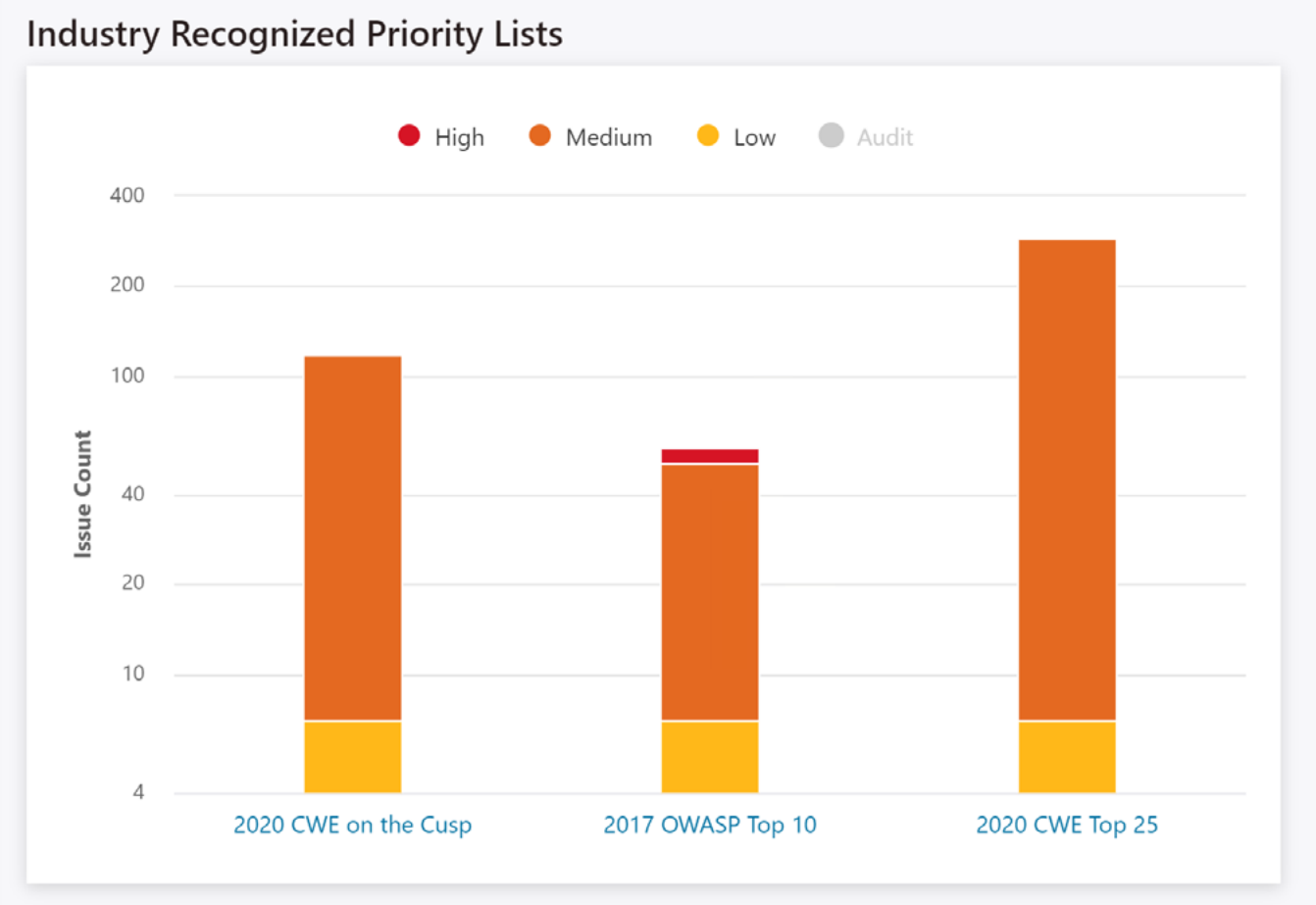

Figure 3: High-level summary of the issues found according to industry-recognized priority lists

The issue trends graph shown in Figure 4 below is generated for every project and updated with each analysis. This helps organizations measure progress over time so they can prove ROI for Coverity and demonstrate improvements to their executives, customers, and auditors. Issue trends also help managers track progress and technical debt pertaining to the issues found. For example, a security team with a goal to reduce the high-severity issues identified by OWASP Top 10 by 50% over a year could monitor their progress with this report.

