BLACK DUCK®

GUIDE

FOUR APPLICATION SECURITY ESSENTIALS FOR SCM AUTOMATION

Developers have utilized source code management (SCM) tools since the 1980s to track, control, and manage changes across the software development life cycle (SDLC). Automation within SCM systems took shape in the 1990s and early 2000s to keep up with agile development methodologies and the increasing complexity of software projects. In recent years, SCM tools have become even more powerful due to the emergence of distributed version control systems such as Git, giving developers more flexibility, scalability, and efficiency than ever before.

But what about security?

Application security (AppSec) can't rely on manual processes when every other facet of software development is automated. To achieve true DevSecOps, it's essential to run automated AppSec testing (AST) within the SCM system. This leads to quicker discovery and remediation of vulnerabilities, saving time and money.

To secure code within SCM systems, developers need an AppSec platform that automatically onboards new projects, provides visibility into all the code they own, orchestrates AST within their SCM, and monitors their SCM continuously.

This guide outlines these four essentials so organizations can select an AppSec platform that manages vulnerabilities within their SCM tools of choice without hindering development velocity.

ESSENTIAL 1: AUTOMATED ONBOARDING OF NEW PROJECTS

Automatic onboarding of applications for AST significantly streamlines testing, enabling faster vulnerability detection, consistent application evaluation, and early intervention. This reduces the risk of security issues slipping through the cracks due to manual delays or oversight, ultimately improving overall application security and compliance with industry standards.

Developers need an AST platform that

- Automatically onboards new projects/branches from all the widely used SCM tools
- Provides automatic discovery along with bulk/continuous onboarding of applications and projects
- Tracks changes to SCM events and automatically syncs SCM projects and branches with the AST platform
- Checks daily for any changes such as commits, pushes, and merges in the repository branch mapped to the SCM projects
- Assigns policies, such as what to do with issues found, sets test scheduling policies to onboarded applications, and assigns custom policies based on the unique requirements of individual developers
- Assigns roles to users during the onboarding process

ESSENTIAL 2: A CENTRALIZED VIEW OF ALL PROJECTS

For optimal risk management, security teams need a comprehensive understanding of all projects, code, dependencies, and configurations.

Application security posture management (ASPM) provides a way to unify identification, prioritization, and risk visibility across all stages of the SDLC. ASPM tools gather and consolidate security metrics from all the SCM tools an organization is using, as well as from the disparate threat modeling, static application security testing (SAST), software composition analysis (SCA), and dynamic application security testing (DAST) tools, to provide a unified view into all application risk. This comprehensive view into risk helps detect vulnerabilities at every stage, ensuring no critical defect is overlooked.

By correlating, aggregating, normalizing, and deduplicating findings, ASPM tools help prioritize security issues based on the potential risk they pose to your business. Security teams can use these insights to implement policies that standardize AST and remediation workflows across pipelines. These tools can also deliver summary and detailed issue reports to provide clear risk visibility across applications and projects.

ESSENTIAL 3: AST ORCHESTRATION WITHIN SCM

To ensure on-time, comprehensive, and consistent vulnerability detection—the foundation of DevSecOps—it is vital to automate and orchestrate AST within the SCM environment, including

- **Application inventory.** This ensures that applications in the AST platform are updated in real time when there are changes to code repositories, and that applications are scanned as soon as they are created. Users can monitor onboarding progress through dashboards to gain an overview of testing coverage, common integration points, and failure scenarios.
- **Scans.** This enables sequential and concurrent scans to be triggered at any point during the SDLC. SAST and SCA scans can be triggered whenever new code is merged into a branch or whenever a pull request is created or updated. AST platforms make scanning efficient by running rapid scans for pull requests and when events are created or edited, and running full scans on merge events. Scans can be orchestrated by invoking CLI from the pipeline, via API, or through integrations with SCM.
- **Configuration.** AST platforms provide users with hierarchical control of key configuration items. This enables workflow management (such as policy administration) by supporting organization-level configurations that can be overridden at the application, project, and branch levels.
- **Issue management**. This leverages policy to notify users of newly discovered issues and automates ticket creation. AST platforms also allow issue triage information to be shared across the different branches of an application. And intelligent triage is immediately reflected on other branches.

ESSENTIAL 4: CONTINUOUS SCM MONITORING

As AI code generation and agents are turbo-charging the speed of software development, change is the only constant in SCM tools.

Robust ASPM functionality is at the heart of every modern AST platform. ASPM tools can continuously monitor multiple SCM repositories to detect vulnerabilities, misconfigurations, and lack of compliance with security policies. ASPM tools also monitor for any SCM events and trigger automated scan analysis per defined policies.

HOW POLARIS CAN HELP

Black Duck Polaris™ Platform is an integrated, software-as-a-service application security platform that provides fast, multitype scanning capabilities with highly accurate results triaged by Black Duck security experts. It automatically onboards new projects and reduces setup time while maintaining consistent security coverage.

Streamline automatic onboarding

Polaris streamlines the automatic onboarding of new projects through three key capabilities.

- **Bulk repository discovery** automatically detects and onboards projects from SCM platforms.
- **Continuous sync** tracks SCM events (e.g., new branches, commits) in real time, ensuring projects stay updated without manual intervention.
- **DevOps integrations** embed directly into CI/CD pipelines and IDEs, automating security checks within existing developer workflows.

Gain centralized visibility

Polaris provides a centralized approach to efficiently monitor and manage risks across all projects simultaneously.

- **Unified dashboards** provide enterprise-wide visibility, including issue summaries and vulnerabilities categorized by severity.
- **SCM integrations** automatically discover and sync with projects from GitHub, GitLab, and Bitbucket, ensuring real-time updates and centralized tracking.
- **Cross-tool aggregation** consolidates findings from SAST, SCA, and DAST scans into a single interface for holistic risk assessment.
- **Policy-driven management** enforces consistent security policies across projects while providing centralized analytics on compliance.

Orchestrate AST within SCM

Polaris facilitates AST orchestration within SCM systems through several key capabilities.

- **Continuous synch** with repositories tracks new branches and commits, ensuring real-time scanning coverage.
- **SAST, SCA, and DAST scans** are triggered based on SCM events.
- **Concurrent scanning** accelerates feedback while maintaining pipeline velocity.
- **Integration with CI/CD tools** like Jenkins enforces security gates, blocks risky builds, and flags vulnerabilities before deployment.

Continuously monitor SCM systems

Polaris provides continuous and real-time monitoring capabilities.

- **Always-on monitoring** of SCM systems and persistent connections scan updated code without manual intervention.
- **Automated repository synchronization** continuously tracks SCM systems to detect new projects, branches, and commits in real time.
- **Event-driven scanning** triggers security scans automatically for SCM events such as pushes, pull requests, and merges—ensuring immediate vulnerability detection.

Get enterprise-grade SCM security automation without compromise

Polaris offers a cloud-based, integrated approach that enables more efficient vulnerability detection and remediation, ensuring robust application security without slowing down development workflows.

See how Polaris can help you manage vulnerabilities without compromising development

ABOUT BLACK DUCK

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.