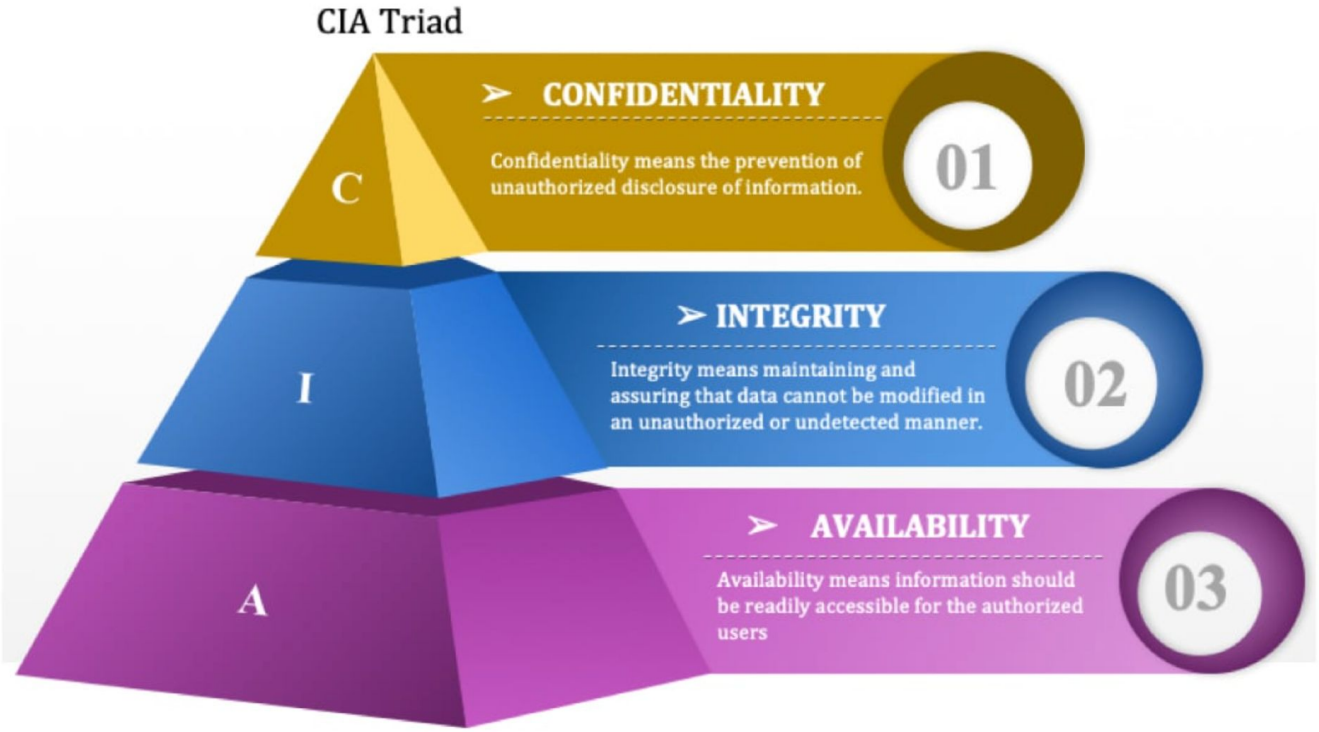
Security

By: Juan, Niaz, Sreedevi & Victoria

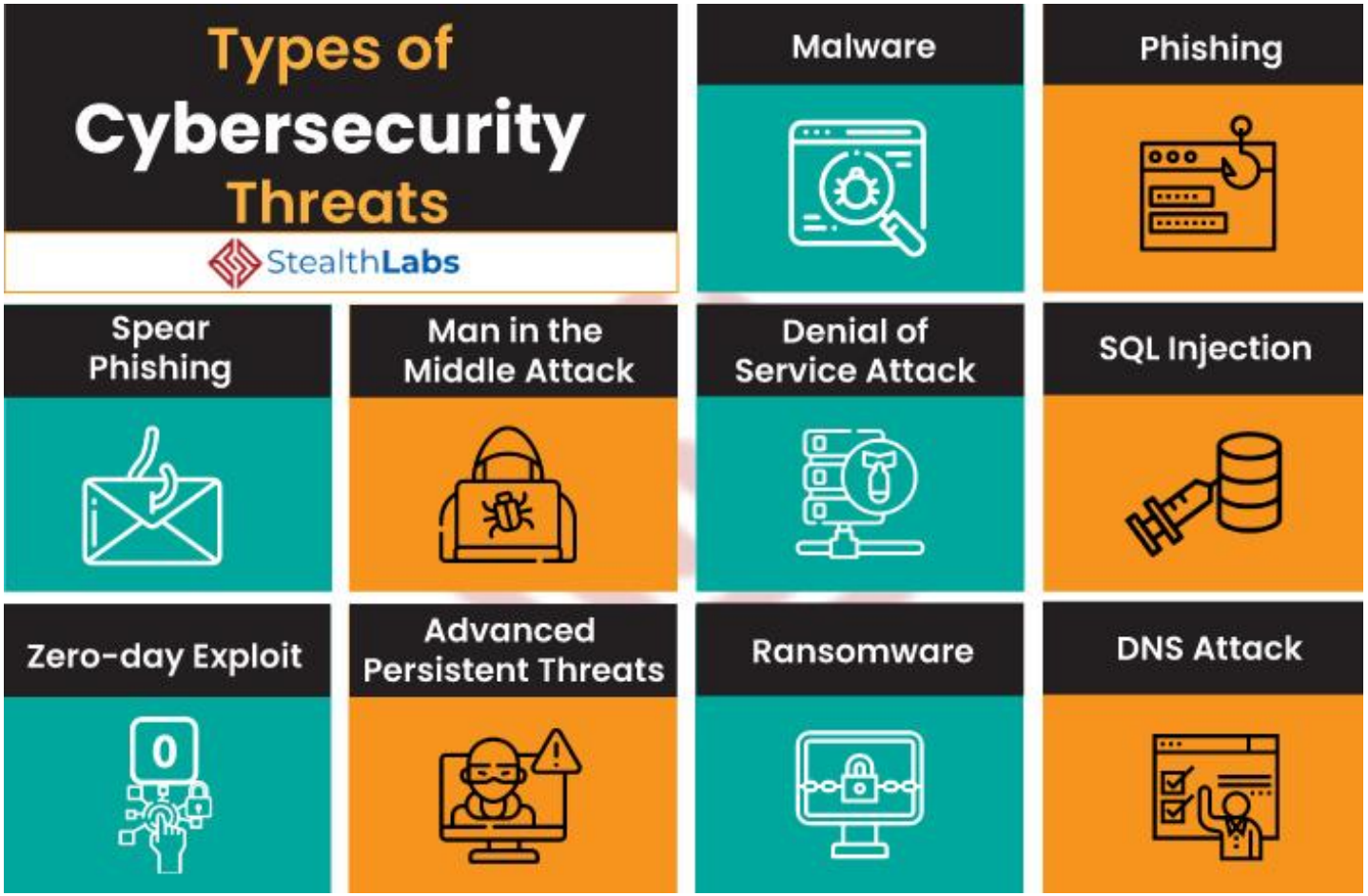
What is Cyber Security?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

