

CyberRes

Cloud DevSecOps

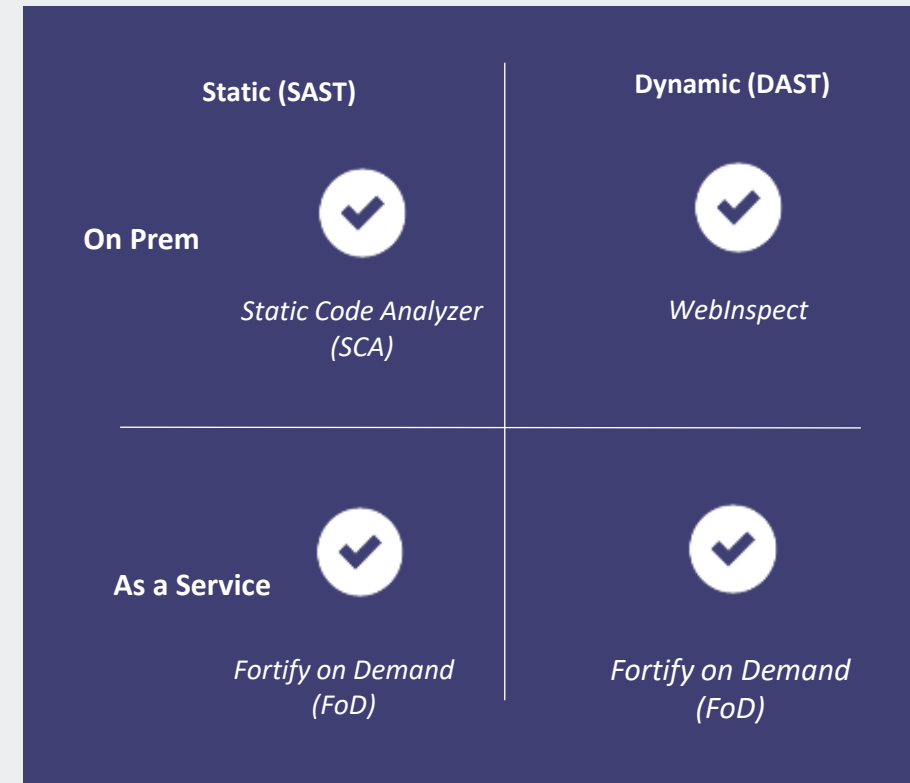
Application Security

Rohit Baryha, CyberRes Market Development Technical Consultant

Fortify Portfolio

Automate testing throughout the CI/CD pipeline, enable developers to quickly resolve issues

- **Static Code Analyzer (SCA):** Analyzes source code for security vulnerabilities (SAST)
- **WebInspect:** Dynamic testing (DAST) analyzes applications in their running state and simulates attacks against an application to find vulnerabilities
- **Fortify on Demand (FoD):** AppSec as a Service, that includes SAST, DAST, and MAST
- **Software Security Center:** Holistic application security platform included with on-premises solutions to get complete visibility of application security risks
- **Sonatype:** Scans open source components for vulnerabilities



Solutions that Align With DevSecOps Success



Integration



Automation



Speed

Backed by the Market Leading Software Security Research Team

1,000+ Vulnerability Categories | 27 Programming Languages | 1M+ Individual APIs

Demo Overview

Azure DevOps

- Integration using Build / Release Tasks
- Integration using YML / Classic UI
- Integration with Fortify On Prem
- Static Analysis Integration
- Source Code Composition analysis using Sonatype
- Dynamic Analysis using ScanCentral

AWS CodeStar

- Integration using YML
- Integration with Fortify On Prem
- Static Analysis Integration
- Source Code Composition analysis using Sonatype
- Dynamic Analysis using ScanCentral
- Continuous Feedback

GCP CloudBuild

- Integration using YML
- Integration with Fortify On Prem
- Static Analysis Integration with docker build

Pre-Requisites

Cloud DevOps – CI / CD Environment

Cloud Hosted Runner / Agent*

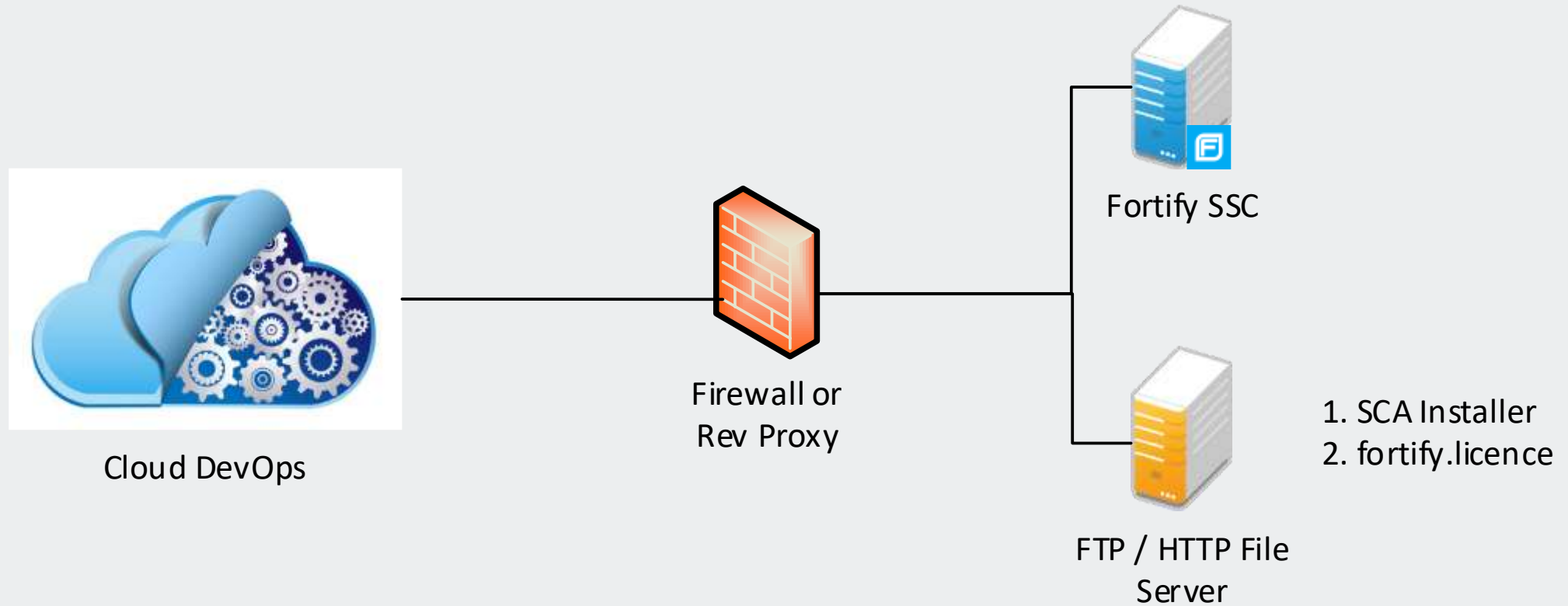
- Standard images - Linux, Windows, MacOS
- Most of the tools are pre-installed
- Can use Container images from Docker Hub*
- Runs on Cloud and Self Destroyed when pipeline stops
- Environment cannot be retained

