Question 1 of 75

Which cloud security category of tools inspect microservices environments such as Kubernetes for security issues?

- ◯ Cloud Access Security Broker
- ◯ Cloud Workload Protection Platform
- ◯ Cloud Security Posture Management

Question 2 of 75

How does using RASP affect an environment?

- ◯ Areas of the code that have not been tested become easier to visualize
- ◯ A proxy server needs to be deployed in order to install RASP tools
- ◯ Runtime overhead is introduced, affecting CPU, memory, and latency
- ◯ Network traffic needs to be redirected for inspection

TRACE - 3.93 LOGS

Question 4 of 75

Which of the following events is highest priority for using a workflow hook to validate code correctness?

- ○ Remote repository: update
- ✓ **Remote repository: post-receive**
- ✗ **Local repository: commit**

✗ **You are incorrect**

Commit hooks can be used to automatically run scripts checking for embedded secrets, code correctness, etc. at different points in workflows:
• Local repository: pre-commit, prepare-commit, commit, post-commit, post-checkout, pre-rebase
• Remote repository: pre-receive, update, post-receive
Three of these events are high-value and so are the highest priority:
Local repository: pre-commit
Remote repository: pre-receive, post-receive

Question 5 of 75

A DevOps team that uses Just-in-Time prioritization to manage their workload is following the principles of which element of CALMS?

- ○ Automation
- ○ Culture
- ○ Lean
- ○ Sharing

JWT REPLAY PREVENTION - NOUNCE

Question 7 of 75

Which of the following is a mitigation to MITRE ATT&CK Containers T1525: Implant Internal Image?

- ○ Sign custom images and store in a private registry
- ○ Configure build time secrets
- ○ Leverage container orchestration software
- ○ Use public image registries such as Docker Hub

Question 8 of 75

What task is accomplished in the code snippet below?

```
...
EncryptRequest req = new
EncryptRequest().withKeyId(KMSKey).withPlaintext(plaintext);
ByteBuffer ciphertext = kms.encrypt(req).getCiphertextBlob();
...
```

- ◯ Client-side data encryption using AWS SDK
- ◯ Creation of a data encryption key using AWS SDK
- ◯ Encrypting and sending data to an RDS instance using AWS CLI
- ◯ AWS CMK creation using a CloudFormation template

A

Question 9 of 75

How does GitLab run each stage of CI/CD workflows?

- ◯ Individual serverless functions
- ◉ **Inside of containers**
- ◯ Kubernetes engine nodes
- ◯ Directly on the runner

B

Question 10 of 75

Which command does BuildKit augment to avoid hard-coding secrets within Dockerfiles?

- attach
- create
- scan
- build

D WRONG ACTULALY - ARG IS --SECRERS

Question 11 of 75

A website streams video-on-demand using CloudFront and controls access to videos using signed URLs with canned policies. All videos can be streamed for 24 hours after they are ordered and paid for.

A user of the service paid for a wonderful mystery video that is 2 hours and 30 minutes long at noon on Monday. They forgot that they ordered it until 11 am on Tuesday, at which time they immediately began playing it. When the video had just 15 minutes left to play - just as the murderer was about to be named! - the video suddenly stopped. When they tried to restart it, it would not play. What would cause this tragedy?

- A TCP reset occurred during download
- The user's IP address access has been blacklisted
- A signed cookie was used when attempting to restart the video

A

Question 12 of 75

Which Azure message-based service allows the use of reactive programming to perform security actions based on specified scenarios?

- ✗ **Analytic Workspaces**
- ○ Event Hubs
- ✓ **Event Grid**
- ○ Service Bus

✗ **You are incorrect**

Different cloud providers have different message-based services. For example, Azure has Event Grid, Event Hubs, and Service Bus. How can you make sense of this plethora of event-related services? For Azure, let's just state it up front that for the security automation tasks that we are most concerned with in our DevOps process we will rely upon Event Grid which enables "reactive programming" where you can react to changes in your cloud resources and take necessary security actions.

Event Hubs are used for streaming large amounts of data, perhaps millions of events per second. This is most useful for distributed data streaming of things like telemetry related information. Service Bus is a message broker (not a reactive event-driven system) that is intended for systems that require transactions, message ordering, and consistency.

Question 13 of 75

Which of the following would be recorded in AWS Application Load Balancer access logs?

- ○ eni-1235b8ca123456789 172.31.16.101 172.31.16.52 20641 80
- ○ Backdoor:EC2/DenialOfService.UnusualProtocol
- ○ "GET /wordpress/?p=1 HTTP/1.1" 200
- ○ TLSv1.2 ECDHE-RSA-AES128-GCMSHA256 Error HTTP/1.1

C

Question 14 of 75

Reconfiguring a Lambda function via the following command could enable which security benefit?

```
$ aws lambda update-function-configuration --function-name mylambdafunctiona -
-layers
```

- ◯ Centralization of package management
- ◯ Ability to assign multiple execution policies
- ◯ Ability to block new child processes
- ◯ Separation of executable code and input

A PAGE 4.130

Question 15 of 75

Which of the following is a feature of the AWS Network Load Balancer?

- ◯ Path-based routing
- ◯ Dynamic port mapping
- ◉ **Elastic IP address support**
- ◯ Optional Web Application Firewall

C PAGE 3.30

Question 16 of 75

Which of the following is paired with Change Failure Rate to measure the reliability and quality of a service?

- ◯ MTTD
- ◯ MTTR
- ◯ MTTF
- ◯ MTBF

B CHECK WHAT IT IS

Question 17 of 75

A Logic App would perform which task within Azure Monitor?

- ◯ Alert generation
- ◯ Metric analysis
- ◯ Service integration
- ◯ Dashboard creation

C PAGE 3.95

Question 19 of 75

What needs to be added to an Azure Content Delivery Network to enable token authentication?

- ◯ JSON web signature
- ◯ Key vault secret
- ◯ SHA-256 hash
- ◯ Encryption key

D 4.27

Question 20 of 75

What do service mesh solutions provide in microservice architectures?

- ◯ Load balancing
- ◯ Credential storage
- ◯ Container build automation
- ◯ Disaster recovery

A 4.84

Question 21 of 75

Which command will validate encryption settings for CloudFormation templates?

- $ checkov --directory ./templates --framework terraform --output json > checkov.json
- **$ cfn_nag_scan -i templates -o json > cfn_nag.json**
- **$ sudo docker run -e LEARNING_MODE=true -v $(pwd):/iac seiso/easy_infra**

You are incorrect

Stelligent's cfn_nag IaC security scanner is a command line CloudFormation template checker. Its rules support IAM, security groups, logging, encryption, and more.

Checkov could be used to accomplish this task, but the command showing Checkov use is being applied to Terraform rather than CloudFormation.

Question 22 of 75

What is the purpose of DNS records like the pair shown below?

```
BlueDNSRecord:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref MyHostedZoneId
    Name: www.example.com.
    Type: A
    TTL: '60'
    SetIdentifier: 'blue-stack'
    Weight: '90'
    ResourceRecords:
    - example.amazonaws.com
GreenDNSRecord:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref MyHostedZoneId
    Name: www.example.com.
    Type: A
    TTL: '60'
    SetIdentifier: 'green-stack'
    Weight: '10'
    ResourceRecords:
    - new.example.amazonaws.com
```

- ○ Differentiates between public and private entities
- ○ Controls TTL for an EC2 instance
- ✓ **Allows for weighted routing**
- ✗ **Identifies individual websites within a web server**

✗ **You are incorrect**

Route 53 is the managed DNS service from AWS. It allows for weighted routing by associating multiple resources with a single domain or subdomain to define how much traffic is routed to each resource.

In the example shown, we have separate "blue" and "green" DNS records in CloudFormation. The blue record has a weight of 90 and the green record has a weight of 10. That means that the green stack will receive 10% of the overall traffic.

Question 23 of 75

Which of the following is introduced by implementing IaC?

- ○ Forcing dynamic code analysis
- ○ Reducing application availability
- ◉ **Disclosing secret keys**

Question 25 of 75

What is a common task of pre-commit hooks?

- ◉ **Scanning for secure handling of code secrets**
- ○ Automating the acceptance testing of new code
- ○ Publishing container images to the registry
- ○ Enforcing branch protections in version control

Question 26 of 75

Which tool integrates IaC static analysis into the CI/CD pipeline?

- ○ SourceClear
- ◉ **Checkov**
- ○ GuardDuty

Question 27 of 75

What can Azure storage managers generate to delegate access to storage objects on a granular basis?

- [x] **Shared Access Signatures**
- [ ] Kerberos Tickets
- [ ] Storage Account Keys
- [ ] TLS Certificates

Question 28 of 75

What are cloud-based WAFs integrated into?

