AWS re:Inforce

JUNE 10 - 12, 2024 | PHILADELPHIA, PA

APS374

Enhancing software supply chain security: SBOMs, signing, slimming

Niaz Khan
(he/him)
GM AWS Signer
AWS

Byron Pogson
(he/him)
Senior Security Architect
AWS

Agenda

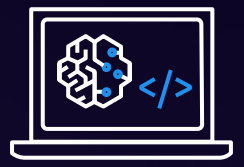
- Benefits of DevOps
- Considerations for security in DevOps
- Overview of workshop architecture
- What you'll be working on today
- Outline of the target state

Challenges of quickly building secure code

Shortage of developers

Time spent on undifferentiated code

Appropriate use of open source



Data privacy

Time spent learning technologies, APIs, and best practices

Writing secure code

Open source software (OSS) accelerates innovation

60M

Over 60 million OSS components available

3.9M

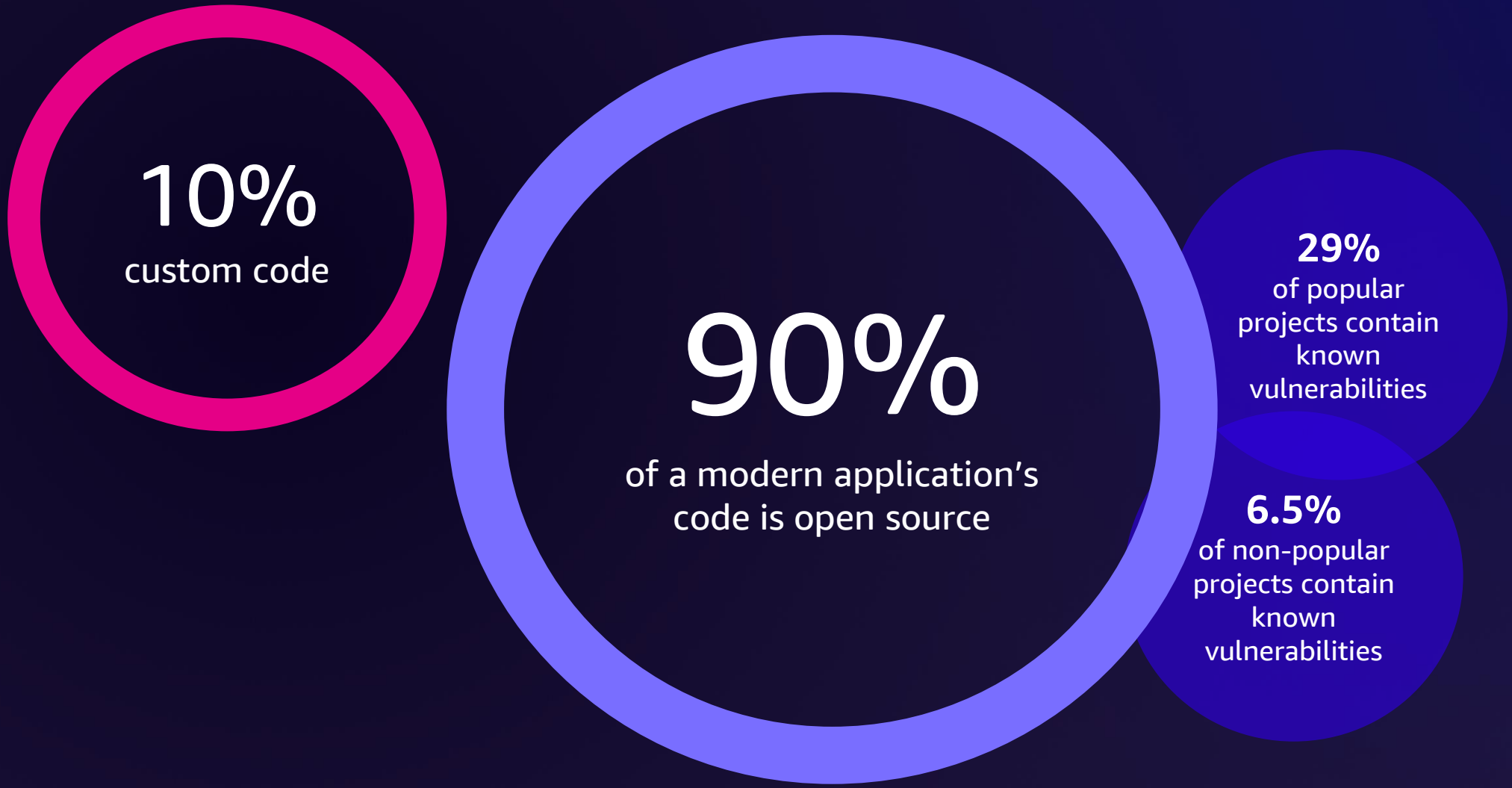
OSS projects available in 2023

4T

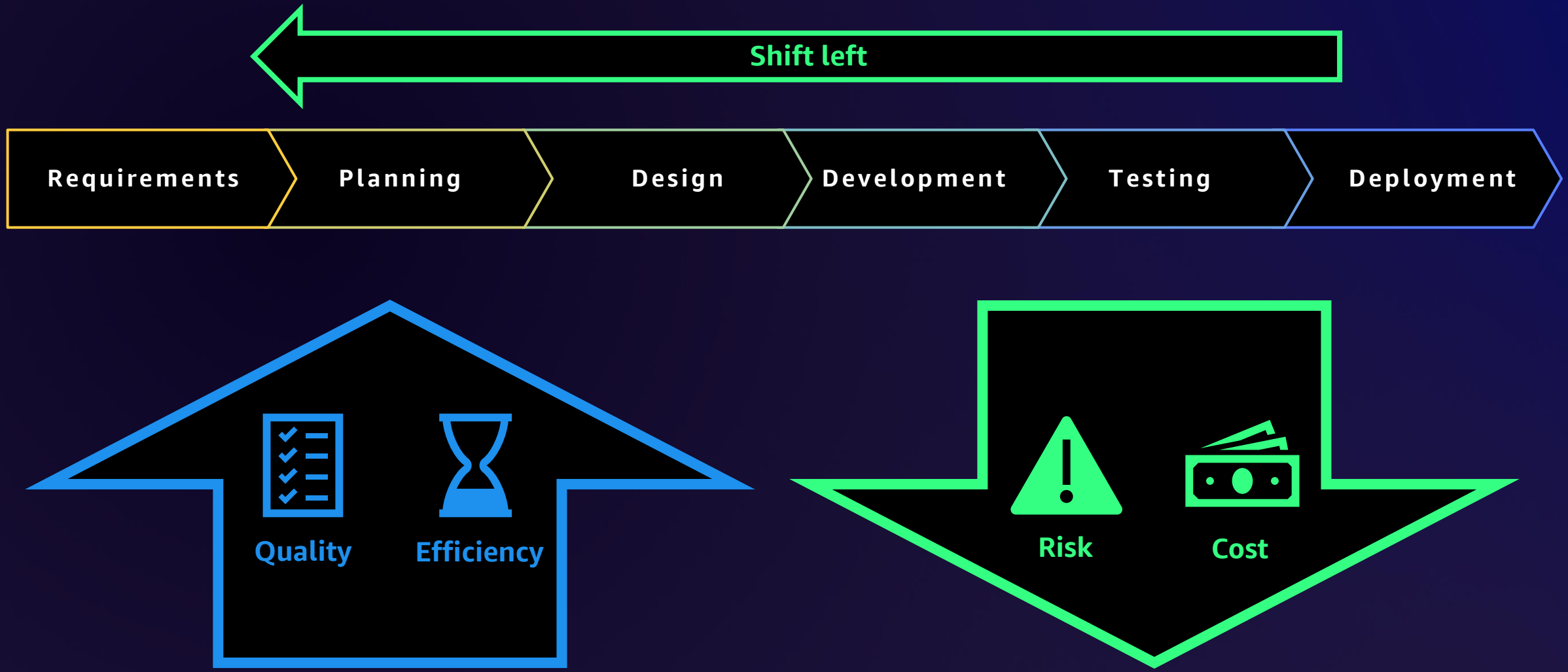
Annual request volume

Source: Sonatype, 2023 State of the Software Supply Chain
https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-and-demand

