Question #1 *Topic 1*

Andrew Gerrard has recently joined an IT company located in Fairmont, California, as a DevSecOps engineer. Due to robust security and cost-effective service provided by AWS, his organization has migrated all the workloads from on-prem to AWS cloud in January of 2020. Andrew's team leader has asked him to integrate AWS Secret Manager with Jenkins. To do so, Andrew installed the "AWS Secret Manager Credentials provider" plugin in Jenkins and configured an IAM policy in AWS that allows Jenkins to take secrets from AWS Secret manager. Which of the following file should Andrew edit to add access id and secret key parameters along with the region copied from AWS?

A. /etc/filebeat/filebeat.yml

B. /etc/sysconfig/Jenkins

C. /etc/file/Jenkins

D. /etc/sysconfig file/Jenkins

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

Gabriel Bateman has been working as a DevSecOps engineer in an IT company that develops virtual classroom software for online teaching. He would like to clone the BDD security framework on his local machine using the following URL, https://github.com/continuumsecurity/bdd-security.git. Which of the following command should Gabriel use to clone the BBD security framework?

A. git clone https://github.com/continuumsecurity/bdd-security.git

B. git clone https://github.com/continumsecurity/bdd-security.git

C. github clone https://github.com/continumsecurity/bdd-security.git

D. github clone https://github.com/continuumsecurity/bdd-security.git

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

William Edwards is working as a DevSecOps engineer at SVR Software Solution Pvt. Ltd. His organization develops software products and applications related to digital marketing. William integrated Prisma Cloud with Jenkins to detect threat-intelligence based threat detection. This integration will allow him to scan container images and serverless functions for security issues in the CI/CD pipeline. Which of the following is employed by Prisma Cloud to understand the normal network behavior of each customer's cloud environment to detect network anomalies and zero-day attacks effectively with minimal false positives?

A. Advanced unsupervised machine learning

B. Advanced supervised data mining

C. Advanced supervised machine learning

D. Advanced unsupervised data mining

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

Terry Crews has been working as a DevSecOps engineer at an IT company that develops software products and web applications related to IoT devices. She integrated Sqreen RASP tool with Slack for sending notifications related to security issues to her team. How can Sqreen send notification alerts to Slack?

A. By creating a cookbook, defining a trigger, Alert a response, and notification

B. By creating a playbook, defining a trigger, security response, and notification

C. By creating a cookbook, defining a trigger, security response, and notification

D. By creating a playbook, defining a trigger, Alert a response, and notification

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

Richard Branson has been working as a DevSecOps engineer in an IT company that develops apps for Android mobiles. To manage the secret information of an application in various phases of development lifecycle and to provide fine-grained access to each secret, he would like to integrate HashiCorp Vault with Jenkins. To access the vault from Jenkins, Richard installed hashicorp-vault-plugin and ran a vault instance; he then selected the AppRole authentication method, which allows apps to access vault with a predefined role. Which of the following commands should Richard use to enable AppRole authentication?

A. enable auth vault approle

B. vault auth enable approle

C. enable vault auth approle

D. auth vault enable approle

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

Rachel Maddow has been working at RuizSoft Solution Pvt. Ltd. for the past 7 years as a senior DevSecOps engineer. To develop software products quickly and securely, her organization has been using AWS DevOps services. On January 1, 2022, the software development team of her organization developed a spring boot application with microservices and deployed it in AWS EC2 instance. Which of the following AWS services should Rachel use to scan the AWS workloads in EC2 instance for security issues and unintended network exposures?

A. AWS WAF

B. Amazon CloudWatch

C. AWS Inspector

D. AWS Config

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

GainInsights is an IT company that develops mobile applications software. On February 11, 2022, the organization became a victim of a cyber-attack. The attacker targeted the organization's application and compromised some important functionality. After the incident, the DevSecOps team of GainInsights identified the cause of the security issue, resolved it, and noted it for future reference. Based on this information, which of the following set of tests was conducted by GainInsights?

