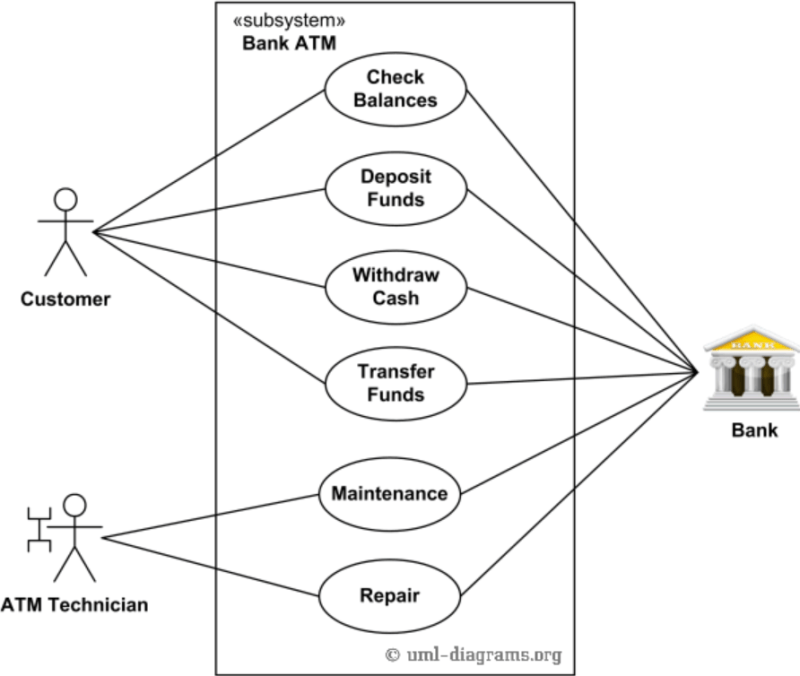
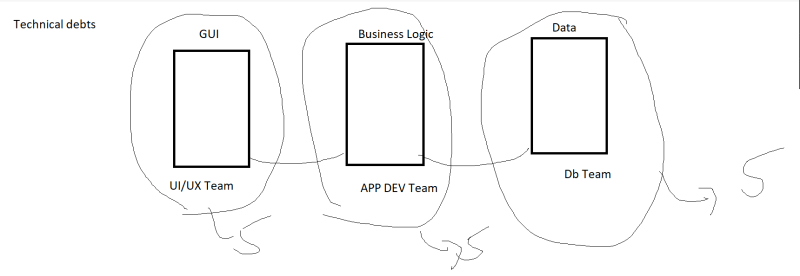
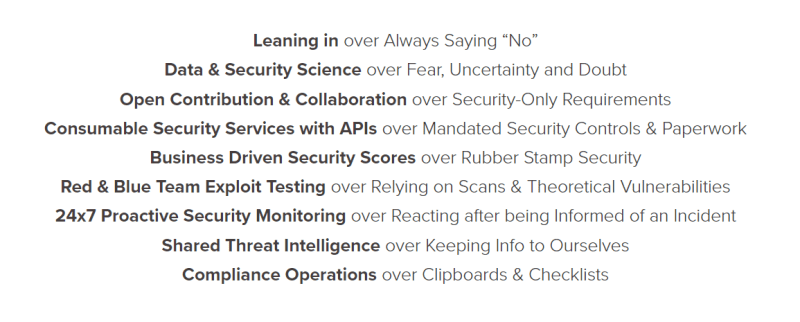
AUGUST 17, 2022

DevOps Classroomnotes 17/Aug/2022

**Software Development Life Cycle and Waterfall Model**

* Waterfall Model
* Requirements:
  + Create a High Level Requirements Document
  + Use Case Diagrams  
    
* Big Bang Integrations:
  + Integration of applications/components developed individually in the last phases of project
  + This generally ends up with issues & major reason for technical debt’s  
    
* Continuous Integration:
  + Here we integrate different components of the application from day 1 and ensure we run some integration tests
  + The basic idea is to fail fast and know the errors upfront.
* Agile Software Methodologies:
  + [Refer Here](https://agilemanifesto.org/) for the Agile Manifesto
  + DevOps enhances the idea of agile by approach which is shift left
* The idea of DevSecOps is to make security shift left.
* What is that we can do for this shift left of Security
  + Code to be scanned for securiy vulnerabilities
  + Scanning application deployed in various test environments for security vulnerabilities
  + Reporting the security issues and eventually breaking build when security issues are reported.
* DevSecOps Manifesto  
  

**Share this:**

AUGUST 18, 2022

DevOps Classroomnotes 18/Aug/2022

**Dependency in Code**

* Any application which developers code, they rely on open source libraries or packages or frameworks for
  + web applications
  + Database connections and query executions (ORM Frameworks)
  + Logging
  + Authentication and Authorizations
  + Notifications.
* Scanning Dependencies for security risks is a mandatory operation as part of DevSecOps.
* If we need to scan dependencies from security issues, we need a database of possible vulnerabilities => CVE and NVD

**Static vs Dynamic Security Testing**

* Two possible ways to test for security
  + Static:
    - When the tool scans the application with the knowledge of code and reports vulnerability
    - This is called as SAST
  + Dynamic:
    - When the tool scans the application which is running and doesn’t have access to source code.
    - This is called as DAST

**OWASP (Open Web Application Security ProjectÂ® (OWASP))**

* This organization publishes top n issues to be concerned with early.
* They also give necessary tools to scan
* [Refer Here](https://owasp.org/Top10/) for OWASP 10:2021
* As a DevSecOps Engineer, We will be
  + performing SAST during packaging/building the application
  + performing DAST post application deployment
  + Ensuring our application doesnot have any issues mentioned/listed in OWASP TOP 10 (latest year)
* Exercises:
  + Find information about what the following are
    - GDPR
    - PCI-DSS

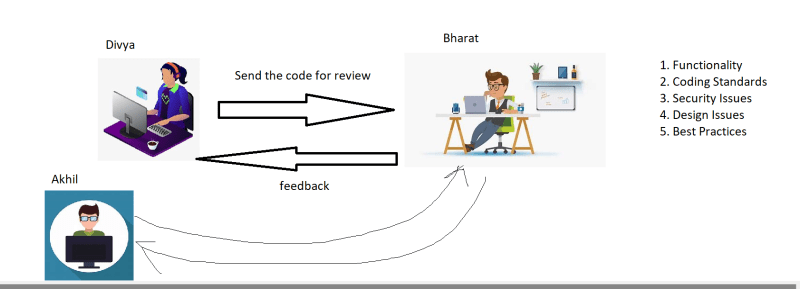
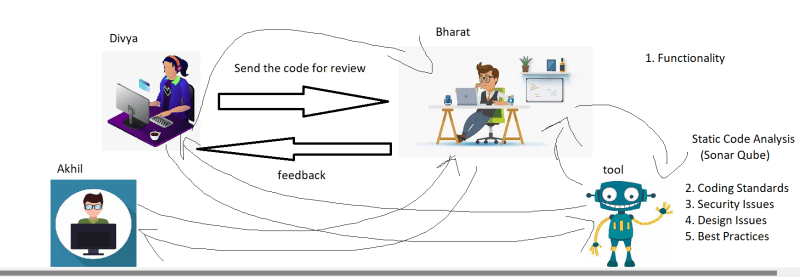
**Share this:**

AUGUST 19, 2022

DevOps Classroomnotes 19/Aug/2022

**DevSecOps Contd….**

**Static Code Analysis**

* Peer Code Review  
  
* Since a person is doing the review, mistakes can happen.
* Static Code Analysis tools take over certain responsibilites from Bharat
  + Coding Standards
  + Best Practices
  + Securiy Issues
  + Design Issues
  + Test Case Quality  
    
* If we can run this static code analysis with every change in the pipeline and
  + Phase-1 : Show the report generated
  + Phase-2: Fail the build if the agreed criteria is not met (Quality Gate)

**Testing By DevTeams**

* Unit Tests: Developers are expected to write tests to check the code developed by team
* When developers perform unit testing, there should be a way to measure the quality of unit tests.
* Line Coverage
* Branch Coverage
* Note: As a devops Engineer, we are expected to create Quality Gates around
  + Test Coverage
  + Static Code Analysis issues

**Softwares To Be Installed**

**Windows Users**

* Install chocolatey
* Windows Terminal
* Visual Studio Code (choco install vscode -y)
* Git For Windows (choco install git -y)

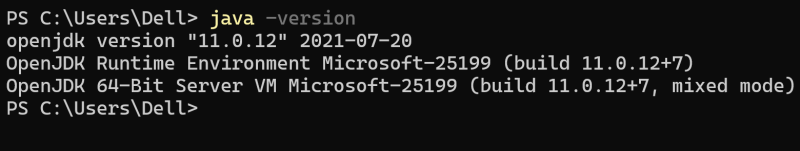
**MAC**

* Homebrew: [Refer Here](https://brew.sh/)
* Visual Studio Code (brew install –cask visual-studio-code)
* git (brew install git)