- [x] **Load Balancers**
- [ ] Network Security Groups
- [ ] Runtime Application Self Protection

Question 29 of 75

In an Azure infrastructure, which of the following is an always-on feature that automatically encrypts the data written to Azure storage?

- [ ] Encrypted File System
- [ ] Service-level Shared Access Signatures
- [x] **Storage Service Encryption**
- [ ] Azure Disk Encryption

Question 30 of 75

Which of the following can determine if a Docker Swarm of containers has applied the latest CIS Benchmark recommendations?

- ✗ DockerScan
- ✓ Docker Actuary
- ○ StackRox

✗ **You are incorrect**

Docker Actuary is an extension to Docker Bench used to scan container against CIS recommendations and is designed to scan all nodes in a Docker Swarm.

DockerScan is a pen-test attack platform. Aqua Container Security Platform is a full-featured offering for protecting containers, including static vulnerability scanning, runtime scanning, monitoring and intrusion protection, fine-grained container network segmentation, user access control, and auditing. StackRox is focused on providing deep visibility into what is happening in every container.

Question 31 of 75

What is a characteristic that differentiates the Azure Firewall service from Network Security Groups (NSG)?

- ○ Supports service tags for source and destination
- ○ Supports permissive rules only
- ✓ **Capable of threat intel-based filtering**
- ○ Applied to an EC2 instance instead of a VPC

Question 32 of 75

Which of the following is a formatted code line from a Markdown file?

- ✓ **## Rapid Risk Assessment**
- ○ /* List disabled accounts */
- ○ "Effect": "Allow"
- ○ <name: Security Scan>

Question 33 of 75

When configuring a security group for a new EC2 instance, what are the default egress and ingress traffic rules?

- ○ Outbound: Do not allow any traffic; Inbound: Do not allow any traffic
- ○ Outbound: Allow all traffic; Inbound: Allow all traffic
- ○ Outbound: Do not allow any traffic; Inbound: Allow all traffic
- ✓ **Outbound: Allow all traffic; Inbound: Do not allow any traffic**

Question 34 of 75

Which of the following is required in order to use Ansible for computer management?

- ○ Agent on each node
- ✓ **Python on each node**
- ✗ **Primary server**
- ○ JSON scripts

✗ **You are incorrect**

Ansible is an easy-to-set-up/easy-to-use configuration management and orchestration tool-strong support for network devices. Ansible is written in Python and works as a thin wrapper to execute commands over SSH (or native PowerShell remoting on Windows).

Ansible does not need agents installed on each machine (but needs Python). It does not need a primary server - any node that has the correct list of servers can be used to push out changes over SSH to the rest of the network. Configuration can be scripted in "playbooks" and "roles" using YAML.

2.67

Question 36 of 75

Which of the following tools can quickly spin up a virtual machine for integration and acceptance testing of recipes?

- ○ Goss
- ○ Test Kitchen
- ○ ChefSpec
- ✓ **Vagrant**

Question 37 of 75

What is the purpose of the CloudFormation snippet below?

```
FlowLog:
  Type: AWS::EC2::FlowLog
  Properties:
    DeliverLogsPermissionArn:
      !GetAtt FlowLogRole.Arn
    LogGroupName:"Flow-Log-Group"
    ResourceId: !Ref VPC
    ResourceType: "VPC"
    TrafficType: "ACCEPT"
```

- ○ Send filtered VPC flow logs to GuardDuty
- ✓ **Publish filtered VPC flow data to CloudWatch**
- ○ Push VPC logs for accepted connections to ELK
- ○ Disable logging for accepted VPC flow traffic

Question 38 of 75

Which of the following replaces the question marks (????) in the configuration below?

```
resource "azurerm_monitor_action_group" "webhook" {
  ???? {
    name = "WebhookNotification"
    function_app_resource_id = azurerm_function_app.webhook.id
    function_name = azurerm_function_app.webhook.name
    http_trigger_url = "https://dghf3.giac.net"
```

- ○ trigger
- ✓ **azure_function_receiver**
- ○ action
- ○ metric_transformation

The following is a description of which OWASP Top 10 CI/CD Security Risk?

"An attacker obtains permissions to a CI/CD process and pushes malicious code or artifacts further down the pipeline."

- ○ CICD-SEC-3: Dependency Chain Abuse
- ✗ **CICD-SEC-4: Poisoned Pipeline Execution**
- ✓ **CICD-SEC-1: Insufficient Flow Control Mechanisms**
- ○ CICD-SEC-5: Insufficient Pipeline-Based Access Controls

You are incorrect

Daniel Krivelevich and Omer Gil from Prisma Cloud maintain an OWASP open-source project called Top 10 CI/CD Security Risks. The risks include:

CICD-SEC-1: Insufficient Flow Control Mechanisms: Attacker obtains permissions to a CI/CD process (version control, CI, artifact repository, etc.) and pushes malicious code or artifacts further down the pipeline.

Which organization maintains provider-specific benchmarks and configuration recommendations for hardening cloud services?

- ✗ **NIST**
- ○ OWASP
- ○ DHS
- ✓ **CIS**

✗ **You are incorrect**

CIS maintains cloud provider-specific benchmarks called the AWS and Azure Foundation Benchmarks. They provide step-by-step implementation, configuration, and assessment procedures for hardening cloud accounts and services.

Which of the following metrics can be measured from the perspective of Change Cycle Time, Development Change Lead Time, or Deployment Lead Time?

- ○ Change Failure Rate
- ○ Change Frequency
- ✓ **Cycle Time**
- ✗ **Mean Time To Repair**

✗ **You are incorrect**

Change Lead Time or Cycle Time is the average time it takes to get a change or fix into production, which is a key metric for DevOps teams (and Lean teams) to optimize for. This can be measured from three points:

- Change Cycle Time looks at the full value stream, both upstream and downstream of development
- Development Change Lead Time focuses on speeding up development, testing, and deployment
- Deployment Lead Time focuses on speeding up acceptance testing, change control, and deployment

The following AWS policy statement defines access for which type of resource?

```
Statement:
  - Action:
    - "ssm:GetParameters"
    Effect: "Allow"
```

- ○ An S3 bucket
- ○ A VPC security group
- ✗ **A CloudFront distribution**
- ✓ **An EC2 instance**

✗ **You are incorrect**

The example shows the policy settings to allow an EC2 instance profile access to read a parameter store value. The example shows how to grant the "ssm:GetParameters" action:

```
Statement:
  - Action:
    - "ssm:GetParameters"
    Effect: "Allow"
```

Separately, the EC2 instance profile must also be configured with decrypt access to the KMS key backing the parameter value.

Based on the Same Origin Policy, which of the following sites would be able to access the data at `http://www.mysite.com/description/tutorials/webdesign.html` if default port assignments are in use?

- ○ http://www.yoursite.com/description/tutorials/
- ○ https://www.mysite.com:80
- ✓ **http://www.mysite.com/contact/**
- ○ https://www.mysite.com:443

Given the following configuration, what is included in the dataplane-log.conf?

```
apiVersion: v1

kind: ConfigMap

metadata:

               name: fluent-bit-config

                namespace: amazon-cloudwatch

                labels:

                  k8s-app: fluent-bit

data:

                @INCLUDE application-log.conf

                @INCLUDE dataplane-log.conf

                @INCLUDE host-log.conf
```

- ✗ **/var/log/containers/*.log**
- ○ /var/log/secure
- ○ /var/log/messages
- ✓ **/var/log/containers/aws-node***

You are incorrect

The dataplane configuration includes logs from the container service, containerd, and the kubelet stored in the /var/log/containers/aws-node*, /var/log/containers/kube-proxy* directories.

How does a distributed version control system like Git track changes?

- ○ Temporary files appended with the user's account name are created for working files
- ○ Separate version data file is stored alongside each working file in the central repository
- ✓ **Unique identifiers in the form of cryptographic hashes are generated for each state of a repository**
- ○ File locks are placed when a file is checked out until it is checked back in on the server

A DevOps team embracing a CALMS approach will use which technique to identify waste, bottlenecks, and delays?

- [x] **Value stream mapping**
- [ ] Backlog dashboards
- [ ] Deployment scripts and runbooks
- [ ] Change frequency measurements

Which of the following is a difference between WAF and RASP?

- [ ] RASP relies on signatures for detection and WAF does not
- [x] **WAF does not focus on the internal state of the application and RASP does**
- [ ] WAF cannot inspect traffic if it is encrypted by TLS, but RASP can
- [ ] RASP cannot inspect traffic if it is encrypted by TLS, but WAF can

What information is found in line 3 of the following JSON Web Token?

```
1 eyJhbGciOiJSUzI1NiJ9.
2 eyJ1aWQiOiI1NDIxMDU0OCIsIjbGFpbSI6IkdldEFjY291bnQifQ.
3 Kho7o2Rz9p42HKi84KfWBxAxJAwwKIAdy4msKSy0ZY
```

- [x] **Signature**
- [ ] Payload
- [ ] Claims
- [ ] Algorithm

When implementing sigstore, what does rekor accomplish?