Self Hosted Runner / Agent

- Customized & Flexible images – Linux, Windows, MacOS
- Customer has to install and configure the environment
- Cloud DevOps Agent need to be installed and configure.
- Cloud DevOps Agent and Cloud Environment has to communicate to each other.
- Environment can be retained & tailored as per requirement

* Depends on cloud vendor

Native SAST Integration – Traditional Approach



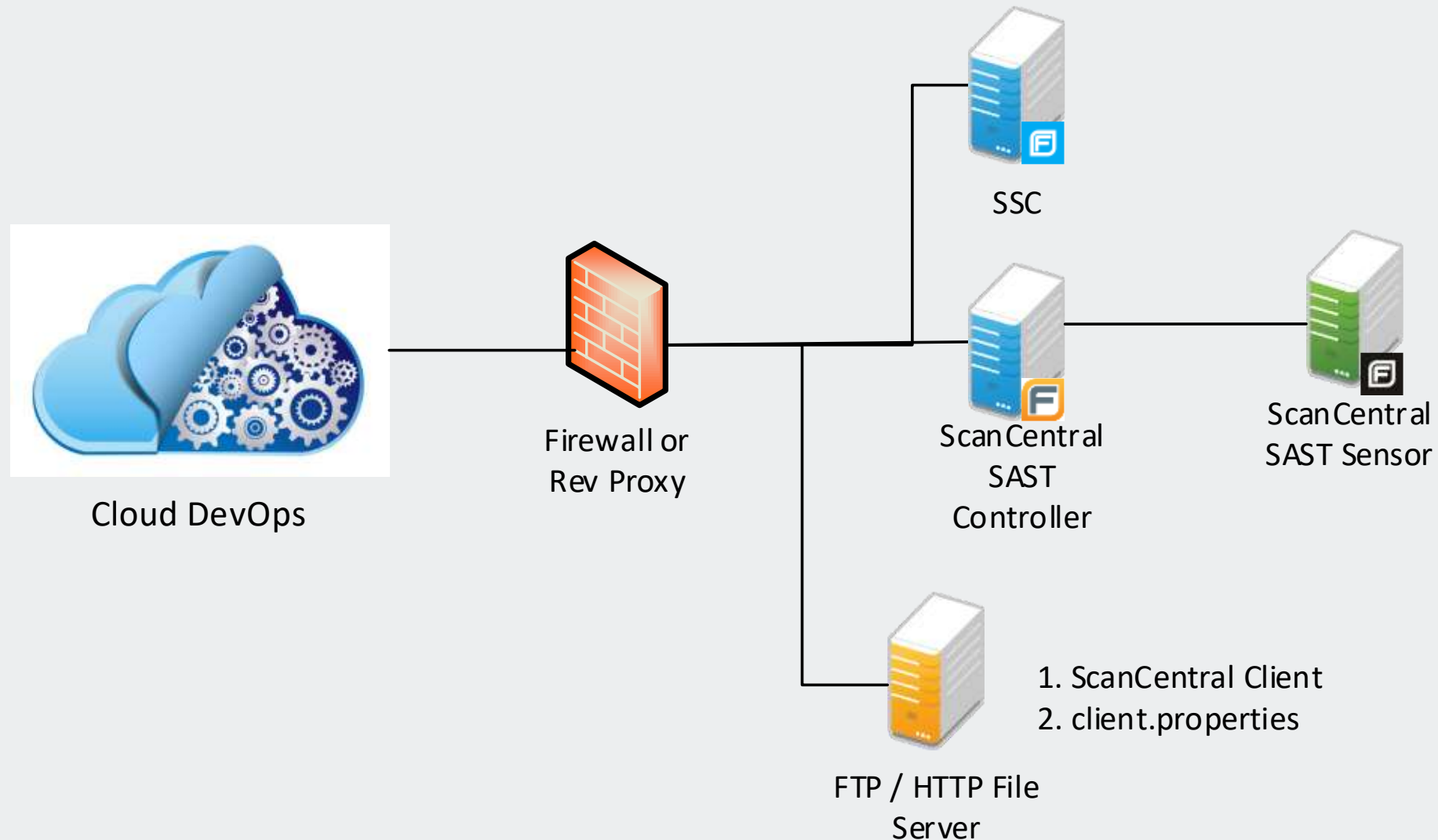
Native SAST Integration - Traditional Approach - Steps

1. Download the SCA Installer file ~1 GB
2. Download the fortify.license file
3. Install the SCA using installer and license file
4. Update the Rulepacks
5. Translate the code using SCA CLI
6. Analyze the code using SCA CLI
7. Upload the results to SSC via FortifyClient
8. Apply Quality Gate via FPRUtility (Optional)

