Streamline Security With Shift Left

A Cloud approach

Avinash Jain, a.k.a logicbomb

Security Engineer by mind

A Cricket Player by heart

Blogger at medium @logicbomb

I break stuff to learn

What is Shift Left?

Bringing something close to the source



Considerable rise in the final resultant

Bitwise Left Shift (<<)

Security concerns are taken into consideration during the whole application development, rather than at the end of the process.

Security shouldn't be treated as an after-thought.

Cost of Security increases rapidly as it moves away from the source



Scanning every single code change AWS Codepipeline





Code Pipeline

Continues deployment service. It allows to module visualise. It orchestrate all activities and automate release of software

AWS CI/CD tools



Code Commit

Managed source control code repository service



Code Build

Compose code source code, runs basics tests and create software packages ready to deploy



Automated deployment service, deploy your code to ec2, on premise or Lambda functions



This webhooks configured URL is the heart of our "Continuous Code Hacking"

Add source stage Info Choose pipeline settings Step 2 Source Add source stage Step 3 Source provider This is where you stored your input artifacts for your pipeline. Choose the provider and then provide the connection details. GitHub (Version 1) • Add deploy stage Grant AWS CodePipeline access to your GitHub repository. This allows AWS CodePipeline to upload commits from GitHub to your pipeline. Step 5 **Connect to GitHub** Review The GitHub (Version 1) action is not recommended **(i)** The selected action uses OAuth apps to access your GitHub repository. This is no longer the recommended method. Instead, choose the GitHub (Version 2) action to access your repository by creating a connection. Connections use GitHub Apps to manage authentication and can be shared with other resources. Learn more Change detection options Choose a detection mode to automatically start your pipeline when a change occurs in the source code GitHub webhooks (recommended) AWS CodePipeline Use webhooks in GitHub to automatically start my pipeline Use AWS CodePipeline to check periodically for changes when a change occurs Next Cancel Previous

Webhooks

Developer Tools > CodePipeline > Pipelines > Create new pipeline

Webhooks allow external services to be notified when certain events happe to each of the URLs you provide. Learn more in our Webhooks Guide.

https://ap-south-1.webhooks.a... (push)

https://ap-south-1.webhooks.a... (push)

Add as many build security steps as you want

Stat_scan Failed Pipeline execution ID: f4611e4f-48ac-	-47f7-8050-c3e229abfdf5
dast_scan AWS CodeBuild	٩
791c6a84 🗹 Source: Update buildspe	ec_security_hub.yml
Disable transition	
⊘ dependency_scan Suc Pipeline execution ID: 49565452-d6ar	:ceeded Ie-473a-bd6a-e82247ca75ea
dependency_scan AWS CodeBuild Succeeded - 8 days ago Details	٢
dfcb470f IZ Source: Create buildspe	ec_dast.yml
Disable transition	
Sast_scan Succeeded Pipeline execution ID: 49565452-d6ad	e-473a-bd6a-e82247ca75ea
sast_scan AWS CodeBuild Succeeded - 8 days ago Details	٩

How Buildspec Setup Looks like

Pre_Build

- Setup dependencies
- Pull scanners

Build

- Run scanners and scripts
- Parse result

Post_Build

- Call lambda
- Push results

Eg. Git Secret buildspec.yml

🕑 lo	gicbomb-1 Create Secretscanning_buildspec.yml
ନ୍ୟ 1 cc	ontributor
23 lin	es (22 sloc) 835 Bytes
	version: 0.2
	phases:
	pre_build:
	commands:
	– echo "Setting CodeCommit Credentials"
	– git config ––global credential.helper '!aws codecommit credential-helper
	- git configglobal credential.UseHttpPath true
	– echo "Copying secrets_config.json to the application directory"
10	- cp secrets_config.json \$CODEBUILD_SRC_DIR_AppSource/secrets_config.json
11	 echo "Switching to the application directory"
12	– echo "Installing truffleHog"
13	- which pip3 && pip3version
14	– which python3 && python3 –-version
15	<pre>- pip3 install 'truffleHog>=2.1.0,<3.0'</pre>
16	build:
17	commands:
18	– echo "Build started on \$(date)"
19	– echo "Scanning with truffleHog"
20	– trufflehog ––regex ––rules secrets_config.json ––entropy=False \${PR0JECT
21	post_build:
22	commands:
23	– echo "Build completed on \$(date)"

AWS_Devsecops / Secretscanning_buildspec.yml

ያ main 🚽

Continuous code hacking capabilities:

- 1. **SAST** Scanning source code for vulnerabilities.
- 2. **DAST** Performing Dynamic Application Security Testing.
- 3. Dependency Scanning Analyze external dependencies for known vulnerabilities.
- 4. Secret Detection Detecting secrets in the PR.
- 5. Additional Capabilities Dockerfile linter, Check whitelist of base images.