- [x] **Tracks signature transparency logs**
- [ ] Stores signed and verified containers
- [ ] Automates 20-minute certificates for code signing
- [ ] Enforces git commit and tag signing

When implementing sigstore, what does rekor accomplish?

- [x] **Tracks signature transparency logs**
- [ ] Stores signed and verified containers
- [ ] Automates 20-minute certificates for code signing
- [ ] Enforces git commit and tag signing

What does AWS's Key Management Service use to perform extra integrity checks when decrypting data?

- ◯ HSA Backing Key
- ◉ **Encryption context**
- ◯ Data Key
- ◯ Customer Master Key

What is a characteristic of programmable infrastructure?

- ◯ Configuration definitions are customized and unique
- ◯ The build pipeline is overseen by change control committee
- ◉ **Source control manages configuration changes**

An organization needs MFA to be required for all IAM users and roles within their AWS organization. Which control can ensure that this is in place?

- ◯ CIS Benchmarks
- ◯ Security Hub
- ◯ Permission Boundary
- ◉ **Service Control Policies**

Which Terraform HCL code sample can be used to get information about an Azure container that is not defined or managed by the current configuration?

- ○ resource "null_resource" "ABC_Corp_Build" { provisioner "local-exec" { command = "az acr build --resource-group ${var.resource_group_name} --registry ${var.container_registry_name} --image abc_corp_app_srv:v1 ." } }
- ✓ **data "azurerm_container_registry" "ABC_Corp" { name = var.container_registry_name resource_group_name = var.resource_group_name}**
- ○ output "ABC_Corp_Host" { value = "${azurerm_kubernetes_cluster.ABC_Corp.kube_config.0.host}" }
- ✗ **resource "azurerm_resource_group" "ABC_Corp" { name = var.resource_group_name location = var.location }**

✗ You are incorrect

In the HashiCorp Configuration Language (HCL), data sources are used to get information about resources that are not defined or managed by the current configuration. The code block beginning with `data` correctly returns information about an undefined or unmanaged resource.

The `resource` code block referencing `azurerm_resource_group` is used to define an Azure Resource Manager (ARM) resource. The code block beginning with `output` is used to return information from configuration run for a defined or managed resource. The `resource` code block that references the `null_resource` is used to define a provisioner that is not associated with a specific resource.

An engineer wants to use the `aws logs filter-log-events` command to retrieve data from an AWS flow log group. What does the engineer need to get from the output of the following command to successfully retrieve this data?

```
$ aws ec2 describe-flow-logs
```

- ○ Log destination type
- ○ Log format
- ○ Flow log ID
- ✓ **Log group name**

Which category of cloud security tools provides visibility and control of software-as-a-service solutions?

- ○ Cloud Workload Protection Platform
- ○ Cloud Security Posture Management
- ✓ **Cloud Access Security Broker**

Which git secrets command would produce the following output showing all possible secret expression pattern matches?

```
secrets.providers git secrets --aws-provider
secrets.patterns [A-Z0-9]{20}
secrets.patterns ("|')?(AWS|aws|Aws)?_?(SECRET|secret|Secret)?_?(ACCESS|access|Access)?_?(KEY|key
)("|')?\s*(:|=>|=)\s*("|')?[A-Za-z0-9/\+=]{40}("|')?
secrets.patterns ("|')?(AWS|aws|Aws)?_?(ACCOUNT|account|Account)_?(ID|id|Id)?("|')?\s*(:|=>|=)\s*("|'
)?[0-9]{4}\-?[0-9]{4}\-?[0-9]{4}("|')?
secrets.allowed AKIAIOSFODNN7EXAMPLE
secrets.allowed wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

- [x] **--list**
- [ ] --aws-provider
- [ ] --add
- [ ] --register-aws
- [ ] --scan

What is one of the keys to integrating security with Continuous Delivery (CD)?

- [x] **Perform long-running tests outside the CD pipeline**
- [ ] Focus on front-loading security tests in the pre-commit phase
- [ ] Provide feedback to engineers only when they request it
- [ ] Use tools that require manual setup and review

Which feature is available with Azure Firewall but is not supported by Network Security Groups (NSG)?

- [ ] Protocol based traffic filtering
- [ ] Stateful inbound rules
- [x] **Support for service tags**
- [x] **Network Address Translation support**

You are incorrect

Azure Network Security Groups is a very basic software defined firewall solution that filters traffic at the Network layer. Azure Firewall is a more robust, managed firewall service that can filter and analyze L3, L4 and L7 traffic. Both are stateful, provide protocol-based traffic filtering and support service tags. Some additional features that the Azure Firewall provides are the ability to tag traffic based on the fully qualified domain names (FQDNs) of Azure services and NAT support.

When using Terraform, what command will change the infrastructure?

- ○ push
- ◉ **apply**
- ○ init
- ○ plan

Which of the following parameters determines which type of data is used in Azure Monitor?

- ✓ **product**
- ○ workspace_name
- ✗ **sku**
- ○ location
- ○ resource_group_name

✗ **You are incorrect**

The product parameter defines the type of data will be used in the Azure Monitor solution. Values include: SecurityCenterFree, Security, Updates, ServiceMap, AzureActivity, ChangeTracking,

VMInsights, SecurityInsights, NetworkMonitoring, SQLVulnerabilityAssessment, SQLAdvancedThreatProtection, AntiMalware, AzureAutomation, LogicAppsManagement, SQLDataClassification.

What can be inferred about the following Terraform code?

```
resource "azurerm_web_application_firewall_policy" "app_gateway" {
    name    = "WAFPolicy"

policy_settings {
    enabled                     = true
    mode                        = "Prevention"
    request_body_check             = true
    max_request_body_size_in_kb     = 128
}

managed_rules   {
    managed_rule_set    {
        type    = "OWASP"
        version = "3.1"
       }
    }
}
```

- ✓ **Rule severity is correlated to an anomaly score before traffic is blocked**
- ✗ **Any traffic that matches a rule will be denied**
- ○ Any single occurrence of traffic that triggers a severity of 'Warning' will be blocked

✗ **You are incorrect**

The Terraform code shows an Azure WAF configuration using Core Rule Set (CRS) version 3.1. Anomaly scoring was introduced in version 3.1 and is used in Prevention mode. Anomaly scoring considers the rule severity (Critical, Error, Warning, or Notice) to build an overall Anomaly Score. For something to be blocked, the total anomaly score must be a 5. A Warning severity only scores a 3, so traffic causing a single Warning will not be blocked. A Critical severity item has a score of 5, so just a single instance of it will be blocked.

In contrast to anomaly scoring is "traditional mode" used by CRS versions prior to 3.1, in which any traffic that simply matches the rule triggers a block regardless of any other context.

Which of the following characteristics fits into the Advanced Zero Trust Maturity level?

- ○ Just in time policy assignment
- ✓ **Centralized visibility**
- ○ Full automation
- ○ Cross-pillar integrations

When employing an API Gateway, which of the following is a liability?

- ✗ **More roundtrips between client and application**
- ○ Complicates the logic for the client
- ○ More client exposure to backend changes
- ✓ **Longer roundtrip time**

✗ **You are incorrect**

By relying on the API gateway to perform multiple calls to the backend services, the client will have to wait longer for its response. While this longer roundtrip time may not be much of an issue on a high-speed system, slowdowns in network connections between the API gateway and its integrated services will greatly increase the delay in returning the data to the client.

An API gateway can reduce this time cost by allowing all of the data processing to be performed with a single request and response. By providing a single point of contact for making all web service calls, clients can be protected from the impact of changing backend services or introducing new data sources. As with reducing the number of roundtrips, using an API gateway reduces and simplifies the amount of programming logic needed by a client to process web service data.

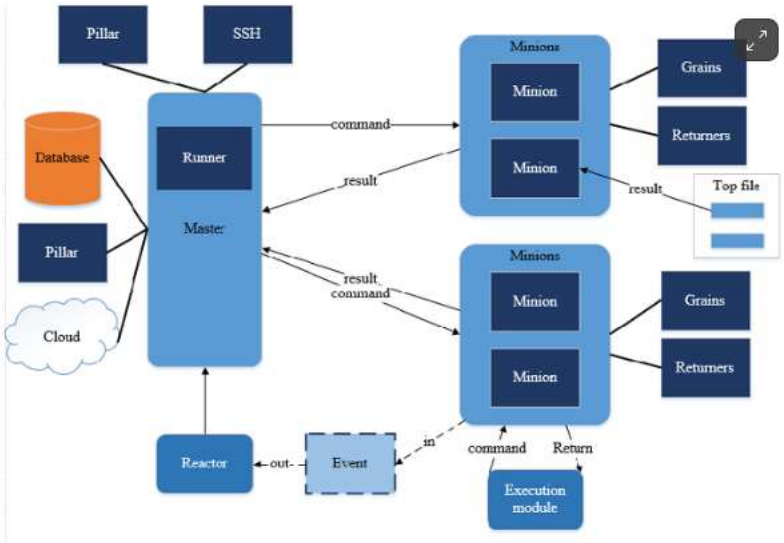
Which of the following is a recommended practice for running a Static Analysis Security Testing (SAST) tool in the CI/CD pipeline?

- ○ Implement low-confidence and high-confidence checks
- ✓ **Create custom rules to enforce specific guidelines**
- ○ Run active and passive scans
- ○ Perform full code scans after changes are committed

Which of the following security protections adds runtime overhead to a production application?

- ○ IAST
- ○ DAST
- ◉ **RASP**
- ○ WAF

Based on the infrastructure diagram shown below, what tool is used to manage the infrastructure?



- ◉ **Salt**
- ○ Chef
- ○ Puppet
- ◉ **Ansible**

You are incorrect

Salt is built on a fast, efficient, and scalable parallel remote command execution framework - instructions are executed over encrypted ZeroMQ connections between one or more masters and the remote systems to be managed (called "minions"). Salt, like Ansible, can be used to execute ad hoc commands across many different remote systems, gather information (called "grains") or apply configuration changes to the remote systems, spin up or shut down cloud instances, or proactively monitor the network.

Which serverless practice allows granular permissions to be defined that restrict access to the bare minimum needed to perform a task?

- Use a monorepo to store applications
- Minimize the functions with access to sensitive data
- Create policies that have broad access
- **Limit the scope of each function**

The command below is run for which purpose?