AUGUST 20, 2022

DevOps Classroomnotes 20/Aug/2022

**SonarQube**

* [Refer Here](https://docs.sonarqube.org/latest/) for the official docs of SonarQube
* Installing SonarQube on Local System
* Sonar Qube requires JDK 11
  + If java is not installed on your system, launch powershell as admin and execute choco install jdk11 -y
  + Close and Relaunch powershell java -version  
    
* Run sonarqube by executing the commands from docs and navigate to [http://localhost:9000](http://localhost:9000/). Default username is admin and password is admin
* Lets run the analysis of one maven project (java). To install maven choco install maven
* Lets get some opensource code. [Refer Here](https://github.com/spring-projects/spring-petclinic.git)

mkdir c:\temp\spc

cd c:\temp\spc

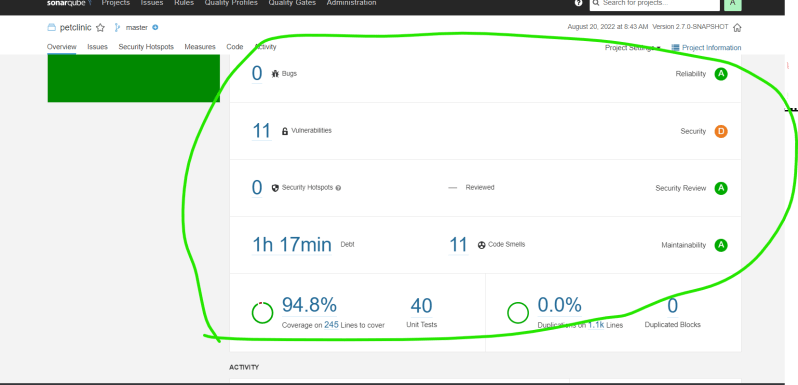
git clone https://github.com/spring-projects/spring-petclinic.git

cd spring-petclinic

mvn package

* Now run the scanning based on the command from sonar qube

mvn clean verify sonar:sonar -Dsonar.projectKey=test -Dsonar.host.url=http://localhost:9000 -Dsonar.login=sqp\_b9a78cff3c8a840035070fa05f043fd4e324b15f



**Share this:**

AUGUST 21, 2022

DevOps Classroomnotes 21/Aug/2022

**Running servers easily**

* Register to Docker hub [Refer Here](https://hub.docker.com/)
* We can play with docker [Refer Here](https://labs.play-with-docker.com/)
* Login into playground and create a new instance

docker container run -d -P <image-name>:<tag-name>

docker container run -d -P jenkins/jenkins:lts-jdk11

docker container ls

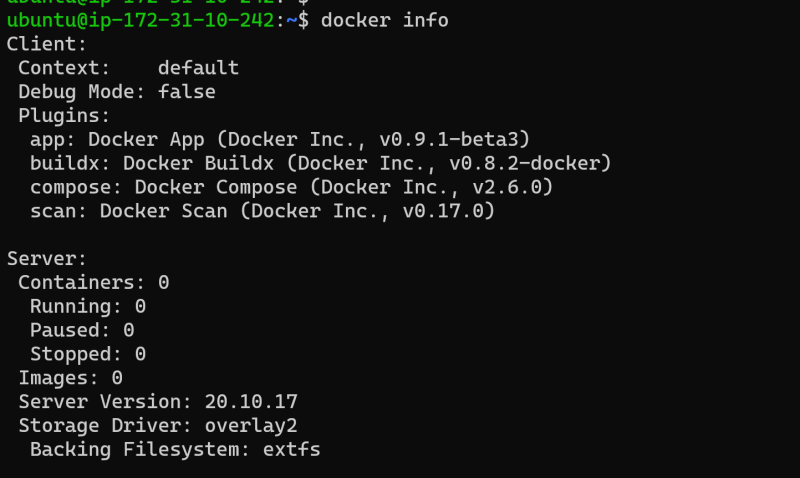
* We can run the sonarqube by executing the following command

docker run -d --name sonarqube -e SONAR\_ES\_BOOTSTRAP\_CHECKS\_DISABLE=true -p 9000:9000 sonarqube:latest

**Installing Docker on Ubuntu**

* AWS:
  + Create a security group with all ports opened (not a secure approach but its okay for lab setup)
  + Create an ec2 instance with ubuntu 20.04
  + login into ec2 instance and execute the following commands  
    “`  
    curl -fsSL [https://get.docker.com](https://get.docker.com/) -o get-docker.sh  
    sh get-docker.sh  
    sudo usermod -aG docker ubuntu  
    exit

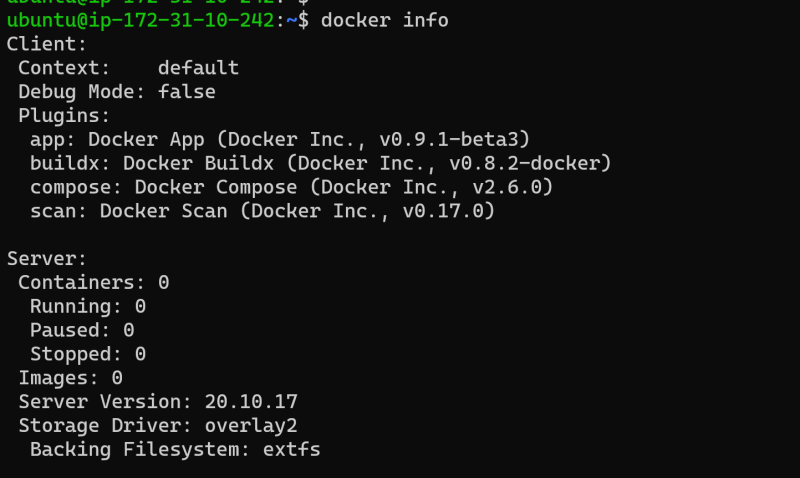
**relogin**

docker info  


\* Now run sonar qube using following command docker run -d –name sonarqube -e SONAR\_ES\_BOOTSTRAP\_CHECKS\_DISABLE=true -p 9000:9000 sonarqube:latest\* Navigate to sonar qube using[http://publicip:9000](http://publicip:9000/)`

* Azure:
  + Create a ubuntu vm
  + login into vm after opening all ports in nsg  
    “`  
    curl -fsSL [https://get.docker.com](https://get.docker.com/) -o get-docker.sh  
    sh get-docker.sh  
    sudo usermod -aG docker ubuntu  
    exit

**relogin**

docker info  


\* Now run sonar qube using following command docker run -d –name sonarqube -e SONAR\_ES\_BOOTSTRAP\_CHECKS\_DISABLE=true -p 9000:9000 sonarqube:latest\* Navigate to sonar qube using[http://publicip:9000](http://publicip:9000/)`

**Share this:**

AUGUST 25, 2022

DevOps Classroomnotes 25/Aug/2022

**DevSecOps**

* This is the practice that involves security earlier in SDLC.
* To implement DevSecOps, Organizations consider variety of applications security tools (AST) to integrated with various stages of CI/CD Process. Commonly used AST tools include
* SCA (Software Composition Analysis)
* SAST (Static Application Security Testing)
* DAST (Dynamic application security Testing)

**Software Compostion Analysis (SCA)**

* SCA tools scan source code and binaries to identify known vulnerabilities in open source and third-party components.
* They also provide insight into security and license risks.

**Static application Security Testing (SAST)**

* These tools scan propietary code or custom code for coding errors and design flaws that could lead to exploitable weakness.

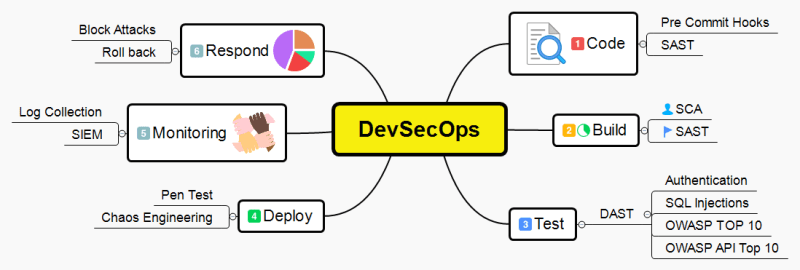
**Dynamic Application Security Testing (DAST)**

* DAST is automated opaque black box testing technology that mimics how a hacker could interact with your web application or API.
* This tests application over a network connection & by examining the client side rendering of application.

