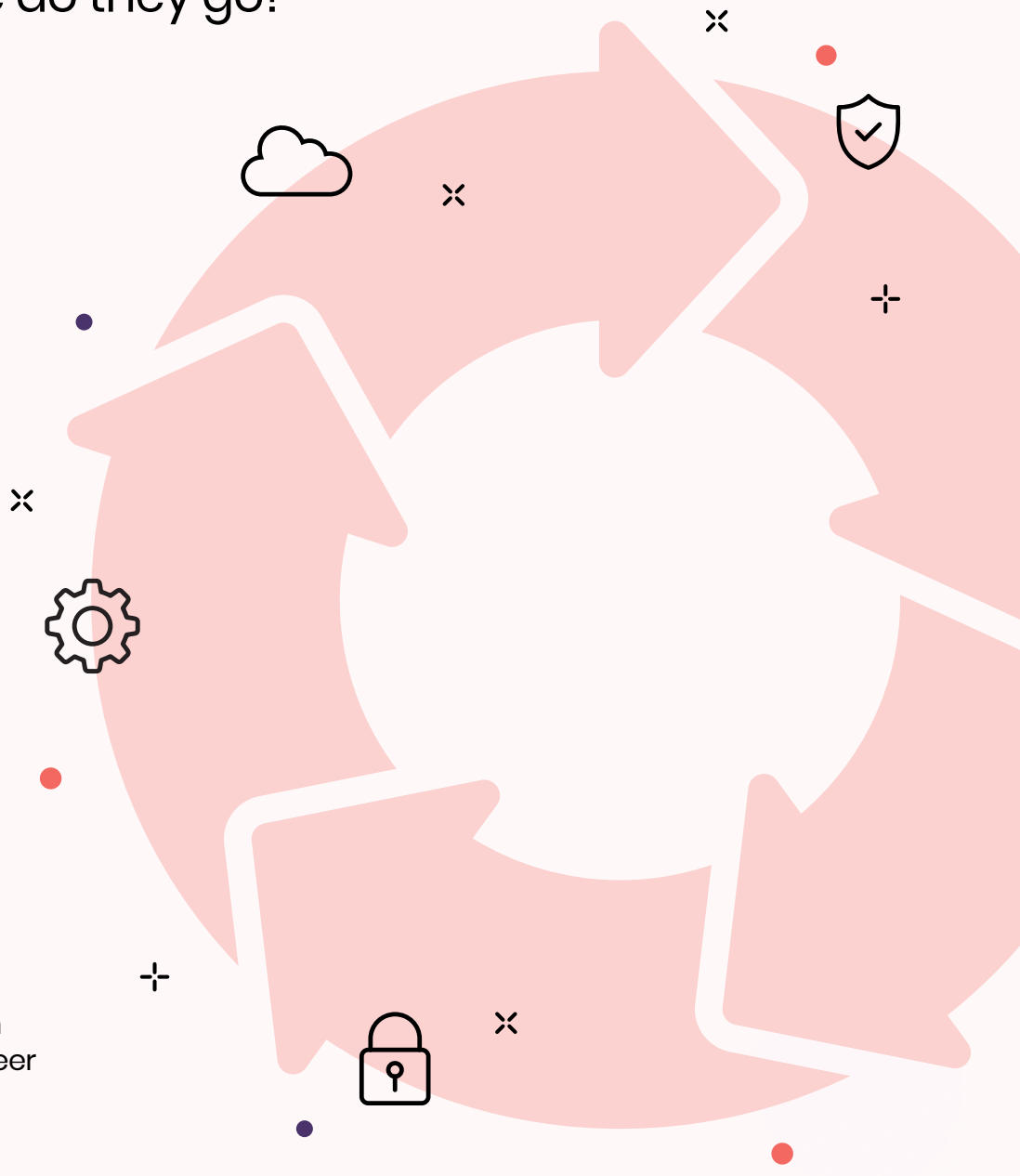
DAZZ.

WHITE PAPER

A Guide to Building a Secure SDLC

Which Scanning Tools Should I look at, and where do they go?