```
inspec exec ${local.inspecs}/dm
```

- Audit log analysis
- Dynamic code vulnerability scanning
- **Configuration management compliance**
- Unit testing during code commit

Which of the following should be reviewed to identify what cross-account access has been granted invoke permissions to an AWS Lambda function?

- **ClaimsPrincipal object**
- Execution policy
- CORS header
- **Resource policy**

You are incorrect

AWS Lambda Resource policies can be defined to grant cross-account access.

Execution policies are used to grant permissions to the function when invoked. CORS headers are used to request or respond to a request for access to resources from a different origin. ClaimsPrincipal objects are an Azure function feature.

What provisioner is an administrator using to invoke an executable on the machine running Terraform?

- ○ file
- ✓ **local-exec**
- ○ null_resource
- ✗ **remote-exec**

You are incorrect

Provisioners allow Terraform to execute specific commands, agents, or actions as part of resource creation or destruction. The *local-exec* provisioner invokes a local executable after a resource is created. This invokes a process on the machine running Terraform, not on the resource.

Use the *remote-exec* provisioner to run commands on the resource. It invokes a script on a remote resource after it is created that can be used to run a configuration management tool, bootstrap into a cluster, etc. The *file* provisioner is used to copy files or directories from the machine executing Terraform to the newly created resource. The *null_resource* is a resource that allows you to configure provisioners that are not directly associated with a single existing resource. null_resource is technically not a provisioner, but a resource that allows you to configure provisioners when the commands or actions the provisioners need to execute do not apply to a specific resource.

Which Continuous Deployment release technique initiates a change by pushing it onto a single server and monitoring?

- ✓ **Canary Releasing**
- ○ Dark Launching
- ○ A/B Testing
- ○ Blue/Green Deployment

Which of the following is a characteristic of an imperative DSL for configuration management/provisioning?

- ✗ **Is less flexible than a declarative DSL**
- ✓ **Explains the steps to set up the configuration**
- ○ Answers the question "What?"
- ○ Describes the desired end state

✗ **You are incorrect**

Domain-specific languages (DSLs) for configuration management/provisioning tools are basically either procedural or declarative. Imperative/Procedural describes the steps to set up the configuration that is desired. Much more flexible because one is free to program their own solution rather than being locked into how the tool works.

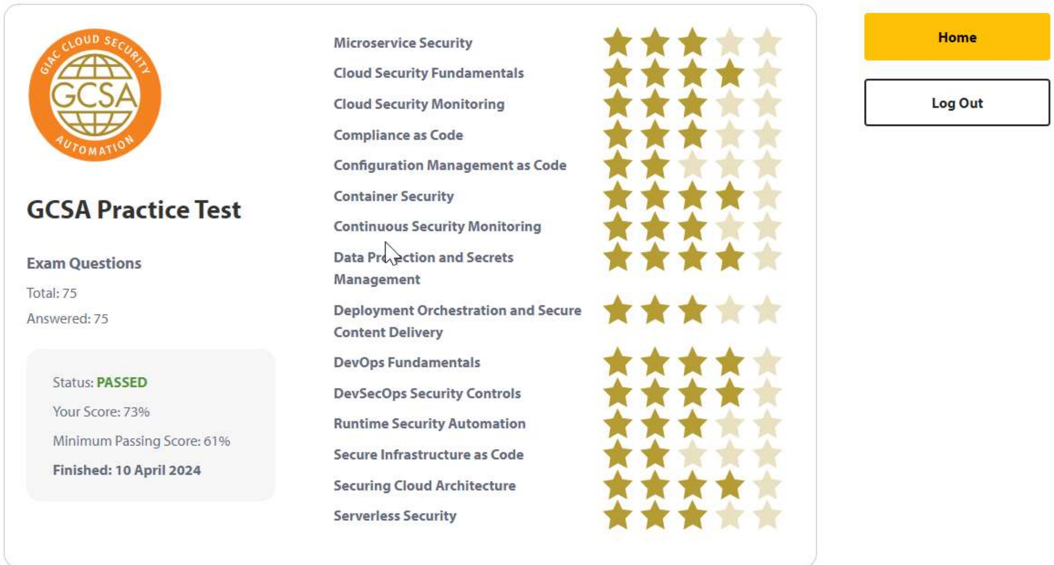
Declarative/Intentional describes the end state that is desired, not the steps to achieve it. What, not How.

Which is a defined action that AWS Security Hub Automated Response and Remediation (SHARR) playbooks provide?

- ○ Collecting security events from Guard Duty and AWS Config
- ✓ **Changing a Security Hub finding's status from NEW to RESOLVED**
- ○ Determining Security Group changes from CloudTrail logs
- ○ Detecting a CIS benchmark violation in a virtual machine

Which of the following enforces security policies during the version control step of the container lifecycle?

- ○ Production tags
- ○ Image signing
- ○ Dynamic analysis
- ✓ **Pre-commit hooks**



AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Which of the following is a characteristic of the Continuous Deployment pipeline?

- ○ Code is manually reviewed before being pulled to production
- ○ Acceptance tests are performed before integration tests
- ○ Unit testing is performed after the code is deployed
- ✓ **Code is deployed to production automatically at the end of the pipeline**

What security control can force access to S3 content to be allowed only via CloudFront?

- ○ HTTP Strict Transport Security
- ✓ **Origin Access Identity**
- ○ Signed cookies
- ○ URL signing

The following command detects tampering of which type of artifact?

```
$ cosign verify
```

- ◯ S3 bucket
- ◯ Terraform template
- ◉ **Container image**
- ◯ Source code

An analyst wants to review recent AWS console login attempts for suspicious activity. Which log source should the analyst investigate?

- ◯ VPC Flow
- ◯ Application Load Balancer
- ◯ Cloud Custodian
- ◉ **CloudTrail**

What provisioner is an administrator using to invoke an executable on the machine running Terraform?

- ◯ remote-exec
- ◉ **local-exec**
- ◯ null_resource
- ◯ file

Reconfiguring a Lambda function via the following command could enable which security benefit?

```
$ aws lambda update-function-configuration --function-name mylambdafunctiona --layers
```

- ○ Separation of executable code and input
- ○ Ability to assign multiple execution policies
- ◉ **Centralization of package management**
- ○ Ability to block new child processes

An engineer would like to send operating system log data from a Linux server to CloudWatch Logs using an AWS-provided tool. What would be used?

- ◉ **awslogs**
- ○ EC2Launch
- ○ EC2Config

The following template code would be applied to which CloudFormation resource type?

```
- CidrIp: 0.0.0.0/0
  IpProtocol: "TCP"
  FromPort: 443
  ToPort: 443
```

- ○ AWS::EC2::NetworkAclEntry
- ○ AWS::EC2::InternetGateway
- ○ AWS::EC2::EIP
- ◉ **AWS::EC2::SecurityGroup**

In which DevOps workflow step is continuous monitoring performed?

- [x] Operations
- [ ] Acceptance
- [ ] Commit
- [ ] Production

What can be inferred about the following Terraform code?