**DevSecOps Tools**

* Aqua Security:
  + Used with cloud-native applications i.e cloud native application protection platform (CNAPP).
  + This is very popular for kubernetes, serverless, container security etc
  + [Refer Here](https://www.aquasec.com/) for the offical web page for aqua security
* Checkmarx:
  + This is very popular is application security testing (AST).
  + We can perform
    - SCA
    - SAST
    - Interactive Application Secirity testing
  + [Refer Here](https://checkmarx.com/) for the official web page for CheckMarx
* Micro Focus Cyber Res Fortify:
  + This is very popular in IDE scanning of the code and they offer different products around
    - SAST
    - DAST
    - SCA
  + [Refer Here](https://www.microfocus.com/en-us/cyberres/application-security) for the official web page for Fortity
* Synopsys:
  + AST tools include SCA, interactive,DAST and SAST
  + [Refer Here](https://www.synopsys.com/software-integrity/solutions/devsecops.html) for the official web page
* Veracode:
  + This is cloud solution provider for SAST
  + [Refer Here](https://www.veracode.com/) for veracode
* WhiteSource:
  + This offers SAST, dependecy scanning and risk exposure
  + [Refer Here](https://www.mend.io/) for official web page
* OWASP ZAP:
  + This is from OWASP community which is opensource.
  + Automated active and passive scanning of web applications for vulnerabilities
  + This is DAST testing
  + [Refer Here](https://owasp.org/www-project-zap/) for the official pages for OWASP ZAP

**Integrating Security To CI/CD Pipelines**

* Overview of Integration  
  

**Terms To Be Understood**

* OWASP
* OWASP TOP 10
* SIEM
* NVD
* CVE

**Share this:**

AUGUST 26, 2022

DevOps Classroomnotes 26/Aug/2022

**NVD (National Vulnerability Database)**

* This is list of all known vulnerabilities

**CVE**

* This is a number given to vulnerability and we can search vulnerabilities by technology/platform which we use

**Vulnerability Sources**

* Propietary Code
* Dependencies/libraries/frameworks your application is using
* Network
* Hardware
* Operating Systems.
* Container

**OWASP**

* [Refer Here](https://owasp.org/) for the official website
* OWASP TOP 10 [Refer Here](https://owasp.org/www-project-top-ten/)
* OWASP API TOP 10 [Refer Here](https://owasp.org/www-project-api-security/)

**SCA (Software Composition Analysis)**

* Try creating free trail account in fortify [Refer Here](https://www.microfocus.com/en-us/products/application-security-testing/free-trial)
* Open Source Codes which we will be scanning
  + Openmrs (Java) [Refer Here](https://github.com/openmrs/openmrs-core)
  + Mezzazine (Python) [Refer Here](https://github.com/stephenmcd/mezzanine)
  + Nop Commerce .net [Refer Here](https://github.com/nopSolutions/nopCommerce)

**Share this:**

AUGUST 27, 2022

DevOps Classroomnotes 27/Aug/2022

**DevSecOps (Contd)**

* Here is the list of some opensource free tools for SAST, SCA and DAST [Refer Here](https://owasp.org/www-community/Free_for_Open_Source_Application_Security_Tools)

**OWASP Dependency Check**

* [Refer Here](https://owasp.org/www-project-dependency-check/) for the official web site
* [Refer Here](https://jeremylong.github.io/DependencyCheck/) for the documentation of dependency check
* Installation:
  + Ensure JAVA is installed

sudo apt update

sudo apt install openjdk-11-jdk -y

* Download the dependency check [Refer Here](https://objects.githubusercontent.com/github-production-release-asset-2e65be/5663857/3535be4b-a468-41e0-9979-1215580abe52?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20220827%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220827T131135Z&X-Amz-Expires=300&X-Amz-Signature=0714be8bdc48d95b955b506985ea7a39ec975e849448832c379ceae656282ecc&X-Amz-SignedHeaders=host&actor_id=2438317&key_id=0&repo_id=5663857&response-content-disposition=attachment%3B%20filename%3Ddependency-check-7.1.2-release.zip&response-content-type=application%2Foctet-stream)
* To upload this into linux use sftp
  + Get into the directory where you have zip downloaded
  + Figure out ssh command to connect to ubuntu instance, replace ssh with sftp `sftp -i ~/Downloads/ansiblelearning.pem ubuntu@100.100.100.100
  + upload using put <filename>
* Now install unzip sudo apt install unzip -y

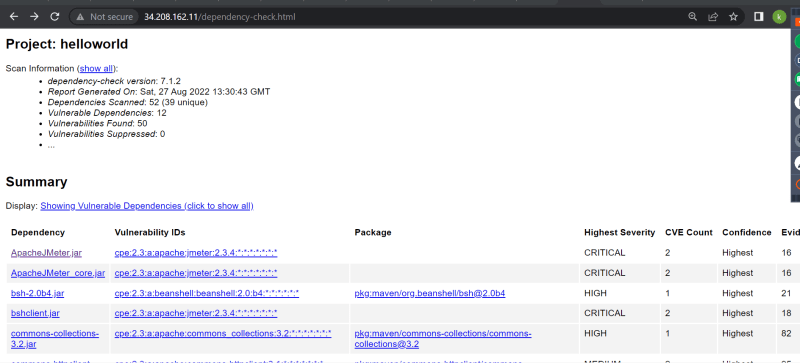
unzip ~/dependency-check-7.1.2-release.zip

cd ~

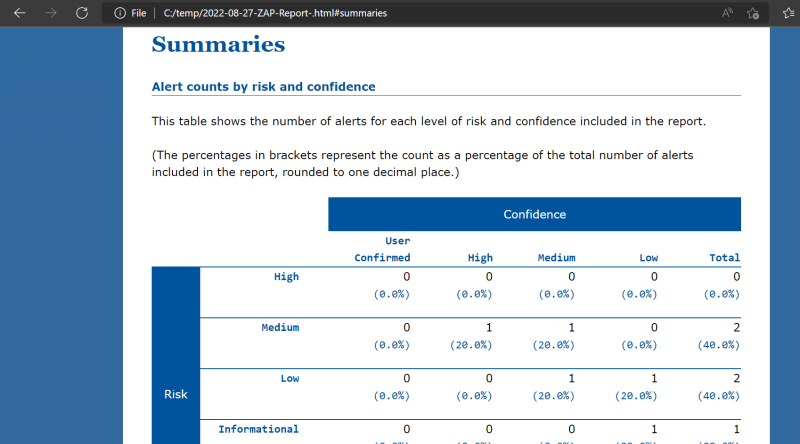
git clone https://github.com/wakaleo/game-of-life.git

cd game-of-life/

~/dependecy-check/dependency-check/bin/dependency-check.sh --project "helloworld" --scan ~/game-of-life/



**OWASP ZAP (DAST)**

* Install OWASP ZAP either from chocolatey or manual install and then scan any url
* Generated report in your CI/CD Tool  
  
* When we work with CI/CD we generate this report by running ZAP from Command line [Refer Here](https://www.zaproxy.org/docs/desktop/cmdline/)

**Activities**

1. Create a Synk account [Refer Here](https://snyk.io/plans/)
2. Ensure you have a Github account and docker hub account.

AUGUST 28, 2022

# DevOps Classroomnotes 28/Aug/2022

## Docker Image Scanning

* In CI/CD Pipelines we build docker images, so we are expected to scan images for vulnerabilities.
* Docker has its own scan as part of its command line
* To perform extensive Scanning Organizations opt for third party tools
  + Aqua Security
  + ECR Scanning [Refer Here](https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning.html)
  + Microsoft Defender for Image Scanning [Refer Here](https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction)
  + Qualysis [Refer Here](https://www.qualys.com/)
* Refer the below two part articles
  + part 1 [Refer Here](https://www.prplbx.com/resources/blog/docker-part1/)
  + part 2 [Refer Here](https://www.prplbx.com/resources/blog/docker-part2/)
* CIS benchmark for docker [Refer Here](https://www.cisecurity.org/benchmark/docker)
* Scanning for vulnerabilities for docker local images [Refer Here](https://docs.docker.com/engine/scan/)
* Docker images are store in Registries (Docker Hub, Elastic Container Registry, Azure Container Registry) and all of them support image scanning.

