AWS SysOps Administrator – Associate Level

Security

```
#include <iostream>
#include <cstdlib>
using namespace std;
int main()
{
  cout << "Hello, world!" << endl;
  return 0;
}
```

Learning Objectives

By the end of this lesson, you will be able to:

- Configure DDoS attack blocks, STS, and hypervisors
- Work with **AWS Config**
- Run scripts using **Systems Manager Run Command**
- Work with CloudTrail

Security on AWS

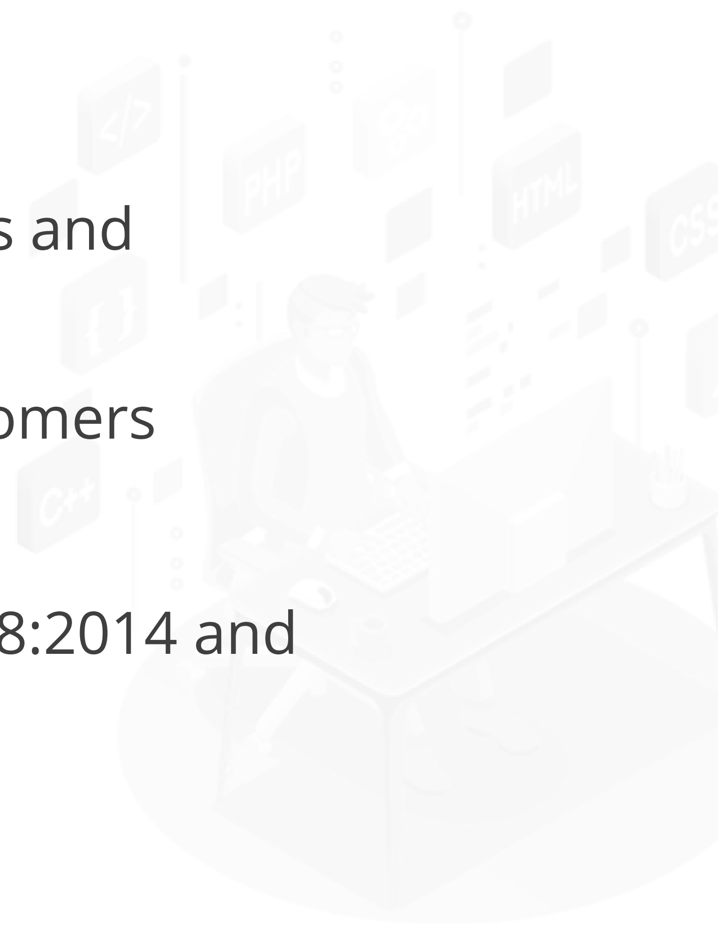
Compliance Frameworks

The AWS Compliance Program provides detailed information about AWS security and compliance in the cloud.

The three major compliance frameworks are given below:

ISO 27001

ISO/IEC 27001:2013 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO/IEC 27002 best practice guidelines.



- AWS performs the following operations:
  1. Evaluates the information security risks, taking into account the impact of threats and vulnerabilities
  2. Designs the suite of information security controls and risk management for customers

- AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, and 27018:2014 and is managed by third-party auditors.
- It doesn't have any impact on the services used by the end user.

Source: https://aws.amazon.com/compliance/iso-27001-faqs/

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a US government program for security assessment, authorization, and continuous monitoring of cloud products and services.

- FedRAMP is important because it provides:

1. Consistency and confidence in the security of cloud solutions
2. Transparency between the US government and cloud providers
3. Real-time continuous monitoring
4. Automation and reuse of assessments and authorizations

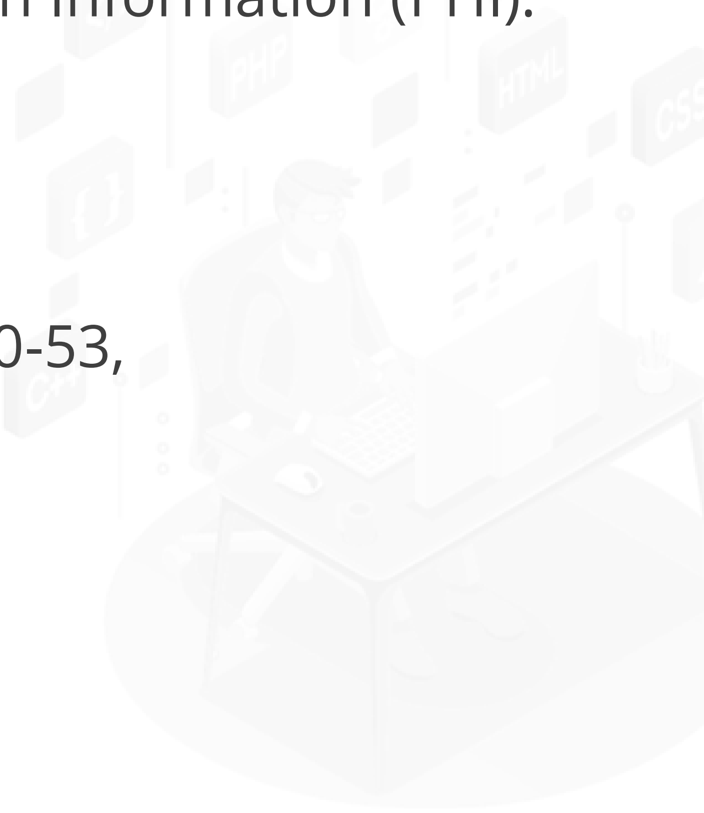
- AWS FedRAMP compliance doesn’t result in increase in service cost.

Source: https://aws.amazon.com/compliance/fedramp/

HIPAA and HITECH

Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a legislation that is designed to make it easy for US workers to retain health insurance coverage when they change or lose their jobs.