```
resource "azurerm_web_application_firewall_policy" "app_gateway" {
    name    = "WAFPolicy"

policy_settings {
    enabled                     = true
    mode                        = "Prevention"
    request_body_check             = true
    max_request_body_size_in_kb     = 128
}

managed_rules   {
    managed_rule_set    {
        type    = "OWASP"
        version = "3.1"
       }
    }
}
```

- [ ] Any traffic that matches a rule will be denied
- [x] **Rule severity is correlated to an anomaly score before traffic is blocked**
- [ ] Any single occurrence of traffic that triggers a severity of 'Warning' will be blocked

Which of the following is a characteristic of an imperative DSL for configuration management/provisioning?

- [x] **Is less flexible than a declarative DSL**
- [ ] Explains the steps to set up the configuration
- [ ] Answers the question "What?"
- [ ] Describes the desired end state

Which of the following is a characteristic of an imperative DSL for configuration management/provisioning?

- ✗ **Is less flexible than a declarative DSL**
- ✓ **Explains the steps to set up the configuration**
- ○ Answers the question "What?"
- ○ Describes the desired end state

✗ **You are incorrect**

Domain-specific languages (DSLs) for configuration management/provisioning tools are basically either procedural or declarative. Imperative/Procedural describes the steps to set up the configuration that is desired. Much more flexible because one is free to program their own solution rather than being locked into how the tool works.

Declarative/Intentional describes the end state that is desired, not the steps to achieve it. What, not How.

0

What is stored in Azure Monitor's time series database?

- ✓ **Metrics**
- ○ Logs
- ✗ **Thresholds**
- ○ Alerts

✗ **You are incorrect**

Azure Monitor stores numeric data (metrics) in a time series database.

What is a limitation of using Customer Managed Keys to directly encrypt data in AWS?

- ◯ Plaintext data must also be encrypted with a data key
- ◯ Must use the CMK identifier for both encryption and decryption
- ◯ Size of the plaintext data must be 4 kilobytes or less

Given the following configuration, what is included in the dataplane-log.conf?

```
apiVersion: v1

kind: ConfigMap

metadata:

              name: fluent-bit-config

               namespace: amazon-cloudwatch

               labels:

                 k8s-app: fluent-bit

data:

               @INCLUDE application-log.conf

               @INCLUDE dataplane-log.conf

               @INCLUDE host-log.conf
```

- ◯ /var/log/secure
- ◉ **/var/log/containers/aws-node***
- ◯ /var/log/messages
- ◯ /var/log/containers/*.log

ANS CHECK

What is a benefit of having build and test servers able to be built up only when needed and torn down when not in use?

- [x] **Ensures a known and reproducible environment**
- [x] **The server hardening requirements are reduced**
- [ ] Build and test servers can be maintained by connecting repositories to the Internet
- [ ] The servers will be available for production use during downtime

You are incorrect

Treat build and test servers as "Phoenix Server" instances: build them when you need them; tear them down when you are done. This ensures that the test environment is always in a known and traceable state - where it is easier to reproduce/debug problems.

Continuous Delivery and Continuous Deployment extend the attack surface of your production systems to include all of the tooling and source and artifact repositories that you use to build and deploy systems. These systems (and the infrastructure that they run on) should be hardened, managed, and monitored in the same way that you harden, manage, and monitor your production systems. Make sure that you do not expose your repos, CI server, or other tools to the internet as publicly available. Isolate development and test environments from production - make sure that it is not possible to accidentally reference a production system from dev/test.

The following command fails with HTTP 403 Forbidden:

```
curl --head -H "Content-Type: application/json" -H "Authorization:
${JWT_PAM}" "${API_GATEWAY_ENDPOINT}/api/employee/1"
```

Which line in the following decoded JWT indicates the reason for the 403 response?

```
1   jwt-decode $JWT_PAM
2
3   {
4   "iss": "https://sts.dm.paper",
5   "aud": "https://api.aws.dm.paper",
6   "sub": "3",
7   "username": "pbeesly@dm.paper",
8   "resources": [
9       {
10          "resource": "/api/customerservice/*",
11          "methods": [
12              "GET",
13              "PUT",
14              "POST",
15              "DELETE"
16          ]
17      }
18  ],
19  "iat": 1696446040,
20  "exp": 2706289240
21  }
```

- [x] Line 10
- [ ] Line 12
- [ ] Line 6
- [ ] Line 14

Continuous security monitoring of the system's activity occurs in which DevOps workflow phase?

- [ ] Acceptance
- [ ] Commit
- [ ] Production
- [ ] Pre-Commit
- [x] **Operations**

The command below is run for which purpose?

```
inspec exec ${local.inspecs}/dm
```

- Audit log analysis
- Dynamic code vulnerability scanning
- Unit testing during code commit
- **Configuration management compliance**

A scanner is crawling a web page gathering HTTP GET responses to observe the web application's behavior. Which type of Dynamic Application Security Testing (DAST) is taking place?

- Headless
- Active
- **Passive**
- Fuzzing

Which cloud security category of tools inspect microservices environments such as Kubernetes for security issues?

- **Cloud Workload Protection Platform**
- Cloud Access Security Broker
- Cloud Security Posture Management

What is a benefit of using serverless technologies?

- Code reviews are no longer needed
- Supply chain vulnerabilities are eliminated
- **Cost savings from reduced operational overhead**
- Input validation is not necessary

Which of the following is introduced by implementing IaC?

- **Disclosing secret keys**
- Forcing dynamic code analysis
- Reducing application availability

Which tool can an administrator use to configure an AWS instance to listen for the Windows Remote Management service from a specific source IP address?

- ○ Deployment Manager
- ○ Availability Zone
- ○ Resource Manager
- ✓ **Security Group**

What security weakness is introduced in a microservice architecture that implements the Command Query Responsibility Segregation pattern?

- ○ A single point of failure
- ✗ **Less granular access control**
- ○ Reduced system availability
- ✓ **Increased complexity**

✗ **You are incorrect**

The Command Query Responsibility Segregation (CQRS) pattern breaks down a microservice architecture into separate read, write, and delete APIs. The notion is that a different model is used to update information than the model used to read information. For some situations, this separation can be valuable, but organizations should be aware that for most systems CQRS adds risky complexity.

Which of the following Continuous Deployment techniques uses feature switches to allow developers to release incomplete features to production?

- ○ Canary Releasing
- ○ A/B Testing
- ✓ **Dark Launching**
- ○ Blue/Green Deployment

Which of the following should be reviewed to identify what cross-account access has been granted invoke permissions to an AWS Lambda function?

- [x] **Resource policy**
- [ ] ClaimsPrincipal object
- [ ] Execution policy
- [ ] CORS header

Analyze the following Dockerfile. Which line has a security issue?