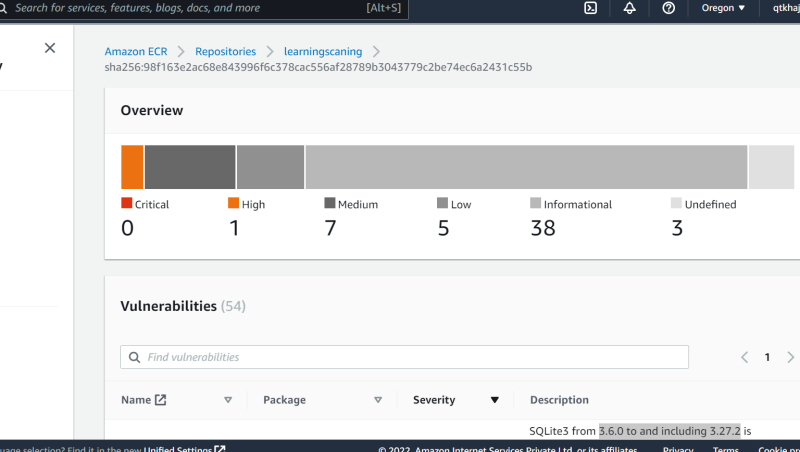
### Sample Scanning of Docker images in Registries

#### AWS ECR

* Sample Dockerfile

FROM httpd

EXPOSE 80

* After installing docker on the build server
* Create a repository in AWS ECR and select the option to scan on push
* After building the docker image, when we push the report will be ready  
  
* Configuration required on your build server
  + aws cli [Refer Here](https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html)
  + Create an IAM user and configure [Refer Here](https://sst.dev/chapters/create-an-iam-user.html)
  + Execute aws configure
* In Azure, lets do this activity after some time.

## Linux Vulnerability Scanning

* Scanning Linux For Vulnerabiliteis [Refer Here](https://geekflare.com/linux-security-scanner/)
* Nessus [Refer Here](https://www.tenable.com/products/nessus)
* Open VAS [Refer Here](https://www.openvas.org/)

### Share this:

* [Click to share on Twitter (Opens in new window)](https://directdevops.blog/2022/08/28/devops-classroomnotes-28-aug-2022/?share=twitter&nb=1)
* [Click to share on Facebook (Opens in new window)](https://directdevops.blog/2022/08/28/devops-classroomnotes-28-aug-2022/?share=facebook&nb=1)
* [Click to share on WhatsApp (Opens in new window)](https://directdevops.blog/2022/08/28/devops-classroomnotes-28-aug-2022/?share=jetpack-whatsapp&nb=1)

### Like this:

### Leave a Reply

Top of Form

Bottom of Form

This site uses Akismet to reduce spam. [Learn how your comment data is processed](https://akismet.com/privacy/).



## About continuous learner

devops & cloud enthusiastic learner

[**VIEW ALL POSTS**](https://directdevops.blog/author/shaikkhajaibrahim6e5af9224a/)

[PREVIOUS POST](https://directdevops.blog/2022/08/28/aws-classroomnotes-28-aug-2022/)

# [AWS Classroomnotes 28/Aug/2022](https://directdevops.blog/2022/08/28/aws-classroomnotes-28-aug-2022/)

[NEXT POST](https://directdevops.blog/2022/08/30/azure-classroomnotes-30-aug-2022/)

# [Azure Classroomnotes 30/Aug/2022](https://directdevops.blog/2022/08/30/azure-classroomnotes-30-aug-2022/)

[POWERED BY WORDPRESS.COM](https://wordpress.com/?ref=footer_custom_powered).

[](http://www.facebook.com/khaja.ibrahim.334)[](http://linkedin.com/in/khaja-ibrahim-34977a1a0)[](https://www.youtube.com/c/LearningThoughts)

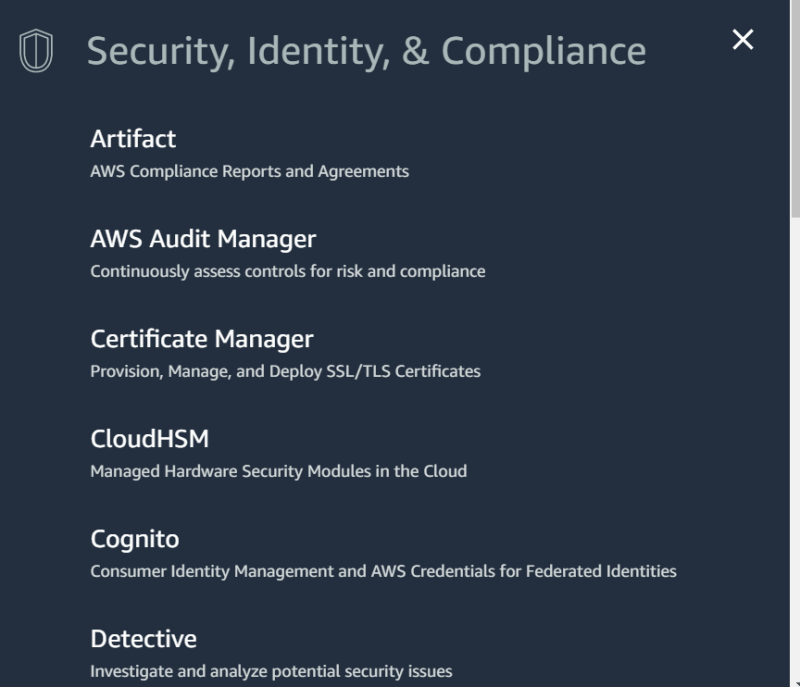
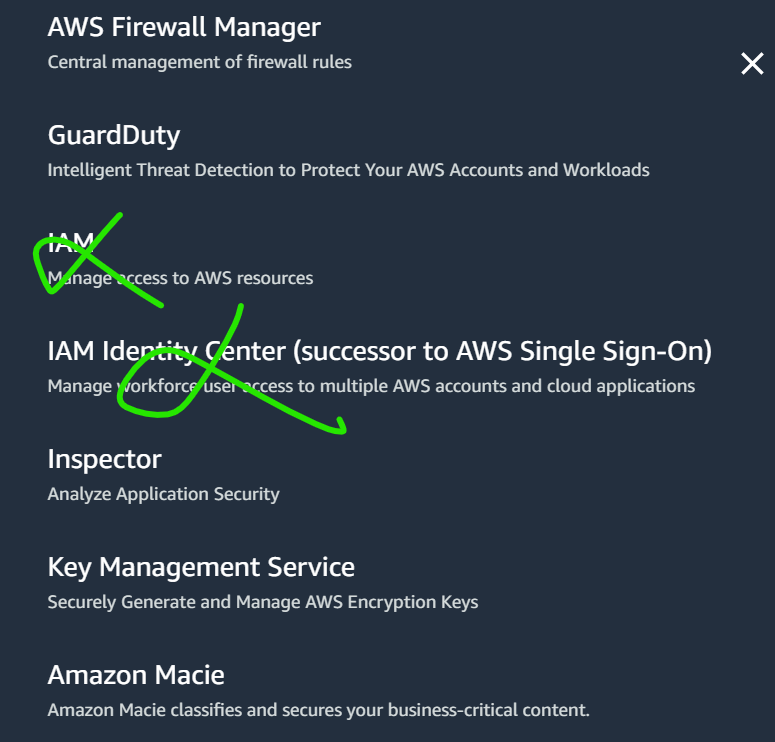
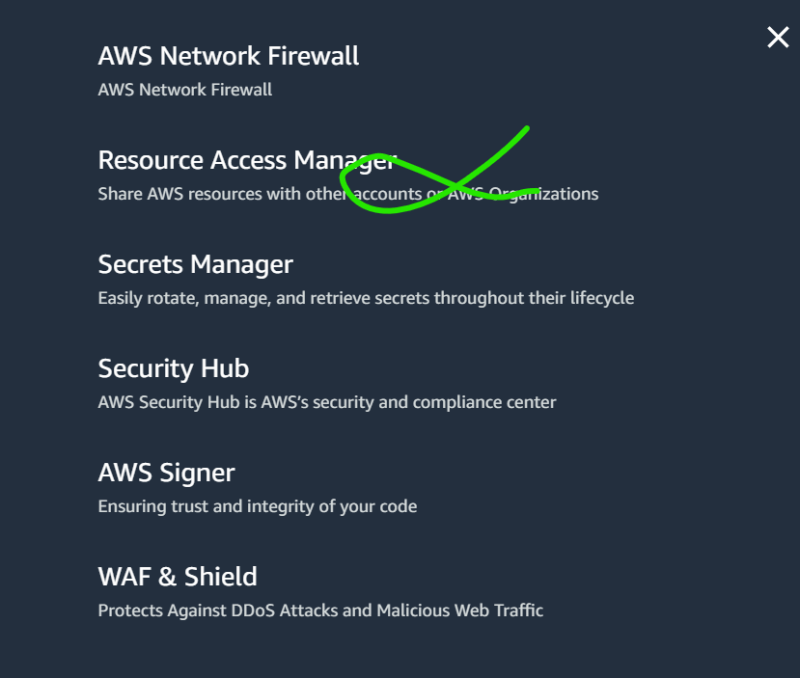
AUGUST 30, 2022