A. Security smoke tests

B. Security acceptance tests

C. White box testing

D. Blameless post-mortem

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Kevin Williamson is working as a DevSecOps engineer in an IT company located in Los Angles, California. His team has integrated Jira with Jenkins to view every issue on Jira, including the status of the latest build or successful deployment of the work to an environment. Which of the following can Kevin use to search issues on Jira?

A. Java query language

B. Jira query language

C. Structured query language

D. Atlassian query language

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

William Friedkin has been working as a DevSecOps engineer in an IT company for the past 3 years. His team leader has asked him to validate the host configuration that runs the Docker containers and perform security checks at the container level by implementing Docker's CIS Benchmark Recommendations. Therefore, William would like to integrate Docker Bench with Jenkins to incorporate security testing in DevOps workflow and secure the Docker Container. Before starting the procedure, he would like to install openssh on Ubuntu. Which of the following command should William run to install openssh on Ubuntu?

A. sudo apt-get -s install openssh-server

B. sudo apt-get install openssh-server

C. sudo apt.get install openssh-server

D. sudo apt.get -s install openssh-server

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

William O'Neil has been working as a senior DevSecOps engineer in an IT company that develops software products related to ecommerce. At this point in time, his team is working on securing a python-based application. Using GitGraber, William would like to detect sensitive information in real-time in his organizational GitHub repository. Therefore, he downloaded GitGraber and installed the dependencies. Which of the following commands should William use to find secrets using a keyword (assume the keyword is yahoo)?

A. python3 gitGraber.py -p wordlist/keywordsfile.txt -q "\yahoo\" -s

B. python3 gitGraber.py -g wordlist/keywordsfile.txt -q "\yahoo\" -s

C. python3 gitGraber.py -k wordlist/keywordsfile.txt -q "\yahoo\" -s

D. python3 gitGraber.py -w wordlist/keywordsfile.txt -q "\yahoo\" -s

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Sandra Oliver joined SinClare Soft Pvt. Ltd. as a DevSecOps engineer in January of 2010. Her organization develops software and web applications related to the healthcare industry. Using IAST runtime security testing technology, she is detecting and diagnosing security issues in applications and APIs. The IAST solution used by Sandra encompasses a web scanner with an agent that works inside the server that hosts the application to provide additional analysis details such as the location of the vulnerability in the application code. Based on the given information, which of the following IAST solutions is Sandra using?

A. Active IAST

B. Semi-active IAST

C. Semi-passive IAST

D. Passive IAST

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

Katie Holmes is working as a DevSecOps engineer at SeCSafe Anti-virus. The DevOps team of her organization has developed a distributed application with multiple microservices. Katie deployed all the microservices to the Kubernetes nodes successfully. The DevOps team approached Katie and informed her that the application is not working. Katie wants to check whether the Kubernetes cluster is working or not. Which of the following commands should Katie run step by step to verify that the Kubernetes is working?

A. kube-etcd version kube-etcd cluster-info

B. kube version kube cluster-info

C. kubectl version kubectl cluster-info

D. kubernetes version kubernetes cluster-info

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Brady Coleman is a senior DevSecOps engineer at CloudVac Security Private Ltd. He has created a new container named “eccbrad” from the centos:7 image using the command docker run -i -t --name geeklab centos:7 /bin/bash. Now, Brady wants to install the httpd package inside the eccbrad container. Which of the following commands should Brady use to install the httpd package inside the container?

A. yum install httpd

B. sudo install-httpd

C. sudo install httpd

D. yum install-httpd

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

Peter Dinklage has been working as a senior DevSecOps engineer at SacramentSoft Solution Pvt. Ltd. He has deployed applications in docker containers. His team leader asked him to check the exposure of unnecessary ports. Which of the following commands should Peter use to check all the containers and the exposed ports?

A. docker ps --quiet | xargs docker inspect --format : Ports

B. docker ps --quiet | xargs docker inspect --all --format ':Ports='

C. docker ps --quiet | xargs docker inspect --all --format : Ports=

D. docker ps --quiet | xargs docker inspect --format ': Ports='

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

Thomas Gibson has been working as a DevSecOps engineer in an IT company that develops software products and web applications related to law enforcement. To automatically execute a scan against the web apps, he would like to integrate InsightAppSec plugin with Jenkins. Therefore, Thomas generated a new API Key in the Insight platform. Now, he wants to install the plugin manually. How can Thomas install the InsightAppSec plugin manually in Jenkins?