Not all parts are created equal



A new approach is required



Business benefits of DevSecOps

45%
faster vulnerability remediation

20–50%
operational cost savings

2.5x
likelihood to exceed goals

2x
recruitment retention

Source: *Accelerate: Building and Scaling High Performing Technology Organizations*

Adding security to DevOps

Security **OF** the pipeline

Security **IN** the pipeline

Enforcement of the pipeline

Supply chain security

Adding security to DevOps

Security OF the pipeline

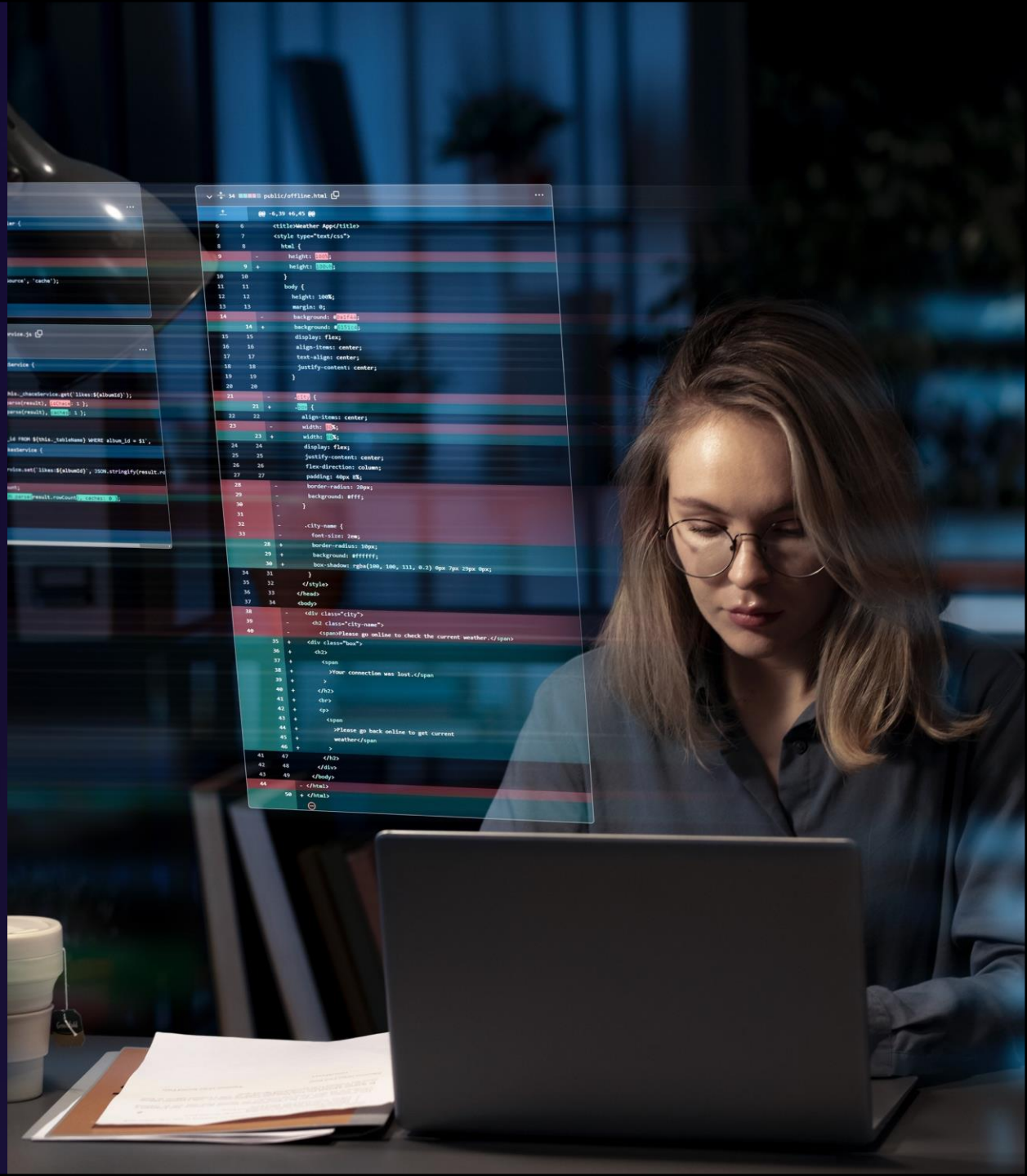
Security **IN** the pipeline

Enforcement of the pipeline

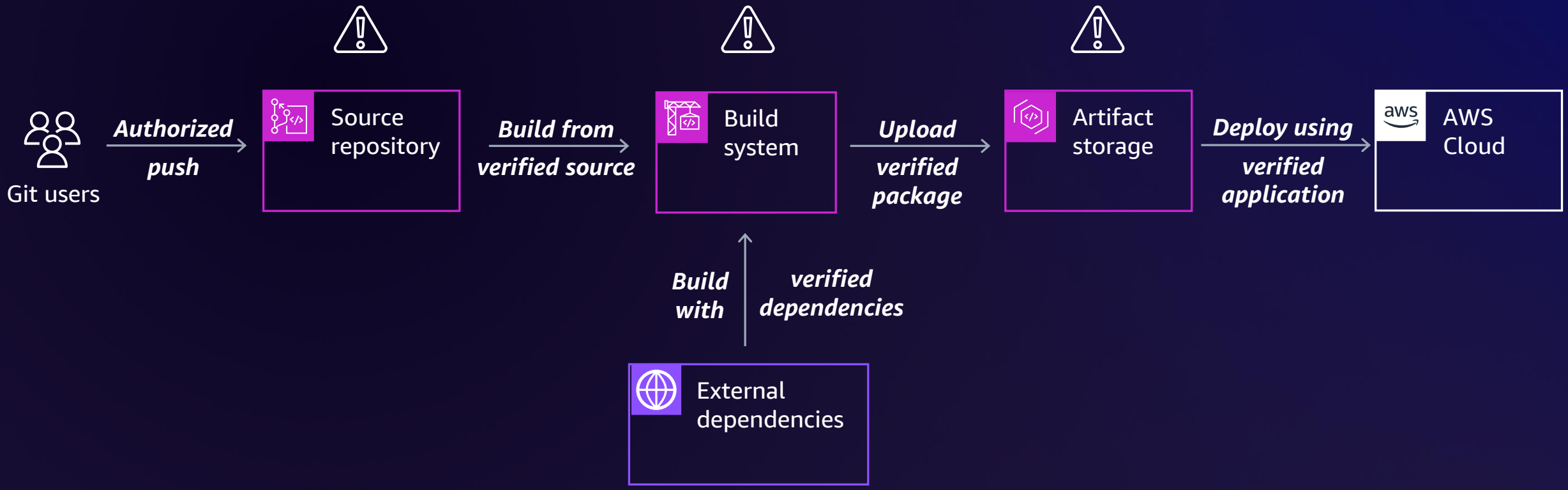
Supply chain security

Security in the pipeline

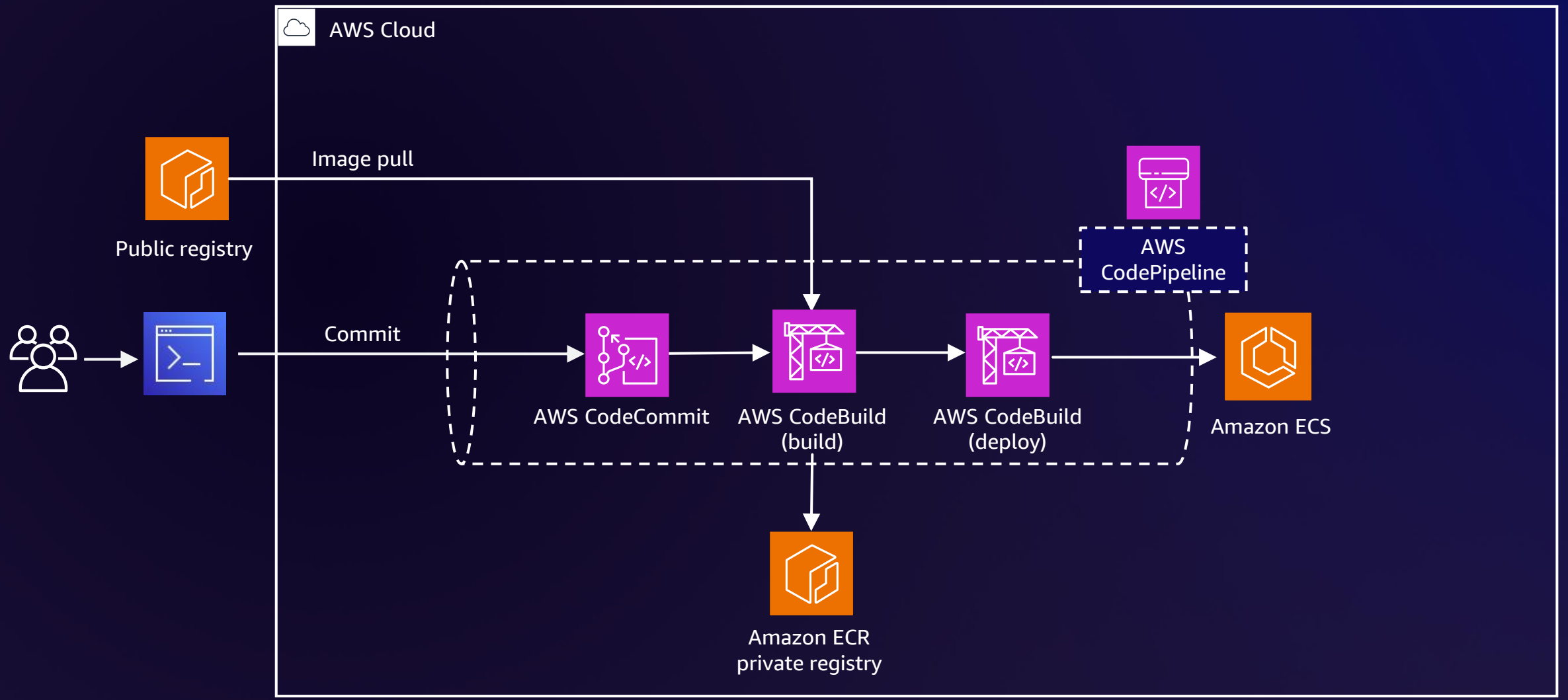
- Preventative
- Proactive
- Detective
- Responsive



Desired security properties



Workshop architecture



Workshop steps

Control 1: Signing

- AWS Signer is a fully managed code-signing service for code integrity and authenticity
- Signer eliminates customer overhead of managing cryptographic resources
- Available at no additional charge for Lambda code signing, container images, and IoT firmware

Benefits

Validate code against a digital signature to confirm that the code is unaltered and from a trusted publisher