DevOps Classroomnotes 30/Aug/2022

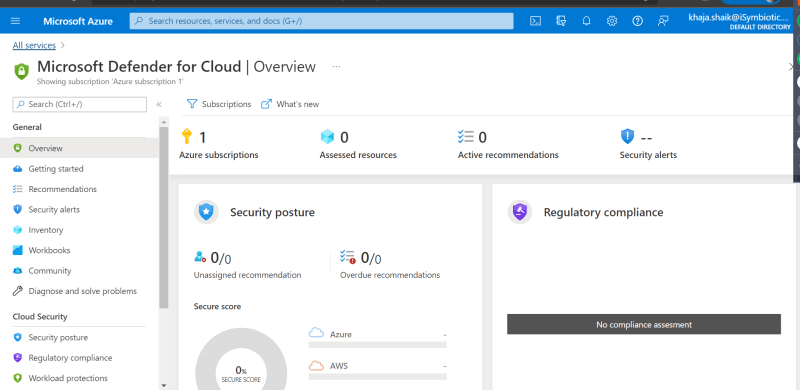
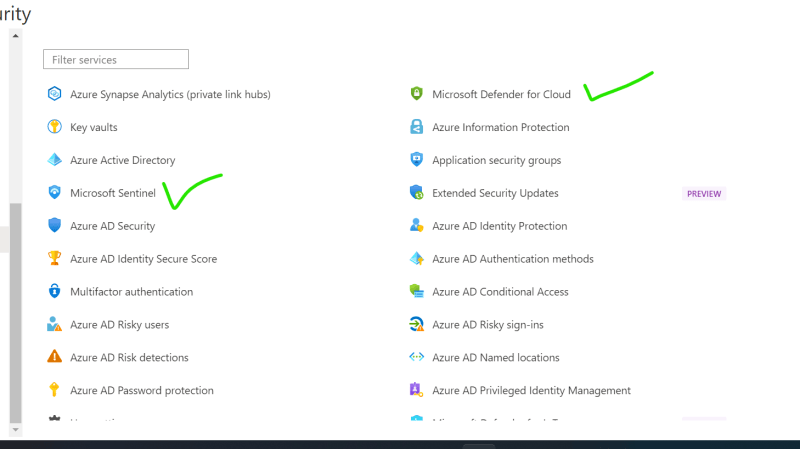
**Attack Surface and Attack Vector**

* [Refer Here](https://www.techtarget.com/whatis/definition/attack-surface)
* Attack surfaces are where unauthorized entry can be done. The attack surfaces to be protected are
  + Operating Systems
  + Ports
  + Code
  + Servers
* An attack vector is a path or means by which an attacker or hacker can gain access…

**AWS Cloud Security**

* The tools available in Aws are  
    
    
  
* Gaurd Duty: We can enable security scanning for some services in AWS
* Inspector: Vulnerability Management
* AWS WAF: Provides firewall for your APIs
* AWS Security Hub
* AWS Sheild: Protects for DDOS

**Azure Cloud Security**

* Microsoft Defenders  
  
* The tool used is Microsoft Defender for Azure  
  

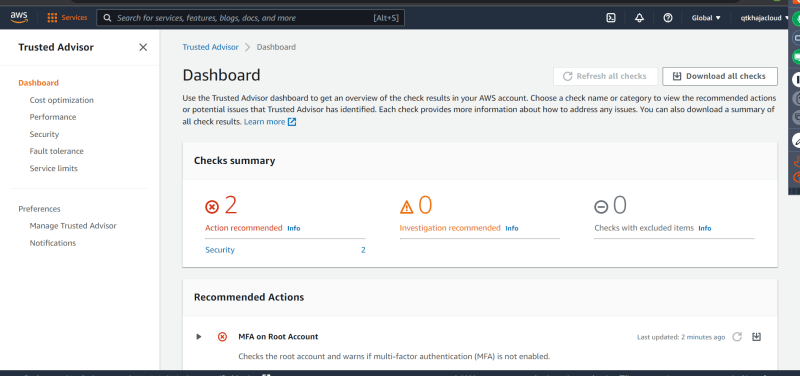
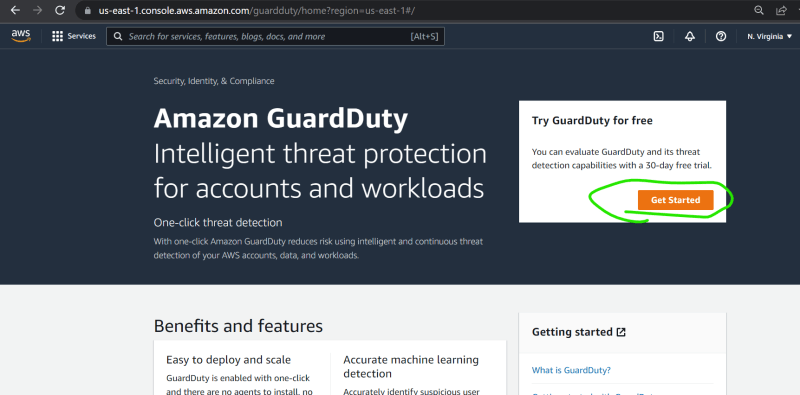
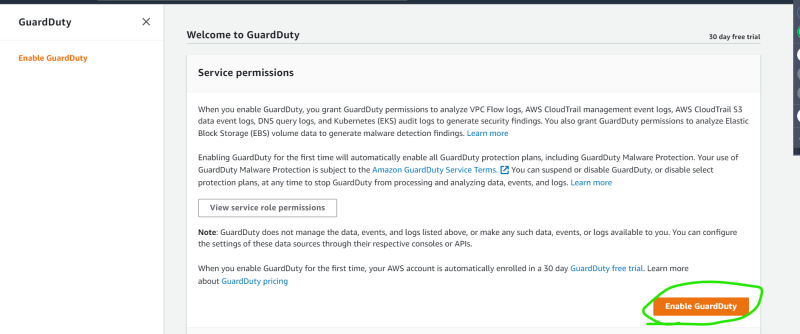
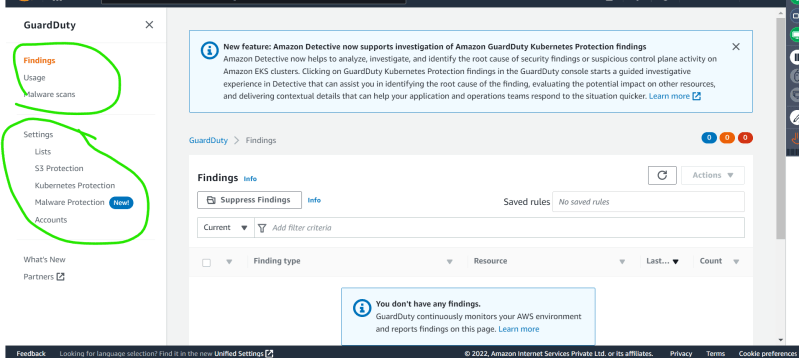
**Share this:**

* [Click](https://directdevops.blog/2022/08/30/devops-classroomnotes-30-aug-2022/?share=twitter&nb=1)

SEPTEMBER 1, 2022

DevOps Classroomnotes 01/Sep/2022

**Security on AWS**

* Trusted Advisor:
  + This AWS service to provide recommendations on cost, performance and security  
    
* AWS GaurdDuty  
    
    
  
