



Welcome to Security Lifecycle – Analysis.

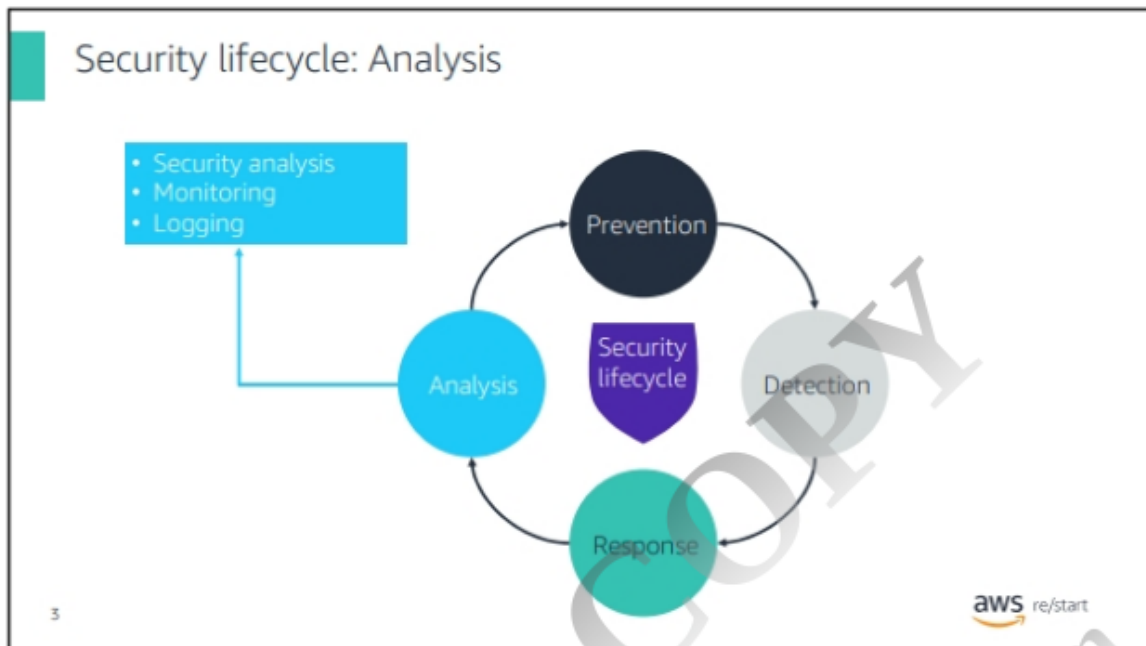
## What you will learn

### At the core of the lesson

You will learn how to:

- Identify tools and processes for security analysis to identify vulnerabilities
- List guidelines on how to conduct security analysis
- Describe how different types of testing, monitoring, and logging support security analysis