SSC – Allow Download files

- Modify \ssc\WEB-INF\internal\securityContext.xml
- Uncomment –
 - `<security:intercept-url pattern="/downloads/**" access="PERM_ANONYMOUS" />`
- Copy required files in \ssc\WEB-INF\downloads or \ssc\downloads folder
 - Fortify_SCA_and_Apps_20.2.0_windows_x64.exe
 - fortify.license file
- http://ip:8180/ssc/downloads/Fortify_SCA_and_Apps_20.2.0_windows_x64.exe
- <http://ip:8180/ssc/downloads/fortify.license>

NextGen SAST Integration – ScanCentral SAST Approach



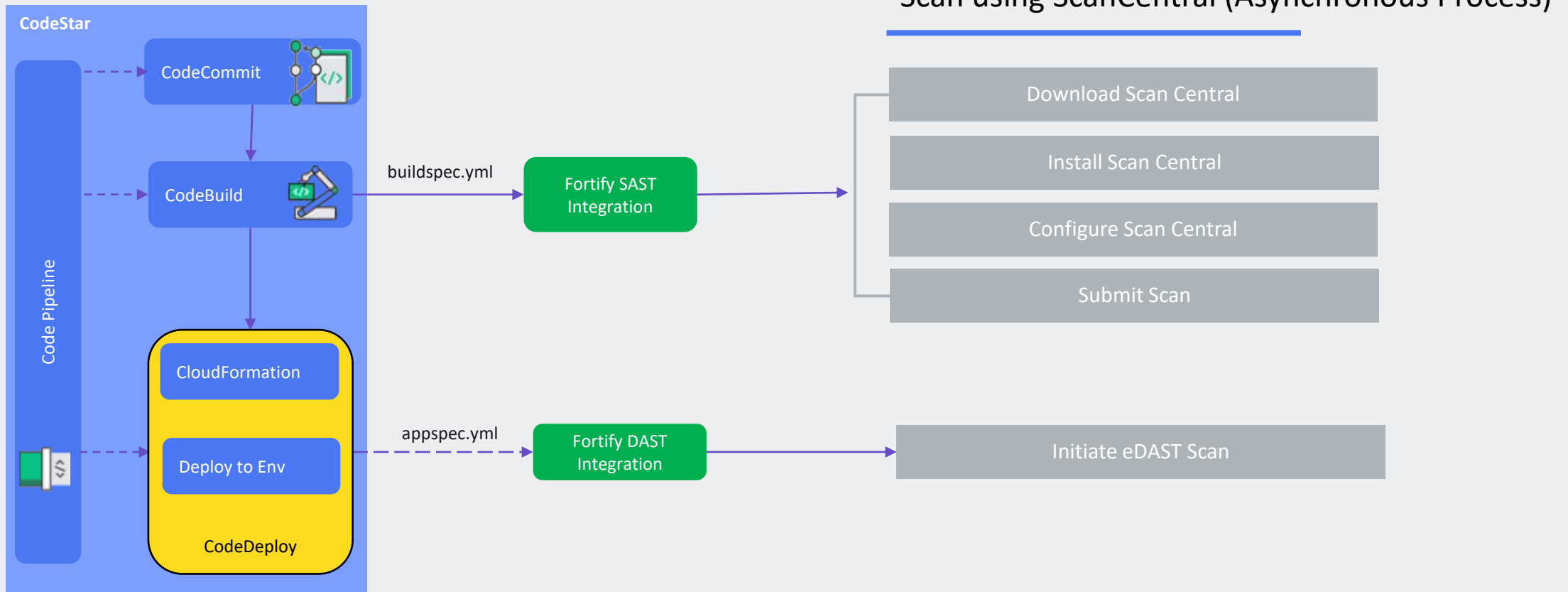
NextGen SAST Integration – ScanCentral Approach

1. Download the ScanCentral Client file ~60 MB, {required Java version >=1.8}
2. Extract the ScanCentral Client
3. Download / Create the client.properties file
4. Translate the code (conditional)
5. Upload the code via ScanCentral Client to ScanCentral Controller
6. Results will be uploaded to SSC
7. Quality Gate (may be in next release)

The AWS CodeStar logo is displayed in white text on a dark blue background. The background features a pattern of various geometric shapes, including circles, squares, and triangles, some of which are partially visible or cut off by the edges of the frame. The text "AWS CodeStar" is written in a clean, sans-serif font, with "AWS" in a smaller weight than "CodeStar".

AWS CodeStar

CodeBuild using SCA and ScanCentral



AWS DevOps

Components of AWS CodeStar

- AWS Module: CodeStar
- `appspec.yml` - this file is used by AWS CodeDeploy when deploying the web application to EC2
- **`buildspec.yml`** - this file is used by AWS CodeBuild to build the web application
- `pom.xml` - this file is the Maven Project Object Model for the web application
- `src/main` - this directory contains your Java service source files
- `src/test` - this directory contains your Java service unit test files
- `scripts/` - this directory contains scripts used by AWS CodeDeploy when installing and deploying your application on the Amazon EC2 instance
- `template.yml` - this file contains the description of AWS resources used by AWS CloudFormation to deploy your infrastructure
- `template-configuration.json` - this file contains the project ARN with placeholders used for tagging resources with the project ID

AWS - buildspec.yml

DVJA / buildspec.yml [Info](#)

```
1 version: 0.2
2
3 phases:
4   install:
5     runtime-versions:
6       java: corretto11
7     commands:
8       # Upgrade AWS CLI to the latest version
9       - pip install --upgrade awscli
10  pre_build:
11    commands:
12      #- mvn clean compile test
13      - mvn clean
14  build:
15    commands:
16      - mvn package
17  post_build:
18    commands:
19      # Do not remove this statement. This command is required for AWS CodeStar projects.
20      # Update the AWS Partition, AWS Region, account ID and project ID in the project ARN in template-configuration.json file so AWS CloudFormation can tag project resources.
21      - sed -i.bak 's/\$PARTITION\$/'${PARTITION}'/g;s/\$AWS_REGION\$/'${AWS_REGION}'/g;s/\$ACCOUNT_ID\$/'${ACCOUNT_ID}'/g;s/\$PROJECT_ID\$/'${PROJECT_ID}'/g' template-configuration.json
22      - bash scascan.bash
23  artifacts:
24    files:
25      - 'appspec.yml'
26      - 'template.yml'
27      - 'scripts/*'
28      - 'target/ROOT.war'
29      - 'template-configuration.json'
30
```