Health Information Technology for Economic and Clinical Health (HITECH) act is an expansion of HIPAA which includes a set of federal standards to protect the security and privacy of the Protected Health Information (PHI).

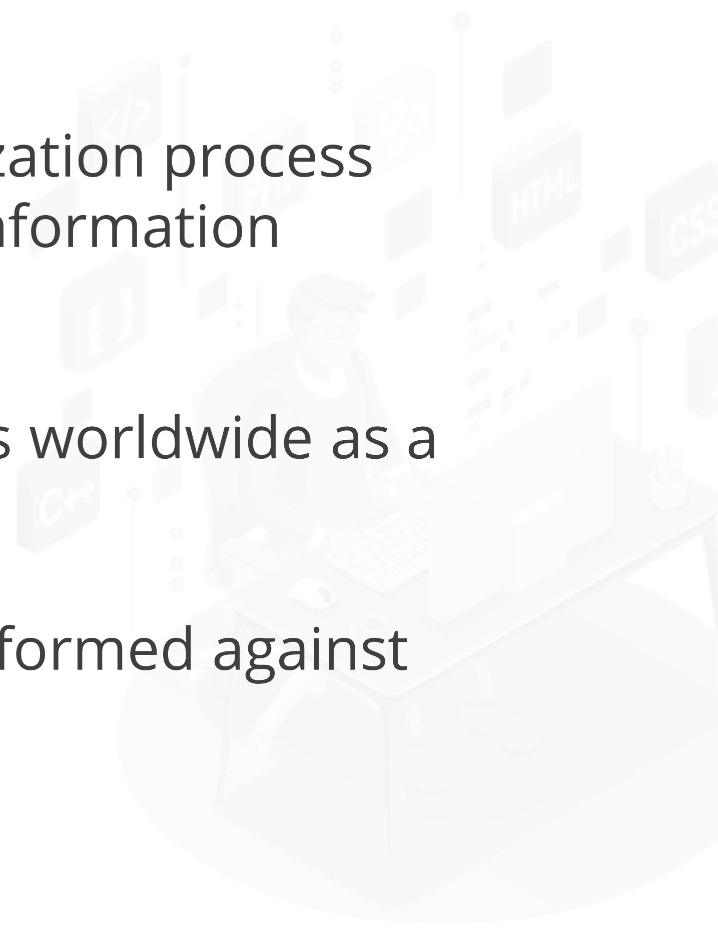


- AWS aligns the HIPAA risk management program with FedRAMP and NIST 800-53, which are higher security standards that map to the HIPAA Security Rule.
- HIPAA or HITECH doesn’t restrict end users from using any AWS services.

Source: https://aws.amazon.com/compliance/hipaa-compliance/

NIST

The National Institute of Standards and Technology (NIST) 800-53 security controls are generally applicable to the US Federal Information System.

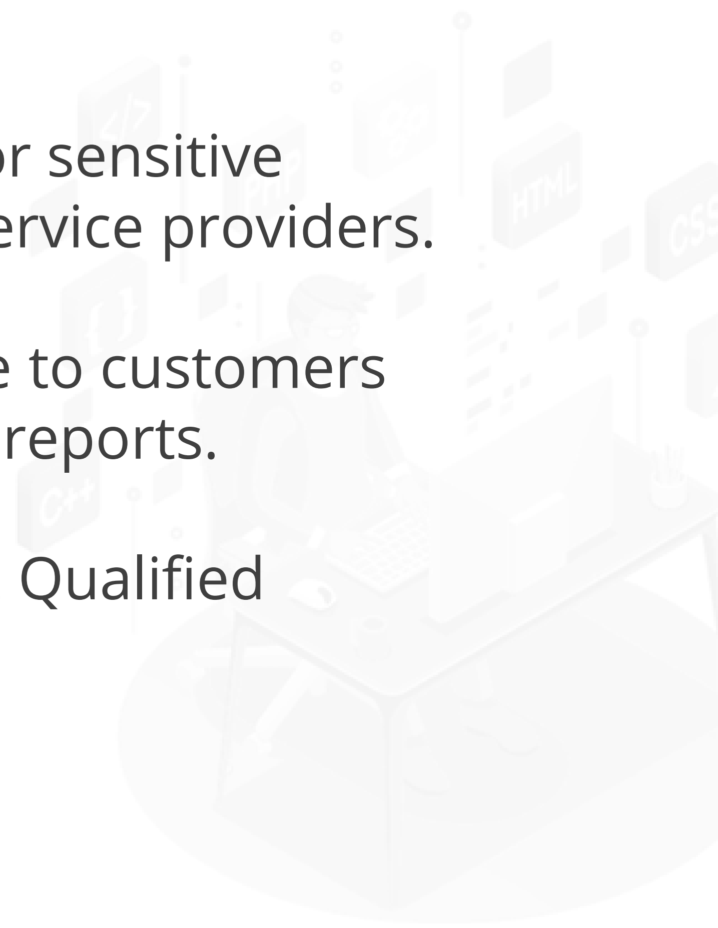


- The Federal Information System typically follows the formal assessment and authorization process to ensure protection of confidentiality, integrity, and availability of information and information system.
- The NIST Cybersecurity Framework (CSF) is supported by governments and industries worldwide as a recommended baseline for use by any organization.
- AWS Cloud infrastructure and services have been validated by third-party testing performed against the NIST 800-53 Revision 4 controls.

Source: https://aws.amazon.com/compliance/nist/

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council.



- PCI DSS applies to all entities that store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD), including merchants, processors, acquirers, issuers, and service providers.
- The PCI DSS Attestation of Compliance (AOC) and Responsibility Summary is available to customers by using AWS Artifact, a self-service portal for on-demand access to AWS compliance reports.
- The compliance assessment was conducted by Coalfire Systems Inc., an independent Qualified Security Assessor (QSA).

Source: https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

DDoS

What Is DDoS?