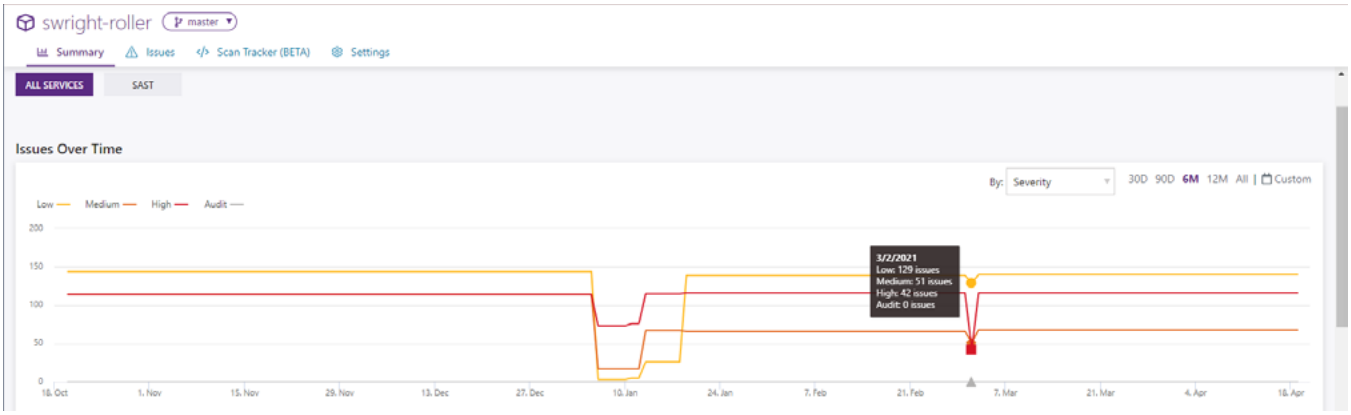

Figure 4: Trend graphs help organizations demonstrate their progress and understand ROI for Coverity

A more detailed report that includes the cause, technical risk, and severity of identified vulnerabilities can be generated to provide application risk analysis, as shown in Figures 5 and 6 below. The vulnerabilities shown in this report can also be ranked based on their severity or grouped by associated technical risks. Coverity assigns each technical risk a severity score based on the business impact of a breach. Security managers can also view those vulnerabilities by issue IDs, by technical risks, and by associated CWEs. The report also includes details about the cause and impact of each CWE, as well as remediation guidance.

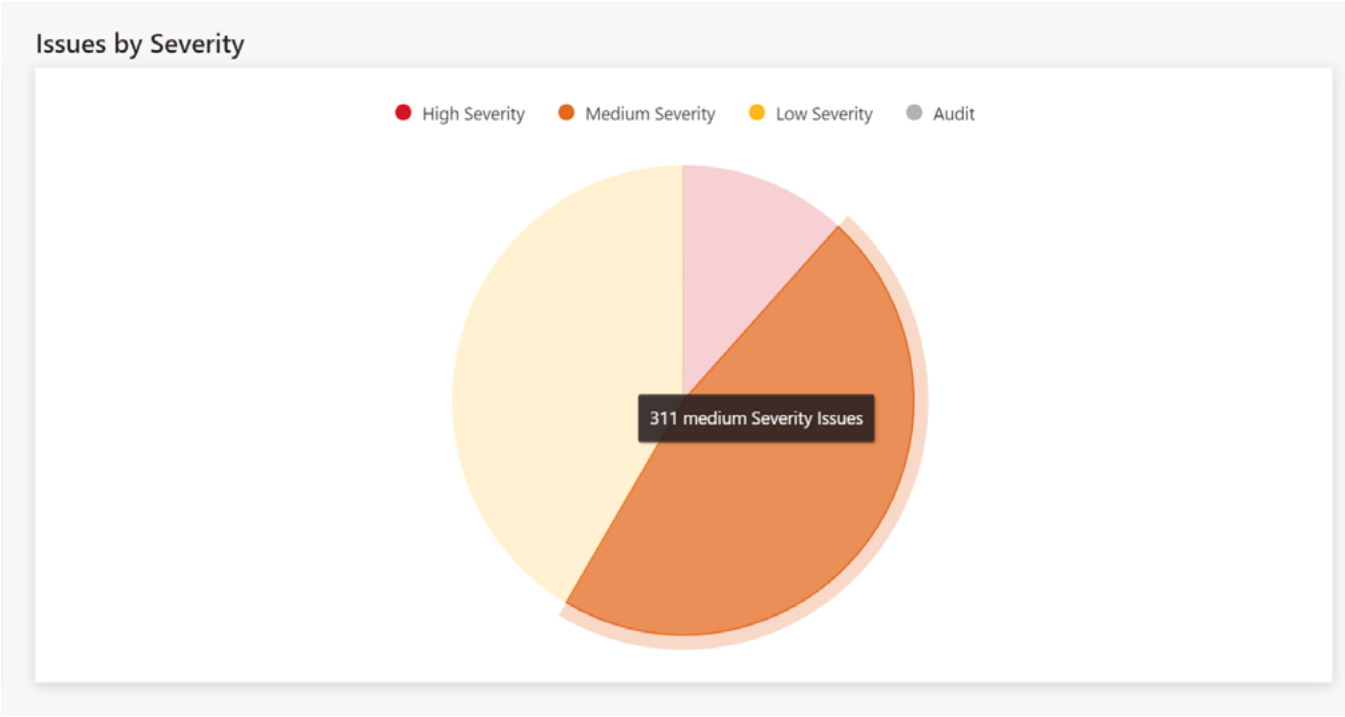

Figure 5: Pie chart providing a high-level view of issues by severity

Categories	Open Issues	Critical	High	Medium	Low	Audit
Injection	20	0	1	0	4	15
Broken Authentication	7	0	0	4	3	0
Sensitive Data Exposure	2	0	0	2	0	0
XML External Entities (XXE)	0	0	0	0	0	0
Broken Access Control	21	0	6	4	3	8
Security Misconfiguration	4	0	0	0	4	0
Cross-Site Scripting (XSS)	20	0	11	0	0	9
Insecure Deserialization	0	0	0	0	0	0
Using Components with Known Vulnerabilities	0	0	0	0	0	0
Insufficient Logging & Monitoring	0	0	0	0	0	0