A. By creating a .hpi file and uploading to his Jenkins installation

B. By creating a .conf file and uploading to his Jenkins installation

C. By creating a .war file and uploading to his Jenkins installation

D. By creating a .zip file and uploading to his Jenkins installation

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

Craig Kelly has been working as a software development team leader in an IT company over the past 8 years. His team is working on the development of an Android application product. Sandra Oliver, a DevSecOps engineer, used DAST tools and fuzz testing to perform advanced checks on the Android application product and detected critical and high severity issues. She provided the information about the security issues and the recommendations to mitigate them to Craig's team. Which type of security checks performed by Sandra involve detection of critical and high severity issues using DAST tools and fuzz testing?

A. Deploy-time checks

B. Commit-time checks

C. Test-time checks

D. Build-time checks

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

Gabriel Jarret has been working as a senior DevSecOps engineer in an IT company located in Houston, Texas. He is using Vault to manage secrets and protect sensitive data. On February 1, 2022, Gabriel wrote the secret using vault kv put secret/wejskt command. On February 10, 2022, his team detected a brute-force attack using Splunk monitoring tool. Gabriel would like to delete the secrets in the vault that he wrote on February 1, 2022. Which of the following commands should Gabriel use to delete a secret in Vault secret management tool?

A. vault kv del secret/wejskt

B. vault kv -delete secret/wejsktyup[

C. vault kv -del secret/wejskt

D. vault kv delete secret/wejskt

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Michael Rady recently joined an IT company as a DevSecOps engineer. His organization develops software products and web applications related to online marketing. Michael deployed a web application on Apache server. He would like to safeguard the deployed application from diverse types of web attacks by deploying ModSecurity WAF on Apache server. Which of the following command should Michael run to install ModSecurity WAF?

A. sudo apt install libapache2-mod-security2 –x

B. sudo apt install libapache2-mod-security2 –z

C. sudo apt install libapache2-mod-security2 –w

D. sudo apt install libapache2-mod-security2 –y

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

Rachel McAdams applied for the position of DevSecOps engineer at TetraSoft Pvt. Ltd. She gave her interview on February 23, 2022, and was selected as a DevSecOps engineer. Her team is working on securing Ruby on Rails application. Rachel's team leader asked her to integrate Brakeman SAST tool with Jenkins. To perform the integration, she navigated to Jenkins Plugin Manager and installed Warnings Next Generation Plugin. To run the tool in Jenkins, she invoked Brakeman as part of an Execute shell build step. In the Execute shell column, she wrote the following commands with brakeman options bash -l -c ' rvm install 3.0.0 && \ rvm use 3.0.0@brakeman -create && \ gem install brakeman && \ brakeman -no-progress -no-pager -no-exit-on-warn -o brakeman-output.json
What is the function of the -no-exit-on-warn option in the above-mentioned command?

A. It tells Brakeman to return a 1 exit code even if warnings are found

B. It tells Brakeman to return a 2 exit code even if warnings are found

C. It tells Brakeman to return a 3 exit code even if warnings are found

D. It tells Brakeman to return a 0 exit code even if warnings are found

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

DWART is an IT company that develops cyber security software and web applications. The organization ensures that all users should be identified and authorized, enforces proper auditing, secures data at rest, ensures that the attacker cannot bypass the security layers, implements multiple layers of defense, maintains proper data integrity, and performs proper input validation for the application. Based on the above-mentioned information, which of the following secure coding principles is achieved by DWART?

A. Secure by implementation

B. Secure by communication

C. Secure by design

D. Secure by default

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

Jason Barry has been working as a DevSecOps engineer in an IT company that develops software products and applications for ecommerce companies. During the build-time check, Jason discovered SQL injection and XXS security issues in the application code. What action does the build-time check perform on the application code?