A distributed denial-of-service (DDoS) attack is a malicious act to disturb the normal traffic of a server, a service, or a network.

- Attackers generate large volumes of packets or requests which overload the target system.
- It can also be done by multiple mechanisms, such as a combination of reflection and amplification techniques and also by using large botnets.
- In DDoS, attackers use multiple sources to generate attacks.
- DDoS attack makes an application or a website unavailable to the end user.

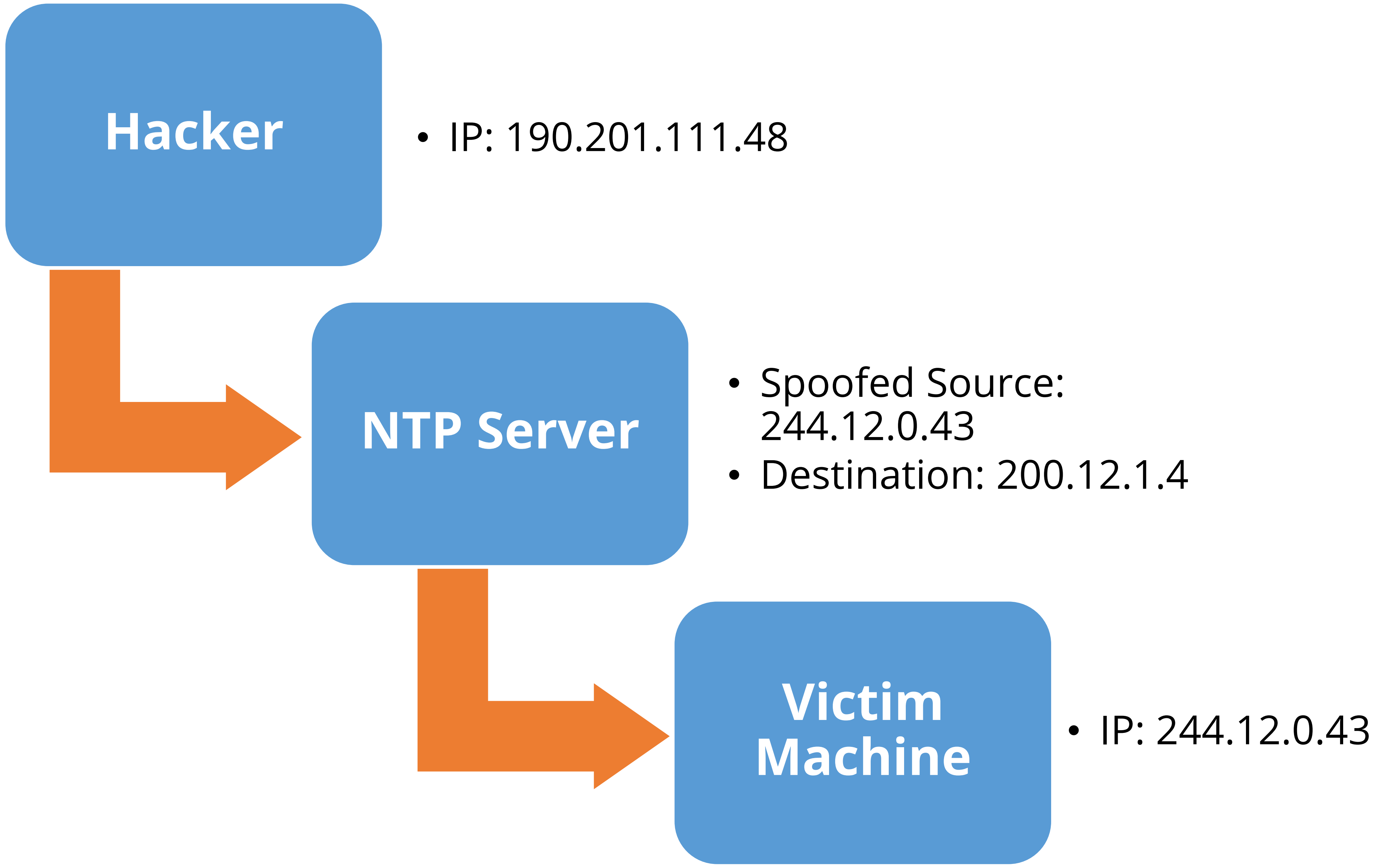
Types of DDoS Attacks

Amplification or Reflection

- It includes NTP, SSDP, DNS, Chargen, and SNMP attacks.
- In this attack, the attacker sends a request to a third-party server, such as NTP, using a spoofed IP address.
- Here, the server responds to this request with a larger payload than the initial request.
- Example: If the attacker sends a request of 64 bytes, the server responds with up to 3500 bytes of traffic.
- Attackers can use multiple third-party servers and make the server busy with huge payload.
- These attacks are also called infrastructure layer attacks.

Types of DDoS Attacks

Representation of amplification or reflection is given below:



Hacker

- IP: 190.201.111.48

NTP Server

- Spoofed Source: 244.12.0.43
- Destination: 200.12.1.4

Victim Machine

- IP: 244.12.0.43

Types of DDoS Attacks

Application Attacks (L6 and L7)

- These attacks occur on the layers 6 and 7 of the OSI model.
- They tend to focus on particularly expensive parts of an application thereby making it unavailable for real users.
- Example: A flood of HTTP requests to a login page or an expensive search API are the the most common ways to attack layers 6 and 7.
- These attacks are also called application layer attacks.

Mitigating DDoS

The ways to mitigate DDoS attacks are as follows:

1. Reduce the attack surface area using ALBs with web application files.
1. Scale the system to handle the attack using auto scaling groups.
1. Safeguard exposed resources.
1. Learn the behavior of an application to analyze if it acts abnormally.
1. Create a plan for attacks.

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.