Written by **Matt Brown**
Senior Solutions Engineer

February 2023

Table of Contents:

Introduction

There is certainly no shortage of security scanning tools when it comes to building a secure SDLC. The below architecture is really well put together, but just look at the sheer amount of different tools that can be selected (and this isn't close to all of the options out there!):

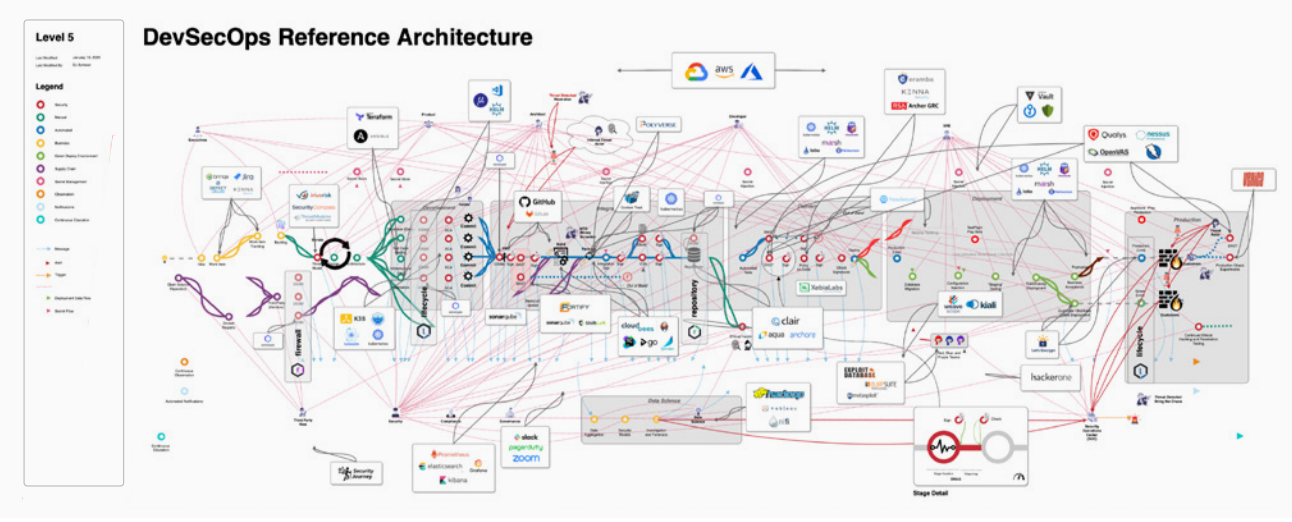


Image Source: DevSecOps Reference Architecture - DJ Schleen

Figuring out which tool to pick for which purpose and where the tool should go in your SDLC is such a large part of the challenge of building a secure SDLC. When trying to navigate this space, it's really easy to get lost really quickly and go down rabbit holes you can't dig yourself out of. In this guide, we're going to cover the following about the different tools offered in each stage of a secure SDLC:

- What are the "typical" stages of a secure SDLC
- What tool types are typically used in each stage, and what do they do (e.g. DAST vs. SAST vs. CSPM vs. CWPP)
- Examples of the vendors offering those tools, along with a quick blurb about them, and a direct link to the specific vendor's product website
- Some additional resources that can help you build a secure SDLC

What's a Secure SDLC?

A secure SDLC is a process that companies follow to ensure that the software they develop and deploy is secure by design, and minimizes vulnerabilities and misconfigurations. The steps involved in a secure SDLC can vary depending on the specific organization, but it typically involves identifying and addressing security concerns at each stage of the software development lifecycle - from design and code (early in the SDLC) to deployment and monitoring (later in the SDLC). By following a secure SDLC, companies can reduce the risk of security & infrastructure breaches and protect their software and data from potential threats.

About this Guide:

What this guide is:

- This guide can be used as a reference to help you navigate all of the different vendors that offer tools to scan for vulnerabilities and misconfigurations across your secure SDLC.

What this guide is *not:*

- This guide is not a recommendation to purchase one tool over another.

So. Many. Tools.

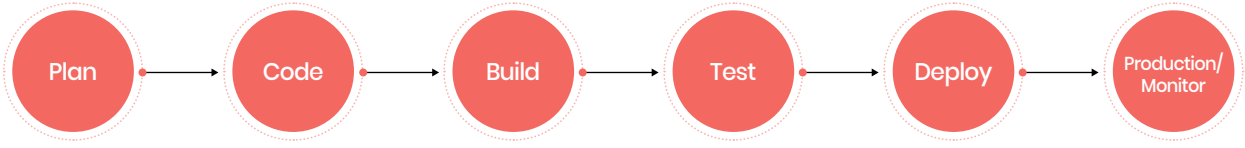
- After a while, I was beginning to think that the list of scanning tools was really just endless. Did I miss a few tools? Probably (definitely). Please reach out and let us know if we've missed something, and we can add it to the guide!

That Tool Should Go Here, Not There!