Confidentiality, Integrity, and Availability (CIA)



THREATS


Types of
Cybersecurity
Threats
StealthLabs
Malware
Phishing
Spear Phishing
Man in the Middle Attack
Denial of Service Attack
SQL Injection
Zero-day Exploit
Advanced Persistent Threats
Ransomware
DNS Attack

STRATEGY

Security strategy for the cloud

A cloud security strategy defines:

What
security measures to implement:

Security controls

+

When
to implement security measures:

Security lifecycle

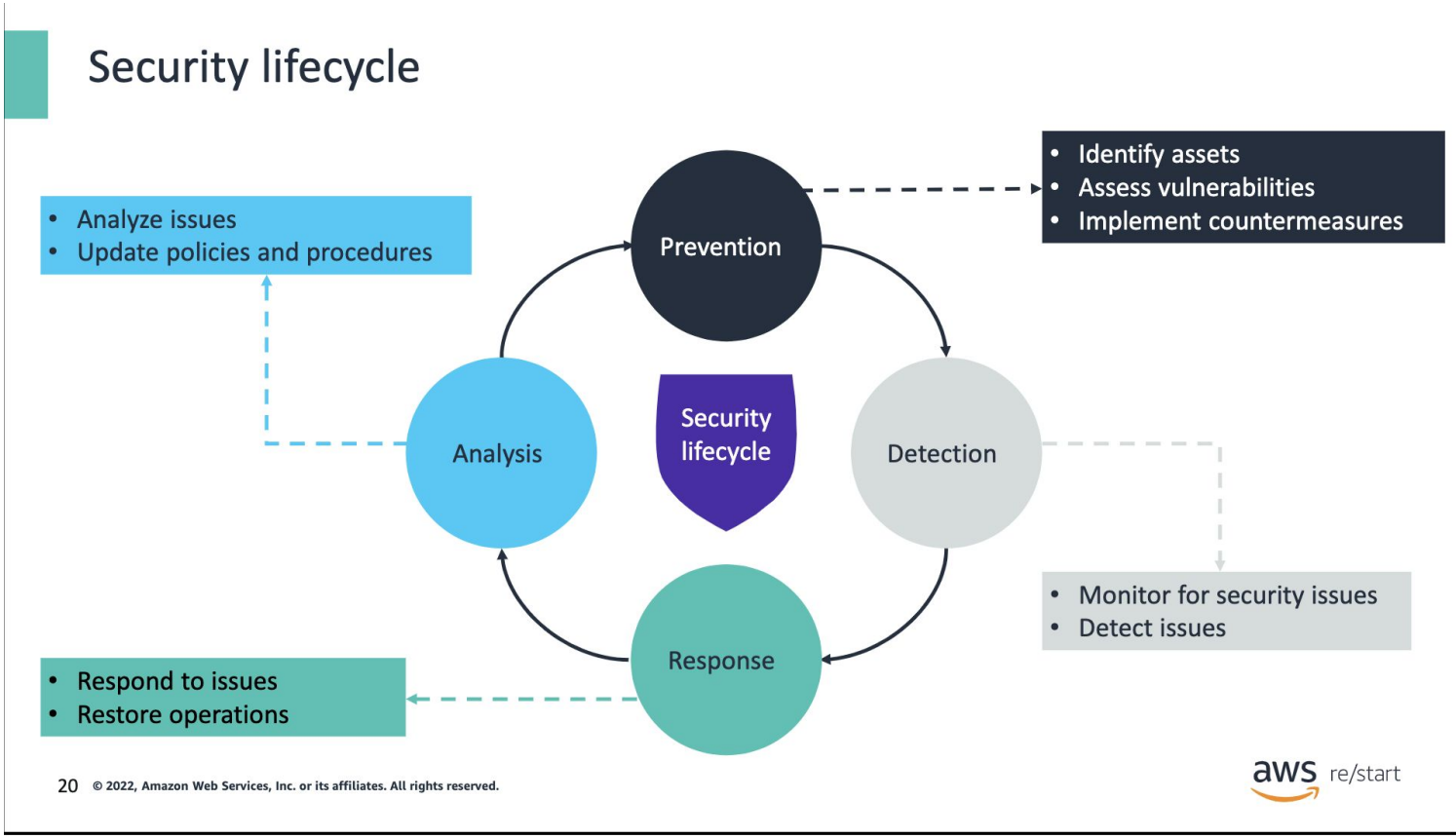
+

Who
is responsible for implementing security measures:

Security responsibility

aws re/start

SECURITY LIFE CYCLE



aws re/start

NETWORK HARDENING

VPC

IDS/IPS

Encryption

NACL

IAM

Audits &
Assessments

DDoS Protection

Security Groups

Network
Monitoring and
Logging

SYSTEM HARDENING

Secure Configurations

Firewalls

Authentication

Least Privilege Access

Patch Management

Disable Unused Protocols

Logging and Monitoring

Host-based Firewalls

Prevention: Data Security

- Encryption protects confidentiality of data.
- Encryption includes three types: Symmetric, asymmetric, and hybrid. Hybrid is widely used in internet communication protocols such as the TLS/SSL protocol.
- Hashing protects the integrity of data.
- Permissions define who can access a resource and how a resource can be accessed. Implement permissions by using an ACL or a role-based approach.

Public Key Infrastructure

- Public Key infrastructure (PKI) defines principles and components that you can use to secure resources by using keys and digital certificates.
- A digital certificate is an electronic credential that is used to represent the online identity of an individual, computer, or other entity.
- A certificate authority (CA) signs and issues certificates to entities and manages trust relationships.
- A digital certificate can be self-signed, or a CA can sign it.