SCAScan.bash

DVJA / scascan.bash [Info](#)

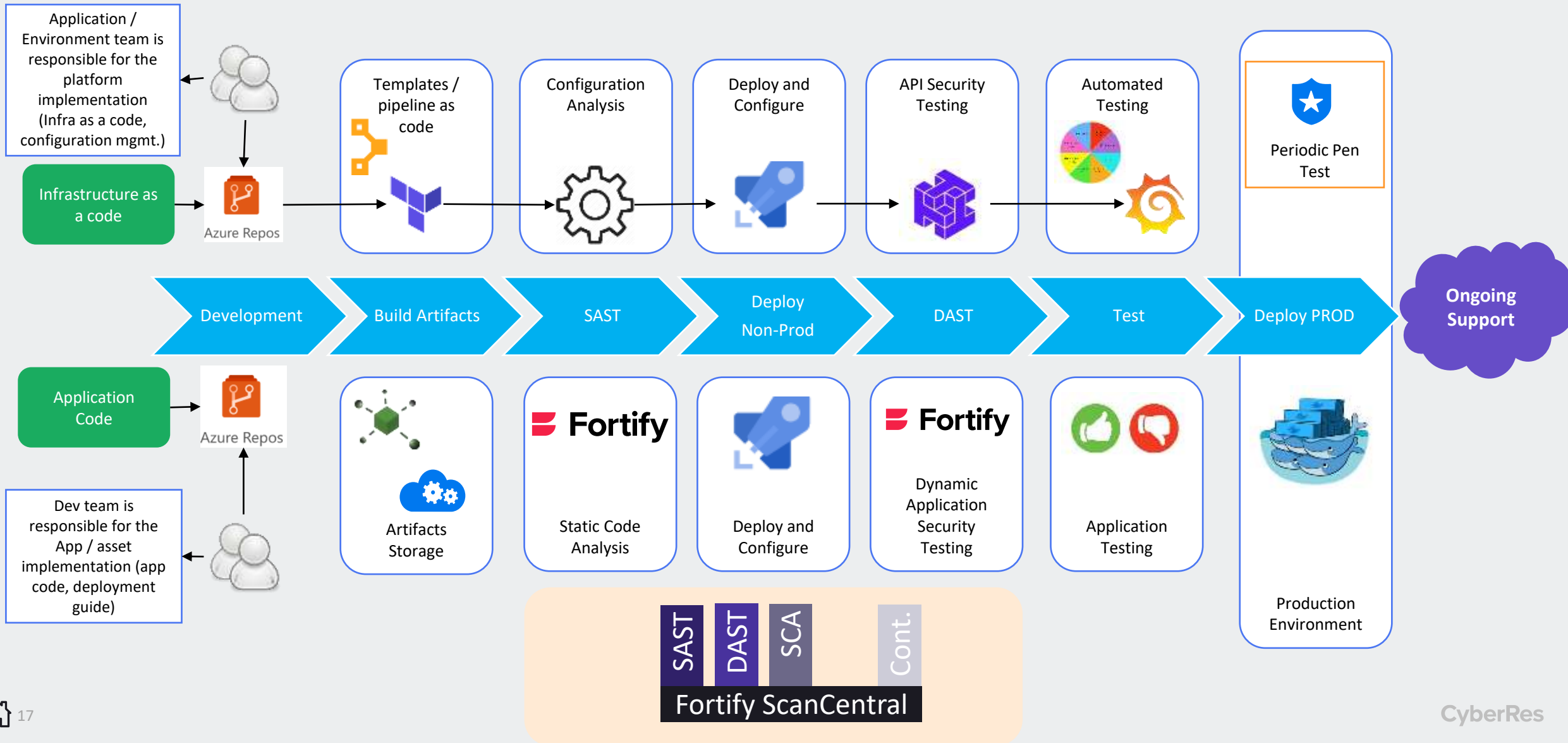
Edit

```
1 #!/bin/bash
2
3 #Getting downloaders
4 wget -nv --no-check-certificate https://[REDACTED]:8443/ssc/downloads/Fortify_SCA_and_Apps_20.2.0_linux_x64.run
5
6 wget -nv --no-check-certificate https://[REDACTED]:8443/ssc/downloads/fortify.license
7
8 wget --no-check-certificate https://[REDACTED]:8443/ssc/downloads/SSC.cer
9 chmod +x ./Fortify_SCA_and_Apps_20.2.0_linux_x64.run
10 ./Fortify_SCA_and_Apps_20.2.0_linux_x64.run --fortify_license_path ./fortify.license --mode unattended --installdir
/opt/Fortify/Fortify_SCA_and_Apps_20.2.0/
11 /opt/Fortify/Fortify_SCA_and_Apps_20.2.0/bin/fortifyupdate
/opt/Fortify/Fortify_SCA_and_Apps_20.2.0/jre/bin/keytool -importcert -trustcacerts -alias SSC -keystore
12 /opt/Fortify/Fortify_SCA_and_Apps_20.2.0/jre/lib/security/cacerts -file ./SSC.cer -storepass changeit -noprompt
13 /opt/Fortify/Fortify_SCA_and_Apps_20.2.0/bin/sourceanalyzer -b aws-java -clean
/opt/Fortify/Fortify_SCA_and_Apps_20.2.0/bin/sourceanalyzer -b aws-java -source 1.8 -cp ".*/*/*.jar" ".*/*/*.java"
14 ".*/*/*.js" ".*/*/*.jsp" ".*/*/*.html" ".*/*/*.properties" ".*/*/*.xml"
15 /opt/Fortify/Fortify_SCA_and_Apps_20.2.0/bin/sourceanalyzer -b aws-java -scan -f AWS-SAST.fpr
/opt/Fortify/Fortify_SCA_and_Apps_20.2.0/bin/fortifyclient -url https://[REDACTED]:8443/ssc/ -authtoken 169c2c01-
16 8902-4b42-af2c-1b11f8536f85 -applicationVersionID "10023" uploadFPR -file AWS-SAST.fpr
17
```