```
1   FROM ubuntu:22.04
2
3   ARG ENVIRONMENT=prod
4   ENV PUBLICWEB_ENVIRONMENT=${ENVIRONMENT}
5
6   RUN apt-get update && apt-get install -y \
7       curl \
8       libcap-dev \
9       ruby1.9.1 \
10      apache2 \
11
12  EXPOSE 80/tcp
13
14  COPY cert.conf ./cert.conf
15  RUN openssl req -x509 -nodes -days 3650 -newkey rsa:4096 -keyout app.key
16      -out app.crt -config cert.conf -passin pass:${CERTIFICATE_PASSPHRASE}
17  RUN openssl pkcs12 -export -out app.pfx -inkey app.key -in app.crt
18      -passout pass:${CERTIFICATE_PASSPHRASE}
19
20      USER webguy
21      WORKDIR /www
```

- ○ 3
- ○ 20
- ○ 6
- ● **9**

Which of the following serves as the basis for the AWS Lambda power rating?

- CPU
- Bandwidth
- Memory
- Storage

Which of the following serves as the basis for the AWS Lambda power rating?

- CPU
- Bandwidth
- **Memory**
- Storage

You are incorrect

Resources are allocated for Lambda functions based on a scaled power model. This model allows development teams to select a power rating appropriate for their Lambda function's execution and let AWS manage the rest. Each function can be assigned a specific amount of computing power based on memory size from 128MB to 3GB, and AWS will automatically provide a comparable amount of CPU and network bandwidth to accommodate.

What git-related term is used to refer to the ".git" directory?

- ○ Branch
- ◉ **Repository**
- ○ Staging area
- ○ Working tree

Which of the following should be performed after code changes are deployed?

- ✓ **Smoke tests**
- ○ Static analysis tests
- ✗ **Acceptance tests**
- ○ Unit tests

✗ **You are incorrect**

After the changes are deployed, run a quick set of automated tests and checks. The Smoke Test should include some basic security assertions and tests.

Unit tests occur before or after code is created, acceptance tests occur before deployment, and static analysis testing is done prior to code check-in.

Which of the following events is highest priority for using a workflow hook to validate code correctness?

- ○ Remote repository: update
- ◉ **Remote repository: post-receive**
- ○ Local repository: commit

An organization needs MFA to be required for all IAM users and roles within their AWS organization. Which control can ensure that this is in place?

- ○ Security Hub
- ◉ **Service Control Policies**
- ○ CIS Benchmarks
- ○ Permission Boundary

What is the purpose of immutable image tagging within an AWS Elastic Container Registry?

- ○ Allows traffic to span availability zones
- ◉ **Prevents images from being overwritten**
- ○ Requires a dedicated AWS account to use images
- ○ Enables enhanced image scanning

Based on the Same Origin Policy, which of the following sites would be able to access the data at `http://www.mysite.com/description/tutorials/webdesign.html` if default port assignments are in use?

- ○ https://www.mysite.com:80
- ◉ **http://www.mysite.com/contact/**
- ○ https://www.mysite.com:443
- ○ http://www.yoursite.com/description/tutorials/

Which encryption type ensures data is encrypted before it is received by AWS?

- ○ Server-side
- ○ SHA-256
- ◉ **Client-side**
- ○ OpenSSH

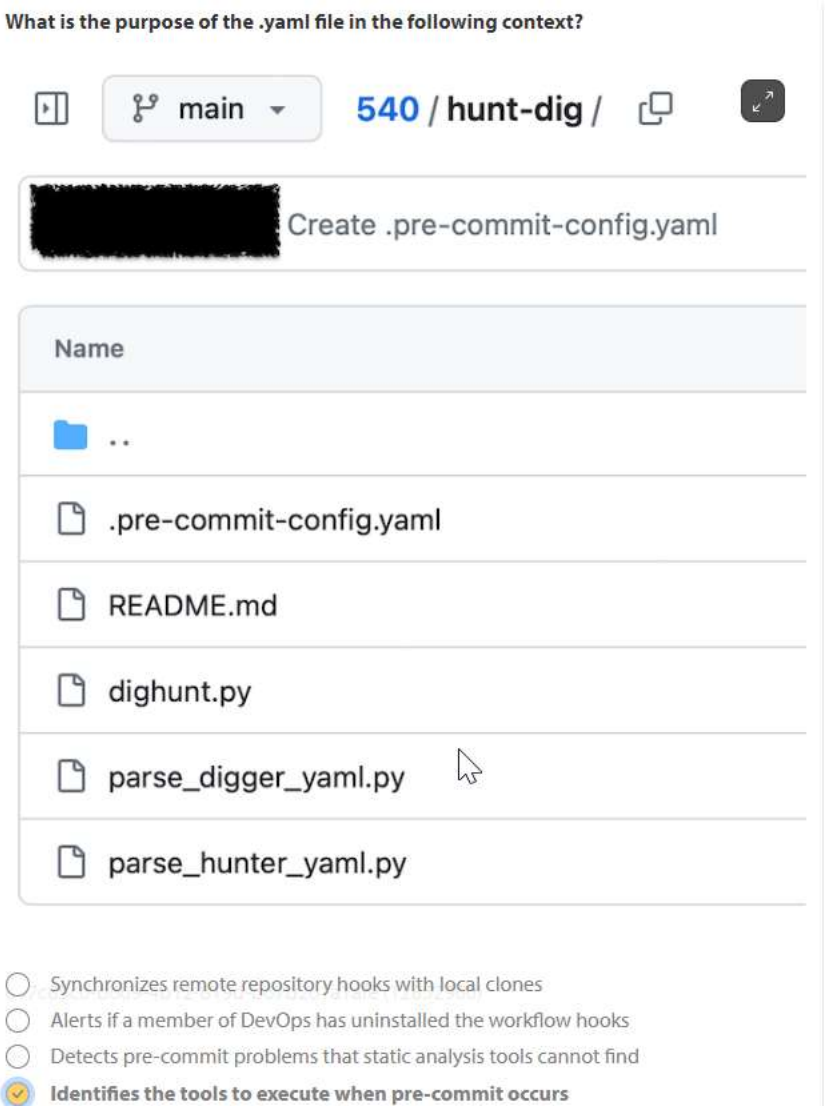
Which of the following is a CSPM solution that is compatible with Azure?

- ◉ **Defender for Cloud**
- ○ Security Hub
- ○ Ansible
- ○ SaltStack

A nonce should be added to which JWT parameter to prevent replay attacks when using microservices?

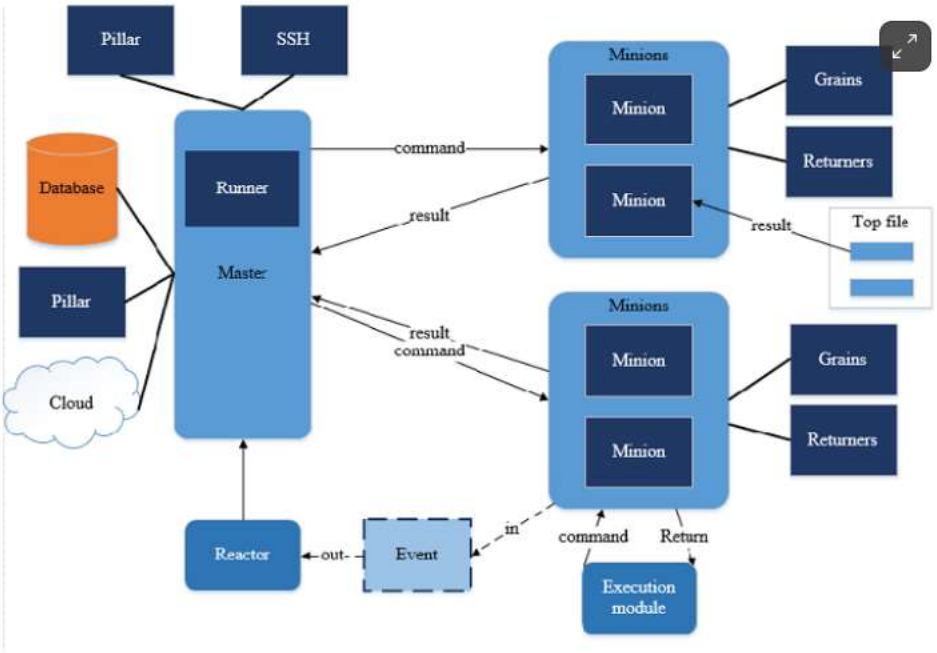
- [x] jti claim
- [ ] token field
- [ ] alg value
- [ ] web signature

What is the purpose of the .yaml file in the following context?



- [ ] Synchronizes remote repository hooks with local clones
- [ ] Alerts if a member of DevOps has uninstalled the workflow hooks
- [ ] Detects pre-commit problems that static analysis tools cannot find
- [x] **Identifies the tools to execute when pre-commit occurs**

Based on the infrastructure diagram shown below, what tool is used to manage the infrastructure?



- ○ Ansible
- ○ Puppet
- ● **Salt**
- ○ Chef

Which of the following can determine if a Docker Swarm of containers has applied the latest CIS Benchmark recommendations?

- ○ StackRox
- ● **Docker Actuary**
- ○ DockerScan

How does GitLab run each stage of CI/CD workflows?

- ○ Directly on the runner
- ○ Kubernetes engine nodes
- ○ Individual serverless functions
- ◉ **Inside of containers**

Which of the following is a characteristic of the declarative approach for defining configuration changes?

- ○ Changes are pushed out from a central update server
- ✓ **Changes are defined in terms of the desired end state**
- ✗ **Changes are defined using the steps to set up the configuration**
- ○ Agents periodically check the central server for new changes

✗ **You are incorrect**

When using configuration management tools, there are two primary approaches to defining configuration changes. Using the declarative approach, configuration changes are described using the desired end state, not the steps to achieve it.

Using the imperative approach, changes are defined using the steps to set up the desired configuration. There are also two primary approaches to applying configuration changes. Using the push approach, changes are pushed out from a central server. With a pull approach, agents periodically check into a central server for new changes.

The following AWS policy statement defines access for which type of resource?

```
Statement:
  - Action:
    - "ssm:GetParameters"
    Effect: "Allow"
```

- ○ A VPC security group
- ○ A CloudFront distribution
- ◉ **An EC2 instance**
- ○ An S3 bucket

What task is being executed with the command shown below?