Prevention: Identity Management

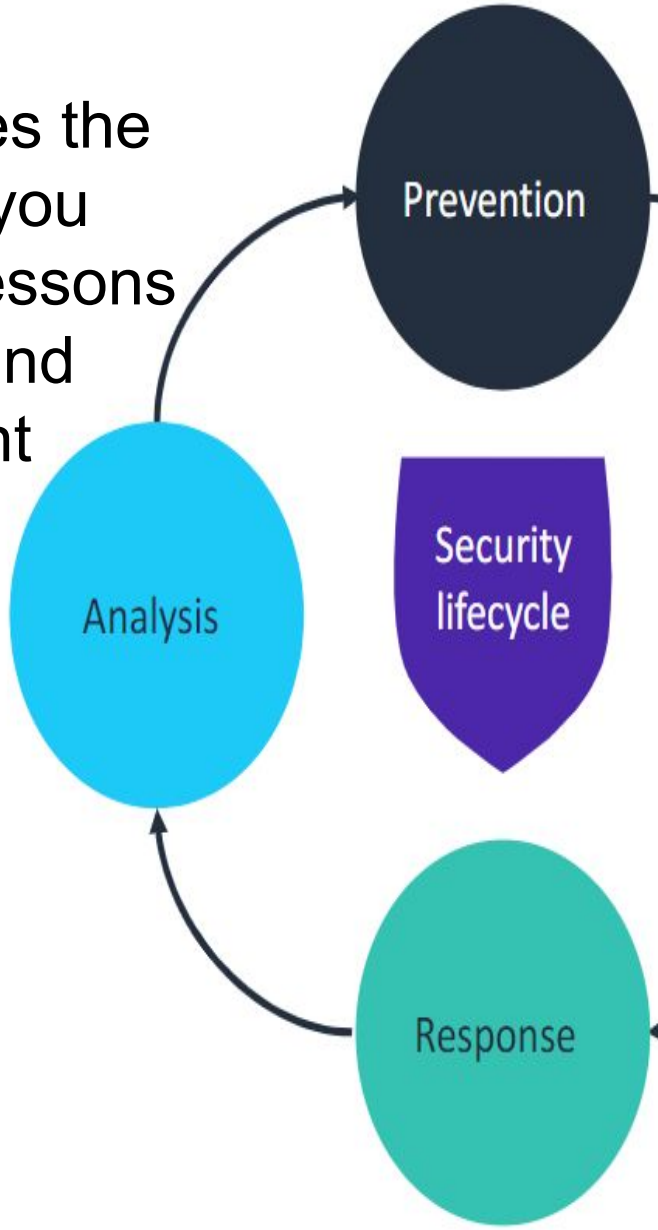
- Identity management ensures that users receive the appropriate access to the resource they need, at the right level, and at the appropriate time.
- Authentication factors can be categorized as the following:
    - Something you know: For example, a password.
    - Something you have: For example, a smart card
    - Something you are: For example, your fingerprint
- A good identity management solution includes creating password policies, using password managers, and using single sign-on and federated identity management
- AWS Identity and Access Management (IAM) is a service that helps you control access to AWS resources in a secure way by using authentication and authorization.

AWS Identity and Access Management (IAM)

- IAM is a service that helps securely control access to AWS resources.
- IAM provides different types of security credentials:
  - Email address and passwords
  - IAM user name and password
  - Access and secret access keys
  - MFA
  - Key pairs

- Use IAM to create users and groups and assign roles to them.
- An IAM role specifies permissions that define which actions can be taken against a given resource

Security lifecycle: Detection



Completes the cycle as you identify lessons learned and implement

Is the first line of defense

Occurs when prevention fails

Antivirus

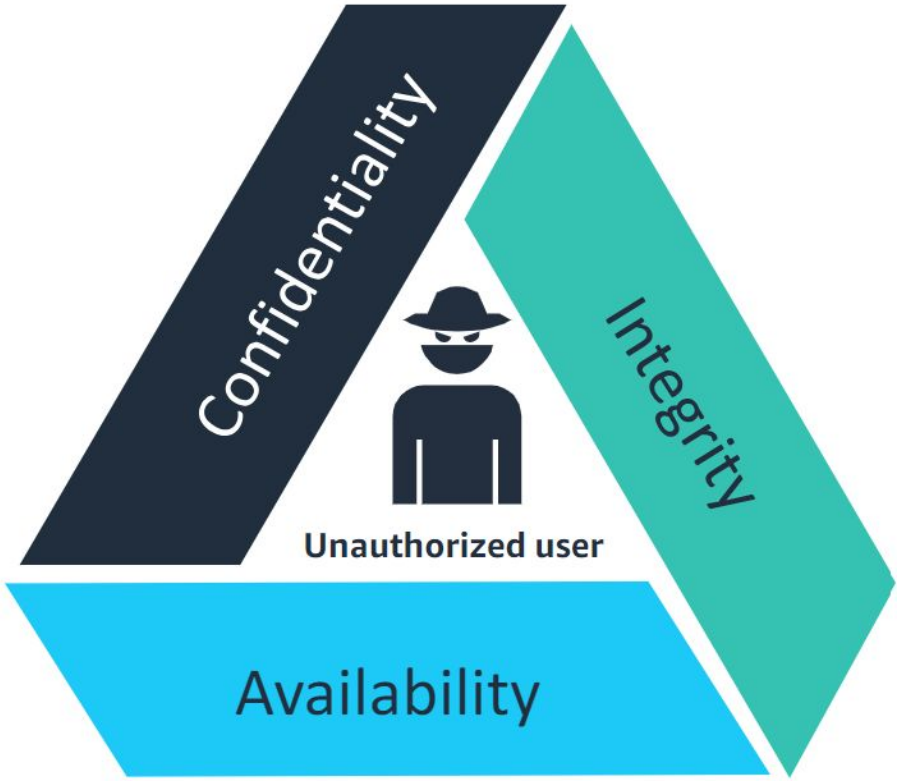
Intrusion detection system

Describes what you do when you detect a security threat

Malware threat

The threat of malware

- Malicious software (malware) is designed to cause harm to a computer system by interrupting one of the CIA triad elements:
  - Confidentiality
  - Integrity
  - Availability
- The following are types of malware:
  - Worms
  - Bots
  - Ransomware
  - Viruses
- The following are infection methods:
  - Untrusted websites
  - Emails
  - Removable devices