Azure DevOps

Fortify enable Azure DevOps



Azure DevOps

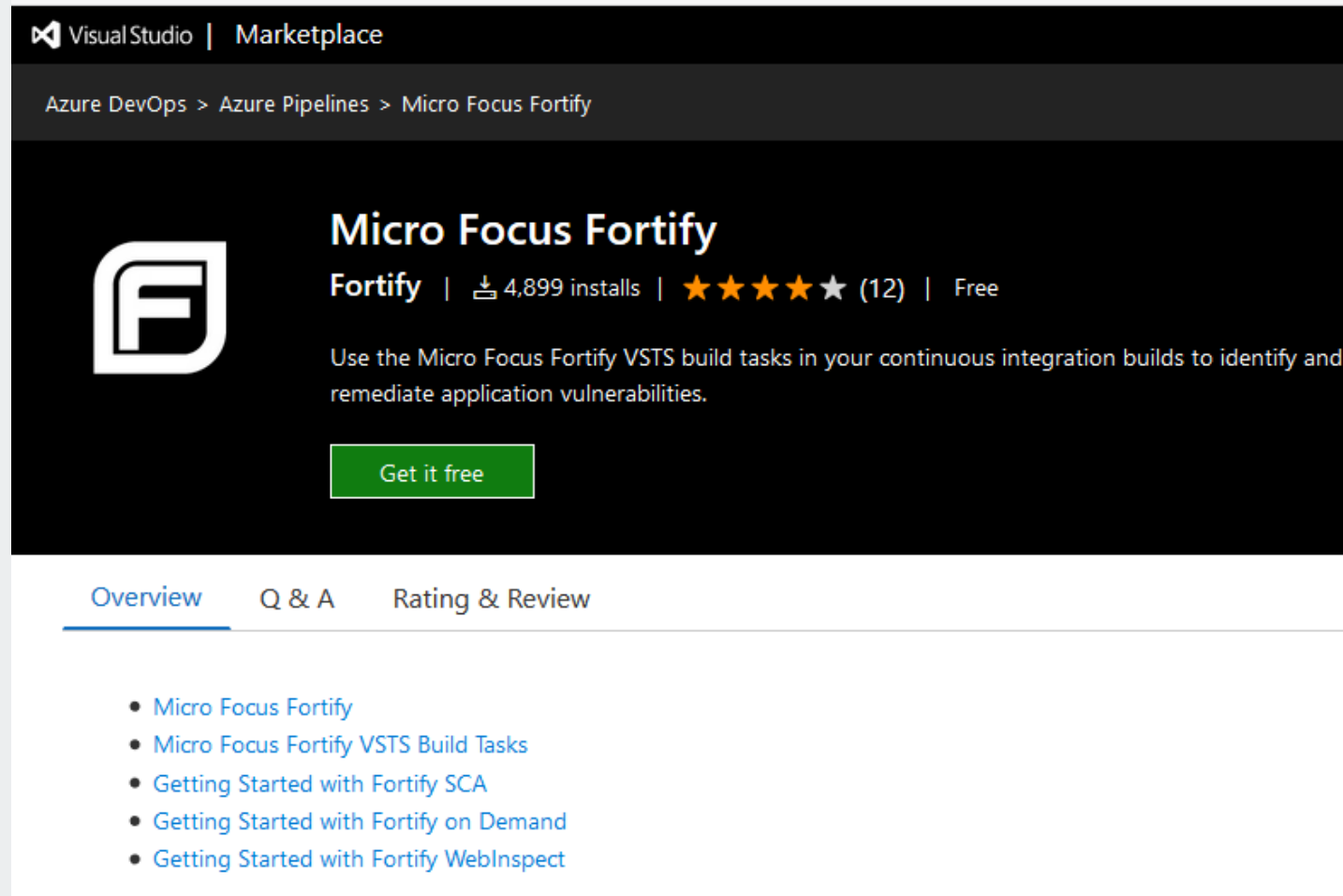
- Integration is with Build Pipeline
- Plugins are available
- Main config file is **azure-pipelines.yml** file

Azure DevOps “Free Tier” Limitation

- Public project: 10 free Microsoft-hosted parallel jobs that can run for up to 360 minutes (6 hours) each time, with no overall time limit per month.
- Private project: One free job that can run for up to **60 minutes** each time, until you've used 1,800 minutes (30 hours) per month.
 - This 60 minutes limitation requires special attention on DAST Pipeline
- Ref: <https://docs.microsoft.com/en-us/azure/devops/pipelines/licensing/concurrent-jobs?view=azure-devops>

Fortify Azure DevOps Extension


- <https://marketplace.visualstudio.com/items?itemName=fortifyvsts.hpe-security-fortify-vsts>



The screenshot shows the Visual Studio Marketplace interface for the 'Micro Focus Fortify' extension. The breadcrumb trail at the top reads 'Azure DevOps > Azure Pipelines > Micro Focus Fortify'. The extension's logo, a stylized 'F' inside a square, is displayed on the left. To the right of the logo, the title 'Micro Focus Fortify' is shown in a large font, followed by 'Fortify' in a smaller font. Below the title, the text '4,899 installs' and a star rating of 4.5 (represented by four full stars and one half star) with '(12)' reviews are visible. A green button labeled 'Get it free' is positioned below the description. The description text states: 'Use the Micro Focus Fortify VSTS build tasks in your continuous integration builds to identify and remediate application vulnerabilities.' At the bottom of the page, there are three tabs: 'Overview' (which is selected), 'Q & A', and 'Rating & Review'. Under the 'Overview' tab, a list of links is provided: 'Micro Focus Fortify', 'Micro Focus Fortify VSTS Build Tasks', 'Getting Started with Fortify SCA', 'Getting Started with Fortify on Demand', and 'Getting Started with Fortify WebInspect'.