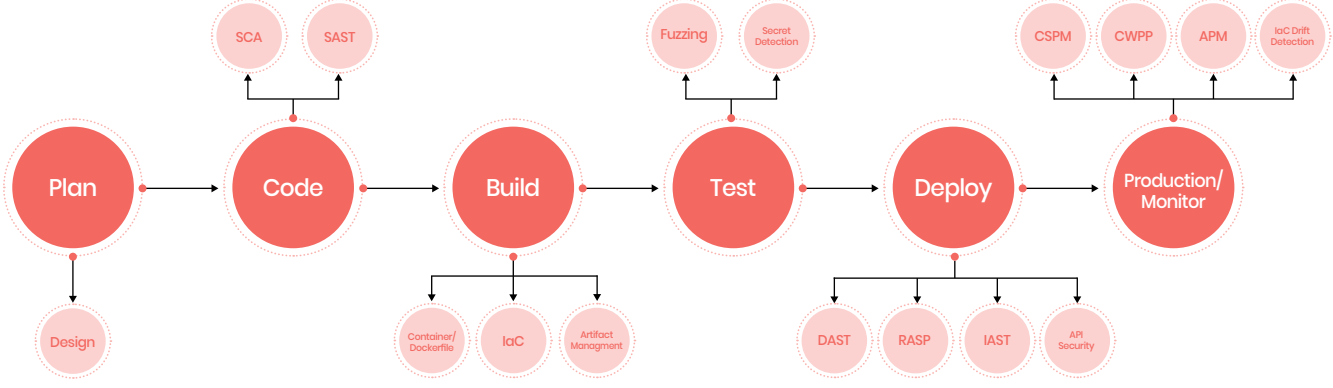
- The guide and SDLC we show here is just that - a guide. It's meant to point the reader in the right direction. For example - in the below SDLC example, we show that SCA and SAST are in the Code stage of the SDLC. Different terms mean different things to different readers - some readers may say that SCA and SAST need to go in the Build stage as well, since that's where they implement CI/CD. Can you use a certain tool or type of tool in more than one place in the SDLC? Yes, please do! As you go through this guide and see all of the different vendors, you'll discover that almost all of these tools can go almost anywhere in the SDLC, and in multiple stages throughout. What's the best way to implement each tool and what are the best practices for each specific tool? Well, that's an excellent topic for another whitepaper.

SDLC & Secure SDLC:

Now that we have that all cleared up, let's take a look at an example SDLC. I'll preface this by saying we understand that not all SDLCs look alike or are built the same way. Below is a very general SDLC that we think is a great starting point:



Now, we're not going to go into each stage of a standard SDLC (that's for another white paper, and there are great resources here and here). What we will do is make the above SDLC more secure - let's do that, shall we?



That's *much* better! Let's go over the security tools and methods used in each stage of the SDLC.

Secure SDLC Stages and their Tools:

Plan

Design

- The design stage in a Software Development Lifecycle (SDLC) is the phase where the system, application, or product being developed is designed and planned. During the design stage of a secure SLDC, we identify and document the security requirements for the system, develop the overall architecture and design, identify and document any potential security risks or vulnerabilities, and develop a plan for addressing these potential security issues. The security design is then reviewed and validated with relevant stakeholders to ensure that it meets the necessary security standards.

A great resource for learning more about secure design: *Designing Secure Software: A Guide for Developers by Loren Kohnfelder*

Code

SCA

- Software Composition Analysis (SCA) is a scanning technique that looks at the open source software components that you are knowingly and unknowingly (through transitive dependencies) bringing into your application, and identifying any known vulnerabilities within those components. SCA can also check the licenses of these third party components, to ensure compliance needs are met when it comes to open source software use.

SAST

- Static Application Security Testing (SAST) is a vulnerability scanning technique that focuses on source code. It works early in the SDLC and CI pipeline and scans source code, bytecode, or binary code in order to identify problematic coding patterns that go against best practices, or that could cause vulnerabilities. SAST can often result in "false positives", which are alerts generated from SAST, but aren't actual vulnerabilities for a multitude of reasons.