A. It will stop the build process

B. It will ignore the security issue and continue the build process

C. It will send a message to issue and project management tool and continue with deploy-time check

D. It will send an alert to SIEM and continue with test-time check

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Joe Adler has recently been offered a job as a DevSecOps engineer in an IT company that develops software products and web applications for the healthcare industry. He would like to implement DevSec Hardening Framework to add a layer into the automation framework that configures operating systems and services and takes care of difficult settings, compliance guidelines, cryptography recommendations, and secure defaults. To apply DevSec Hardening Framework to the machine, he scanned the machine using Nessus scanning tool; he then checked the compliance results before using DevSec Hardening Framework. Which of the following commands should Joe use to run DevSec Hardening Framework?

A. Chef-solo -h solo.rb -m solo.json

B. Chef-solo -c solo.rb -j solo.json

C. Chef-solo -m solo.rb -h solo.json

D. Chef-solo -j solo.rb -c solo.json

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

Dustin Hoffman has been working as a DevSecOps engineer in an IT company located in San Diego, California. For detecting new security vulnerabilities at the beginning of the source code development, he would like to integrate Checkmarx SCA tool with GitLab. The Checkmarx template has all the jobs defined for pipeline. Where should Dustin incorporate the Checkmarx template file 'https://raw.githubusercontent.com/checkmarx-ltd/cx-flow/develop/templates/gitlab/v3/Checkmarx.gitlab-ci.yml'?

A. gitlab-ci/cd.yml root directory

B. gitlab-ci.yml root directory

C. gitlab-cd.yml root directory

D. gitlab.yml root directory

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Charles Rettig has been working as a DevSecOps engineer in an IT company that develops software and web applications for IoT devices. He integrated Burp Suite with Jenkins to detect vulnerabilities and evaluate attack vectors compromising web applications. Which of the following features offered by Burp Suite minimizes false positives and helps detect invisible vulnerabilities?

A. QAST

B. MAST

C. NAST

D. OAST

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Walter O'Brien recently joined as a junior DevSecOps engineer in an IT company located in Lansing, Michigan. His organization develops robotic process automation software for various clients stretched across the globe. Walter's team leader asked him to configure username and user email for git in VS Code. Therefore, he opened Visual Studio Code IDE console, then clicked on Terminal tab and selected New terminal. Which of the following command should Walter execute in the terminal to configure username and user email for git in VS Code?

A. get config --global user-name "walter username for git" get config --global user-email "walter email address used for git"

B. get git config --global user.name "walter username for git" get git config -global user.email "walter email address used for git"

C. get config --global user_name "walter username for git" get config --global user_email "walter email address used for git"

D. get config --global user.name "walter username for git" get config -global user.email "walter email address used for git"

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

Teresa Wheeler is a DevSecOps engineer at Altschutz Solution Pvt. Ltd. She would like to test the web applications and API's from outside without accessing the source code using BDD security framework. The framework is a collection of Cucumber-JVM features that are pre-configured with OWASP ZAP, Nessus scanner, SSLyze, and Selenium. Hence, she downloaded and ran the jar application, and then cloned the BDD security framework. Next, she utilized a command for executing the authentication feature. Which of the following commands allows Teresa to execute all the features of BDD security framework, including the OWASP ZAP?

A. ./gardlev

B. ./gardlew

C. /gardlew

D. /gardlev

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

Erica Mena has been working as a DevSecOps engineer in an IT company that provides customize software solutions to various clients across United States. To protect serverless and container applications with RASP, she would like to create an Azure container instance using Azure CLI in Microsoft PowerShell. She created the Azure container instance and loaded the container image to it. She then reviewed the deployment of the container instance. Which of the following commands should Erica run to get the logging information from the Azure container instance? (Assume the resource group name as ACI and container name as aci-test-closh.)