* A small script to access home page continuously

#!/bin/bash

while true

do

curl http://18.212.20.237

done

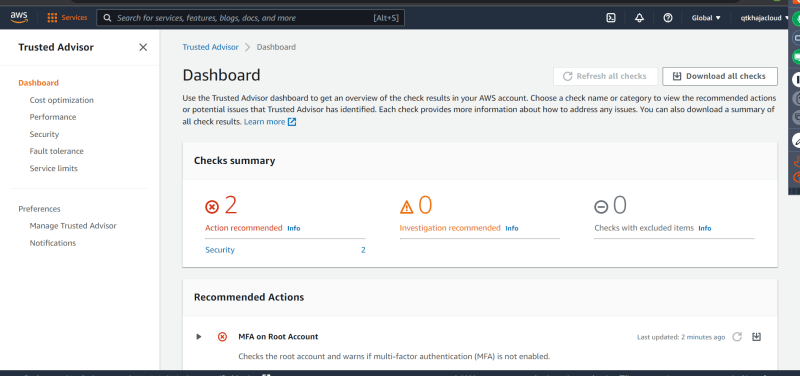
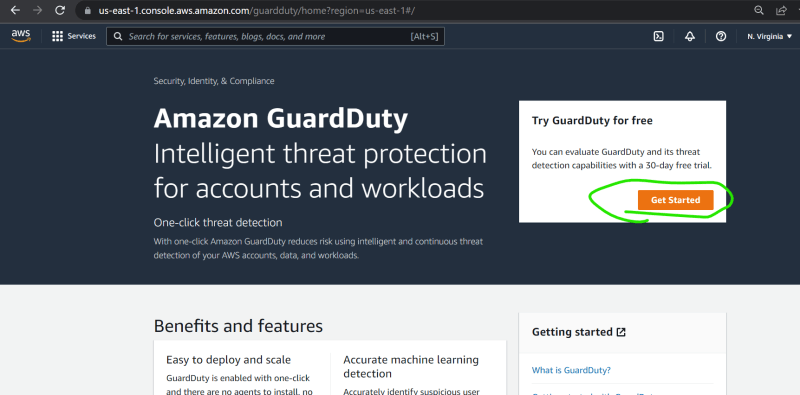
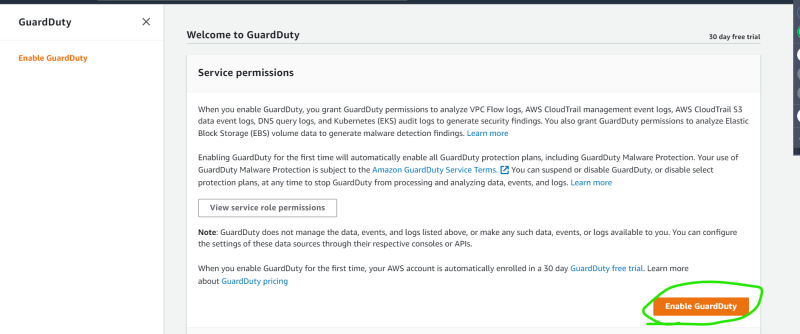
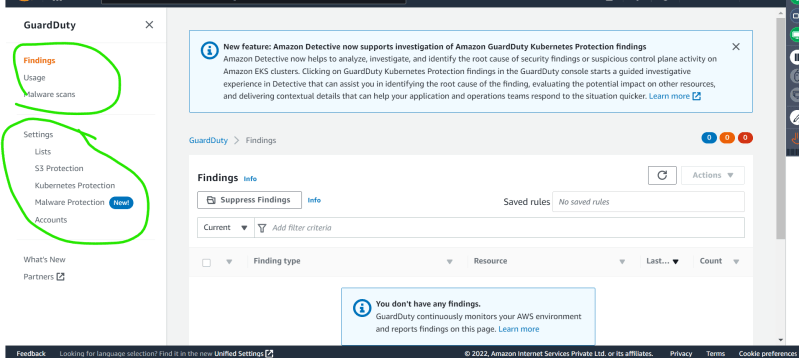
* Then we can add trusted ip list (Whitelist) and threat ip list (blacklist)
* AWS Macie:
  + This service scans for sensitive content on the S3 buckets
  + PII (Personally Identifiable Information) should not be stored in logs of your application.

**Share this:**

SEPTEMBER 1, 2022

DevOps Classroomnotes 01/Sep/2022

**Security on AWS**

* Trusted Advisor:
  + This AWS service to provide recommendations on cost, performance and security  
    
* AWS GaurdDuty  
    
    
  
* A small script to access home page continuously

#!/bin/bash

while true

do

curl http://18.212.20.237

done

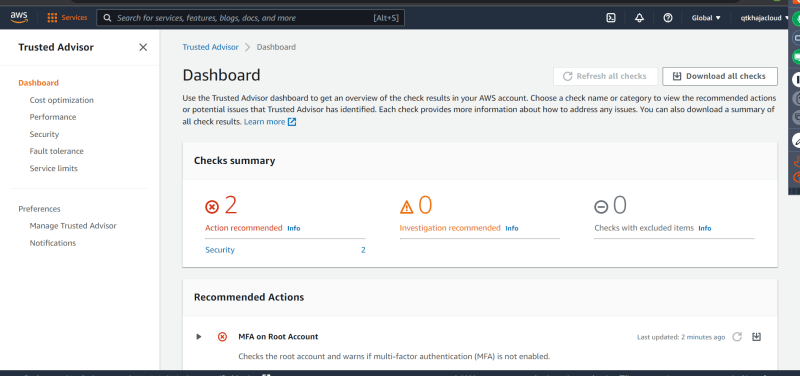
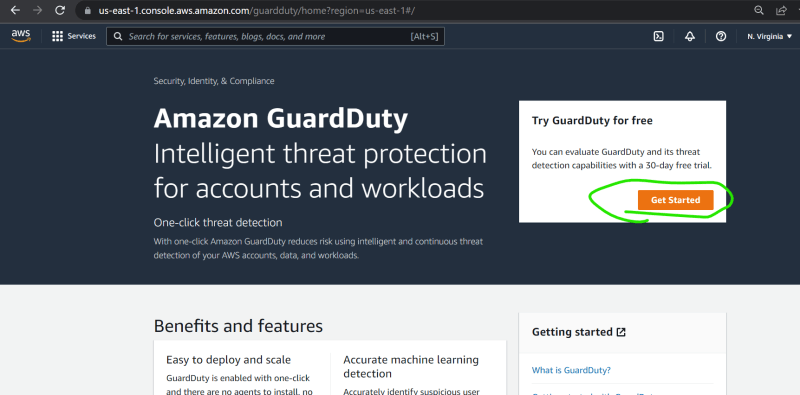
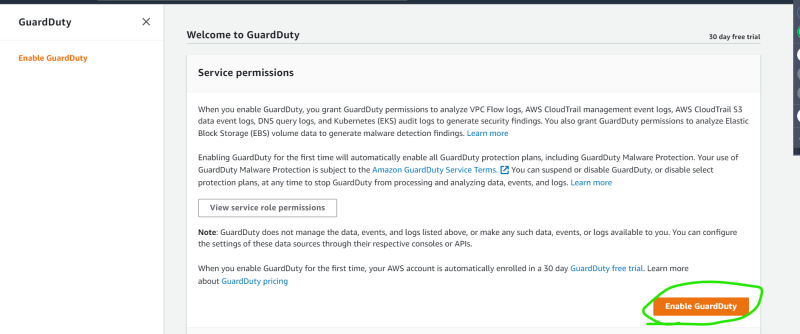
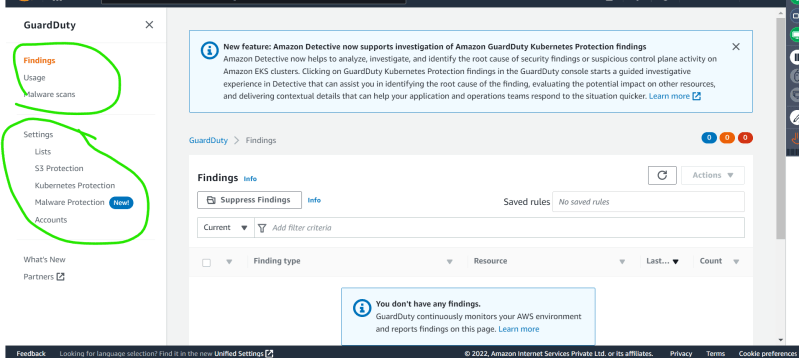
* Then we can add trusted ip list (Whitelist) and threat ip list (blacklist)
* AWS Macie:
  + This service scans for sensitive content on the S3 buckets
  + PII (Personally Identifiable Information) should not be stored in logs of your application.

**Share this:**

SEPTEMBER 1, 2022

DevOps Classroomnotes 01/Sep/2022

**Security on AWS**

* Trusted Advisor:
  + This AWS service to provide recommendations on cost, performance and security  
    
* AWS GaurdDuty  
    
    
  