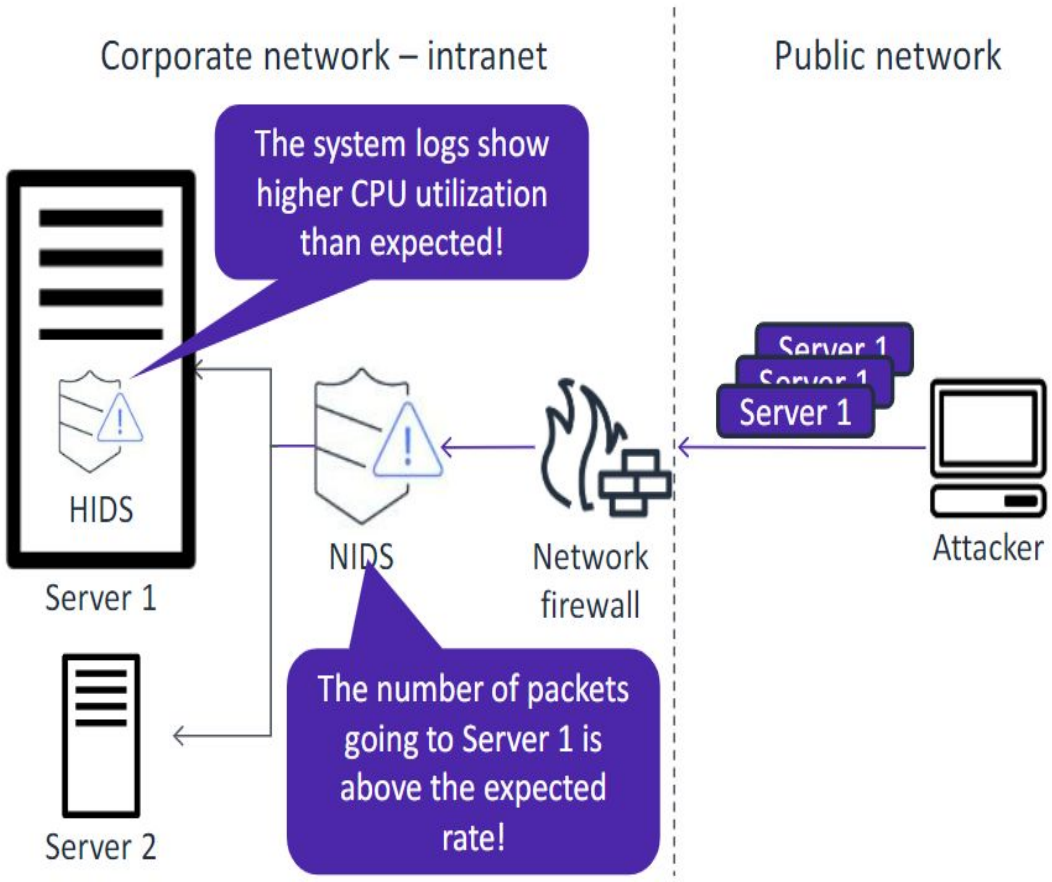


Intrusion Detection Systems

Network-based IDS and host-based IDS

There are two main types of intrusion detection systems:

- Network-based intrusion detection system (NIDS):
  - Monitors network traffic, detects threats, and raises alerts
  - Is installed on the **network**
- Host-based intrusion detection system (HIDS):
  - Monitors logs and critical files on the server, detects threats, and raises alerts
  - Is installed on a **server**



GuardDuty

GuardDuty is a threat detection that monitors your AWS accounts and workloads for malicious activity.

GuardDuty detects unauthorized and unexpected activity in your AWS environment by analyzing and processing data from different AWS service logs.

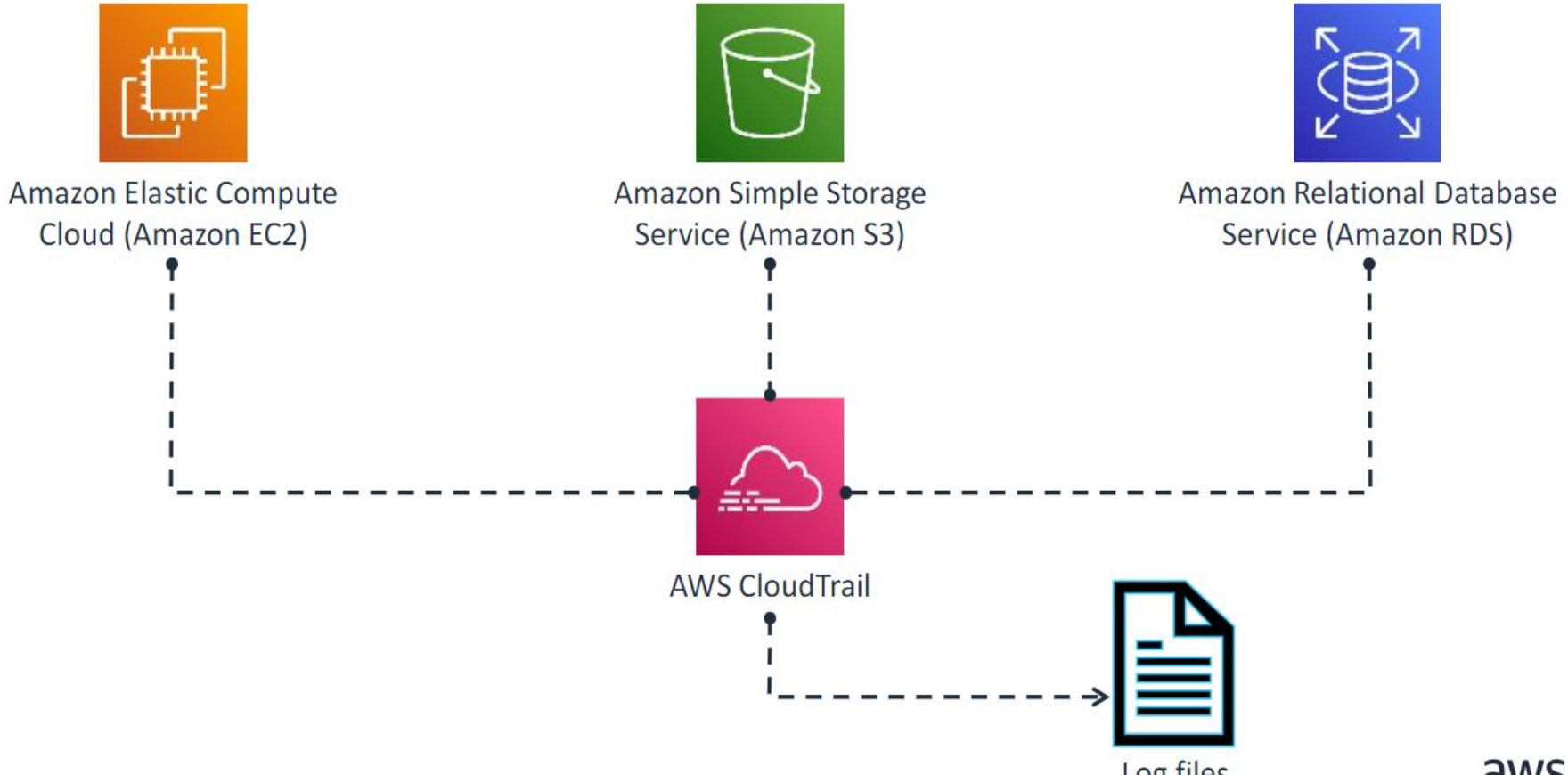
•AWS CloudTrail event logs
Virtual private cloud (VPC) flow logs
Domain Name System (DNS) logs