```
$ aws lambda update-function-configuration --function-name
jwt-authorizer \
--layers arn:aws:lambda:us-east-1:123456789012:layer:node-8-
libraries:3 \
arn:aws:lambda:us-east-1:210987654321:layer:public-node-
layer:2
```

- ○ IAM roles are being assigned
- ◉ **Adding libraries in the function execution environment**
- ○ Policy being established to run function from one region
- ○ KMS authentication is being configured

Which Azure message-based service allows the use of reactive programming to perform security actions based on specified scenarios?

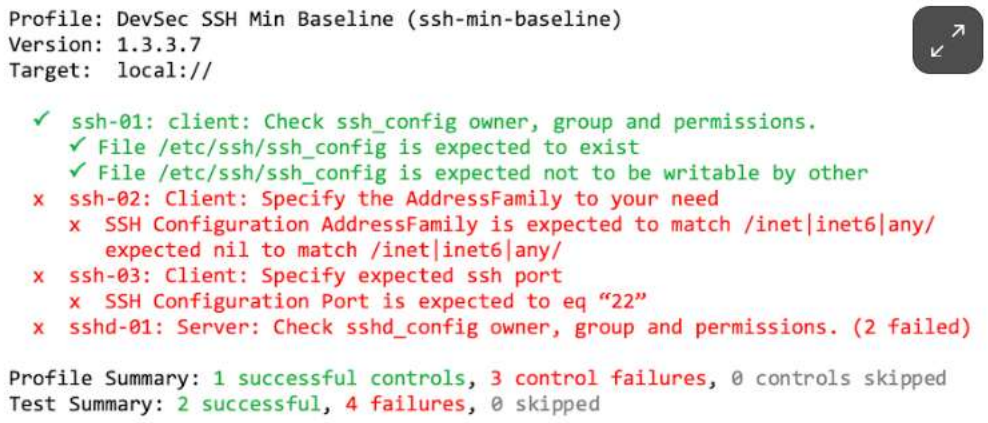
- [x] **Event Grid**
- [ ] Event Hubs
- [ ] Analytic Workspaces
- [ ] Service Bus

The following is a description of which OWASP Top 10 CI/CD Security Risk?

"An attacker obtains permissions to a CI/CD process and pushes malicious code or artifacts further down the pipeline."

- [ ] CICD-SEC-5: Insufficient Pipeline-Based Access Controls
- [ ] CICD-SEC-4: Poisoned Pipeline Execution
- [ ] CICD-SEC-3: Dependency Chain Abuse
- [x] **CICD-SEC-1: Insufficient Flow Control Mechanisms**

What tool generated the output in the image?



- ◯ Morgue
- ◯ puppet-lint-security
- ◯ puppet-lint
- ◉ **InSpec**

Which of the following should be done first when auditing an AWS environment?

- ◯ Use Trusted Advisor to check if MFA on the root account is enabled
- ◉ **Select a benchmark to identify the configuration baseline**
- ◯ Verify IAM users have been created with AWS Config
- ◯ Run CloudMapper scans against all regions in the environment

Which of the following is used to control ingress and egress traffic for an EC2 instance network?

- ○ Systems Integrity Management Platform
- ○ Runtime application security protection
- ◉ **Security groups**
- ○ Mandatory access control

Which practice can reduce the effectiveness of reconnaissance vulnerability scans against a web application?

- ✗ **Include IAST tools in CI/CD**
- ○ Activate Microsoft Security Risk Detection
- ○ Deploy CSRF tokens in hidden forms
- ✓ **Activate AWS WAF Security Automations**

✗ **You are incorrect**

AWS WAF Security Automations provides preconfigured protections for AWS WAF that block common SQL Injection and XSS attacks, stop scanners, HTTP floods, and bad bots, and prevent access from known bad IP addresses.

The other answers will not stop scanners. Microsoft Security Risk Detection provides a Virtual Machine to the customer so they can upload and install the binaries to be fuzz tested. CSRF tokens are useful to help prevent Cross Site Request Forgery attacks. IAST performs automated testing in CI/CD, so are not effective against scans of production resources.

What does AWS's Key Management Service use to perform extra integrity checks when decrypting data?

- ○ HSA Backing Key
- ○ Data Key
- ○ Customer Master Key
- ✓ **Encryption context**

What can Azure storage managers generate to delegate access to storage objects on a granular basis?

- ○ TLS Certificates
- ○ Storage Account Keys
- ✓ **Shared Access Signatures**
- ○ Kerberos Tickets

Which of the following parameters determines which type of data is used in Azure Monitor?

- ○ resource_group_name
- ✗ **sku**
- ○ location
- ○ workspace_name
- ✓ **product**

✗ **You are incorrect**

The product parameter defines the type of data will be used in the Azure Monitor solution. Values include: SecurityCenterFree, Security, Updates, ServiceMap, AzureActivity, ChangeTracking,

VMInsights, SecurityInsights, NetworkMonitoring, SQLVulnerabilityAssessment, SQLAdvancedThreatProtection, AntiMalware, AzureAutomation, LogicAppsManagement, SQLDataClassification.

Which claim field represents when a JWT was created?

- ○ aud
- ✗ **jti**
- ○ iss
- ✓ **iat**

> ✗ **You are incorrect**
>
> It is a JWT Security best practice to set expiration of the token by setting the `iat` (Creation) and `exp` (Expiration) fields. The `aud` field represents the scope of for the appropriate "audience", such as your system. The `jti` claim is a token replay mitigation because it adds a nonce to the ID. The `iss` field is the claim issuer field.

What type of Terraform variable contains multiple key value pairs?

- ✓ **map**
- ○ string
- ○ list
- ○ tuple

Which of the following is focused on supply chain security and uses fulcio for code signing certificates?

- ✓ **Sigstore**
- ○ SLSA Provenance
- ○ CycloneDX
- ○ Docker Content Trust

What information is found in line 3 of the following JSON Web Token?

```
1 eyJhbGciOiJSUzI1NiJ9.
2 eyJ1aWQiOiI1NDIxMDU0ODQiLCJjbGFpbSI6IkdldEFjY291bnQifQ.
3 Kho7o2Rz9p42HKi84KfWBxAxJAwwKIAdy4msKSy0ZY
```

- ◯ Algorithm
- ◉ **Signature**
- ◯ Claims
- ◯ Payload

In Azure Key Vault, what is used for authorization when retrieving a key?

- ◯ Security Token Service
- ◯ OpenID Connect
- ◉ **Key Vault access policy**
- ◯ Azure Active Directory

What does Azure Container Registry (ACR) recommend for container registry isolation?

- ◉ **A resource group**
- ◯ A DevOps account
- ◯ An immutability tag
- ◯ An AD service principal

A website streams video-on-demand using CloudFront and controls access to videos using signed URLs with canned policies. All videos can be streamed for 24 hours after they are ordered and paid for.

A user of the service paid for a wonderful mystery video that is 2 hours and 30 minutes long at noon on Monday. They forgot that they ordered it until 11 am on Tuesday, at which time they immediately began playing it. When the video had just 15 minutes left to play - just as the murderer was about to be named! - the video suddenly stopped. When they tried to restart it, it would not play. What would cause this tragedy?

- ◯ A signed cookie was used when attempting to restart the video
- ◉ **A TCP reset occurred during download**
- ◯ The user's IP address access has been blacklisted

Which of the following is a recommended practice for running a Static Analysis Security Testing (SAST) tool in the CI/CD pipeline?

- ◉ **Create custom rules to enforce specific guidelines**
- ◯ Perform full code scans after changes are committed
- ◯ Run active and passive scans
- ◯ Implement low-confidence and high-confidence checks

User A opens a browser on a shared computer to access an online banking site and closes the browser when finished. Later, using the same computer, User B authenticates to a social media site, closing the browser when finished. Which of the following will prevent an attacker with physical access to the computer from obtaining cookie values from other users of this computer?

- ○ Same Origin Policy prevents access to other users' data
- ◉ **Session cookies without an expiration date or Max-Age set**
- ○ Using an HTTP/HTTPS proxy for web browsing
- ○ Cookies with the Secure flag set

The syntax below is taken from which of the following?