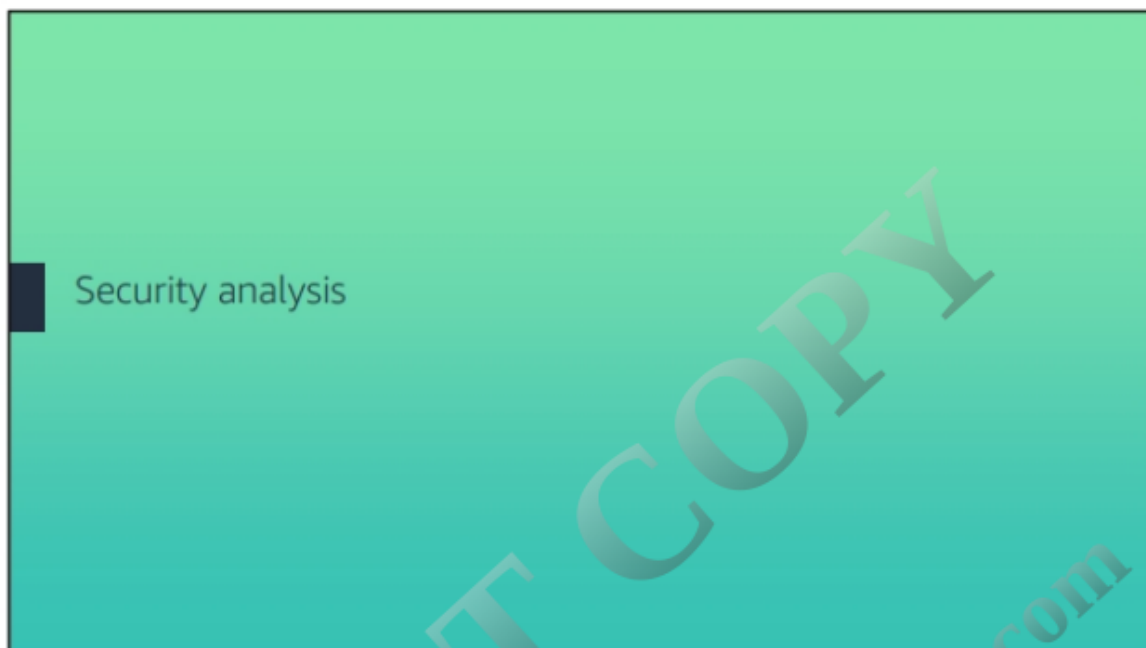




As a review, the phases of the security lifecycle consist of:

- **Prevention** – The first line of defense.
- **Detection** – Occurs when prevention fails.
- **Response** – Describes what you do when you detect a security threat.
- **Analysis** – Completes the cycle as you implement new measures to prevent the incident from occurring again in the future.

In this lesson, you will learn about the *Analysis* phase of the security lifecycle. Specifically, you will discover tools and techniques for doing security monitoring, logging, and analysis.



## What is analysis?

Reviewing what happened after a security breach

For an effective analysis, ask:

- How many security breaches did you experience?
- How did it happen?
- How many did it affect?
- How do you prevent it from happening again?