GuardDuty extracts various fields from these logs and uses them for profiling and anomaly detection.

CloudTrail

What is CloudTrail?

CloudTrail provides auditing, security monitoring, and operational troubleshooting.



How does CloudTrail work?

CloudTrail captures and records that activity, which is referred to as a CloudTrail event.

The event contains details about the following:

Who performed the request

When the event occurred (that is, the date and time of the request)

What the source Internet Protocol (IP) address

How the request was made

Which actions were performed

Where the action occurred (that is, in which Region)

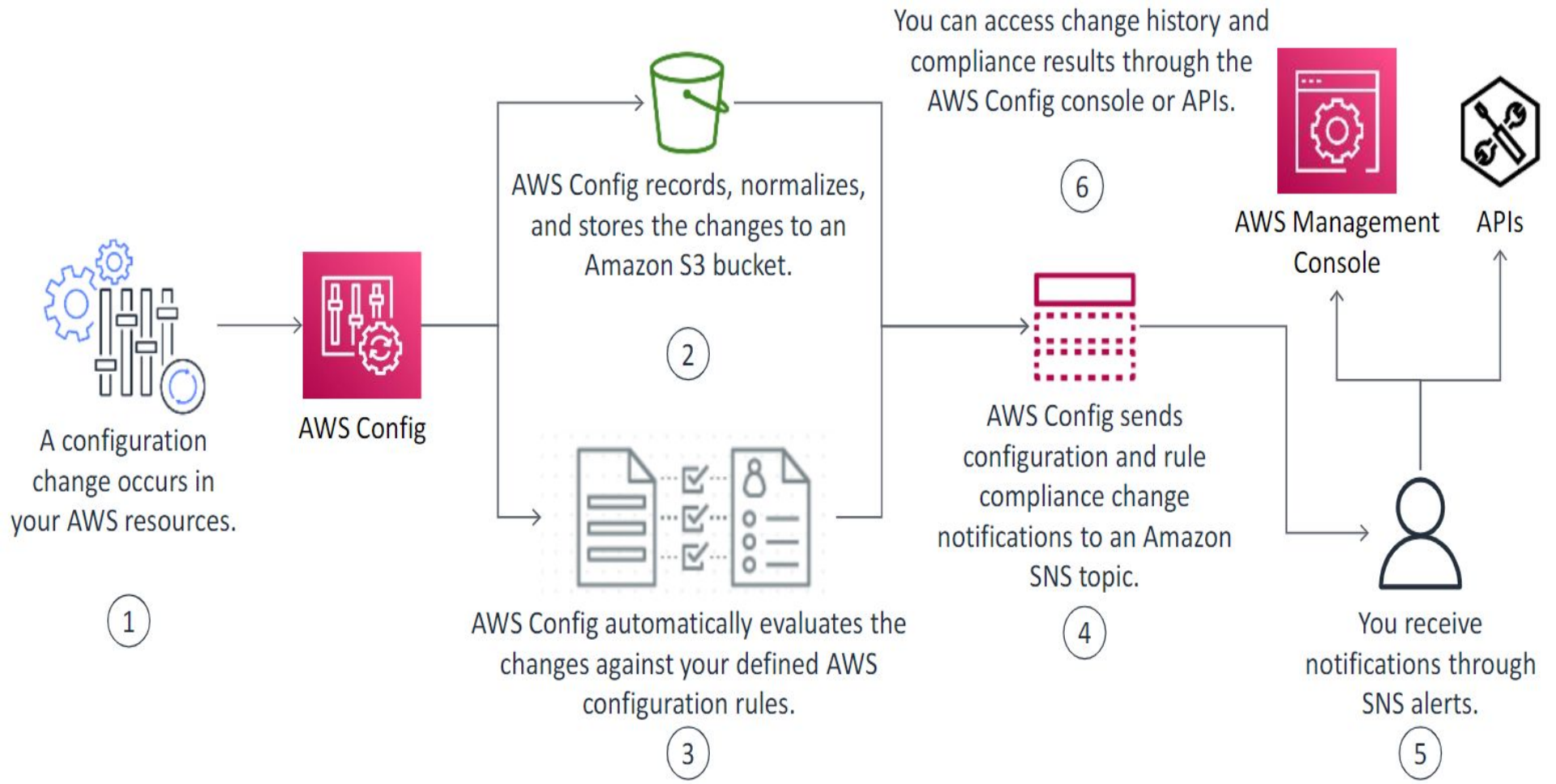
What the response was for

CloudTrail example: Amazon EC2 event (1 of


```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "accountId": "123456789012",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:22:54Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
```