- AWS Shield provides detection and automatic mitigation mechanism to reduce application downtime.
- There are two levels of AWS Shield subscriptions: Standard and Advanced protection.
- Standard subscription is free and can be used for applications hosted on services, like **CloudFront,** for protection against the most common DDoS attacks.

Source: https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

AWS Shield

- For applications hosted over services, such as EC2 and ELBS, the advanced-level subscription is helpful.
- AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks.

Source: https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

Benefits of AWS Shield

- Seamless integration and deployment: By default, the Standard protection is automatically enabled for the resources, and the Advanced one can be enabled in the service configurations. No routing changes are required.

- Customizable protection: Users can write customized rules with AWS WAF and deploy them immediately.

Source: https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

Benefits of AWS Shield

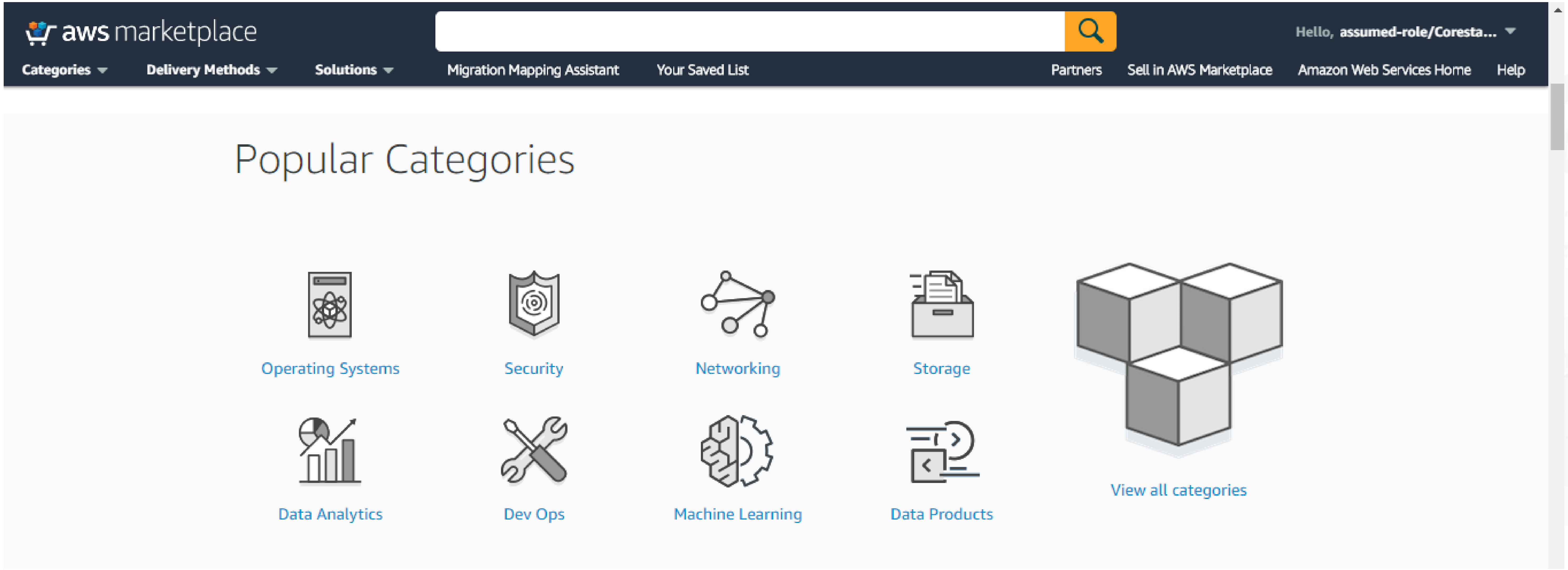
- Managed protection and attack visibility: AWS Shield is an always-on monitoring and protection mechanism and enables access to DRT for manual mitigation of risks. It provides a dashboard to keep an eye on the activities that are occurring to mitigate attacks.

- Cost-efficient: AWS Shield Standard is automatically enabled and is free of cost. AWS Shield Advanced provides AWS WAF and AWS firewall manager free of cost.