A. az container logs -resource-group ACI -name aci-test-closh

B. az get container logs --resource-group ACI --name aci-test-closh

C. az container logs --resource-group ACI --name aci-test-closh

D. az get container logs -resource-group ACI --name aci-test-closh

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

Jeremy Renner has been working as a senior DevSecOps engineer at an IT company that develops customized software to various customers stretched across the globe. His organization is using Microsoft Azure DevOps Services. Using an IaC tool, Jeremey deployed the infrastructure in Azure. He would like to integrate Chef InSpec with Azure to ensure that the deployed infrastructure is in accordance with the architecture and industrial standards and the security policies are appropriately implemented. Therefore, he downloaded and installed Chef InSpec. He used Azure CLI command for creating an Azure Service Principal with reader permission to the Azure resources, then he exported the generated credentials. After installation and configuration of Chef InSpec, he would like to create the structure and profile. Which of the following commands should Jeremy use to create a new folder jyren-azureTests with all the required artifacts for InSpec tests?

A. chef inspec init profile jyren-azureTests

B. chef inspec init profile jyren-azureTests

C. inspec init prof jyren-azureTests

D. inspec init profile jyren-azureTests

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

Evan Peters has been working as a DevSecOps engineer in an IT company located in Denver, Colorado. His organization has deployed various applications on Docker containers. Evan has been running SSH service inside the containers, and handling of SSH keys and access policies is a major security concern for him. What will be the solution for Evan security concern?

A. Run SSH on the host and utilize docker exec for interacting with the container

B. Run SSH on the docker build and utilize docker exec for interacting with the container

C. Run SSH on the registry and utilize docker exec for interacting with the container

D. Run SSH on the client and utilize docker exec for interacting with the container

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

Dave Allen is working as a DevSecOps engineer in an IT company located in Baltimore, Maryland. His team is working on the development of Ruby on Rails application. He integrated Brakeman with Jenkins to detect security vulnerabilities as soon as they are introduced; he then installed and configured Warnings Next Generation Plugin in Jenkins. What will be the use of Warnings Next Generation Plugin to Dave?

A. It will regulate the function of Brakeman

B. It will inspect TypeScript code for readability, functionality, and maintainability issues

C. It will gather and manage the results from Brakeman

D. It will validate Jenkins compiler settings

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

SinCaire is a software development company that develops web applications for various clients. To measure the successful implementation of DevSecOps, the organization enforced U.S. General Service Administrator (GSA) high-value DevSecOps metrics. Which of the following metrics implemented by SinCaire can measure the time between the code commit and production, and tracks the bug fix and new features throughout the development, testing, and production phases?

A. Time to value

B. Mean time to recovery (for applications)

C. Change lead time (for application)

D. Change volume (for application)

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

Kevin Williamson has been working as a DevSecOps engineer in an MNC company for the past 5 years. In January of 2017, his organization migrated all the applications and data from on-prem to AWS cloud due to the robust security feature and cost-effective services provided by Amazon. His organization is using Amazon DevOps services to develop software products securely and quickly. To detect errors in the code and to catch bugs in the application code, Kevin integrated PHPStan into the AWS pipeline for static code analysis. What will happen if security issues are detected in the application code?

A. The integrated PHPStan into the AWS pipeline will invoke the AWS Lambda function to parse and send result to the security hub

B. The integrated PHPStan into the AWS pipeline will invoke AWS Config to parse and send result to the security hub

C. The integrated PHPStan into the AWS pipeline will invoke AWS Elastic Beanstalk to parse and send result to the security hub

D. The integrated PHPStan into the AWS pipeline will invoke AWS CloudFormation to parse and send result to the security hub

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

Elizabeth Moss has been working as a DevSecOps engineer in an IT company located in San Diego, California. Due to the robust security and cost-effective service provided by AWS, her organization transferred all the workloads from on-prem to AWS cloud in 2017. Elizabeth would like to prevent committing AWS keys into repositories; therefore, she created a global git-templates directory using command line. Then, she created another directory, named it as hooks, wherein she created a file named pre-commit. In the pre-commit file, Elizabeth pasted the script that would prevent committing AWS keys into the repositories. She would like to ensure that the hook is executable. Which of the following command should Elizabeth run to make sure that the pre-commit hook is executable?