```
stages {
  stage('Build') {
    agent {
      dockerfile {
        filename 'Dockerfile'
        dir 'builder_base'
        additionalBuildArgs '--tag dmtools/builder_base:stable'
      }
    }
    steps {
      sh "python --version"
    }
  }
}
```

- ○ Terraform provisioner script
- ○ Docker JSON configuration
- ✓ **Jenkins declarative pipeline**
- ○ AWS CloudFormation template

IAST tools are used for which of the following purposes?

- ○ Fuzzing code input fields to identify common injection flaws
- ○ Analyzing source code as it is being developed before code commit
- ○ Sending malformed requests to an application running in production
- ✓ **Passively analyzing running code during acceptance testing**

Which of the following would a WAF use to detect CSRF threats?

- ◯ Session ID
- ◯ Server certificate
- ◯ Parameterized query
- ◉ **Token presence**

When combined with Change Failure Rate, which of the following metrics measures the reliability/quality of service and availability?

- ◯ Mean Time to Acknowledge
- ◯ Mean Time to Failure
- ◉ **Mean Time to Recover**
- ◯ Mean Time to Detect

What must be discovered during a rapid risk assessment?

- ◯ Vulnerable code
- ◯ Unpatched software
- ◉ **Key technology stacks in use**
- ◯ Dynamic security test results

Which command-line interface (CLI) supports the use of `init` and `destroy` for interacting with resources?

- ◉ **Terraform**
- ◯ Docker
- ◯ Kubernetes
- ◯ CloudFormation

What is a limitation of using Customer Managed Keys to directly encrypt data in AWS?

- ○ Plaintext data must also be encrypted with a data key
- ✗ **Must use the CMK identifier for both encryption and decryption**
- ✓ **Size of the plaintext data must be 4 kilobytes or less**

✗ **You are incorrect**

The KMS permits the use of Customer Managed Keys (CMK) to directly encrypt and decrypt relatively small blocks of data. Currently these blocks of data are limited to 4 kilobytes or less. The idea is to use direct encryption for small secrets such as API keys and passphrases.

When using CMKs to directly encrypt data, data keys are not necessary. When a CMK is used to directly encrypt data, the CMK's key material is used for the encryption. With envelope encryption, a unique key is created, and its key material is used for the encryption, which is, in turn, encrypted with the CMK. Because envelope encryption is used, the CMK identifier must be specified for encryption, but is not required for decryption.

Given the following configuration, what is included in the dataplane-log.conf?

```
apiVersion: v1

kind: ConfigMap

metadata:

              name: fluent-bit-config

               namespace: amazon-cloudwatch

               labels:

                 k8s-app: fluent-bit

data:

               @INCLUDE application-log.conf

               @INCLUDE dataplane-log.conf

               @INCLUDE host-log.conf
```

- ○ /var/log/secure
- ✓ **/var/log/containers/aws-node***
- ✗ **/var/log/messages**
- ○ /var/log/containers/*.log

You are incorrect

The dataplane configuration includes logs from the container service, containerd, and the kubelet stored in the /var/log/containers/aws-node*, /var/log/containers/kube-proxy* directories.

What source sends aggregate packet statistics, network addresses, ports, and actions (accept/reject) to CloudWatch every 10-15 minutes?

- ○ ALB Access logs
- ○ CloudTrail
- ○ GuardDuty
- ✓ **VPC flow logs**

Which Terraform HCL code sample can be used to get information about an Azure container that is not defined or managed by the current configuration?

◯ output "ABC_Corp_Host" { value = "${azurerm_kubernetes_cluster.ABC_Corp.kube_config.0.host}" }

✓ **data "azurerm_container_registry" "ABC_Corp" { name = var.container_registry_name resource_group_name = var.resource_group_name}**

✗ **resource "null_resource" "ABC_Corp_Build" { provisioner "local-exec" { command = "az acr build --resource-group ${var.resource_group_name} --registry ${var.container_registry_name} --image abc_corp_app_srv:v1 ." } }**

◯ resource "azurerm_resource_group" "ABC_Corp" { name = var.resource_group_name location = var.location }

${var.resource_group_name} --registry
${var.container_registry_name} --image abc_corp_app_srv:v1 ." } }

◯ resource "azurerm_resource_group" "ABC_Corp" { name = var.resource_group_name location = var.location }

You are incorrect

In the HashiCorp Configuration Language (HCL), data sources are used to get information about resources that are not defined or managed by the current configuration. The code block beginning with `data` correctly returns information about an undefined or unmanaged resource.

The `resource` code block referencing `azurerm_resource_group` is used to define an Azure Resource Manager (ARM) resource. The code block beginning with `output` is used to return information from configuration run for a defined or managed resource. The `resource` code block that references the `null_resource` is used to define a provisioner that is not associated with a specific resource.

What can be used to enable and track concurrent changes to source code?

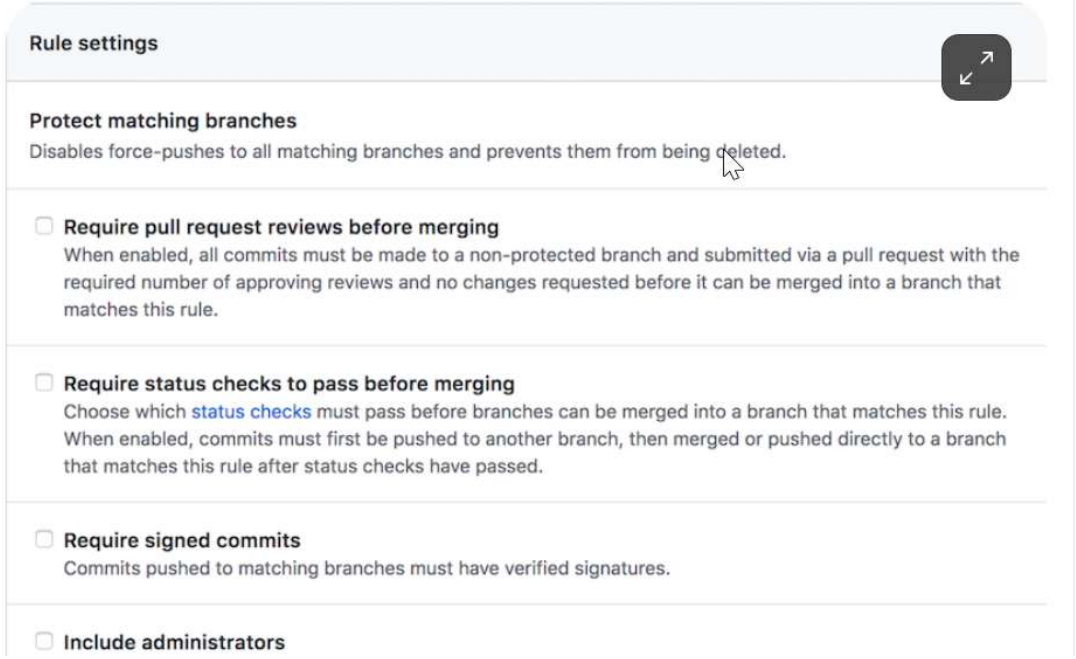
- ✗ **Revision Control System**
- ○ Source Code Control System
- ✓ **Git**
- ○ .bak files

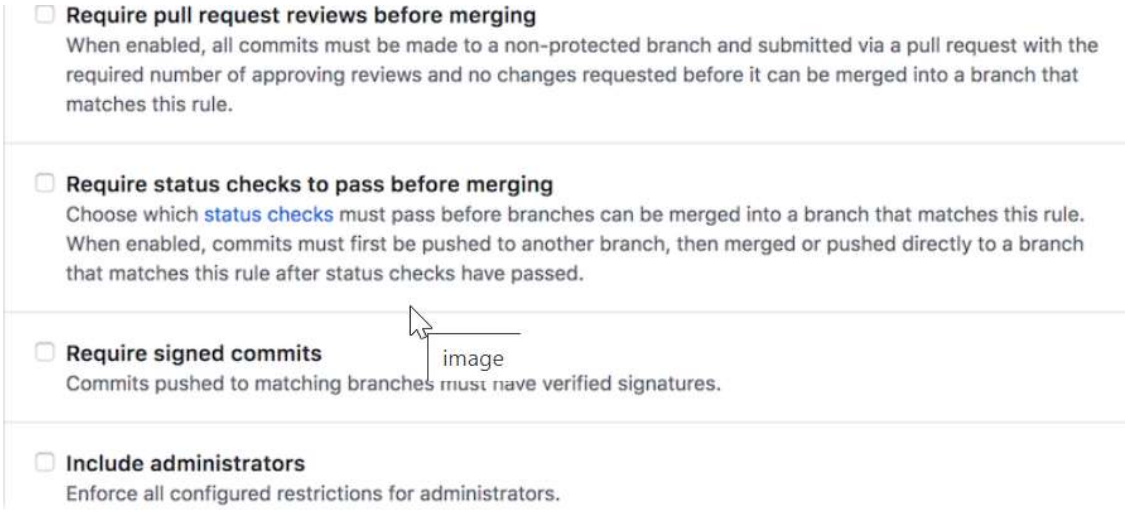
✗ **You are incorrect**

Git is a Distributed Version Control System, which enables multiple users to perform changes to the same file and provides the means to resolve conflicting changes.

Source Code Control System and Revision Control System were early version control systems. Both focused on tracking versions of an individual file and allowed just one user to edit a file at a time. .bak files are an archaic mechanism to keep track of a previous code version.

Which service's branch protection policy is shown in the screenshot?





image

Show description