5

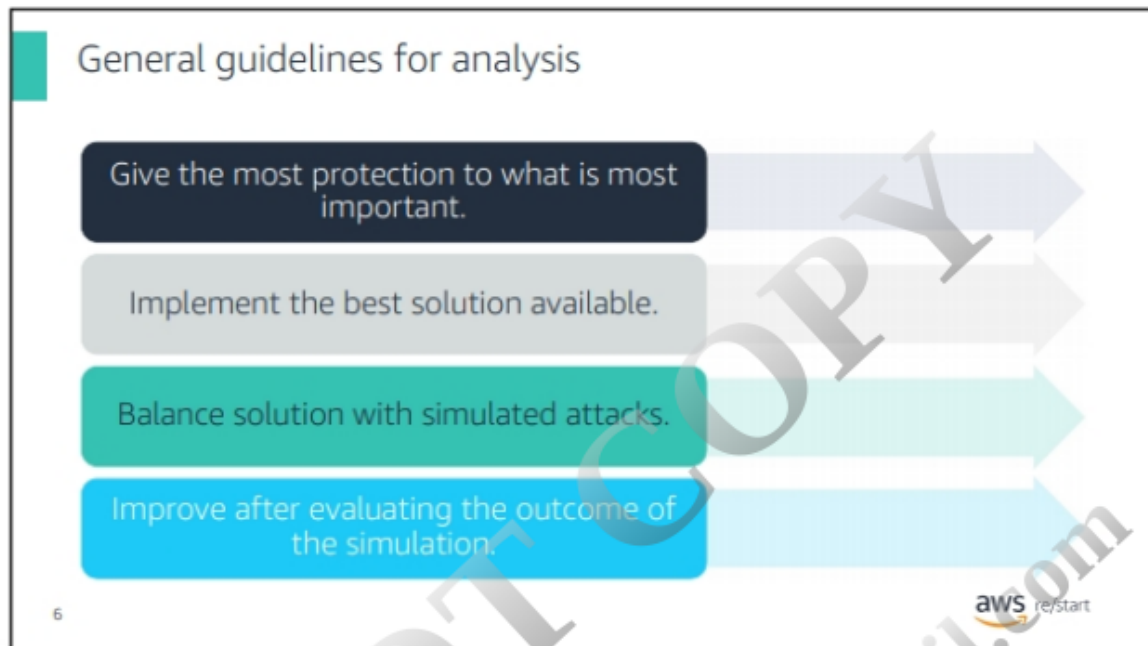
aws re/start

Analysis is the final phase of the security lifecycle. In the Analysis phase, you review the cause of security incidents and analyze current security controls to determine weaknesses. The objective is to improve and strengthen those controls to better protect your network, facilities, and organization.

Questions that you ask during analysis include:


- How many security breaches did you experience?
- How did they happen?
- How many people did they affect?
- How could you prevent it from happening again?

The next topic describes some guidelines and techniques that you can apply during the Analysis phase to answer these questions.



The main goal of analysis is to improve and strengthen the existing security of your environment. These general guidelines are for performing security analysis, including the need to test by using simulated attacks.

### General guidelines for analysis, continued

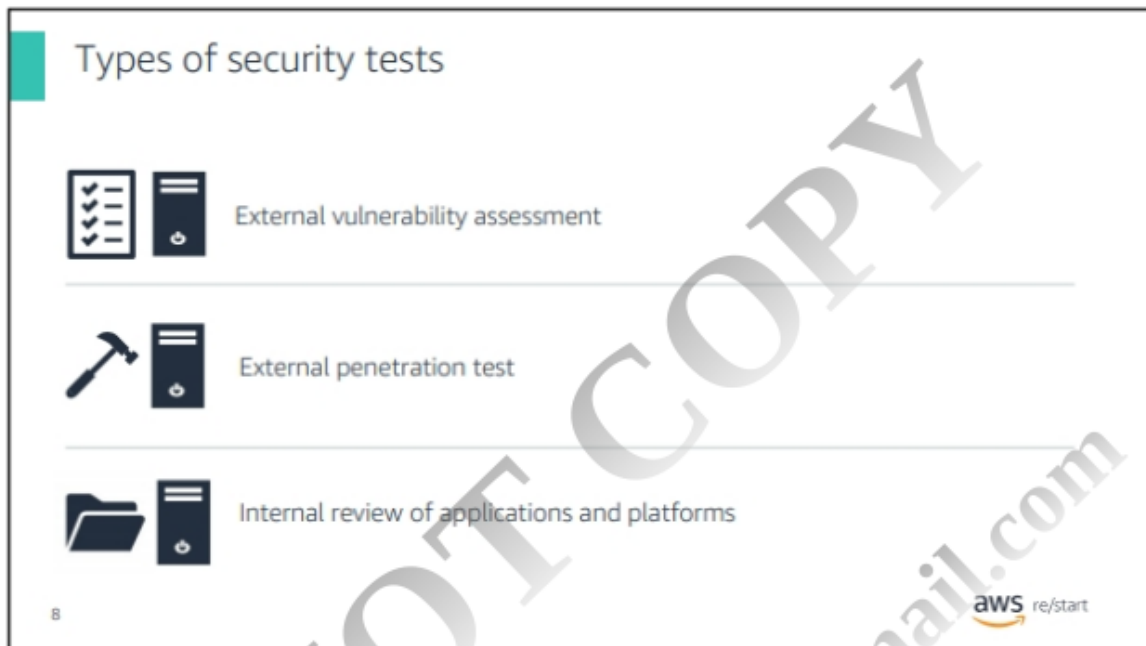


- Ensure that each threat yields a better security solution, even if no breach occurred.
- Be flexible in adding to the solution.
- Maintain a testing environment to test solutions to potential threats.

7

aws re/start

When you test to simulate attacks, do so in a separate test environment that is representative of your production environment.