Define your signing environment in a **single place**

Manage the code-signing certificate public and private keys

Enable management of the code-signing lifecycle

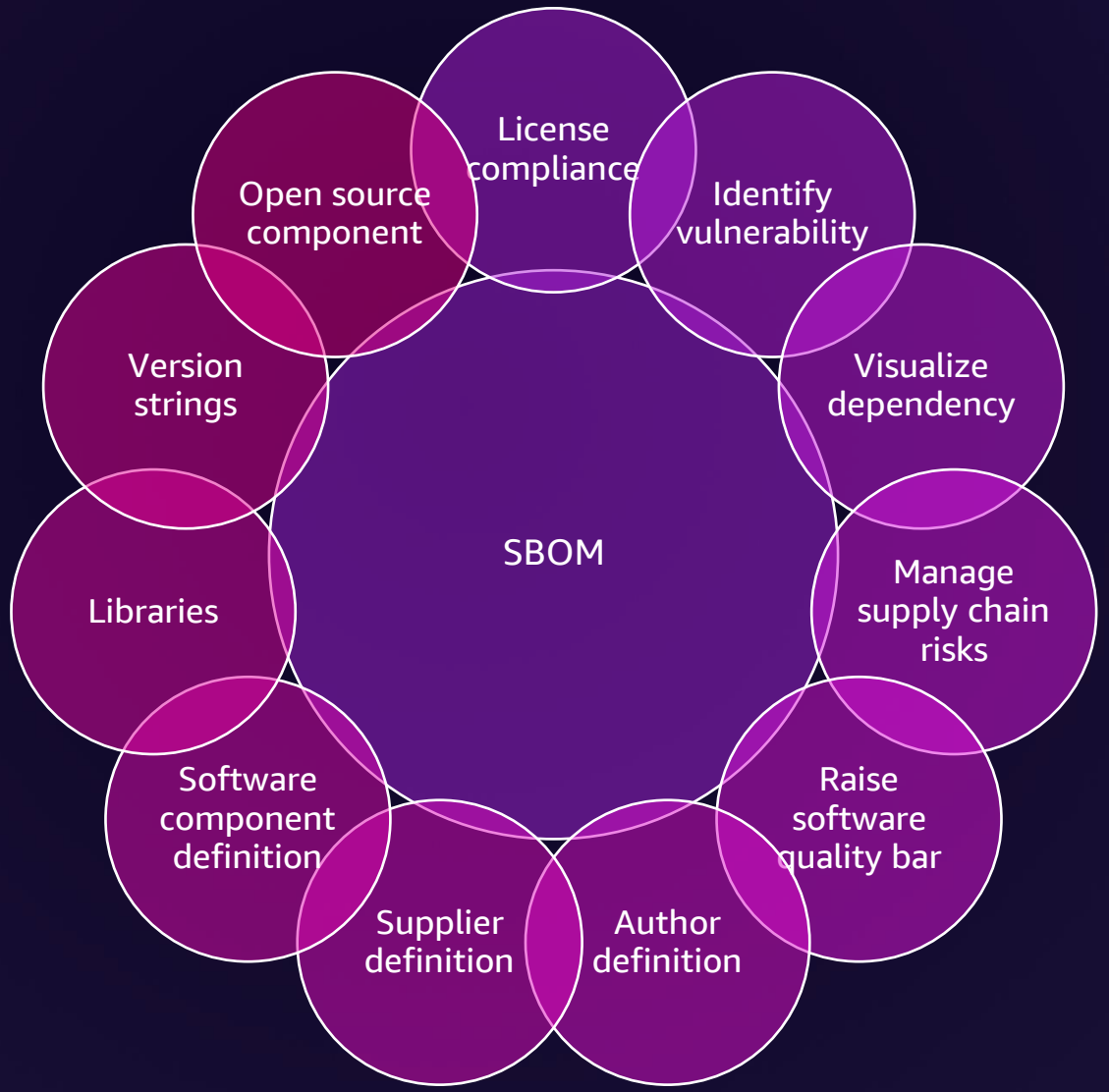
AWS Signer key concepts for workshop

Signing profile

Trust policy

Managed certificates

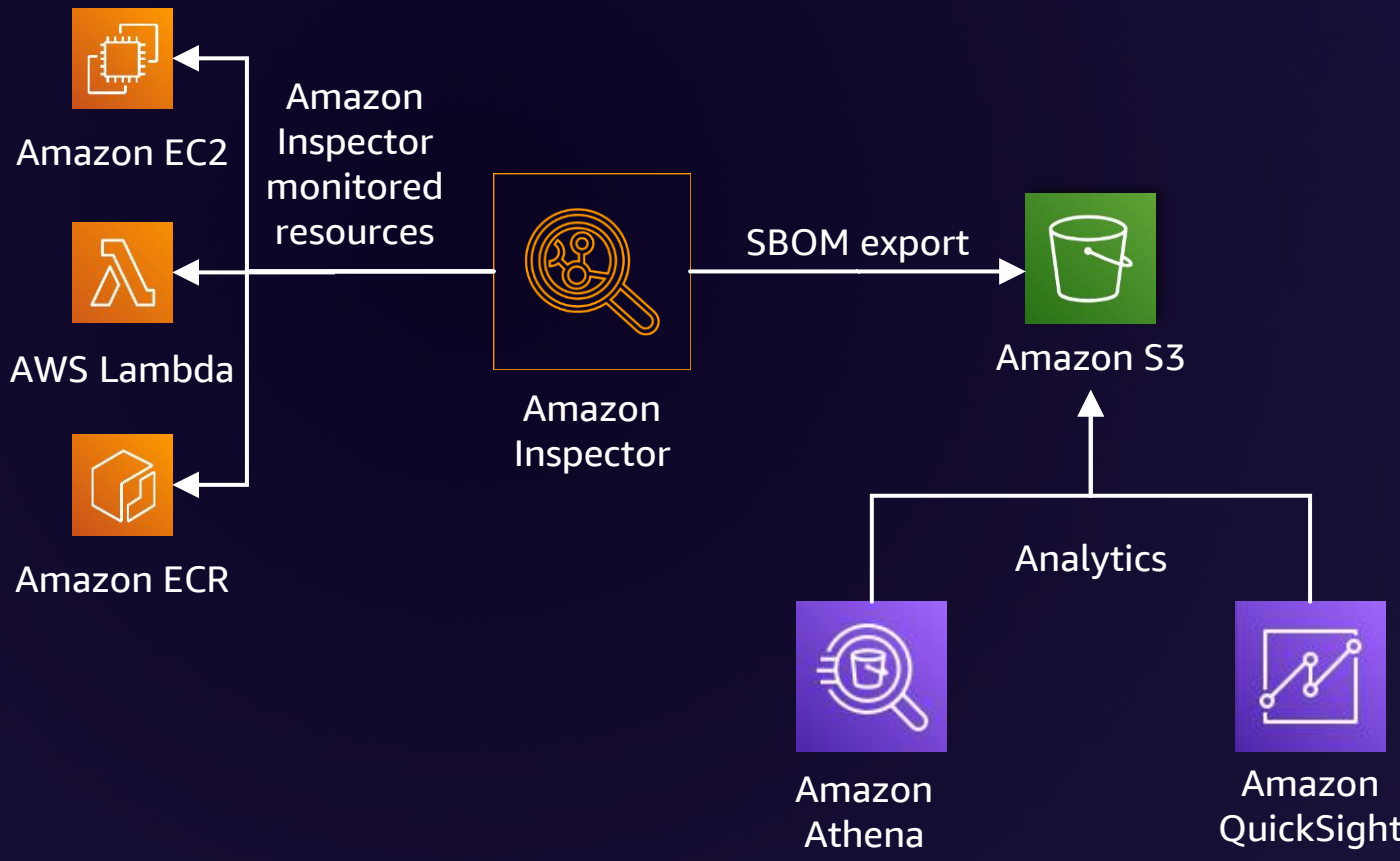
Control 2: Software Bill of Materials (SBOM)




```
{
    "bomFormat": "CycloneDX",
    "components": [
    {
        "bom-ref": "comp-1",
        "name": "Debian GNU/Linux",
        "type": "operating-system",
        "version": "12"
    },{
        "bom-ref": "comp-2",
        "components": [
        {
            "bom-ref": "comp-3",
            "name": "libexpat1",
            "properties": [
            {
                "name": "amazon:inspector:sbom_scanner:info",
                "value": "Component skipped: no rules found."
            } ],
            "purl": "pkg:deb/debian/libexpat1@2.5.0",
            "type": "application",
            "version": "2.5.0-1"
        } ]
    }
}
```