A. chmod a+e ~/.hooks/git-templates/pre-commit

B. chmod a+e ~/.git-templates/hooks/pre-commit

C. chmod a+x ~/.git-templates/hooks/pre-commit

D. chmod a+x ~/.hooks/git-templates/pre-commit

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

Patrick Fisher is a DevSecOps engineer in an IT company that develops software products and web applications. He is using IAST to analyze code for security vulnerabilities and to view real-time reports of the security issues. Patrick is using IAST in development, QA, and production stages to detect the vulnerabilities from the early stage of development, reduce the remediation cost, and keep the application secure. How can IAST perform SAST on every line of code and DAST on every request and response?

A. Because IAST has access to offline and runtime environment

B. Because IAST has access to server and local machine

C. Because IAST has access to internal and external agents

D. Because IAST has access to the code and HTTP traffic

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

Steven Gerrard has been working as a DevSecOps engineer at an IT company that develops software products and applications related to the healthcare industry. His organization has been using Azure DevOps services to securely and quickly develop software products. To ensure that the deployed infrastructure is in accordance with the architecture and industrial standards and the security policies are appropriately implemented, she would like to integrate InSpec with Azure. Therefore, after installation and configuration of InSpec, she created InSpec profile file and upgraded it with personal metadata and Azure resource pack information; then she wrote the InSpec tests. Which of the following commands should Steven use to run InSpec tests to check the compliance of Azure infrastructure?

A. inspec exec inspec-tests/integration/ -it azure://

B. inspec exe inspec-tests/integration/ -t azure://

C. inspec exec inspec-tests/integration/ -t azure://

D. inspec exe inspec-tests/integration/ -it azure://

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

Victor Garber is a DevSecOps team leader in SanSec Pvt. Ltd. His organization develops various types of software products and web applications. Currently, his team is working on security of Java-based web application product. How can Victor identify vulnerabilities that are missed in pre-production testing activities?

A. By performing deploy-time checks

B. By performing test-time checks

C. By performing commit-time checks

D. By performing build-time checks

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

Robin Tunney has been working as a DevSecOps engineer in an IT company located in Charleston, South Carolina. She would like to build a customized docker image using HashiCorp Packer. Therefore, she installed Packer and created a file docker-ubuntu.pkr.hcl; she then added HCL block to it and saved the file. Which of the following commands should Robin execute to build the Docker image using Packer?

A. packer -b docker-ubuntu.pkr.hcl

B. packer b docker-ubuntu.pkr.hcl

C. packer -build docker-ubuntu.pkr.hcl

D. packer build docker-ubuntu.pkr.hcl

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

Curtis Morgan is working as a DevSecOps engineer at Orchid Pvt. Ltd. His organization develops online teaching software. Beth McCarthy is working in a software development team, and she requested Curtis to help her in making pre-commit hooks executable on her local machine. Curtis went through the “repo\.git\hooks” directory and removed the “.sample” extension from “pre-commit.sample” file by using “chmod +x filename” command and made the pre-commit hook executable on Beth’s local machine. On the next day while developing the code for the software product, Beth accidentally committed the code with sensitive information. What will be the result of this commit?

A. The script will exit with 0

B. The script will exit with 3

C. The script will exit with 1

D. The script will exit with 2

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

Dustin Hoffman is a DevSecOps engineer at SantSol Pvt. Ltd. His organization develops software products and web applications related to mobile apps. Using Gauntlt, Dustin would like to facilitate testing and communication between teams and create actionable tests that can be hooked in testing and deployment process. Which of the following commands should Dustin use to install Gauntlt?

A. $ gems install gauntlt

B. $ gem install gauntlt

C. $ gem install Gauntlt

D. $ gems install Gauntlt

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

Scott Morrison is working as a senior DevSecOps engineer at SUTRE SOFT Pvt. Ltd. His organization develops software and applications for IoT devices. Scott created a user story; he then created abuser stories under the user story. After that, he created threat scenarios under the abuser story, and then he created test cases for the threat scenarios. After defining the YAML, Scott would like to push the user-story driven threat model to the ThreatPlaybook server. Which of the following command Scott should use?