Build/Artifact

Static Container Scanning

- Static container scanning is the process of analyzing the contents of a container image for vulnerabilities and policy violations *before* the container is deployed and run. While there are countless benefits to containers, they can also introduce security risks if they contain vulnerabilities or policy violations. Static container scanning is a way to identify and address these risks before the container is deployed. A static container scanning tool will typically analyze the contents of the container image, including the application code, libraries, and system packages, looking for known vulnerabilities and policy violations

Static IaC (Infrastructure as Code) Scanning

- Much like static container scanning, static Infrastructure as Code (IaC) scanning is the process of analyzing the configuration files that define infrastructure resources, (e.g. virtual machines, networks, and storage) for vulnerabilities and policy violations *before* the infrastructure is deployed. The key with static IaC scanning is the fact that it helps to ensure that the infrastructure is secure and compliant with policies before it's deployed, thus achieving a more "shift left" approach to IaC.

Artifact Management

- Artifact management during the SDLC refers to the process of managing and storing the various documents, containers, code, and other materials that are created and used during the development of a software application. These artifacts can include requirements documents, design documents, source code, test cases, and more. Several of the artifact management tools can include their own native vulnerability scanning capabilities.

Test

Fuzzing

- Fuzzing, (aka fuzz testing) is a method of testing software applications by providing them with invalid, unexpected, or malformed input in an attempt to discover vulnerabilities or cause the application to crash. Fuzzing can be used to test the robustness of an application and identify potential security vulnerabilities that might not be detected by other types of testing. Fuzzing tools can be used to automate the process of generating and sending random or malicious input to an application, to ensure that the application is stable.

Secrets Detection

- Secrets detection tools work by scanning code and other files for patterns that may indicate the presence of sensitive information, such as strings of characters that match known password patterns or API keys that are stored in plain text. Once a potential secret is identified, the tool will alert the user and provide them with the option to remove or mask the sensitive information from the repository.

Deploy

DAST

- Dynamic Application Security Testing (DAST) is a black-box testing method that scans applications in runtime. It is applied later in the CI pipeline. DAST is a good method for preventing regressions and doesn't depend on a specific programming language. While DAST is still early in the SDLC, it is typically done later in the CI pipeline.

RASP

- Runtime Application Self-Protection (RASP) is a security technology that is designed to protect applications from attacks while they are running. It is often used to protect web applications from attacks such as cross-site scripting (XSS), SQL injection, and other types of injection attacks. RASP works by integrating security capabilities directly into the application itself, rather than relying on external security measures such as firewalls or intrusion prevention systems. This allows for real-time protection of the application and monitoring for potential threats.

IAST

- Interactive application security testing (IAST) applies to security testing where the testing tool interacts with a running application and observes it from the inside in real-time. Interactive application security testing solutions are designed to test web application frameworks and APIs. IAST can also be referred to as gray-box testing.

API Security

- API security is the protection of APIs from unauthorized access or abuse. It involves the use of authentication, authorization, data encryption, and input validation to secure APIs. API security tools can help prevent the same types of vulnerabilities that other scanners help prevent, such as unauthorized access, DDoS attacks, injection attacks, etc.

Production/Monitor

CSPM

- Cloud security posture management (CSPM) tools work by continuously examining and comparing a cloud environment against a defined set of best practices (misconfigurations) and security risks (CVEs and vulnerabilities). CSPM is typically more "right" in the software development life cycle (SDLC). CSPM tools don't take into consideration the findings brought by tools that are more "left" on the SDLC (SAST, SCA, etc.).

CNAPP/CWPP (Cloud &/or Dynamic/Runtime Container Scanning)

- Cloud Workload Protection Platforms (CWPP) provide tailored security needs for deployed workloads that are in public, private, or hybrid environments. CWPP enables you to perform security functions across multiple environments. The main difference between CWPP and CSPM is that CWPP looks at the deployed workloads (cloud, Kubernetes, etc.), while CSPM continuously monitors the cloud environment.

APM (Application Performance Monitoring)

- Application Performance Monitoring (APM) is the activity of monitoring the performance and availability of software applications. The goal of APM is to identify and diagnose problems that might negatively impact the performance of the application, and to identify opportunities for improvement. APM systems often offer a variety of functions, including monitoring the application's performance and resource use, tracing requests as they move through the application, and alerting when specific performance criteria are surpassed. APM can help to ensure that an application is performing optimally and meet the needs of its users.

IaC Drift Detection

- Infrastructure as Code (IaC) drift detection tools are used to identify and report on differences between the intended infrastructure configuration defined in the IaC codebase and the actual configuration of the deployed infrastructure. These tools are designed to help organizations ensure that their infrastructure is configured as intended and to identify any deviations from the expected configuration. Basically - the infrastructure that was deployed with IaC is not what you were expecting.