Source: https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

AWS Marketplace

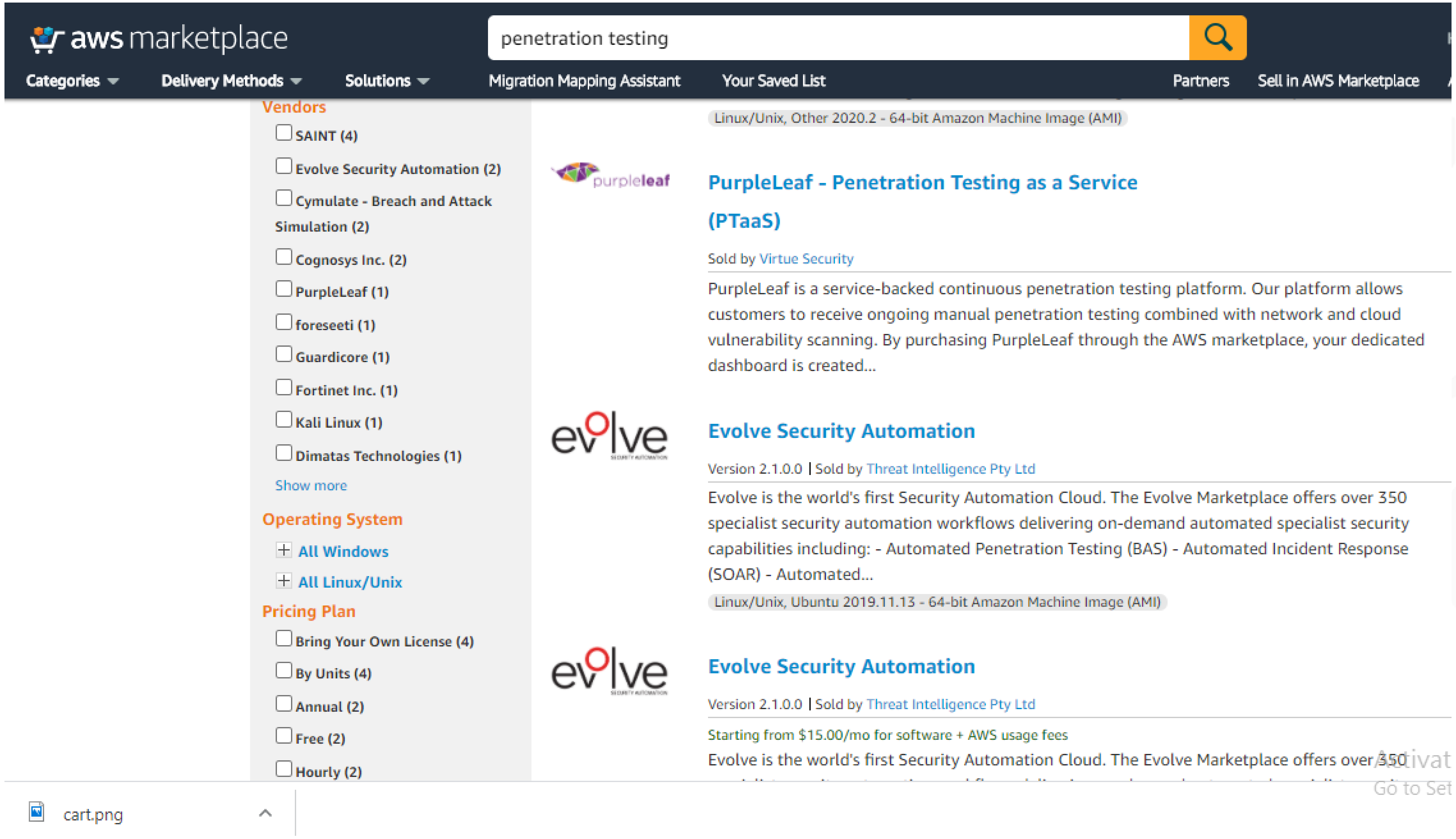
AWS marketplace is an online portal for purchasing products or services for your applications or projects.



Source: https://aws.amazon.com/shield/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

AWS Marketplace Security Products

AWS marketplace contains products for security purposes with all types of testing and protection tools. Examples of penetration testing tools are given below:



Vendors

□ SAINT (4)

□ Evolve Security Automation (2)

□ Cymulate - Breach and Attack Simulation (2)

□ Cognosys Inc. (2)

□ PurpleLeaf (1)

□ foreseeti (1)

□ Guardicore (1)

□ Fortinet Inc. (1)

□ Kali Linux (1)

□ Dimatas Technologies (1)

Show more

Operating System

+ All Windows

+ All Linux/Unix

Pricing Plan

□ Bring Your Own License (4)

□ By Units (4)

□ Annual (2)

□ Free (2)

□ Hourly (2)

Linux/Unix, Other 2020.2 - 64-bit Amazon Machine Image (AMI)

PurpleLeaf - Penetration Testing as a Service (PTaaS)

Sold by Virtue Security

PurpleLeaf is a service-backed continuous penetration testing platform. Our platform allows customers to receive ongoing manual penetration testing combined with network and cloud vulnerability scanning. By purchasing PurpleLeaf through the AWS marketplace, your dedicated dashboard is created...

Evolve Security Automation

Version 2.1.0.0 | Sold by Threat Intelligence Pty Ltd

Evolve is the world's first Security Automation Cloud. The Evolve Marketplace offers over 350 specialist security automation workflows delivering on-demand automated specialist security capabilities including: - Automated Penetration Testing (BAS) - Automated Incident Response (SOAR) - Automated...

Linux/Unix, Ubuntu 2019.11.13 - 64-bit Amazon Machine Image (AMI)

Evolve Security Automation

Version 2.1.0.0 | Sold by Threat Intelligence Pty Ltd

Starting from $15.00/mo for software + AWS usage fees

Evolve is the world's first Security Automation Cloud. The Evolve Marketplace offers over 350

Custom IAM Policy

Duration: 10 Min.

Problem Statement:

Create and configure a custom IAM policy.

Assisted Practice: Guidelines

Steps to create and configure a custom IAM policy:

1. Login to AWS lab

1. Select **IAM** from **Services**

1. Select a policy from the menu on the left

1. Create a custom IAM policy

Roles and Instances

Duration: 10 Min.

Problem Statement:

Create roles and custom policies, and integrate them with an S3 bucket.

Assisted Practice: Guidelines

Steps to create and integrate roles and policies with S3 bucket:

1. Create an S3 bucket

1. Create an IAM role

1. Connect the S3 bucket with the IAM role

1. Upload files to the S3 bucket

TECHNOLOGY

Security Token Service

Security Token Service

AWS Security Token Service (STS) is a web service that allows users to have limited and temporary access to AWS resources.

Federation (active directory)

- Uses SAML
- Grants temporary-access-based active directory credentials
- Allows single sign-on without providing IAM credentials