Figure 6: Detailed security report displaying issue types and severity, to help prioritize resources for the issues that matter most to the organization

Automating vulnerability prioritization

To help reduce developer fatigue and optimize resource utilization, security teams must prioritize which vulnerabilities to fix and which may be considered an acceptable risk. SAST tools can help security teams achieve these objectives by providing precise and automated vulnerability prioritization, as well as automated triage to reduce the burden on security managers.

Coverity can be preconfigured to identify, prioritize, and triage software vulnerabilities during development. It can also notify developers via email or create Jira tickets when security weaknesses that meet predefined criteria are identified. Coverity can also act as a quality gate that will fail builds when predefined criteria are not met. This can alert developers during the code review process. And automated triage workflows can significantly reduce the number of vulnerabilities that make it to the security review process. Security teams can also monitor and review vulnerability dismissals by development teams and approve or reject them to ensure that critical vulnerabilities are fixed.

The vulnerability filtering mechanisms in Polaris allow security teams to filter issues by triage status, severity, industry priority lists, and more. This powerful tool quickly filters identified issues by CWE type, security standard, technical risk, severity, code path, or even owner. This allows security teams to triage these filtered groups to specific developers.

For example, a security organization may choose to filter for CWEs in OWASP Top 10 (2017), CWEs in CWE Top 25 (2019), or CWEs with a high or critical severity rating. All issues meeting the selection criteria are sent quickly to the developers responsible so they can be fixed with high priority.

Polaris also enables oversight into the triage workflow, including the option to limit who can and cannot dismiss issues. And it provides the appropriate notifications for approvals and auditing. Additionally, security managers can review specific issues during triage, so they can make sure business-critical vulnerabilities are correctly fixed. This type of oversight gives the security organization greater control over triage processes.

Managing policies with Intelligent Orchestration

Synopsys Intelligent Orchestration enables teams to integrate application security analysis into their DevOps pipeline while maintaining development velocity. Intelligent Orchestration supports Synopsys AppSec tools (including Coverity for static analysis and Black Duck® for software composition analysis) as well as security services (e.g., threat modeling, penetration testing) and additional custom options: third-party tools; governance, risk, and compliance; and dashboarding systems. It automatically performs the right security tests at the right time based on user-defined policies, risk profiles, and severity/context-specific code changes that are configured by the organization in advance. Risk-based vulnerability reporting ensures that developers need only remediate the most important issues they are assigned to address, and they can do it all within the issue trackers, development tools, and notification channels they normally use. Developers can integrate security analysis and results seamlessly into their existing development tools and platforms. Application security testing (AST) analytics metrics help identify gaps so that heads of development can understand the effectiveness of their AST and DevSecOps implementation.

Ensuring comprehensive security coverage

Exploitations of web applications are an increasing concern. That's why security standards are focusing on the types of vulnerabilities that organizations need to keep out of their web applications.

Coverity's uses a variety of analysis techniques, including a patented dataflow analysis that looks at the code in multiple ways to find the most exploitable and critical security vulnerabilities. Its analyses are fine-tuned to look at more dataflow paths than other SAST tools. Its best-in-class accuracy finds real security vulnerabilities that competing solutions cannot find.

Frameworks such as Angular, React, and Vue.js are often used as a baseline for web applications. Coverity's support for more than 70 frameworks enables it to understand the programming context and the dataflow path in the combined application framework stack, making its analysis highly accurate. This also gives Coverity a holistic view of vulnerabilities and enables it to provide context-aware remediation guidance that isn't possible by looking only at the application code.

Coverity also understands support templates for JavaScript frameworks, which are a popular means of data binding. This capability enables it to scan the HTML code generated on the fly from these templates for vulnerabilities such as cross-site scripting.

Building security into your SDLC

A recent case study on Finastra, one of the largest FinTech firms in the world, shows how Synopsys application security solutions, including Coverity, helped the company ensure security for applications offered through its FusionFabric.cloud platform. This is a clear demonstration of how Coverity helps organizations achieve their application security objectives.

Coverity helps reduce the number of exploitable software vulnerabilities that make it to security review processes and production. It enables security and development teams to prioritize vulnerabilities based on the business need and impact, and optimally allocate resources to fix them. This in turn helps security teams improve their return on investment, prove its impact on application security, and demonstrate compliance by providing continuous and customizable reporting against key security and industry standards.

The risks from web applications exploits are increasing significantly. Security and development teams must work together to build secure web applications without negatively impacting developer productivity. By integrating into the development environment, and providing an intuitive user and management interface, comprehensive reporting, and a best-in-class analysis engine, Coverity helps security and development teams work together, and helps ensure web application security and compliance.

SYNOPSYS®

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com