Vendors for Each Tool

Now that we know what types of tools we need, what are some vendors for each one? Below is a list of vendors for each type of tool listed above. There's a brief description for each vendor and a direct link to each website of the specific product that's mentioned:

Secure Design & Education

Secure Code Warrior

Secure code learning for today's developers. Equip developers to be security-driven by teaching them the skills needed to defend their organization through secure code.

IriusRisk

IriusRisk is the open threat modeling company that helps developers design secure software from the start.

Snyk Learn

Snyk Learn teaches developers how to stay secure with interactive lessons exploring vulnerabilities across a variety of languages and ecosystems.

Security Compass

Mitigate cyber risks at scale with SD Elements' breakthrough automated approach to threat modeling.

SCA

Snyk Open Source

Snyk Open Source provides a developer-first SCA solution, helping developers find, prioritize, and fix security vulnerabilities and license issues in open source dependencies.

Mend (formally Whitesource)

From identification of open source components (including transitive dependencies) to automated remediation. Use open source freely and fearlessly without compromising on security or agility.

Sonatype Nexus Lifecycle

Sonatype Nexus tools enable teams to build software secure enough to satisfy the most stringent security requirements - without sacrificing speed or innovation.

Synopsys (Black Duck)

Black Duck software composition analysis (SCA) helps teams manage the security, quality, and license compliance risks that come from the use of open source and third-party code in applications and containers.

FOSSA

Comprehensive open source risk management to mitigate license violations, vulnerabilities, and supply chain threats.

JFrog Xray

Secure software delivery from code to containers to devices, integrated in a unified DevOps platform.

Dependabot (GitHub)

Dependabot can fix vulnerable dependencies for you by raising pull requests with security updates.

ShiftLeft

ShiftLeft Intelligent-SCA is the only software composition analysis solution that examines the flow of data across an entire software application to determine which open source libraries contain vulnerabilities that are actually reachable by attackers.

GitLab Dependency Scanning (formally Gemnasium)

The Dependency Scanning feature can automatically find security vulnerabilities in your software dependencies while you're developing and testing your applications.

Veracode

Veracode Software Composition Analysis (SCA) helps you build an inventory of your third-party components to identify vulnerabilities, including open-source and commercial code.

CheckMarx

Checkmarx SCA is a cloud native SaaS solution which enables you to easily identify, prioritize, and remediate the risks posed by your open source packages.

OWASP Dependency Check

Dependency-Check is a Software Composition Analysis (SCA) tool that attempts to detect publicly disclosed vulnerabilities contained within a project's dependencies.

SAST

Snyk Code

Secure your code as it's written with static application security testing built by, and for, developers. Code security with a developer-friendly experience. Get the security intelligence and remediation advice you need, without disrupting the development workflow.

Veracode

Manage risk with Veracode Static Analysis (SAST), a white box testing solution that provides feedback in the IDE and pipeline.

CheckMarx

Checkmarx SAST scans source code to uncover application security issues as early as possible in your software development life cycle. You don't need to build your code first - just check it in, start scanning, and quickly get the results you need.

Semgrep

Semgrep is a fast, open source, static analysis engine for finding bugs, detecting dependency vulnerabilities, and enforcing code standards.

SonarQube

Commit to developer-led project security by detecting Security Vulnerabilities and Security Hotspots during code review.

Fortify

Build secure software fast. Find security issues early with the most accurate results in the industry and fix at the speed of DevOps.

ShiftLeft

ShiftLeft allows developers to spend more time coding and less time fixing vulnerabilities by prioritizing real, attackable risks in their code.

Mend (formally Whitesource)

Mend's next-generation SAST product seamlessly integrates with software developers' existing workflow and development environments, so they can easily trigger security tests when they need them the most — when they're writing code.

GitHub (GitHub Advanced Security with CodeQL)

Code scanning is a feature that you use to analyze the code in a GitHub repository to find security vulnerabilities and coding errors. Any problems identified by the analysis are shown in GitHub.

Synopsis (Coverity)

Coverity® is a fast, accurate, and highly scalable static analysis (SAST) solution that helps development and security teams address security and quality defects early in the software development life cycle (SDLC), track and manage risks across the application portfolio, and ensure compliance with security and coding standards.

GitLab

If you're using GitLab CI/CD, you can use Static Application Security Testing (SAST) to check your source code for known vulnerabilities. The analyzers output JSON-formatted reports as job artifacts.

Static Container Scanning

Snyk Container

Container and Kubernetes security that helps developers and DevOps find and fix vulnerabilities throughout the SDLC - before workloads hit production.

