COLOMBIA POTENCIA DE LA VIDA

TIC

BOOTCAMP ARQUITECTURA EN LA NUBE

INTEGRADOR - MÓDULO 3

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Objetivo general

UNIDAD 2

- Identificar un incidente
- Describir los servicios de Amazon Web Services (AWS) que se utilizan para el reconocimiento y la reparación de incidentes
- Identificar las prácticas recomendadas para la respuesta ante incidentes

Competencias a desarrollar

- Identificar y describir las herramientas de monitoreo de AWS, como CloudWatch, CloudTrail, y AWS Config.
- Explicar cómo estas herramientas pueden ser utilizadas para detectar incidentes y monitorizar el estado de la infraestructura.
- Explicar cómo estos servicios pueden ser configurados para alertar sobre posibles incidentes y tomar medidas correctivas.
- Identificar las mejores prácticas para la preparación de un plan de respuesta ante incidentes.
- Establecer canales de comunicación efectivos para la colaboración entre equipos durante la respuesta a incidentes.
- Evaluar el rendimiento de la respuesta ante incidentes a través de ejercicios de simulación y análisis post-mortem.

Activación de saberes previos

Tiempo de Ejecución: 12 horas

PLANTEAMIENTO DE LA LECCIÓN	MATERIALES
Lección 1: Identificación de un incidente **Objetivos de aprendizaje:** Comprender qué es un incidente en el contexto de AWS. Aprender cómo identificar y clasificar incidentes de seguridad, rendimiento y disponibilidad. **Contenido:** Definición de un incidente en el entorno de AWS. Tipos comunes de incidentes. Indicadores de compromiso (IOCs) y señales de alerta. Procesos de notificación y gestión de incidentes.	AWS Trusted Advisor en la Guía del usuario https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html. Guía del usuario de Amazon CloudWatch en https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html. Guía del usuario de Amazon Inspector en https://docs.aws.amazon.com/inspector/latest/user/what-is-inspector.html.

Activación de saberes previos

PLANTEAMIENTO DE LA LECCIÓN	MATERIALES
Actividad: Presentar a los estudiantes varios escenarios de incidentes y solicitarles que identifiquen los posibles indicadores de compromiso y señales de alerta. Discutir en grupos pequeños cómo se clasificaría cada incidente y qué acciones se tomarían para manejarlo. **Lección 2: Servicios de AWS que soportan la fase de descubrimiento y reconocimiento** **Objetivos de aprendizaje:** Conocer los servicios de AWS que ayudan en la fase de descubrimiento y reconocimiento de incidentes. Aprender cómo utilizar estos servicios para detectar y analizar anomalías en la infraestructura.	Guía del usuario de Amazon GuardDuty en https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html. AWS Trusted Advisor en la Guía del usuario de AWS Support https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html. Guía para desarrolladores de AWS Lambda https://docs.aws.amazon.com/lambda/latest/dg/welcome.html

Activación de saberes previos

PLANTEAMIENTO DE LA LECCIÓN	MATERIALES
Contenido: Servicios de AWS para la recopilación de datos de seguridad y eventos. Herramientas de análisis de registros y métricas. Detección de amenazas y comportamientos anómalos. Actividad: Realizar una demostración práctica sobre cómo utilizar AWS CloudTrail, Amazon GuardDuty y Amazon CloudWatch para detectar y analizar anomalías en la infraestructura. Solicitar a los estudiantes que investiguen otros servicios de AWS que podrían ser útiles para el descubrimiento y reconocimiento de incidentes.	Guía del usuario de AWS Systems Manager https://docs.aws.amazon.com/systems-manager/latest/userguide/what-is-systems-manager.html. Guía del usuario de AWS CloudFormation en https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html.

Activación de saberes previos

PLANTEAMIENTO DE LA LECCIÓN	MATERIALES
Lección 3: Servicios de AWS que soportan la fase de resolución y recuperación **Objetivos de aprendizaje:** Entender los servicios de AWS que ayudan en la fase de resolución y recuperación de incidentes. Aprender cómo utilizar estos servicios para mitigar el impacto de un incidente y restaurar la normalidad operativa. Contenido: Servicios de AWS para la respuesta a incidentes y la recuperación de datos. Automatización de acciones de respuesta. Copias de seguridad y restauración de datos.	Guía para desarrolladores de Amazon Simple Notification Service https://docs.aws.amazon.com/sns/latest/dg/welcome.html. Guía para desarrolladores de AWS Step Functions en https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html.

Activación de saberes previos

PLANTEAMIENTO DE LA LECCIÓN

Actividad:

Presentar casos de uso de AWS Systems Manager, AWS Backup y AWS Disaster Recovery para la resolución y recuperación de incidentes.
Realizar ejercicios prácticos sobre cómo configurar acciones de respuesta automatizadas utilizando AWS Lambda y AWS Systems Manager Automation.

Activación de saberes previos

PLANTEAMIENTO DE LA LECCIÓN

Lección 4: Prácticas recomendadas para la gestión de un incidente

Objetivos de aprendizaje:

Conocer las mejores prácticas para la gestión eficaz de un incidente en entornos de AWS.
Aprender cómo establecer procesos y procedimientos para minimizar el impacto de los incidentes.
Contenido:

Planificación de la respuesta a incidentes.
Coordinación y comunicación durante un incidente.
Evaluación post-incidente y lecciones aprendidas.
Actividad:

Discutir en grupos pequeños las mejores prácticas para la gestión de incidentes en entornos de AWS.
Presentar ejemplos de casos de estudio y solicitar a los estudiantes que identifiquen qué prácticas recomendadas se aplicaron en cada situación.
Laboratorio Práctico: Corrección de un incidente utilizando AWS Config y AWS Lambda

Evaluación de Conocimientos

COLOMBIA POTENCIA DE LA VIDA

TIC

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira