AWS Incident Response scenario

ow

Overview

- Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack.
- It aims to minimize the damage caused by the incident, restore normal operations as quickly as possible, and prevent future attacks.
- DOS attack
- Malware infection
- Data breach

Denial of Service (DoS) attack

- A DoS attack is a type of cyberattack in which the attacker attempts to make a network, system, or application unavailable to users by overwhelming it with traffic. This can cause slow performance, errors, and even complete downtime for your applications.
- To respond to a DoS attack on AWS, you can use AWS Shield, which is a managed service that provides protection against common DoS attacks. With AWS Shield, you can enable DDoS protection for your Amazon Elastic Compute Cloud (EC2) instances, Amazon CloudFront distributions, and Amazon Route 53 resources.

..

- Additionally, you can use Amazon CloudWatch to monitor the performance of your applications and identify any potential DoS attacks.
- You can also enable CloudWatch alarms to trigger automated responses, such as scaling up your EC2 instances to handle the increased traffic.

Malware infection

- Malware is a type of malicious software that is designed to gain unauthorized access to a computer system or network. It can come in many forms, including viruses, worms, Trojan horses, and ransomware.
- To respond to a malware infection on AWS, you can use Amazon GuardDuty, which is a managed threat detection service that uses machine learning and other techniques to identify and alert you to potential malware infections. But GuardDuty will only help you detect — you then need to find the root cause of the infection and potential damage.

..

- Additionally, you can use Amazon Inspector to assess the security of your Amazon EC2 instances and identify any vulnerabilities that could be exploited by malware.
- You can also use Amazon S3 and Amazon EBS to create backups of your data, so that you can restore it if it is lost or corrupted as a result of a malware infection.

Data breach

- A data breach occurs when sensitive, confidential, or personal information is accessed, disclosed, or stolen without authorization. This can have serious consequences for organizations, including financial losses, damage to their reputation, and legal liabilities.
- To respond to a data breach on AWS (if it’s an open S3 bucket), you can use Amazon Macie, which is a managed service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. With Amazon Macie, you can monitor access to your data and receive alerts if unauthorized access is detected.

Assessment Setup

You can use the options below to get the following assessments on all of your EC2 instances in this AWS regi
once for a one-time assessment, or **Advanced setup** for custom assessments.

Network Assessments (Inspector Agent is not required)

- **Assessments performed:** Network configuration analysis to checks for ports reachable from outside t
- **Optional Agent:** If the Inspector Agent is installed on your EC2 instances, the assessment also finds p
- **Pricing:** Pricing for **network assessments** is based on the monthly volume of instance-assessments,
  for 100 instances assessed weekly, the monthly cost would be around $61/month. Learn more

Host Assessments (Inspector Agent is required)

- **Assessments performed:** Vulnerable software (CVE), host hardening (CIS benchmarks), and security
- **Agent Deployment:** Inspector assessments require an agent to be installed on your EC2 instances. W
  Learn more about Inspector Agent and how to manually install agent.
- **Pricing:** Pricing for **host assessments** is based on the monthly volume of agent-assessments, where
  instances assessed weekly, the monthly cost would be around $120/month. Learn more

..

- Additionally, you can use Amazon S3 and Amazon EBS to encrypt your data at rest, so that it is protected even if it is accessed without authorization.
- You can also use AWS Identity and Access Management (IAM) to control and monitor access to your AWS resources, including who can access your data and what actions they can perform on it.