ECR (Native scanning tool)

Amazon ECR image scanning helps in identifying software vulnerabilities in your container images.

Sysdig

Prioritize the most critical vulnerabilities using runtime context. Automate CI/CD pipeline and registry scanning and block vulnerabilities before production.

Microsoft Defender for Containers

Microsoft Defender for Containers is the cloud-native solution that is used to secure your containers so you can improve, monitor, and maintain the security of your clusters, containers, and their applications.

Prisma Cloud

Secure Kubernetes and other container platforms on any public or private cloud, from build to run with Prisma Cloud (may also be referred to as Prisma Compute or TwistLock).

Lacework

Discover vulnerabilities, detect threats, and demonstrate compliance in your dynamic container environment.

Wiz

Rapidly build containerized applications without risks. Holistically secure Containers, Kubernetes, and cloud environments.

Aqua

Protect cloud native applications by minimizing their attack surface, detecting vulnerabilities, embedded secrets, and other security issues during the development cycle.

Clair (by Quay)

Clair is an open source project for the static analysis of vulnerabilities in application containers (currently including OCI and docker).

Qualys

Discover, track and continuously secure containers – from build to runtime.

Anchore

Leverage comprehensive APIs and a CLI tool to automate image scanning for development environments, CI/CD pipelines, registries, or runtime environments.

Static IaC (Infrastructure as Code) Scanning

Snyk IaC

Reduce risk by automating IaC security and compliance in development workflows pre-deployment and detecting drifted and missing resources post-deployment.

Checkov (by Bridgecrew)

Created by Bridgecrew, Checkov is an open source policy-as-code tool that scans for security issues in infrastructure as code (IaC) templates, container images, and pipeline configuration.

CheckMarx KICS

KICS (Keeping Infrastructure as Code Secure) is a free, open source solution for static code analysis of IaC.

Terrascan (by Tenable)

Detect compliance and security violations across Infrastructure as Code (IaC) to mitigate risk before provisioning cloud native infrastructure.

Artifact Management

JFrog Artifactory

With JFrog Artifactory, organizations are able to control and monitor the way all binaries flow across their software supply chain (SSC) to production with security thoughtfully integrated into the binary lifecycle management process.

Sonatype Nexus Repository

Manage libraries and store artificats in a universal repository and share them across development teams.

Elastic Container Registry

Amazon Elastic Container Registry (Amazon ECR) is an AWS managed container image registry service that is secure, scalable, and reliable.

Azure Container Registry

Enable fast, scalable retrieval of container workloads. Azure Container Registry handles private Docker container images as well as related content formats, such as Helm charts, OCI artifacts, and images built to the OCI image format specification.

Google Container Registry

Google Container Registry is a single place for your team to manage Docker images, perform vulnerability analysis, and decide who can access what with fine-grained access control.

GitHub Container Registry

You can store and manage Docker and OCI images in the Container registry, which uses the package namespace https://ghcr.io.

Fuzzing

ForAllSecure

Mayhem for Code's unique advantage is in its ability to acquire intelligence of its targets over time. As Mayhem for Code's knowledge grows, it deepens its analysis and maximizes its code coverage.

Synopsys Defensics

Defensics is a comprehensive, versatile, automated black box fuzzer that enables organizations to efficiently and effectively discover and remediate security weaknesses in software.

Google OSS-Fuzz

OSS-Fuzz aims to make common open source software more secure and stable by combining modern fuzzing techniques with scalable, distributed execution.

Burp Suite PortSwigger

Burp Scanner uses PortSwigger's world-leading research to help its users find a wide range of vulnerabilities in web applications, automatically.

Secrets Detection

GitGuardian

GitGuardian secrets detection looks for API keys, database credentials, or security certificates in internal or public repositories.

Nightfall

Nightfall leverages machine learning to detect a wide range of potentially sensitive data in GitHub repositories – ensuring data like secrets, PII, and more are kept safe.

GitLab

Secret Detection uses an analyzer containing the Gitleaks tool to scan the repository for secrets.

GitHub

GitHub scans repositories for known types of secrets, to prevent fraudulent use of secrets that were committed accidentally.

BluBracket

BluBracket automates the detection, identification and removal of secrets in code. BluBracket identifies all categories that make up secrets in code, ranks them by risk and provides a means to remediate.

DAST

StackHawk

Focused on pre-production application security testing, StackHawk gives teams the ability to actively run security testing as part of their CI/CD workflows.

Invicti (formally NetSparker)

Increase confidence in your web app security testing with complete visibility and enablement throughout your team.