Federation with mobile apps

- Uses OpenID providers, such as Facebook, Google, and Amazon to log in

Cross-account access

- Allows access to resources from one user account to another

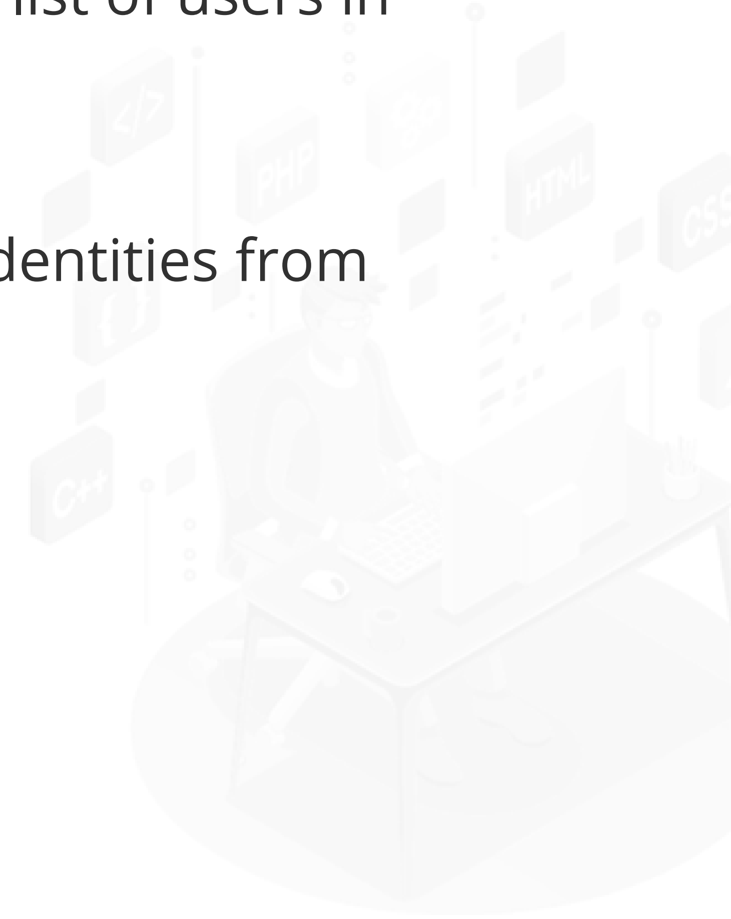
Security Token Service: Key Terms

Federation: Combining a list of users in a single domain, such as IAM, with a list of users in another domain, such as an active directory

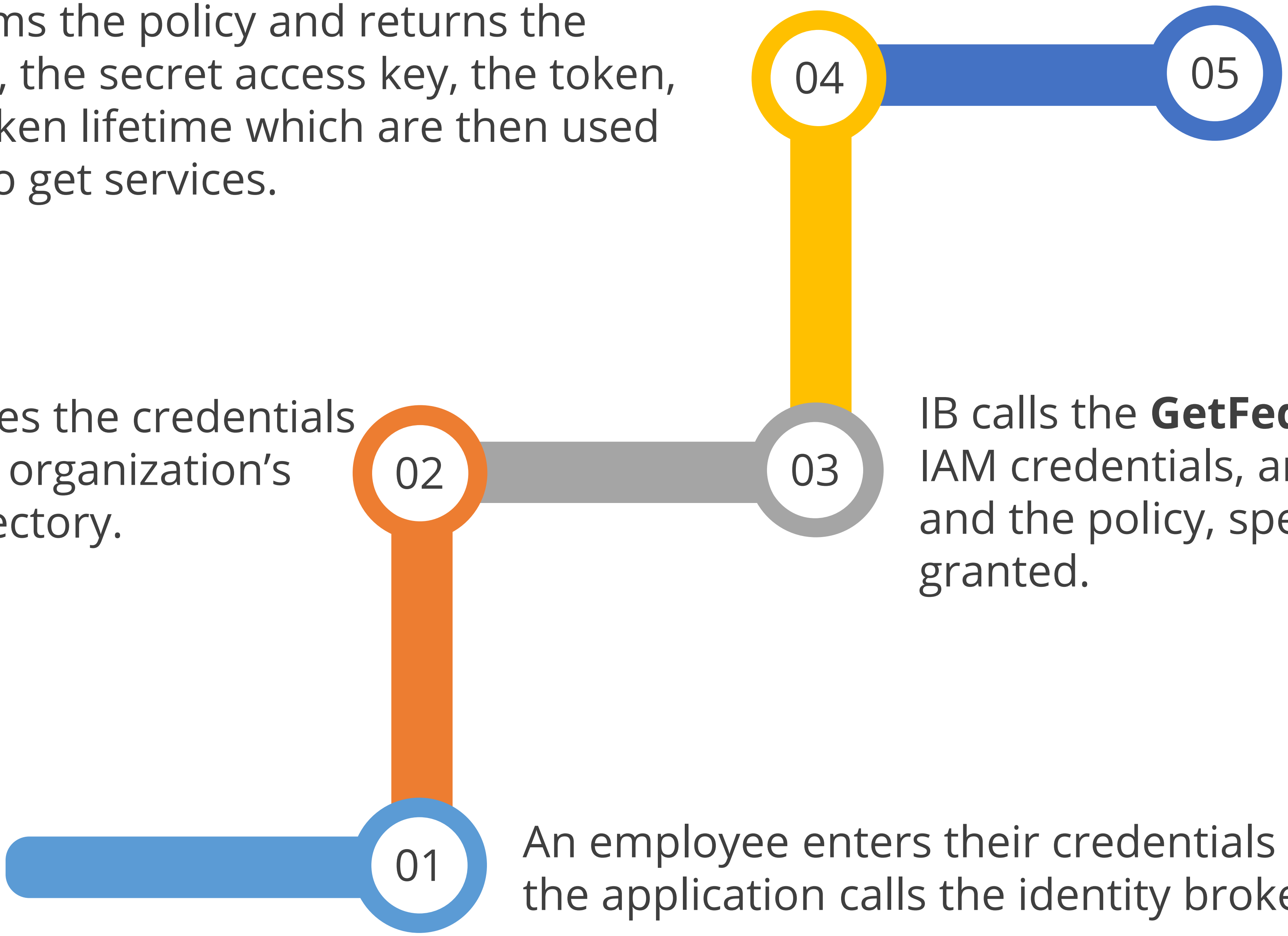
Identity broker: A service that allows a user to take and identify user identities from point A and combine or federate them with point B

Identity store: Services like active directory, Google, and Facebook

Identities: A single user



STS Flow: Example



01 An employee enters their credentials and the application calls the identity broker.

02 IB validates the credentials using the organization’s LDAP directory.

03 IB calls the **GetFederationToken** function with IAM credentials, and it includes the duration and the policy, specifying the permissions to be granted.