AWS Config

How AWS Config works



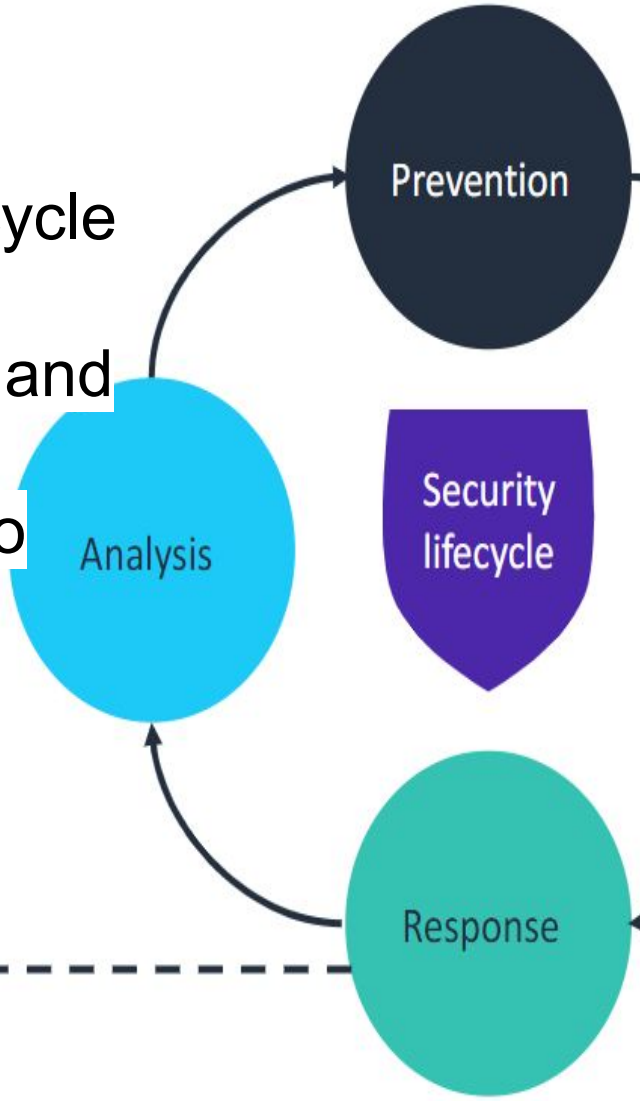
Response

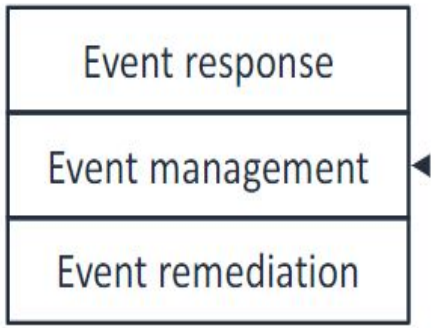
Is the first line of defense.

Occurs when prevention fails.

Describes what you do when you detect a security threat.

Completes the cycle as you identify lessons learned and implement new measures to prevent future incident.





Business Continuity Plan

BCP- is a document that consist of critical information of an organization that is needed to continue operating after an unplanned event.

BCP-has essential informations about the organization. It identifies which systems and process must be sustained.

BCP- covers risk potentials such as cyber-attack, pandemics, natural, disaster, human error and more.

Disaster Recovery Plan

DRP-It is a structured approach that describe how an organization can quickly resume work after an unplanned incident.

Examples of Disasters

Earthquake, Hurricane, Cyber-attacks, Flood Pandemic, Man-Made Incidents, Data breaches, Hardware failure

Recovery Measures

1. You do assessment and business Impact.
2. Define Recovery Objectives (Set recovery time).
3. Develope you Recovery team together.
4. Data Backup and Storage.
5. Communication plan.
6. Test the plan.
7. Document the plane.
8. Training awareness.
9. Regular Review and update.

Analysis

The goal of security analysis is to strengthen security controls to better protect your network facilities, and organization.

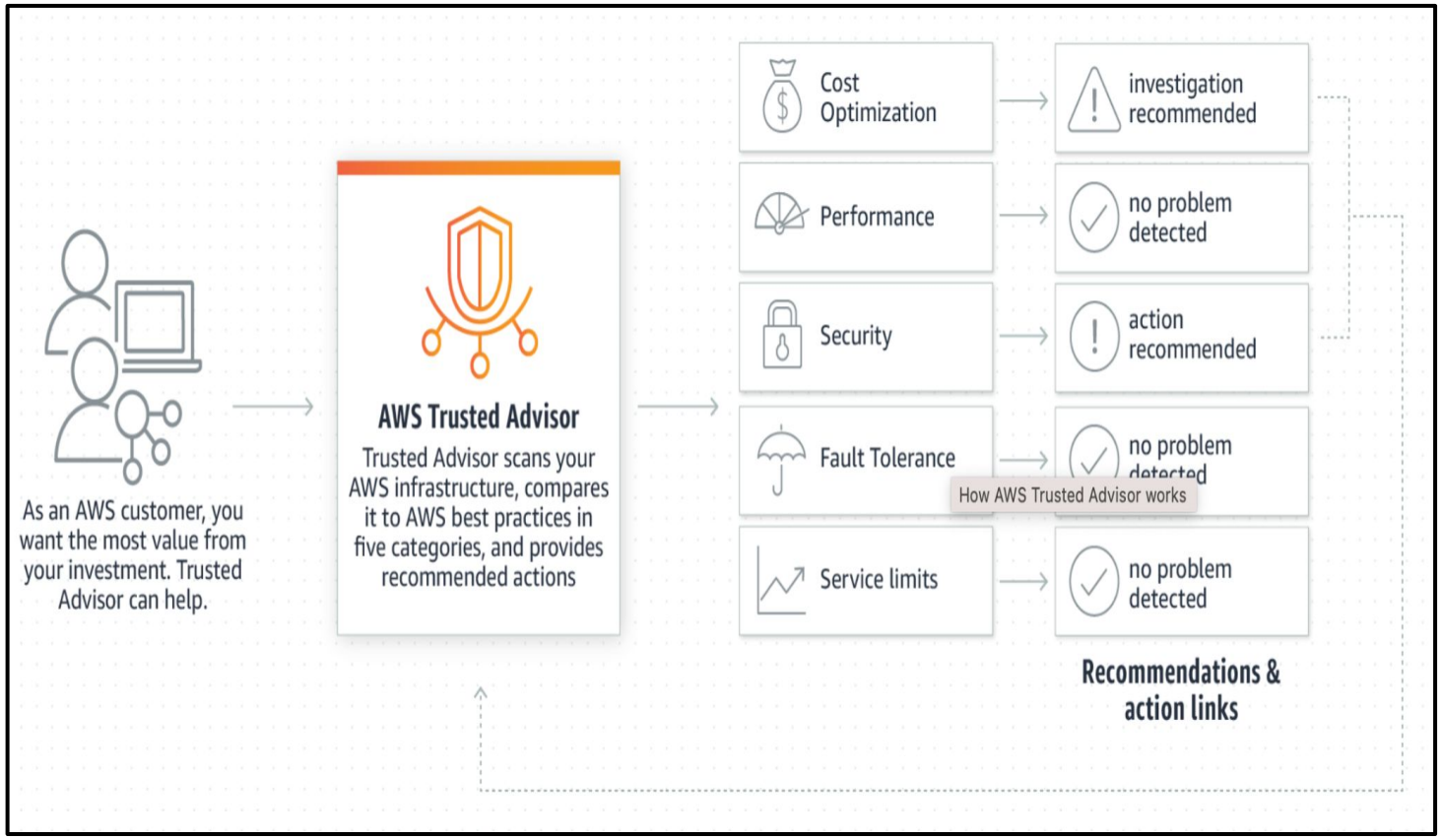
Testing, monitoring and logging are key activities that support security analysis.