AWS DevSecOps Pipeline Architecture



[Container] 2021/04/18 06:56:43 Running command trufflehog --regex --entropy=False \${

[Container] 2021/04/18 06:56:49 Command did not exit successfully trufflehog --regex --[Container] 2021/04/18 06:56:49 Phase complete: BUILD State: FAILED [Container] 2021/04/18 06:56:49 Phase context status code: COMMAND_EXECUTION_ERROR Mes \${SOURCE_REP0_URL} > secret_result.txt. Reason: exit status 1 [Container] 2021/04/18 06:56:49 Entering phase POST_BUILD [Container] 2021/04/18 06:56:49 Running command cat secret_result.txt

Reason: RSA private key Date: 2021-04-18 06:09:34 Hash: dbad4d48682f6aa6e0548283d1baa8373214b91a Filepath: test Branch: origin/master Commit: Update test -----BEGIN RSA PRIVATE KEY-----

~~~~~~~

#### Reason: SSH (OPENSSH) private key Date: 2021-04-18 06:09:34 Hash: dbad4d48682f6aa6e0548283d1baa8373214b91a Filepath: test Branch: origin/master Commit: Update test -----BEGIN OPENSSH PRIVATE KEY-----

Reason: SSH (DSA) private key Date: 2021-04-18 06:09:34 Hash: dbaddd48682f6aa6e0548283d1baa8373214b91a Filepath: test Branch: origin/master Commit: Update test -----BEGIN DSA PRIVATE KEY-----

Reason: SSH (EC) private key Date: 2021-04-18 06:09:34 Hash: dbad4d48682f6aa6e0548283d1baa8373214b91a Filepath: test Branch: origin/master Commit: Update test -----BEGIN EC PRIVATE KEY-----

Reason: PGP private key block Date: 2021-04-18 06:09:34 Hash: dbad4d48682f6aa6e0548283d1baa8373214b91a Filepath: test Branch: origin/master Commit: Update test -----BEGIN PGP PRIVATE KEY BLOCK-----

## Secret Scanning Result

#### Dependency Checker Result

```
[Container] 2021/04/19 16:19:13 Running command high_risk_dependency=$( cat dependency-check-r
[Container] 2021/04/19 16:19:13 Phase complete: BUILD State: SUCCEEDED
[Container] 2021/04/19 16:19:13 Phase context status code: Message:
[Container] 2021/04/19 16:19:13 Entering phase POST_BUILD
[Container] 2021/04/19 16:19:13 Running command cat dependency-check-report.json
  "reportSchema" : "1.1",
  "scanInfo" : {
    "engineVersion" : "6.0.5",
    <u>"data</u>Source" : [ {
      "name" : "NVD CVE Checked",
      "timestamp" : "2021-04-19T16:18:30"
   }, {
      "name" : "NVD CVE Modified",
      "timestamp" : "2021-04-19T14:01:28"
   4,
      "name" : "VersionCheckOn",
      "timestamp" : "2021-04-19T16:18:30"
   }]
  "projectInfo" : {
   "name" : "",
    "reportDate" : "2021-04-19T16:19:11.706616Z",
    "credits" : {
      "NVD" : "This report contains data retrieved from the National Vulnerability Database:
      "NPM" : "This report may contain data retrieved from the NPM Public Advisories: <u>https://</u>
      "RETIREJS" : "This report may contain data retrieved from the RetireJS community: https:
      "OSSINDEX" : "This report may contain data retrieved from the Sonatype OSS Index: https:
  "dependencies" : [ {
    "isVirtual" : false.
   "fileName" : "Counter.js",
    "filePath" : "/codebuild/output/src787654664/src/src/components/Root/Counter/Counter.js",
    "md5" : "ecf0b6eae8c1a2995fa00d419ea76528",
    "sha1" : "f1c7be02c19b61185606aef948a4865492af761e",
    "sha256" : "3f6cb30e19e75ced762f0164f7ea3b32890e5b71ae11350cd8d296f740e22364",
    "evidenceCollected" : {
      "vendorEvidence" : [].
      "productEvidence" : [ ],
      "versionEvidence" : [ ]
```

# Docker Linter Result