Rapid7 InsightAppSec

InsightAppSec performs black-box security testing to automate identification, triage vulnerabilities, prioritize actions, and remediate application risk.

Detectify

Automatically scan custom-built apps, find business-critical security vulnerabilities and strengthen your web app security with Application Scanning.

Veracode (formally Crashtest Security)

Scan hundreds of web applications and APIs simultaneously. Point solutions and managed service solutions simply can't keep up with the scale and pace of modern development cycles.

Fortify WebInspect

WebInspect is an automated dynamic testing solution that provides comprehensive vulnerability detection.

Astra Pentest

Uncover vulnerabilities before hackers with our intelligent scanner and manage your entire security from a CXO- and developer-friendly dashboard.

RASP

Imperva

Imperva RASP protects your applications from the inside out. Built into the application runtime environment, RASP is capable of detecting and preventing attacks real-time.

K2

K2 Security Platform is highly effective at detecting increasingly sophisticated attacks targeting applications in production that often go undetected by network and end point security solutions such as WAF and EDR.

Contrast Protect

Contrast Protect is production application and API protection that blocks attacks and reduces false positives, helping developer teams prioritize vulnerability backlogs

IAST

Synopsys Seeker

Seeker monitors web app interactions in the background during normal testing and can quickly process hundreds of thousands of HTTP(S) requests, giving you results in seconds with near-zero false positives—no need to run manual security scans.

Contrast Assess

Contrast Assess provides developers a mapping of the URL and routes of their software that are executed during the testing phase of the SDLC.

API Security

ForAllSecure - Mayhem for API

Mayhem for API was built to enable a developer to get meaningful testing results within 5 minutes. Mayhem for API was also built so organizations can automatically test APIs with simple integrations with development and build pipeline solutions.

StackHawk

With automated tests for API security risks, StackHawk helps surface potential vulnerabilities in your APIs before they are shipped to production.

Salt Security

Securing Your Innovation. The rich API context you need for robust discovery, attack prevention, and shift left.

Threatx

ThreatX's API protection platform gives you instant API protection, for all your APIs, regardless of their status or which gateway they sit behind, no schema required.

Noname Security

Noname Security Active Testing helps customers stop vulnerabilities before production and innovate faster. True to a shift-left approach, security testing is baked into each step of the DevOps process, ensuring developers can monitor for vulnerabilities throughout the lifecycle.

42crunch

Automate detection of API vulnerabilities from design time. Block attacks in real-time, with no rules to write and no false positives.

CSPM

Snyk Cloud

Reduce risk by automating IaC security and compliance in development workflows pre-deployment and detecting drifted and missing resources post-deployment.

Prisma Cloud

Prisma Cloud is a unique Cloud Security Posture Management (CSPM) solution that reduces the complexity of securing multicloud environments, while radically simplifying compliance.

Orca

Continuously monitor, identify and remediate misconfigurations. Orca is a comprehensive cloud security posture management (CSPM) solution that continuously detects misconfigurations, policy violations and compliance risks in cloud environments, including cloud-native services.

CrowdStrike Falcon Horizon

CrowdStrike Falcon® Horizon is a cloud security posture management (CSPM) that detects and prevents misconfigurations and control plane threats, eliminates blind spots, and ensures compliance, across AWS, Azure, and Google Cloud.

Sysdig

Find, Focus, and Fix Cloud Misconfigurations and Threats. Get a single view of risk into your cloud security posture. Identify, prioritize, and control risks across various cloud environments.

Lacework

Simpler cloud security posture management. Reduce risks and meet compliance requirements without overwhelming your security team.

Wiz

Continuously detect and remediate misconfigurations from build time to runtime across your hybrid clouds – AWS, GCP, Azure, OCI, Alibaba Cloud, and VMware vSphere.

Tenable.cs

Whether you are lifting and shifting workloads to cloud, modernizing hybrid applications, or building new cloud native apps, Tenable Cloud Security can help you take your cloud security posture to the next level.

Sonrai Security

Sonrai provides enterprises with continuous monitoring and smart automation to deploy policies with precision and avoid these issues.

CNAPP/CWPP (Cloud &/or Dynamic/Runtime Container Scanning)

Prisma Cloud (Compute)

Prisma Cloud is a comprehensive Cloud Workload Protection solution that delivers flexible protection to secure cloud VMs, containers and Kubernetes apps, serverless functions and containerized offerings like Fargate tasks.