A. playbook apply feature -f < path to the yaml file > -t test-project

B. playbook apply feature -y < path to the yaml file > -p test-project

C. playbook apply feature -f < path to the yaml file > -p test-project

D. playbook apply feature -p < path to the yaml file > -t test-project

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

Peter McCarthy is working in TetraVerse Soft Solution Pvt. Ltd. as a DevSecOps engineer. His organization develops customized software products and web applications. To develop software products quickly and securely, his organization has been using AWS cloud-based services, including AWS DevOps services. Peter would like to use CloudMapper to examine the AWS cloud environment and perform auditing for security issues. Which of the following privileges should Peter possess in order to collect information about the AWS account?

A. arn:aws:iam::aws:policy/SecurityAudit::SecurityCheck arn:aws:iam::aws:policy/job-role/ViewOnlyAccess::EditOnlyAccess

B. arn:aws:iam::aws:policy/SecurityAudit arn:aws:iam::aws:policy/job-function/ViewOnlyAccess

C. arn:aws:iam::aws:policy/AWSLambdaFullAccess arn:aws:iam::aws:policy/job-role/ViewOnlyAccess

D. arn:aws:iam::aws:policy/SecurityCheck arn:aws:iam::aws:policy/job-function/ViewOnlyAccess::EditOnlyAccess

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

SNF Pvt. Ltd. is a software development company located in Denver, Colorado. The organization is using pytm, which is a Pythonic Framework for threat modeling, to detect security issues and mitigate them in advance. James Harden has been working as a DevSecOps engineer at SNF Pvt. Ltd. for the past 3 years. He has created a tm.py file that describes an application in which the user logs the app and posts the comments on the applications. These comments are stored by the application server in the database and AWS lambda cleans the database. Which of the following command James can use to generate a sequence diagram?

A. tm.py --seq | java -Djava.awt.headless=true -jar plantuml.jar -tpng -pipe > seq.png

B. tm.py --seq | java -djava.awt.headless=true -jar plantuml.jar -tpng -pipe > seq.png

C. tm.py --seq | java -djava.awt.headless=true -jar plantum.jar -tpng -pipe > seq.png

D. tm.py --seq | java -Djava.awt.headless=true -jar plantum.jar -tpng -pipe > seq.png

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

Kenneth Danziger is a certified DevSecOps engineer, and he recently got a job in an IT company that develops software products related to the healthcare industry. To identify security and compliance issues in the source code and quickly fix them before they impact the source code, Kenneth would like to integrate WhiteSource SCA tool with AWS. Therefore, to integrate WhiteSource SCA Tool in AWS CodeBuild for initiating scanning in the code repository, he built a buildspec.yml file to the source code root directory and added the following command to pre-build phase curl -LJO https://github.com/whitesource/unified-agent-distribution/raw/master/standAlone/wss_agent.sh. Which of the following script files will the above step download in Kenneth organization's CodeBuild server?

A. wss.agent.sh

B. ssw_agent.sh

C. cbs_agent.sh

D. aws_agent.sh

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

Sarah Wheeler is an experienced DevSecOps engineer. She recently joined an IT company that develops software products for customers stretched across the globe. Sarah would like to use a security testing tool that protects the application from false positives, network sniffing, tampering with code, etc. The tool should monitor the incoming traffic to the server and APIs for suspicious activities and help her team in remediating them during runtime. Which of the following tools should Sarah select that will help her team in precisely detecting and remediating the security issues in the application code during runtime?

A. IAST

B. DAST

C. SAST

D. RASP

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

Lisa Kramer carries an experience of 4 years as a DevSecOps engineer in an IT company. The software development team of her organization has developed a Ruby on Rails web application and would like to find vulnerabilities in Ruby dependencies. Therefore, the team leader of the software development team approached Lisa for help in this regard. Which of the following SCA tool should Lisa use to detect vulnerabilities in Ruby dependencies?