* A small script to access home page continuously

#!/bin/bash

while true

do

curl http://18.212.20.237

done

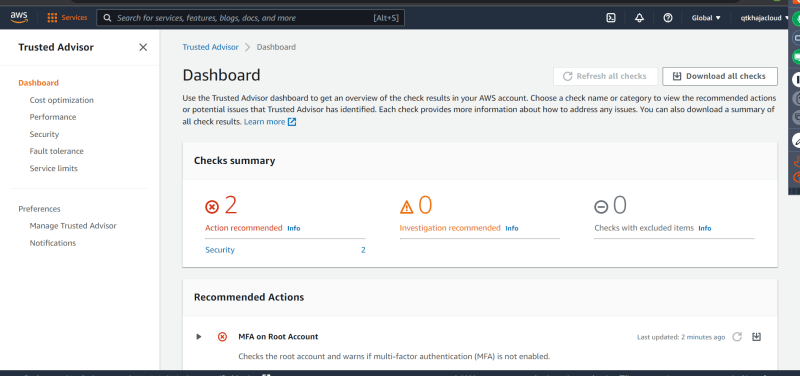
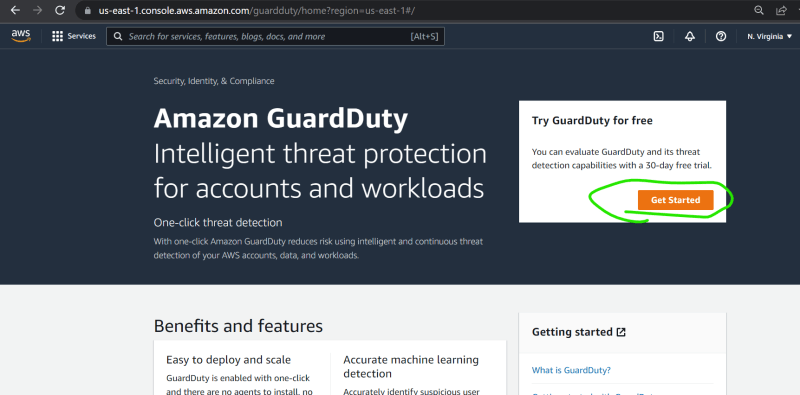
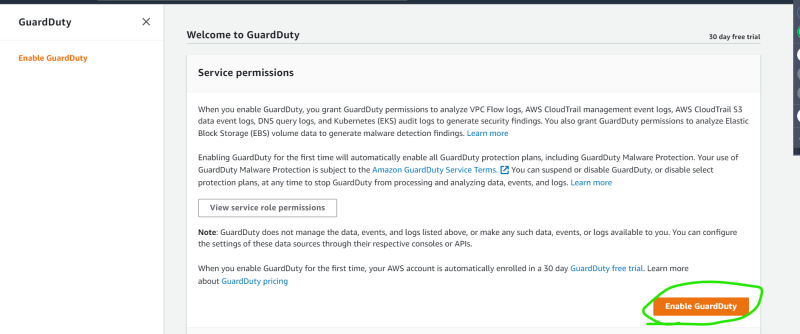
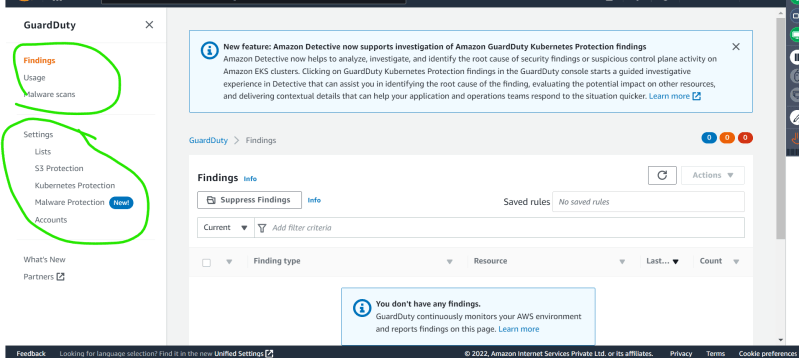
* Then we can add trusted ip list (Whitelist) and threat ip list (blacklist)
* AWS Macie:
  + This service scans for sensitive content on the S3 buckets
  + PII (Personally Identifiable Information) should not be stored in logs of your application.

**Share this:**

SEPTEMBER 1, 2022

DevOps Classroomnotes 01/Sep/2022

**Security on AWS**

* Trusted Advisor:
  + This AWS service to provide recommendations on cost, performance and security  
    
* AWS GaurdDuty  
    
    
  
* A small script to access home page continuously

#!/bin/bash

while true

do

curl http://18.212.20.237

done

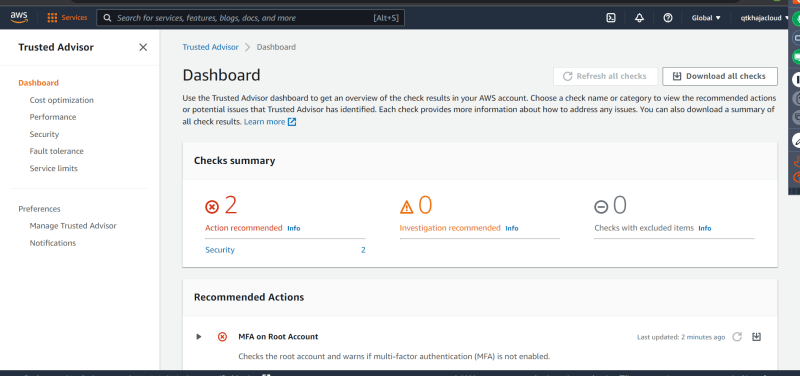
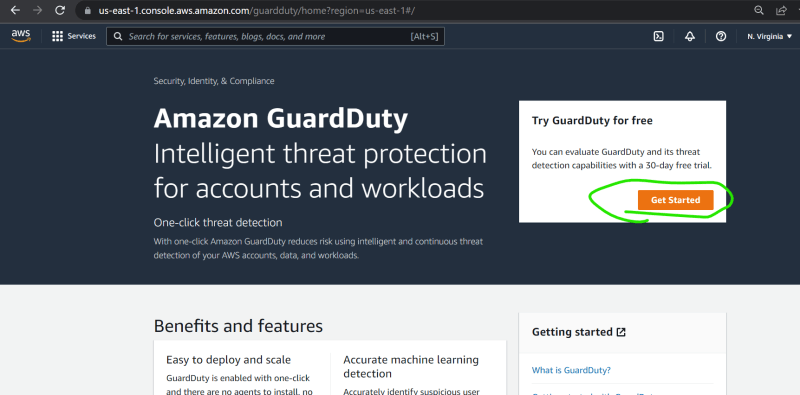
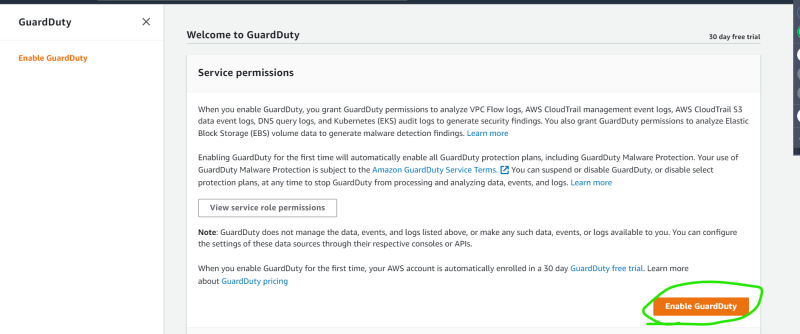
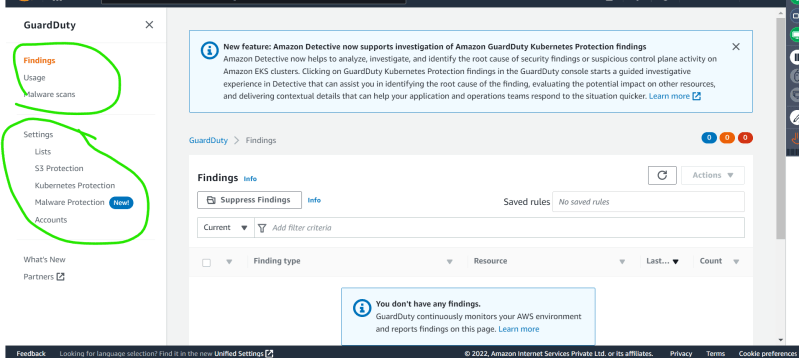
* Then we can add trusted ip list (Whitelist) and threat ip list (blacklist)
* AWS Macie:
  + This service scans for sensitive content on the S3 buckets
  + PII (Personally Identifiable Information) should not be stored in logs of your application.

**Share this:**

SEPTEMBER 1, 2022

DevOps Classroomnotes 01/Sep/2022

**Security on AWS**

* Trusted Advisor:
  + This AWS service to provide recommendations on cost, performance and security  
    
* AWS GaurdDuty  
    
    
  