Orca

Orca offers industry-leading agentless cloud workload protection platform (CWPP) capabilities and provides 100% coverage and deep visibility into cloud workloads—spanning cloud VMs, serverless functions, containers, and Kubernetes applications— without the performance impact, security gaps and operational costs of agents.

Sysdig

Sysdig is an open source-based, SaaS-first container, Kubernetes and host security platform that automatically integrates with existing DevOps tools and workflows.

CrowdStrike Falcon Cloud Workload Protection

CrowdStrike Falcon® Cloud Workload Protection provides comprehensive breach protection for workloads, containers, and Kubernetes enabling organizations to build, run, and secure cloud-native applications with speed and confidence.

Lacework

Get the visibility and context you need to defend your cloud environments with autonomous machine learning.

Wiz

The only agentless, graph-based CNAPP that provides 100% visibility, ruthless risk prioritization, and time-to-value across teams that build and secure your cloud.

Aqua

Aqua Platform protects your entire stack, on any cloud, across VMs, containers, and serverless.

Sonrai Security

Sonrai's Risk Amplifiers and patented identity graph show the hidden "blast radius" of each vulnerability so you can understand how severe a vulnerability truly is and make the next right step to secure your cloud.

Microsoft Defender for Containers

Threat protection at the cluster level is provided by the Defender agent and analysis of the Kubernetes audit logs. Examples of events at this level include exposed Kubernetes dashboards, creation of high-privileged roles, and the creation of sensitive mounts.

Qualys

Qualys CS extends its container security capabilities to the runtime phase of deployment with its add-on Container Runtime Security (CRS) feature.

APM

Datadog APM

Datadog Application Performance Monitoring (APM) provides end-to-end distributed tracing from browser and mobile apps to databases and individual lines of code.

AppDynamics (acquired by Cisco)

Align IT and business leaders to avoid conflict and build unity by reducing noise and focusing on what's most important - your business and your customer's success.

Dynatrace

Automatic and intelligent observability at scale for cloud native workloads and enterprise apps helps you ensure end-to-end hybrid cloud distributed tracing, optimize service performance, innovate faster, collaborate efficiently, and deliver more value with less effort.

IaC Drift Detection

Snyk IaC

Snyk IaC helps you secure faster by reporting cloud infrastructure drift issues and unmanaged resources direct to developers.

Env0

Automatically detect environment drift and ensure real-world cloud resources align with your IaC definitions and descriptions.

Bridgecrew (offered by Prisma Cloud)

Bridgecrew's Multi-Cloud Drift Detection continuously monitors configuration discrepancies between your cloud resources and IaC and provides automated fixes in code.

Sysdig

Apply consistent security policies across multiple IaC, cloud, and Kubernetes environments. Autoremediate drift and close the loop from production to source.

Wiz

Wiz performs a deep analysis of your running cloud environment to detect the most critical risks. This enables security teams to prioritize policy enforcement in the pipeline.

Orca

Orca continuously checks for misconfigurations across multi-cloud estates to ensure controls are set securely and comply with best practices and industry and regulatory standards.

Conclusion

In this paper, we talked about the difference between a standard SDLC and a secure SDLC, what tool types are used in each stage of a secure SDLC, what each tool type does, and did an overview of the several different types of tools in each stage.

I know, I know, there's a lot of information here; thanks for sticking with us through the end! Navigating the world of security tools can be really difficult, especially in the last few years when this space has just expanded so much.

As we mentioned earlier, this paper can be used for several different things - use it as a reference when you're looking for different tools, for enablement in your organization, or to stay up to date on some of the latest tools that are out there (we'll try to keep this paper updated as new tools or technology comes out!). We hope this paper helps guide you toward implementing a secure SDLC, and please reach out to us if you have any questions or would like any help.

About the author

Matt Brown is a Senior Solutions Engineer at Dazz, where he's helping Enterprises with their DevSecOps strategies in AppSec (SCA, SAST, etc.), CloudSec (Containers, IaC, CSPM), and Cloud Native Vulnerability domains. A former developer, his passion is to help security teams understand & empower their software engineering organizations to take a developer-first approach to securing the SDLC. Matt holds his Master's in Computer Science, and enjoys spending time with his family, woodworking, and playing golf.

Feel free to contact our team to discover more:

contact@dazz.io | dazz.io |

About Dazz

We started our journey after years spent building cybersecurity products at Microsoft and beyond, but we wanted to take a different approach to securing the cloud and modern development environments - we're on a mission to solve a critical set of problems while improving the lives of security teams and their business partners, not by adding more alerts, but by simplifying the remediation process.

DAZZ.