```
[Container] 2021/01/29 10:48:17 Running command echo $result | jq .
   "line": 2,
   "code": "DL3006",
   "message": "Always tag the version of an image explicitly",
   "column": 1,
   "file": "/dev/stdin",
   "level": "warning"
 },
    "line": 3.
   "code": "DL4000",
   "message": "MAINTAINER is deprecated",
    "column": 1,
   "file": "/dev/stdin",
   "level": "error"
 },
   "line": 5,
   "code": "DL3009",
   "message": "Delete the apt-get lists after installing something",
    "column": 1,
   "file": "/dev/stdin",
    "level": "info"
 },
    "line": 6,
   "code": "DL3008",
   "message": "Pin versions in apt get install. Instead of `apt-get install
   "column": 1,
    "file": "/dev/stdin",
    "level": "warning"
 },
```

### Static Code Scanning Result

```
[Container] 2021/04/27 17:27:19 Running command echo "build stage completed"
build stage completed
[Container] 2021/04/27 17:27:19 Running command curl https://sonarcloud.io/api/issues/search?compone
 % Total % Received % Xferd Average Speed Time
                                                      Time
                                                                Time Current
                                Dload Upload
                                              Total Spent
                                                                Left Speed
 0
            0
                  0
                       0
                             0
                                    0
                                           0 --:--:-- --:--:--
                                                                           0
 0
            0
                  0
                       0
                             0
                                    0
                                           0 --:--:-- --:--:--
                                                                           0
100 2063 100 2063
                       0
                             0
                                 3069
                                           0 --:--:-- 3065
[Container] 2021/04/27 17:27:21 Running command cat sonarqube_scanreport.json | jq
 "total": 2,
 "p": 1,
  "ps": 100.
  "paging": {
    "pageIndex": 1,
    "pageSize": 100,
    "total": 2
 },
 "effortTotal": 5,
 "debtTotal": 5,
 "issues": [
     "key": "AXdRUyCfxYDiaJy6JNW_",
      "rule": "javascript:S1117",
     "severity": "MAJOR",
     "component": "logicbomb-1_aws-codepipeline-demo:src/components/Root/Counter/Counter.js",
      "project": "logicbomb-1_aws-codepipeline-demo",
      "line": 38.
     "hash": "2293d372f10d104f6265ca91ff972892",
     "textRange": {
       "startLine": 38.
       "endLine": 38.
       "startOffset": 5.
       "endOffset": 12
     },
     "flows": [],
     "status": "OPEN".
     "message": "'counter' is already declared in the upper scope.",
     "effort": "5min",
     "debt": "5min",
     "tags": [],
     "creationDate": "2019-11-23T09:55:35+0100",
     "updateDate": "2021-01-30T04:25:24+0100",
      "type": "CODE_SMELL",
     "organization": "logicbomb-1"
   },
     "key": "AXdRUyEGxYDiaJy6JNXA",
      "rule": "Web:S5254",
     "severity": "MAJOR",
      "component": "logichomb-1 gwg-codenineline-demo:snc/index html"
```

# DAST Scanning Result

| DAST Results                                     | 021/04/27 17:32:30 Running command echo DAST Results                                                                                                       |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Container] 2<br>[INF0]<br>[INF0]<br>[INF0]<br>+ | 021/04/27 17:32:30 Running command cat result.txt<br>Starting ZAP daemon<br>Running a quick scan for <u>http://testphp.vulnweb.com/</u><br>Issues found: 1 |
| Alert<br> <br>                                   | +<br>  Risk   CWE ID   URL                                                                                                                                 |
| Cross Site<br>)//%0D%0A%0d%                      | Scripting (DOM Based)   High   79   <u>http://testphp.vulnw</u><br>Øa//\x3csVg/ <svg onload="&lt;/th"></svg>                                               |
| [INF0]                                           | Shutting down ZAP daemon                                                                                                                                   |
| [Container] 2<br>Build complet                   | 021/04/27 17:32:30 Running command echo Build completed                                                                                                    |

[Container] 2021/04/27 17:32:30 Phase context status code: COMMAND\_EXECUTION\_ quick-scan --self-contained --start-options '-config api.disablekey=true' htt

[Container] 2021/04/27 17:32:30 Entering phase POST\_BUILD

[Container] 2021/04/27 17:32:30 Phase complete: POST\_BUILD State: SUCCEEDED [Container] 2021/04/27 17:32:30 Phase context status code: Message:

#### Other Continuous code hacking capabilities:

- 1. **Reporting** Sharing reports and status over slack and mailbox.
- 2. Alerting Alerts for build success and failure.
- 3. Vulnerability Management All findings are managed over AWS Security Hub.

## Reporting Over Slack channels

incoming-webhook APP 12:01 AM