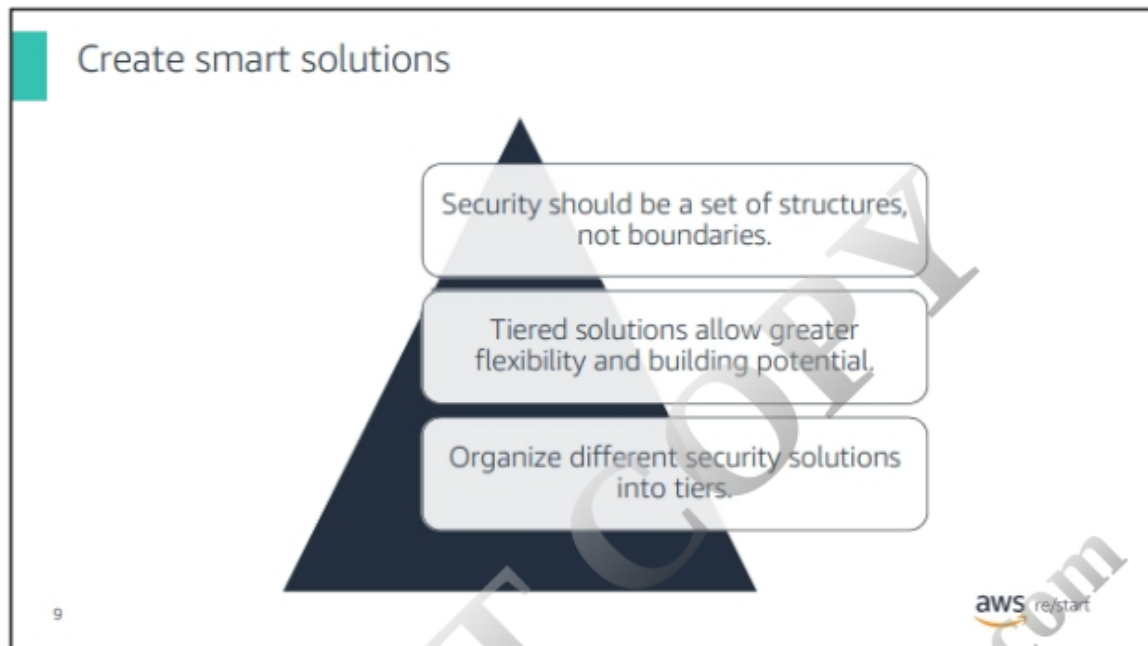


You can conduct security testing during the analysis phase. The types of testing include:

- **External vulnerability assessment** – Third party evaluates system vulnerabilities with little knowledge of the infrastructure and components.
- **External penetration test** – Third party, with little knowledge of the system, actively tries to break into the system in a controlled manner.
- **Internal review of applications and platforms** – A tester with some or full knowledge of the system validates the effectiveness of the following for known susceptibilities:
  - Controls in place
  - Applications and platforms

In the AWS Cloud, AWS customers are encouraged to conduct security assessments or penetration tests against their AWS infrastructure.





As discussed in a previous lesson, a layered or tiered security solution is typically the most effective one.

The Security pillar of the AWS Well-Architected Framework is an example of a blueprint for creating a smart security solution. It provides guidance and best practices for protecting information and systems in the AWS Cloud.

For more information, refer to [Security Pillar - AWS Well-Architected Framework](#) in the *AWS Well-Architected Framework Guide*.

## Root cause analysis (RCA)

Used to identify the root cause of security breaches

Steps to conduct an RCA

1. Identify and describe clearly the fault or problem.
2. Establish a timeline (history of events) from normal situation until the fault or problem occurred.
3. Distinguish between the root cause and causal factors (by using event correlation).
4. Establish a causal graph between the root cause and the fault or problem.

10

aws re/start

A root cause analysis (RCA) is an approach that can be used to provide a clear and accurate answer to the question: How did the breach happen?