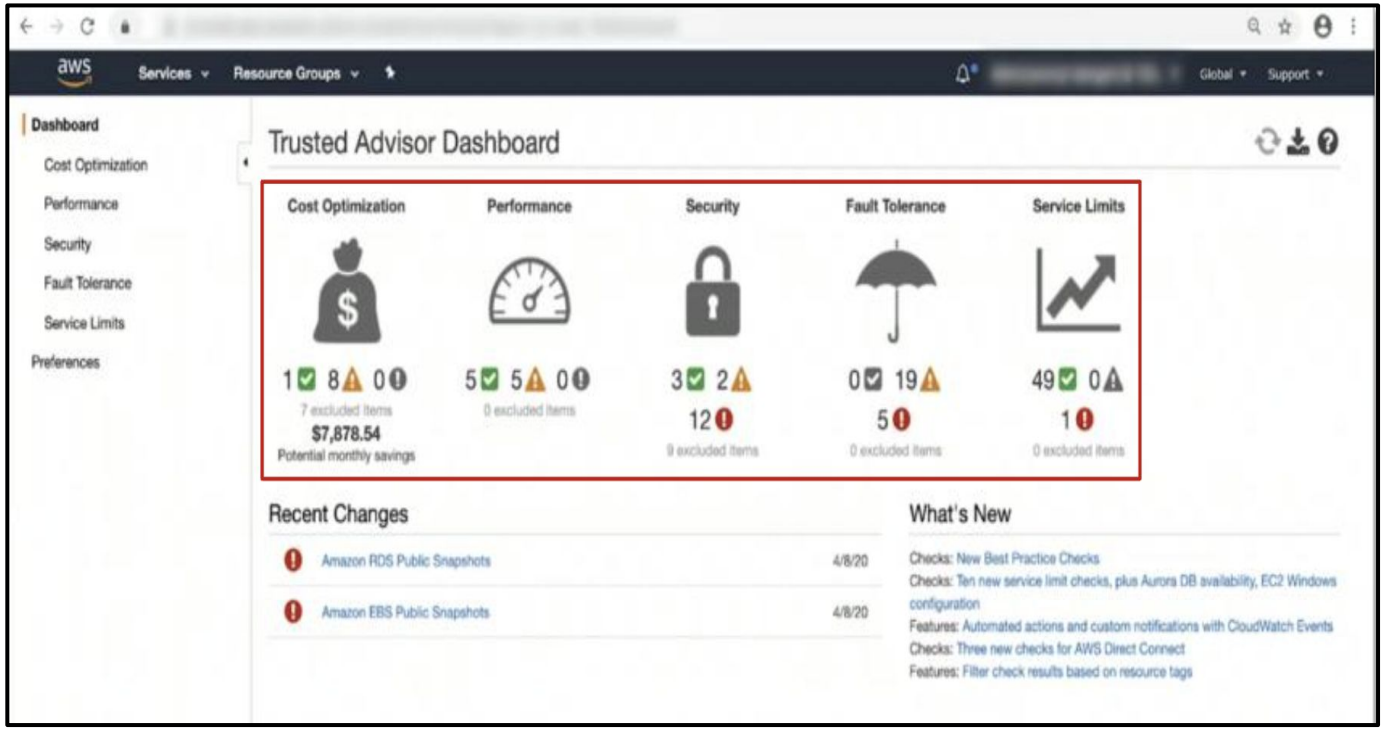
A monitoring policy defines all the details of what who when and how monitoring is to be performed.

A logging policy identifies what should be logged and how to manage logs.

This lesson includes the following key take aways:

AWS Trusted Advisor





Categories:

- Cost Optimization : Save money on AWS
- Performance : Improve the performance of your service
- Security: Improve the security of your application
- Fault Tolerance: Increase the availability and redundancy of your AWS
- Service Limits: Check for service usage

Checks have a status:

Green: No problem detected

Yellow: Investigation recommended

Red: Action recommended

AWS Trusted Advisor - Cost Optimization

Low Utilization Amazon EC2 Instances

Refreshed: 28 minutes ago

Checks the Amazon Elastic Compute Cloud (Amazon EC2) instances that were running at any time during the last 14 days and alerts you if the daily CPU utilization was 10% or less and network I/O was 5 MB or less on 4 or more days. Running instances generate hourly usage charges. Although some scenarios can result in low utilization by design, you can often lower your costs by managing the number and size of your instances.

Estimated monthly savings are calculated by using the current usage rate for On-Demand Instances and the estimated number of days the instance might be underutilized. Actual savings will vary if you are using Reserved Instances or Spot Instances, or if the instance is not running for a full day. To get daily utilization data, download the report for this check.

Alert Criteria

Yellow: An instance had 10% or less daily average CPU utilization and 5 MB or less network I/O on at least 4 of the previous 14 days.

Recommended Action

Consider stopping or terminating instances that have low utilization, or scale the number of instances by using Auto Scaling. For more information, see Stop and Start Your Instance, Terminate Your Instance, and What is Auto Scaling?