A. Bundler-Audit

B. Bandit

C. Retire.js

D. Tenable.io

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

Charles Drew has been working as a DevSecOps team leader in an IT company located in Nashville, Tennessee. He would like to look at the applications from an attacker's perspective and make security a part of the organizations' culture. Imagine, you are working under Charles as a DevSecOps engineer. Charles has asked you to install ThreatPlaybook, which is a unified DevSecOps Framework that allows you to go from iterative, collaborative threat modeling to application security testing orchestration. After installation, you must configure ThreatPlaybook CLI; therefore, you have created a directory for the project and then you go to the current directory where you would like to configure ThreatPlaybook. Which of the following commands will you use to configure ThreatPlaybook? (Here, <your-email> represents your email id; <host info> represents IP address; and <port> represents the nginx port.)

A. ThreatPlaybook configure -e < your-email > -h < host-info > -p < port >

B. playbook configure -e < your-email > -u < host-info > -p < port >

C. ThreatPlaybook configure -e < your-email > -u < host-info > -p < port >

D. playbook configure -e < your-email > -h < host-info > -p < port >

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

Steven Smith has been working as a DevSecOps engineer in an IT company that develops software products related to the financial sector. His team leader asked him to integrate Conjur with Jenkins to secure the secret credentials. Therefore, Steven downloaded Conjur.hpi file and uploaded it in the Upload Plugin section of Jenkins. He declared host and layers, and declared the variables. Which of the following commands should Steven use to set the value of variables?

A. $ conjur variable set -v < policy-path-of-variable-name > -i < secret-value >

B. $ conjur variable set -p < policy-path-of-variable-name > -s < secret-value >

C. $ conjur variable set -i < policy-path-of-variable-name > -v < secret-value >

D. $ conjur variable set -s < policy-path-of-variable-name > -p < secret-value >

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

Orange International Pvt. Ltd. is an IT company that develops software products and web applications for Android phones. The organization recognizes the importance of secure coding principles and would like to enforce it. Therefore, Orange International Pvt. Ltd. established access management, avoided reinventing the wheel, secured the weak links, implemented in-depth defense, and reduced third-party involvement in the application. Based on the above-mentioned information, which of the following secure coding principles is achieved by the organization?

A. Secure by communication

B. Secure by default

C. Secure by implementation

D. Secure by design

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

Charlotte Flair is a DevSecOps engineer at Egma Soft Solution Pvt. Ltd. Her organization develops software and applications related to supply chain management. Charlotte would like to integrate Sqreen RASP tool with Slack to monitor the application at runtime for malicious activities and block them before they can damage the application. Therefore, she created a Sqreen account and installed Sqreen Microagent. Now, she would like to install the PHP microagent. To do so, she reviewed the PHP microagent's compatibility, then she signed in to Sqreen account and noted the token in Notepad. Which of the following commands should Charlotte run in the terminal to install the PHP extension and the Sqreen daemon?

A. curl -i https://download.sqreen.com/php/install.sh < sqreen-install.sh \ && bash sqreen-install.sh [CHARLOTTE'S ORG TOKEN HERE] "[CHARLOTTE'S APP NAME HERE]"

B. curl -s https://download.sqreen.com/php/install.sh < sqreen-install.sh \ && bash sqreen-install.sh [CHARLOTTE'S ORG TOKEN HERE] "[CHARLOTTE'S APP NAME HERE]"

C. curl -s https://download.sqreen.com/php/install.sh > sqreen-install.sh \ && bash sqreen-install.sh [CHARLOTTE'S ORG TOKEN HERE] "[CHARLOTTE'S APP NAME HERE]"

D. curl -i https://download.sqreen.com/php/install.sh > sqreen-install.sh \ && bash sqreen-install.sh [CHARLOTTE'S ORG TOKEN HERE] "[CHARLOTTE'S APP NAME HERE]"

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #50 *Topic 1*

Rachel McAdams has been working as a senior DevSecOps engineer in an IT company for the past 5 years. Her organization embraced AWS cloud service due to robust security and cost-effective features offered by it. To take proactive decisions related to the security issues and to minimize the overall security risk, Rachel integrated ThreatModeler with AWS. ThreatModeler utilizes various services in AWS to produce a robust threat model. How can Rachel automatically generate the threat model of her organization's current AWS environment in ThreatModeler?

A. By using YAML spec-based orchestration tools

B. By using Accelerator

C. By using Architect

D. By using STRIDE per Element

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!