Issue No.: 1, Type: CODE\_SMELL, Vulnerable Component: logicbomb-1\_awscodepipeline-demo:src/components/Root/Counter/Counter.js, Fix: 'counter' is already declared in the upper scope.

Sonarqube Report

Issue No.: 2, Type: BUG, Vulnerable Component: logicbomb-1\_aws-codepipelinedemo:src/index.html, Fix: Add "lang" and/or "xml:lang" attributes to this "<html>" element

Sonarqube Report

Issue No.: 1, Type: CODE\_SMELL, Vulnerable Component: logicbomb-1\_awscodepipeline-demo:src/components/Root/Counter/Counter.js, Fix: 'counter' is already declared in the upper scope.

Sonarqube Report

Issue No.: 2, Type: BUG, Vulnerable Component: logicbomb-1\_aws-codepipelinedemo:src/index.html, Fix: Add "lang" and/or "xml:lang" attributes to this "<html>" element

Sonarqube Report

Issue No.: 1, Type: CODE\_SMELL, Vulnerable Component: logicbomb-1\_awscodepipeline-demo:src/components/Root/Counter/Counter.js, Fix: 'counter' is already declared in the upper scope.

Sonarqube Report

Issue No.: 2, Type: BUG, Vulnerable Component: logicbomb-1\_aws-codepipelinedemo:src/index.html, Fix: Add "lang" and/or "xml:lang" attributes to this "<html>" element

Sonarqube Report

Issue No.: 1, Type: CODE\_SMELL, Vulnerable Component: logicbomb-1\_awscodepipeline-demo:src/components/Root/Counter/Counter.js, Fix: 'counter' is already declared in the upper scope.

#### Build Status Over Mailbox

AWS Codepipeline Security Notification Message (External) D Inbox × To-me × To-respond ×

#### **AWS Notifications**

to me 🔻

("account": 369737379577", "detailType": "CodeBuild Build Phase Change", "region": ap-south-11", "source": "aws.codebuild", "time": 2021-04. 369737379577:notificationrule/84ffa2090036c2daf5919ddd0196fae06e40b79a", "detail": ("completed-phase": "QUEUED", "project-name": "detail": ("type": "NO\_CACHE"), "build-number": 43.0, "tim time": "Apr 27, 2021 5:30:20 PM"; "source": ("type": "CODEPIPELINE"), "source-version"; "arn:aws:s3:::codepipeline-ap-south-1-38547174211 image": "aws/codebuild/standard:5.0", "privileged-mode": true, "image-pull-credentials-type": "CODEBUILD, "compute-type": "BUILD\_GENER type": "PLAINTEXT", "value": "logicbomb1"}, ("name": "DOCKER\_PASSWORD", "type": "PLAINTEXT", "value": "test1234567"})}, "project-file-sys south-1#liggEvent group=null:stream=null"}, "phases": [("phase-context": [], "start-time": "Apr 27, 2021 5:30:20 PM", "end-time": "Apr 27, 2021 5:30:20 PM", "end-time: "Apr 27, 2021 FM", "duration-in-seconds": 1.0, "phase-type: "Completed-phase-status", "SUCCEEDED", "completed-phase-duration-seconds", "Succeenter and "Apr 27, 2021 FM", "resources": ["arn:aws:codebuild:ap-south-1:369737379577:build/dats\_scan:31d311ce-e722-4757-bd50-defa.

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe: https://sns.ap-south-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:ap-south-1:369737379577:codestar-notifications-

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.am

#### AWS Notifications

to me 🔻

{"account"."369737379577","detailType":"CodeBuild Build State Change","region"."ap-south-1","source"."aws.codebuild","time":"2021-04-2 369737379577:notificationrule/84ffa2090036c2daf5919ddd0196fae06e40b79a","detail":{"build-status":"IN\_PROGRESS","project-name"."c 47b7-bd50-dtd79b8fb492","additional-information":{"cache":{"type":"NO\_CACHE"},"timeout-in-minutes":60.0,"build-complete":false,"initiato {"type":"CODEPIPELINE"},"source-version":"am:aws:s3:::codepipeline-ap-south-1-385471742157/devsecops\_1/SourceArti/aVVCUHD.zip mode":true,"image-pull-credentials-type":"CODEBUILD", "compute-type":"BUILD\_GENERAL1\_SMALL","type":"LINUX\_CONTAINER","envi {"name":"DOCKER\_PASSWORD","type":"PLAINTEXT", "value":"test1234567"}}, "project-file-system-locations":[],"logs":("deep-link":"<u>https://</u> stream=null"},"queued-timeout-in-minutes":480.0},"current-phase":"SUBMITTED", "current-phase-context":"[]", "version":"1"},"resources":["a dfd79b8fb492"],"additionalAttributes":{}

...

#### **AWS Notifications**

to me 🔻

("account"."369737379577","detailType"."CodeBuild Build Phase Change", "region":"ap-south-11","source":"aws.codebuild", "time":"2021-04-369737379577:notificationrule/84ffa2090036c2daf5919ddd0196fae06e40b79a","detail":{"completed-phase":"SUBMITTED","project-name" e722-47b7-bd50-dff79b8fb492", "completed-phase-context":"[]","additional-information":{"cache":{"type":"NO\_CACHE"},"build-number":43. time":"Apr 27, 2021 5:30:20 PM", "source":{"type":"CODEPIPELINE"}, "source-version":"am:aws:s3:::codepipeline-ap-south-1-3854717421! image":"aws/codebuild/standard:5.0", "privileged-mode":true, "image-pull-credentials-type":"CODEBUILD", "compute-type":"BUILD\_GENER type":"PLAINTEXT", "value":"logicomb1"}, "name":"DOCKER\_PASSWORD", "type":"PLAINTEXT", "value":"test1234567"}}, "build-number."

## Vulnerability Management Over AWS Security Hub

|       | Workflow statu                         | s 🔻 Create insight                                                              |                             | XSS vulnerability                                                                                          |                                          | × |
|-------|----------------------------------------|---------------------------------------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------|------------------------------------------|---|