* A small script to access home page continuously

#!/bin/bash

while true

do

curl http://18.212.20.237

done

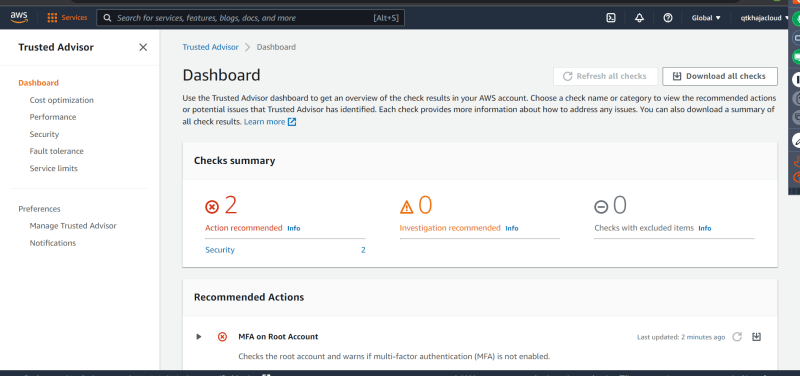
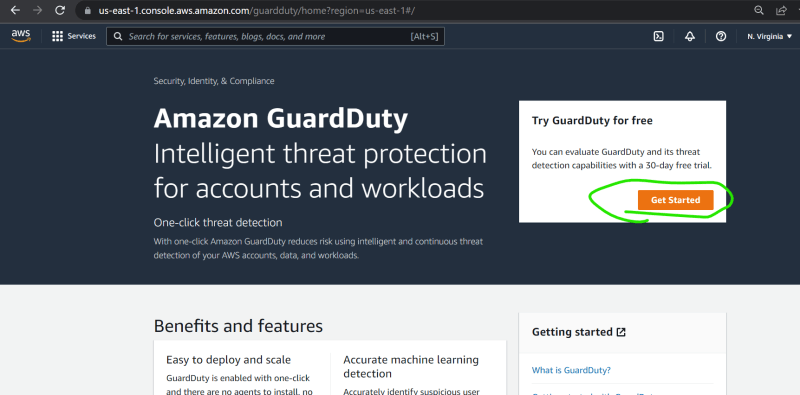
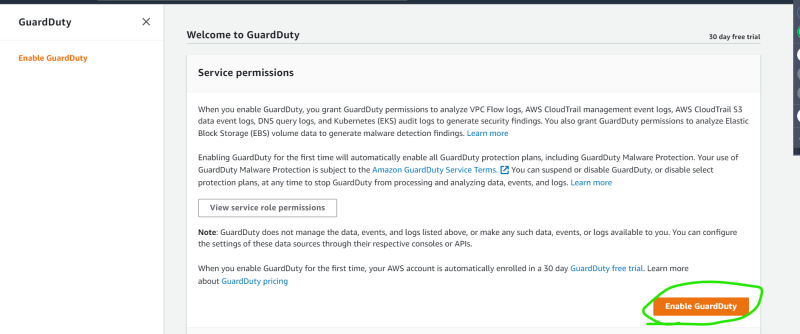
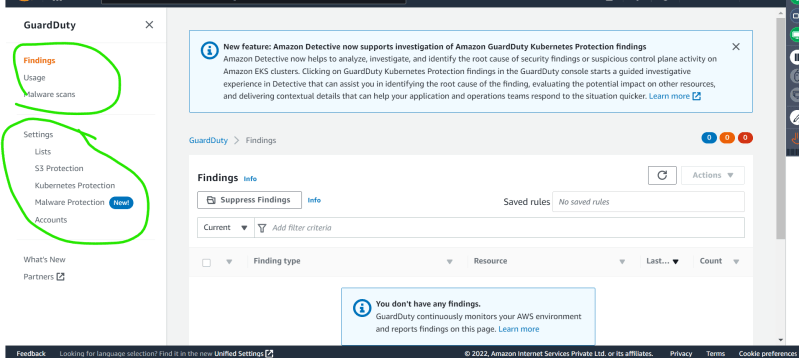
* Then we can add trusted ip list (Whitelist) and threat ip list (blacklist)
* AWS Macie:
  + This service scans for sensitive content on the S3 buckets
  + PII (Personally Identifiable Information) should not be stored in logs of your application.

**Share this:**

SEPTEMBER 1, 2022

DevOps Classroomnotes 01/Sep/2022

**Security on AWS**

* Trusted Advisor:
  + This AWS service to provide recommendations on cost, performance and security  
    
* AWS GaurdDuty  
    
    
  
* A small script to access home page continuously

#!/bin/bash

while true

do

curl http://18.212.20.237

done

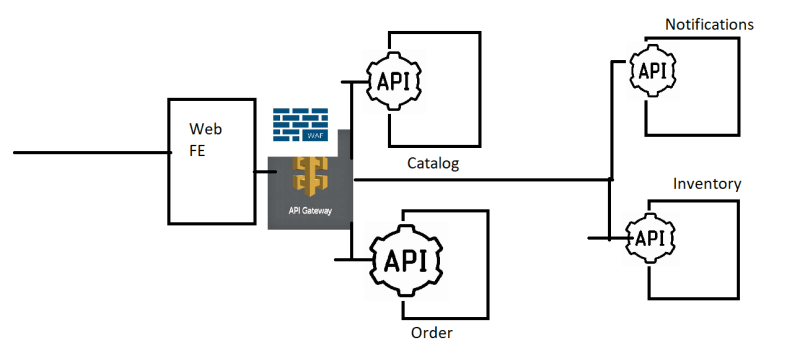
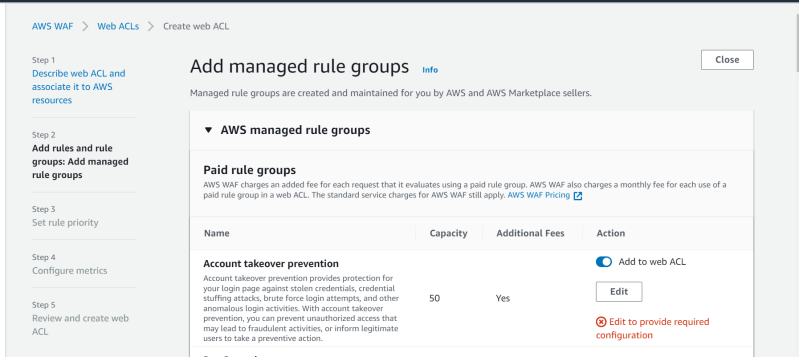
* Then we can add trusted ip list (Whitelist) and threat ip list (blacklist)
* AWS Macie:
  + This service scans for sensitive content on the S3 buckets
  + PII (Personally Identifiable Information) should not be stored in logs of your application.

**Share this:**

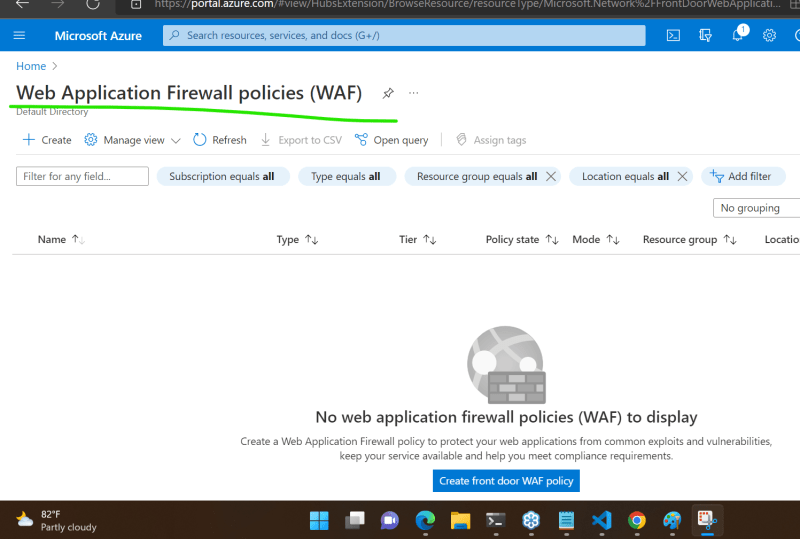
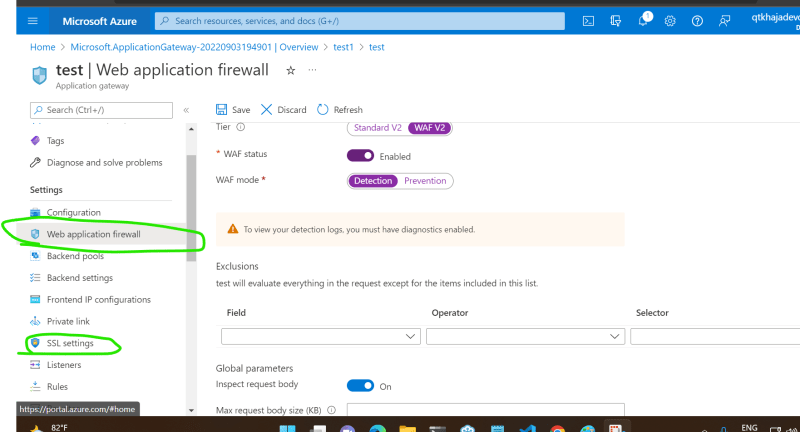
SEPTEMBER 3, 2022

DevOps Classroomnotes 03/Sep/2022

**AWS Security Tools**

* AWS WAF (Web application Firewall): To prevent APIs from DDOS attacks and allow trusted IPs the WAF is enabled at API Gateway level.  
  
* Enable Protections on the API Endpoints by all the known attacks by using Web ACLs  
  

**Microsoft Azure => Microsoft Defender**

* [Refer Here](https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction) for the official docs.
* Enabling Defender in Azure Subscriptions [Refer Here](https://docs.microsoft.com/en-us/azure/defender-for-cloud/get-started)
* pricing [Refer Here](https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/)
* WAF Policies:  
    
  

**Fortify Scanning Docs**

* [Refer Here](https://www.microfocus.com/documentation/fortify-static-code/1720/) for the static code analysis tools docs from micro focus

**Share this:**