04 STS confirms the policy and returns the access key, the secret access key, the token, and the token lifetime which are then used by the IB to get services.

05 The application requests for services, such as S3, and S3 validates IAM credentials for enabling the requested service for the user.

Logging

Logging in AWS

Here are the four major services where logging is essential:

AWS CloudTrail
It records all the API calls.

VPC Flow Logs
It records the network traffic behavior.

AWS Config
It records the status of the environment.

AWS CloudWatch
It records the performance metrics.

Control Access to Log Files

There are two major ways to control access to log files:

Prevent unauthorized access

- Using IAM roles
- Using groups and policies
- Using only the S3 bucket policy
- Multi-factor authentication

Ensure role-based access

- Using IAM roles
- Using groups and policies
- Using isolated S3 bucket policies

Alerts and Changes

Ways to set alerts and manage changes to log files are given below:

Setting Alerts:

During Log File Creation

- Using CloudTrail notifications
- Using AWS Config rules

Note: CloudTrail notifications only point to the log file location.

Managing Changes:

Changes to System Components

- Using AWS Config rules and CloudTrail
- Using IAM and S3 controls and policies to prevent modifications
- Using CloudTrail log file validation and encryption

TECHNOLOGY

WAF and Hypervisors

What Is AWS WAF?

AWS WAF is a web application firewall that lets you monitor HTTP and HTTPS requests that are forwarded to CloudFront, an ALB, or an API gateway.

- Users can configure restrictions and put conditions for the approval of access.
- Control access can be achieved using conditions, such as what IP addresses are allowed to make requests or what parameters are required in the query string.
- Using the above information, ALB or CloudFront decides whether to give permission to receive data or to send 403 error code.

AWS WAF Operations

AWS WAF allows three basic operations:

1. Allows all requests except the excluded ones

1. Rejects all requests except the approved ones

1. Allows requests that match the specified conditions

AWS WAF Conditions

Conditions that a user can specify using characteristics of web requests:

1. IP address for the origin of a request
1. Country for the origin of a request
1. Header values
1. Mandatory strings to be present in the query
1. Length of the requests
1. Presence of SQL code in the query
1. Presence of scripts, such as cross-site scripting, in the query string

WAF Integration

Services with which WAF integrates and doesn’t integrate:

- WAF integrates with:

1. Application load balancer

1. CloudFront

1. API Gateway

- WAF doesn’t integrate with:

1. Classic load balancer

1. Network load balancer

Note: WAF is a layer 7 service, and it needs application visibility. As a result, it doesn’t integrate with classic and network load balancers.

AWS Hypervisor

Hypervisor or virtual machine monitor (VMM) is the software, firmware, or hardware that creates and runs a VM.

- The computer on which the hypervisor runs is called the host machine, and all other VMs are called guest machines.
- EC2 currently runs on Xen hypervisor.
- It can have either paravirtualization (PV) or hardware virtual machines (HVM).
- The VMs on the hypervisor are unaware that the processing time is shared between all the VMs.
- PV is a faster and lighter form of virtualization.

Paravirtualization

Paravirtualization is a form of virtualization in which the guests depend on hypervisors for support for operations that require privileged access.

- The OS in a guest machine doesn’t have any privileged access to the CPU.
- CPU provides four access modes called rings, which are 0-3, where 0 is the most privileged and 3 is the least privileged.
- Host OS runs on Ring-0.
- Guest OS runs on Ring-1, and the applications run on Ring-3.

Instances and Hosts

Dedicated Instances

Dedicated Instances are EC2 instances running in a VPC isolated to a single user.

Isolated at the host hardware level unlike the instances in other AWS accounts

May or may not share hardware with other instances of the same account

Pricing depends on factors, such as region and type of instance, so they are on-demand and not free

Dedicated Hosts vs. Dedicated Instances

Dedicated hosts provide all facilities of dedicated instances along with additional visibility and control on the placement of instances on a physical server.

Characteristics	Dedicated Instances	Dedicated Hosts
Use of dedicated physical servers	X	X
Billing per instance	X	
Billing per host		X
Visibility of sockets, cores, and host ID		X
Affinity between a host and an instance		X
Targeted instance placement		X
Automatic instance placement	X	X
Adding capacity using an allocation request		X

Source: https://aws.amazon.com/ec2/dedicated-hosts/

MFA with AWS

Duration: 10 Min.

Problem Statement:

Create and assign an MFA to a user.

Assisted Practice: Guidelines

Steps to create and assign an MFA to a user:

1. Create an MFA code

1. Scan it from a mobile device

1. Enter code in the **AWS MFA Console**

SSM And Run Command

Duration: 10 Min.

Problem Statement:

Create and assign SSM run command to S3.

Assisted Practice: Guidelines

Steps to create and assign an MFA to a user:

1. Selecting S3 bucket
2. Setting up run command

AWS Config with S3

Duration: 10 Min.

Problem Statement:

Create and assign SSM run command for S3.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to use AWS config with S3:

1. Selecting S3 bucket
2. Creating config rules for S3

Shared Responsibility Model

SRM

Shared responsibility model (SRM) states which security entities and dependencies are managed by AWS and what is the role of the customers in securing their data.