VisualStudio | Marketplace

Azure DevOps > Azure Pipelines > Micro Focus Fortify

 **Micro Focus Fortify**

Fortify | 4,899 installs | ★★★★★ (12) | Free

Use the Micro Focus Fortify VSTS build tasks in your continuous integration builds to identify and remediate application vulnerabilities.

[Get it free](#)

[Overview](#) [Q & A](#) [Rating & Review](#)


- [Micro Focus Fortify](#)
- [Micro Focus Fortify VSTS Build Tasks](#)
- [Getting Started with Fortify SCA](#)
- [Getting Started with Fortify on Demand](#)
- [Getting Started with Fortify WebInspect](#)


Build Tasks Available


- SAST
 - Fortify Static Code Analyzer Install
 - Fortify Static Code Analyzer Assessment
 - Fortify ScanCentral SAST Assessment
- DAST
 - Fortify WebInspect Dynamic Assessment
 - Fortify ScanCentral DAST Assessment


Tasks


forti


 FedRamp - FOD Static Assessment
Submit code for Fortify on Demand security asses...


 Fortify on Demand Dynamic Assessment
Start Fortify assessment of website


 Fortify on Demand Static Assessment
Submit code for Fortify on Demand security asses...

 Fortify ScanCentral DAST Assessment
Submits a dynamic scan using WebInspect

 Fortify ScanCentral SAST Assessment
Installs ScanCentral client and performs a static an...

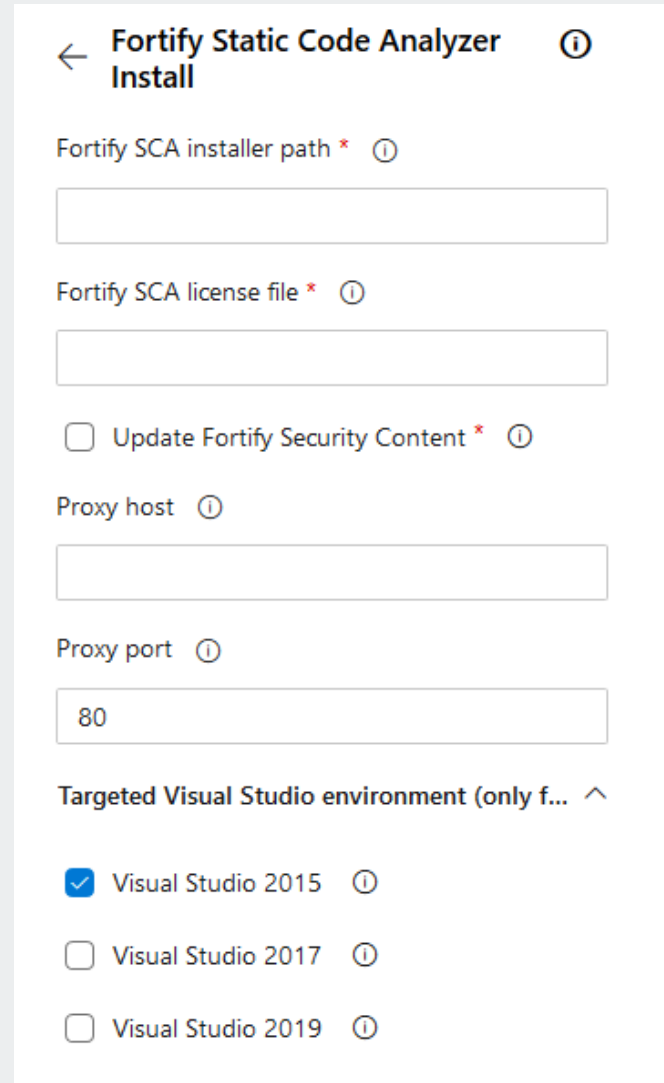
 Fortify Static Code Analyzer Assessment
Run Fortify Static Code Analyzer

 Fortify Static Code Analyzer Install
Install Fortify SCA on an agent

 Fortify WebInspect Dynamic Assessment
Run WebInspect dynamic scan

Task - Fortify Static Code Analyzer Install

- Options
 - Select SCA Installer
 - Select Fortify License file
 - Proxy Settings
 - Visual Studio Environment (only for Windows)
- Questions
 - How to copy the installer?
 - After installation sourceanalyzer will be in path?



The screenshot shows the 'Fortify Static Code Analyzer Install' configuration window. It includes a back arrow and an information icon in the top left. The form contains several fields: 'Fortify SCA installer path' with a red asterisk and an information icon, followed by an empty text box; 'Fortify SCA license file' with a red asterisk and an information icon, followed by an empty text box; a checkbox for 'Update Fortify Security Content' with a red asterisk and an information icon; 'Proxy host' with an information icon, followed by an empty text box; 'Proxy port' with an information icon, followed by a text box containing '80'; and a section titled 'Targeted Visual Studio environment (only f...)' with an expand/collapse arrow. Under this section, there are three radio button options: 'Visual Studio 2015' (selected), 'Visual Studio 2017', and 'Visual Studio 2019', each with an information icon.

← Fortify Static Code Analyzer Install ⓘ

Fortify SCA installer path * ⓘ

Fortify SCA license file * ⓘ

☐ Update Fortify Security Content * ⓘ

Proxy host ⓘ

Proxy port ⓘ

80

Targeted Visual Studio environment (only f... ^

☒ Visual Studio 2015 ⓘ

☐ Visual Studio 2017 ⓘ

☐ Visual Studio 2019 ⓘ

Task - Fortify Static Code Analyzer Assessment

- License File
- Build Id
- Rule Pack Update
- Build Clean
- Build Type
- Projects File

← Fortify Static Code Analyzer Asse...