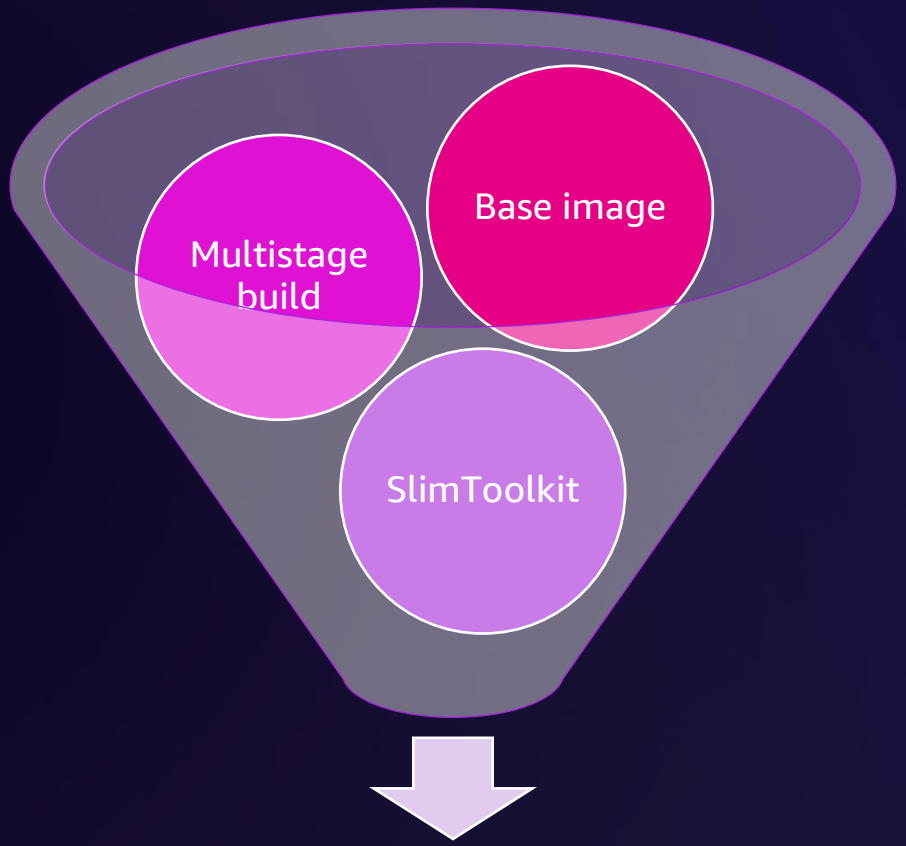
Software Bill of Materials

A Software Bill of Material (SBOM) is defined as a “nested inventory, a list of ingredients” that make up software components



- ✓ SBOM formats supported: CycloneDx and SPDX
- ✓ SBOMs can be exported for the complete org or as granular as a resource
- ✓ Allows export for all resources being actively monitored by Amazon Inspector
- ✓ Includes both operating system (OS) packages and third-party programming language packages
- ✓ Available at no additional charge

Control 3: Slimming



Target architecture