|       |                                        |                                                                                 |                             | Finding ID: Id2                                                                                            |                                          |   |
| Recor | d state is ACTIVE                      | E X X                                                                           |                             | LOW<br>Vulnerability in http://testphp.vulnweb.                                                            | com/                                     |   |
|       |                                        | < 1                                                                             | >                           | Workflow status                                                                                            | RECORD STATE<br>ACTIVE                   |   |
|       |                                        |                                                                                 |                             | utories neer u                                                                                             | Set by the finding provider              |   |
| any   | Product                                | Title 🗸                                                                         | R                           | AWS account ID<br>369737379577 ⊕                                                                           | Created at<br>2021-04-22T17:05:54 8327 ↔ |   |
|       | Systems<br>Manager<br>Patch<br>Manager | Systems Manager<br>Patch Summary -<br>Managed Instance<br>Non-Compliant         | E(<br><u> -</u><br><u>0</u> | Updated at<br>2021-04-22T17:05:54.832Z @                                                                   | Product name<br>Default @                |   |
|       | Systems<br>Manager<br>Patch<br>Manager | Systems Manager<br>Patch Summary -<br>Managed Instance<br>Non-Compliant         | E(<br><u> -</u><br><u>O</u> | Severity label<br>■ LOW @                                                                                  | Company name<br>Personal ତ୍ୱ             |   |
| on    | GuardDuty                              | Unprotected port on<br>EC2 instance i-<br>0d2e271f1475b7ac8<br>is being probed. | E(<br><u>i-</u><br><u>0</u> | <ul> <li>Types and Related Findings</li> <li>Types</li> <li>Software and Configuration Checks/N</li> </ul> | ;<br>/ulnerabilities/CVE                 | • |
| nal   | Default                                | XSS vulnerability                                                               | сі<br>1                     | Resources  Resources detail                                                                                |                                          |   |
|       |                                        |                                                                                 |                             | 123                                                                                                        |                                          | • |
|       |                                        |                                                                                 |                             | Resource type<br>CodeBuild ପ୍                                                                              | Resource ID<br>123 @                     |   |
|       |                                        |                                                                                 |                             | Finding Provider Fields                                                                                    |                                          |   |
|       |                                        |                                                                                 |                             | Finding Provider Fields detail                                                                             |                                          |   |
|       |                                        |                                                                                 |                             | Finding Provider Field                                                                                     |                                          | ▼ |
|       |                                        |                                                                                 |                             | Provider severity label                                                                                    |                                          |   |

nazon

rsonal

#### **Benefits:**

- 1. Real time Checks Real time changes to the code triggers security checks
- 2. **Reporting** Result and status can be shared across different communication channels.
- 3. Highly Flexible Modularity with standardized interfaces.
- 4. **Completely Automated** Automation is the key here.
- 5. Vulnerability Management Manage vulnerabilities at single place.

#### SHORT DEMO



#### Thank You!

Twitter: @logicbomb\_1

Website: <u>https://logicbomb.in/</u>

Email: avinash.logicbomb@gmail.com