SCA license file ⓘ

Build Id for Fortify SCA * ⓘ

☐ Run Fortify Rulepack Update * ⓘ

☒ Run Fortify Clean * ⓘ

☐ SCA verbose * ⓘ

☐ SCA debug * ⓘ

Build (translate) ^

☒ Run Build (translate) * ⓘ

Application Type * ⓘ

.Net ▼

Projects for Fortify SCA Analysis * ⓘ

Additional Build Parameters ⓘ

Task - Fortify Static Code Analyzer Assessment - Cont.

- Scan Type
 - Local
 - ScanCentral
- SSC URL
- Application Name
- Application Version
- Proxy details
- No Quality Gate Available – But workaround available

Scan Options ^

☒ Run Fortify SCA scan * ⓘ

Scan type * ⓘ

Local ▾

Additional Fortify SCA scan options ⓘ

Custom Rulepacks ⓘ

☐ Upload results to SSC ⓘ

☒ Upload results to SSC ⓘ

Fortify SSC service connection * ⓘ

Fortify_SSC ▾

SSC application name * ⓘ

SSC application version * ⓘ

Proxy URL ⓘ

Proxy username

Proxy password

Azure - SCA Integration

DotNet Application - Traditional Approach

```
1 # Starter pipeline
2 # Start with a minimal pipeline that you can customize to build and deploy your code.
3 # Add steps that build, run tests, deploy, and more:
4 # https://aka.ms/yaml
5
6 trigger:
7   - master
8
9 pool:
10  | vmImage: 'windows-2019'
11
12 steps:
13   Settings
14   - task: CmdLine@2
15     displayName: 'Creating Build Folder for RichesDotnet'
16     inputs:
17       script: |
18         Echo "Creating a target folder"
19         MKDIR "D:\hp_la_chouffe\rules\scratch\RichesDotnet\"
20
```

DotNet Application - Traditional Approach – Cont..

Running MS Build.

```
Settings
20  - task: MSBuild@1
21  | inputs:
22  |   solution: '**/*.sln'
23  |   clean: true
24  |   createLogFile: true
25
```

DotNet Code - Traditional Approach – Cont...

Downloading SCA

```
Settings
42 - task: PowerShell@2
43   inputs:
44     targetType: 'inline'
45     script: |
46       # Write your PowerShell commands here.
47       $BaseUrl = "https://11.11.11.11:8443/ssc/downloads"
48       add-type @"
49       using System.Net;
50       using System.Security.Cryptography.X509Certificates;
51       public class TrustAllCertsPolicy : ICertificatePolicy {
52         public bool CheckValidationResult(
53           ServicePoint srvPoint, X509Certificate certificate,
54           WebRequest request, int certificateProblem) {
55           return true;
56         }
57       }
58       @"
59       [System.Net.ServicePointManager]::CertificatePolicy = New-Object TrustAllCertsPolicy
60       Write-Host "Downloading SCA from SSC"
61       Invoke-RestMethod http://ipinfo.io/json | Select -exp ip
62       .
63       New-Item -ItemType directory -Path c:\_agent_distr
64       $url = "$BaseUrl/Fortify_SCA_and_Apps_20.2.0_windows_x64.exe"
65       $output = "c:\_agent_distr\Fortify_SCA_and_Apps_20.2.0_windows_x64.exe"
66       $wc = New-Object System.Net.WebClient
67       $wc.DownloadFile($url, $output)
68       .
69       Write-Host "Downloading fortify.license from SSC"
70       $url = "$BaseUrl/fortify.license"
71       $output = "c:\_agent_distr\fortify.license"
72       Write-Host $url
73       $wc = New-Object System.Net.WebClient
74       $wc.DownloadFile($url, $output)
75       .
76       Write-Host "Downloading SSC Cert from SSC"
77       $url = "$BaseUrl/SSC.cer"
78       $output = "c:\_agent_distr\ssc.cer"
79       $wc = New-Object System.Net.WebClient
80       $wc.DownloadFile($url, $output)
81       .
82       displayName: 'Downloading SCA and License'
83       enabled: true
```

DotNet Code - Traditional Approach – Cont...

Installing SCA

```
Settings
84 - task: InstallFortifySCA@7
85   inputs:
86     installerPath: 'c:\_agent_distr\Fortify_SCA_and_Apps_20.2.0_windows_x64.exe'
87     VS2015: false
88     VS2019: true
89     licenseFile: 'c:\_agent_distr\fortify.license'
90     runFortifyRulepackUpdate: true
91     enabled: true
Settings
92 - task: PowerShell@2
93   inputs:
94     targetType: 'inline'
95     script: |
96       Write-Host "Post SCA Install Script"
97       Write-Host "##vso[task.prependpath]C:\Fortify\bin\"
98       C:\Fortify\jre\bin\keytool.exe -importcert -trustcacerts -alias SSC -keystore C:\Fortify\jre\lib\security\cacerts -file c:\_agent_distr\ssc.cer -storepass changeit -noprompt
99     displayName: 'Setting up Path for SCA'
100     enabled: true
```

DotNet Code - Traditional Approach – Cont...

Environment Setup

```
101  - task: BatchScript@1
102  | inputs:
103  |   filename: 'C:\Program Files (x86)\Microsoft Visual Studio\2019\Enterprise\Common7\Tools\VsDevCmd.bat'
104  |   modifyEnvironment: true
105  |   failOnStandardError: true
106  |   displayName: 'Setting up Visual Studio Environment'
107  |   enabled: true
```

DotNet Code - Traditional Approach – Cont...

Running SCA

```
108 - task: FortifySCA@6
109   inputs:
110     licenseFile: 'c:\_agent_distr\fortify.license'
111     runBuildTranslate: true
112     applicationType: 'dotnet'
113     fortifyProjects: '**\*.sln'
114     fortifyBuildId: 'RichesDotNet_Azure_DevOps'
115     runFortifyRulepackUpdate: true
116     runFortifyClean: true
117     scaVerbose: true
118     scaDebug: true
119     runFortifyScan: true
120     fortifyScanType: 'LocalScan'
121     runFortifyUpload: true
122     fortifyServerName: 'Fortify_SSC'
123     fortifyApplicationName: 'Riches DotNet Project with Fortify Plugins'
124     fortifyApplicationVersion: '1.0'
125   enabled: true
```

DotNet Code - Traditional Approach – Cont...