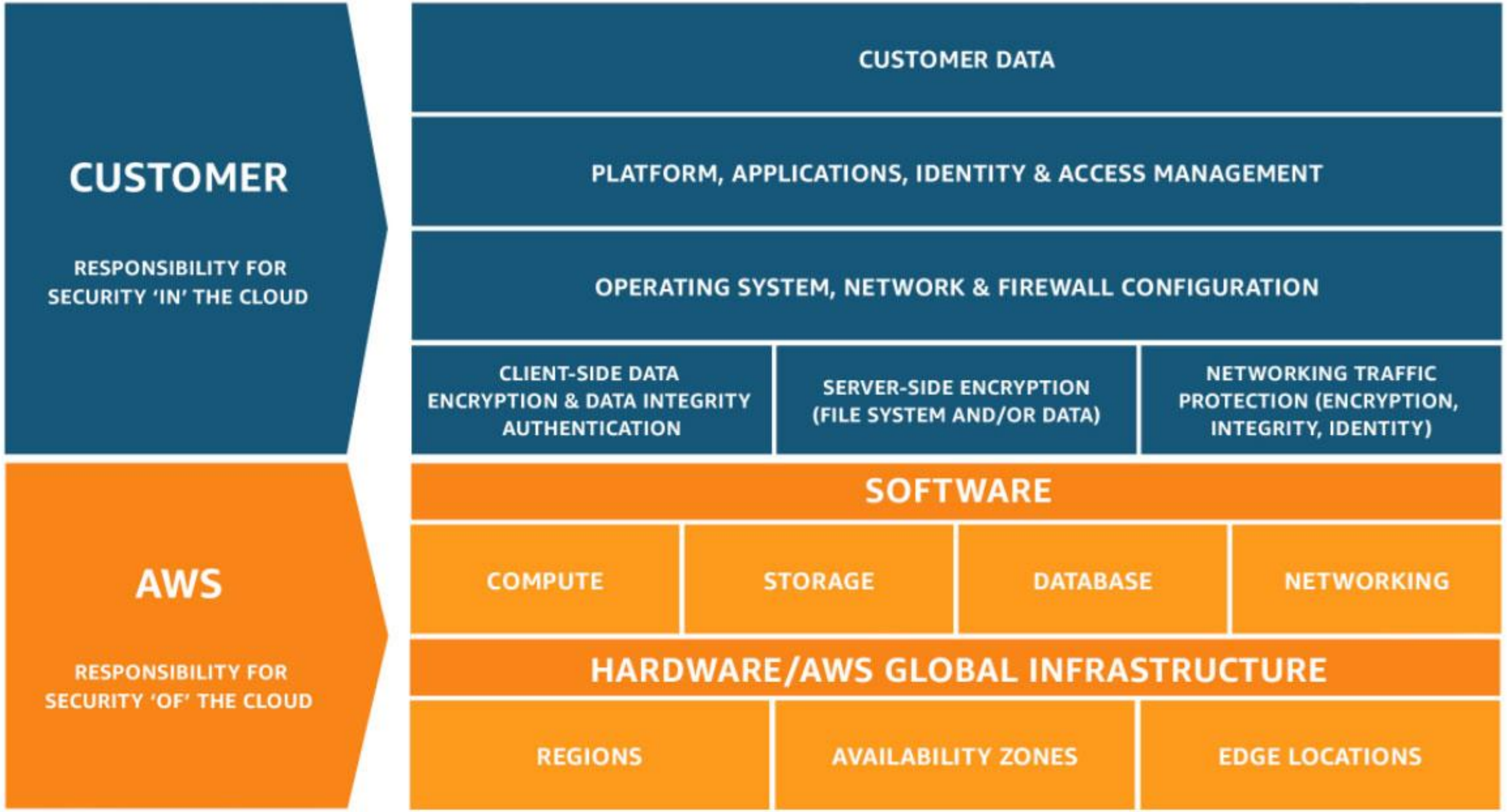
- It reduces the customer’s operational dependencies, as AWS operates, manages, and controls all components of the platform.

- Responsibility is divided into two parts:

1. **Security of the cloud (by AWS):** AWS ensures the security of the infrastructure on which all the services are running including, hardware, software, and networking facilities.

1. **Security in the cloud (by customer):** The customer is responsible for securing data using the services present in AWS by determining the amount of configurations to be set for used services.

SRM Division



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

TECHNOLOGY

Security Groups

What Is a Security Group?

A security group is a virtual firewall to control traffic on an instance.

- Security groups (SGs) are associated with EC2 instances to provide port access and protocol-level security.
- Each security group contains a set of rules that filters inbound and outbound traffic of an EC2 instance.
- A security group can restrict outside access to your instance, and security rules can filter any malicious requests.

SG Rules

A rule in a security group is the condition that helps a user filter any malicious requests to an instance.

- AWS security groups are stateful.
- Each rule comprises five fields, namely: type, protocol, port range, source, and destination.
- These fields apply to both inbound and outbound rules of the security group.

Provisioning Security Group

Security groups can be created through AWS CLI or AWS Management Console.

Steps to create security groups without creating an EC2 instance:

1. Log in to AWS Management Console

1. Select EC2 service

1. Select **Security Groups** from the menu on the left

1. Click on the **Create Security Group** button

1. Enter the name and description of the security group

1. Select a VPC

1. Add the rules

AWS CloudTrail

Duration: 10 Min.

Problem Statement:

Create and configure CloudTrail.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to create and configure CloudTrail:

1. Login to AWS lab

1. Select **CloudTrail** from **Services**

1. Create a trail

1. Select the S3 bucket to store log files

Key Takeaways

- A distributed denial-of-service (DDoS) attack is a malicious act that disturbs the normal traffic of a server, service, or network.
- AWS Shield provides a detection and automatic mitigation mechanism to reduce application downtime.
- STS is a web service that allows users to have limited and temporary access to AWS resources.
- Security groups can be created through AWS CLI or AWS Management Console.
- A rule in a security group is the condition that helps a user filter any malicious requests to an instance.

Implementing CloudTrail Using AWS IAM

Problem Statement:
Create and configure CloudTrail with an attached custom policy and control access to the log files.

Background of the problem statement:
The AWS team wants to implement CloudTrail that has an attached Read and Write custom policy and configured control access to the log files.

LESSON-END PROJECT