Additional Resources

Monitoring Amazon EC2
Instance Metadata and User Data
Amazon CloudWatch Developer Guide
Auto Scaling Developer Guide

39 of 43 Amazon EC2 instances have low average daily utilization. Monthly savings of up to $1,014.05 might be available by minimizing underutilized instances. 1 items have been excluded.

Exclude & Refresh | Item View: Included items | Columns View: Columns Display

1 to 20 of 39 | View: 20

Region/AZ	Instance ID	Instance Name	Instance Type	Estimated Monthly S...	CPU Utilization 14-D...	Network I/O 14-Day ...	Number of Days Low ...
us-east-2b	i-010c2fa842d79ff31		m4.large	$66.24	0.1%	0.00MB	14
us-east-2b	i-037402ae0fa6c2b79		m4.large	$66.24	0.1%	0.00MB	14
us-east-2a	i-016ecd137f1e52e93		m4.large	$66.24	0.1%	0.00MB	14
ca-central-1b	i-0371548ad07d39039		t2.micro	$9.22	0.1%	0.00MB	14
ca-central-1b	i-0ecbfec11e33ef8c5		t2.micro	$9.22	0.2%	0.01MB	14
ca-central-1a	i-08dc511beb13837de		t2.micro	$9.22	0.0%	0.00MB	14

AWS Trusted Advisor- Security

Security Checks:

- AWS Identity and Access MAnagement (IAM) use
- Multi Factor Authentication(MFA) on root account
- Security groups - Specific ports unrestricted
- Amazon Simple Storage Service (s3) bucket permissions
- Amazon Elastic Block Store (EBS) public snapshots
- Amazon Relational Database Service(Amazon RDS) public snapshots

Security Best Practices

- Avoid using root account
- Enable Multi Factor Authentication(MFA)
- Activate AWS Cloud Trail
- Enable billing report - Cost and Usage report

When to use root account

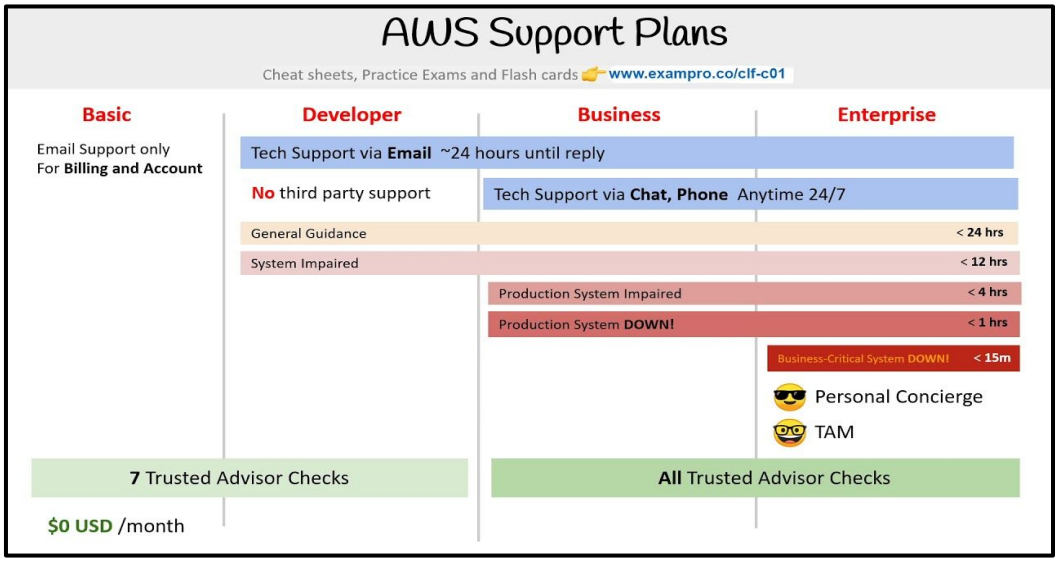
The following tasks require that you sign in to AWS with your root user credentials:

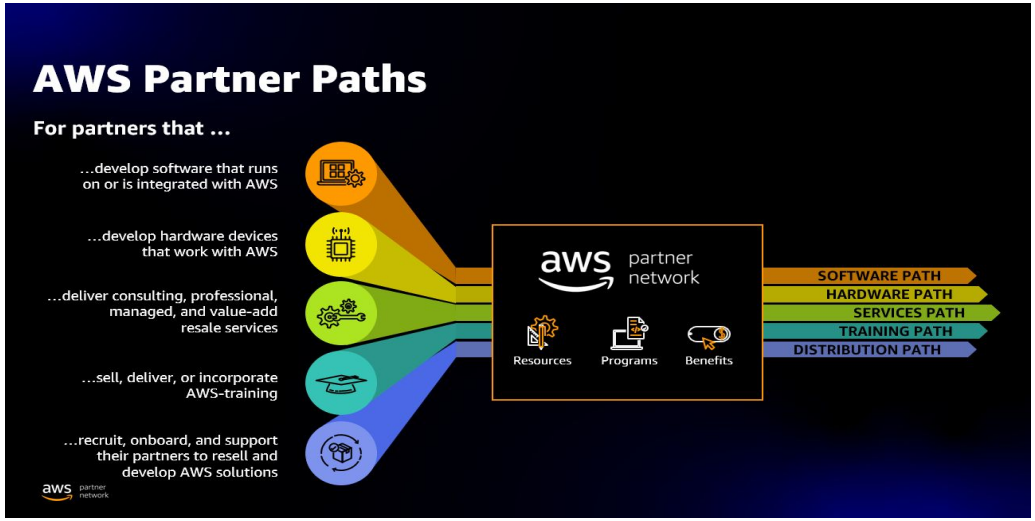
- Change your account settings
- Restore AWS Identity and Access Management (IAM) user permissions
- Change your AWS Support plan or cancel your AWS Support plan
- Activate IAM access
- View certain tax invoices
- Close your AWS account
- Register as a seller
- Configure an Amazon Simple Storage Service (Amazon S3) bucket
- Edit or delete an S3 bucket

AWS Compliance Program

AWS Security Resources

- AWS Account Teams
- AWS Support Plans
- AWS Professional Services and the AWS Partner Network
- AWS Advisories and Bulletins
- AWS Auditor Learning Path





Lab - Monitor an EC2 Instance

- Create an Amazon SNS notification
- Configure a CloudWatch alarm
- Stress test an EC2 instance
- Confirm that an Amazon SNS email was sent
- Create a CloudWatch dashboard

Thank You