Quality Gate

```
- task: CmdLine@2
  inputs:
    script: |
      Echo Quality Gate for SCA

      FPRUtility -information -search -query "[fortify priority order]:critical" -
project D:\a\1\a\sca_artifacts\RichesDotNet_Azure_DevOps.fpr | findstr /I /C:"No iss
es matched search query."

      rem If %ERRORLEVEL% EQU 0 Echo "Clean Build"
      rem If %ERRORLEVEL% EQU 1 Echo "Dirty Build"
      If %ERRORLEVEL% EQU 0 exit 0
      If %ERRORLEVEL% EQU 1 exit 1
  displayName: 'Running Quality Gate Check'
  enabled: true
```


Azure - ScanCentral Plugin Integration

ScanCentral – Plug-ins Support

Running Maven Build

```
trigger:
- main

pool:
- vmImage: windows-2019

steps:
  Settings
- task: Maven@3
- inputs:
- mavenPomFile: 'pom.xml'
- mavenOptions: '-Xmx3072m'
- javaHomeOption: 'JDKVersion'
- jdkVersionOption: '1.8'
- jdkArchitectureOption: 'x64'
- publishJUnitResults: true
- testResultsFiles: '**/surefire-reports/TEST-*.xml'
- goals: 'package'
- enabled: true
```

ScanCentral – Plug-ins Support

Run the scan using build task plug-ins

Settings

```
- task: FortifyScanCentralSAST@7
  inputs:
    scanCentralCtrlUrl: 'http://[redacted]:8280/scancentral-ctrl'
    scanCentralClientToken: '$(ScanCentral.ClientToken)'
    sscCiToken: '$(ScanCentral.SscCiToken)'
    uploadToSSC: true
    applicationName: 'simplistic.rabbitMQ.via.ScanCentral'
    applicationVersion: '3.0'
    applicationVersionId: '10005'
    buildTool: 'mvn'
    displayName: 'Fortify ScanCentral SAST Scan'
    enabled: true
```



GCP CloudBuild

GCP – Code Build

- Google Cloud – Code Build
- Config File - **cloudbuild.yaml** or cloudbuild.json or docker file
- It runs only docker images
- Supported apps / languages –
 - Node.js
 - Java
 - Python
 - Go
 - VM using Packer

Python Project

☆ cloudbuild.yaml

```
1 steps:
2 - name: 'python:3.7.9'
3   args: ['python', '-m', 'pip', 'install', '-r', 'requirements.txt', '--user']
4 - name: 'python:3.7.9'
5   args: ['bash', './myscript.bash']
```

myscript.bash for Python Project

```
#!/bin/bash

wget http://[REDACTED]:8080/ssc/downloads/Fortify_SCA_and_Apps_20.1.0_linux_x64.run
wget http://[REDACTED]:8080/ssc/downloads/fortify.license

chmod +x ./Fortify_SCA_and_Apps_20.1.0_linux_x64.run

./Fortify_SCA_and_Apps_20.1.0_linux_x64.run --fortify_license_path ./fortify.license
--mode unattended

/opt/Fortify/Fortify_SCA_and_Apps_20.1.0/bin/fortifyupdate

/opt/Fortify/Fortify_SCA_and_Apps_20.1.0/bin/sourceanalyzer -b python_django -debug-
verbose -logfile pyscan.log "./**/*.js" "./**/*.html"

/opt/Fortify/Fortify_SCA_and_Apps_20.1.0/bin/sourceanalyzer -b python_django -debug-
verbose -logfile pyscan.log -python-version 3 -python-path
"/usr/local/lib/python3.7:/usr/local/lib/python3.7/site-
packages:/usr/local/lib64/python3.7:/usr/local/lib64/python3.7/site-
packages:/usr/lib/python3.7:/usr/lib/python3.7/site-
packages:/usr/lib64/python3.7:/usr/lib64/python3.7/site-packages" "./**/*.py"
```

Java Project

☆ cloudbuild.yaml

```
1 steps:
2 - name: 'java'
3   args: ['bash', './scascan.bash']
4   id: 'SCA_Task'
5   waitFor: ['-']
6   timeout: '1200s'
```


scascan.bash for Java Project

```
#!/bin/bash

wget http://[redacted]:8080/ssc/downloads/Fortify_SCA_and_Apps_20.1.0_linux_x64.run
wget http://[redacted]:8080/ssc/downloads/fortify.license
chmod +x ./Fortify_SCA_and_Apps_20.1.0_linux_x64.run
./Fortify_SCA_and_Apps_20.1.0_linux_x64.run --fortify_license_path ./fortify.license --mode unattended
/opt/Fortify/Fortify_SCA_and_Apps_20.1.0/bin/fortifyupdate

/opt/Fortify/Fortify_SCA_and_Apps_20.1.0/bin/sourceanalyzer -b richsjava -debug-verbose -logfile richsjava.log
"./**/*.js" "./**/*.html" ".7**/*.properties" "./**/*.xml" "./**/*.sql" "./**/*.jsp"

/opt/Fortify/Fortify_SCA_and_Apps_20.1.0/bin/sourceanalyzer -b richsjava -debug-verbose -logfile richsjava.log -cp
"jsplibs/**/*.*jar:lib/**/*.*jar:WEB-INF/lib/**/*.*jar" -source 1.5 "./**/*.java"

echo Done with Translate

echo Starting Scan Stage

/opt/Fortify/Fortify_SCA_and_Apps_20.1.0/bin/sourceanalyzer -b richsjava -scan -f richsjava.fpr

echo FPR Generated

/opt/Fortify/Fortify_SCA_and_Apps_20.1.0/bin/fortifyclient -url http://[redacted]:8080/ssc/ -authToken 70340f5e-
eb79-452f-9a31-c8c475f9a88d -application "Riches Java GCP" -applicationVersion "1.0" uploadFPR -file richsjava.fpr

echo Done with Upload
```

CyberRes

Find. Fix. Fortify.

End-to-end application security.

