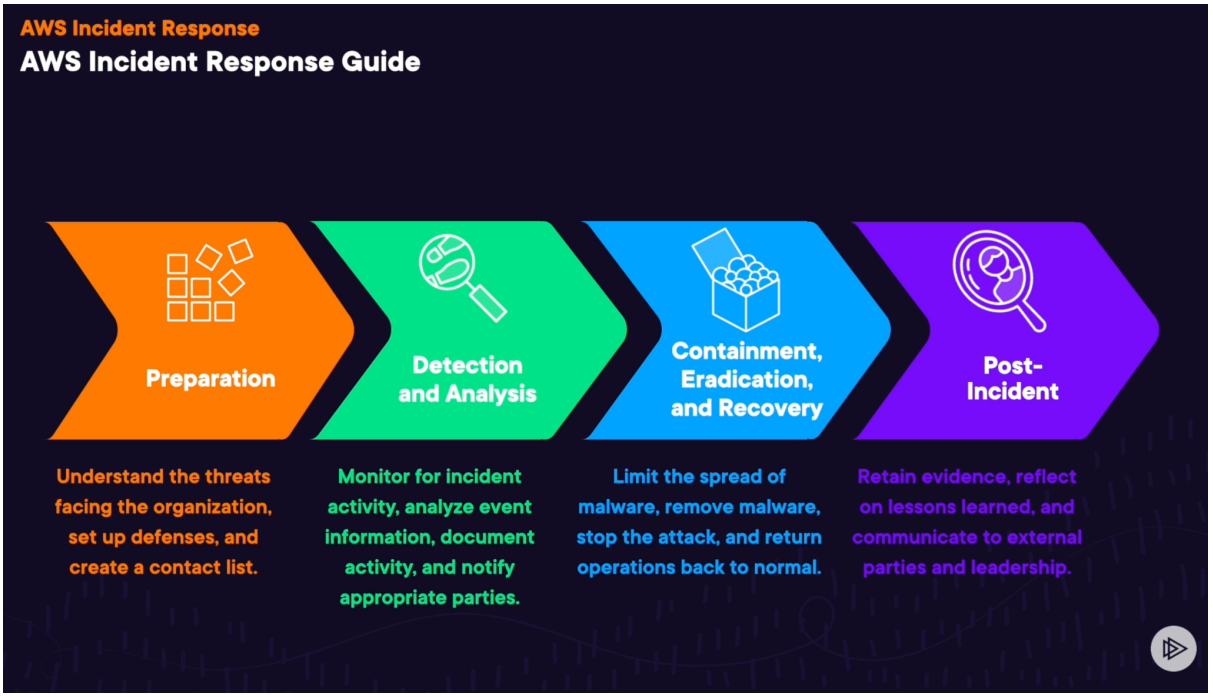
# Incident response

Even with mature preventive and detective controls, your organization should implement mechanisms to respond to and mitigate the potential impact of security incidents. Your preparation strongly affects the ability of your teams to operate effectively during an incident, to isolate, contain and perform forensics on issues, and to restore operations to a known good state. Putting in place the tools and access ahead of a security incident, then routinely practicing incident response through game days, helps ensure that you can recover while minimizing business disruption

The foundation of a successful incident response program in the cloud is Preparation, Operations, and Post-incident activity.

1. **Preparation:** Prepare your incident response team to detect and respond to incidents within AWS by enabling detective controls and verifying appropriate access to the necessary tools and cloud services. Additionally, prepare the necessary playbooks, both manual and automated, to verify reliable and consistent responses.
2. **Operations:** Operate on security events and potential incidents following NIST's phases of incident response: detect, analyze, contain, eradicate, and recover. (Second and third stages in the picture below.)
3. **Post-incident activity:** Iterate on the outcome of your security events and simulations to improve the efficacy of your response, increase value derived from response and investigation, and further reduce risk. You have to learn from incidents and have strong ownership of improvement activities.




## 1. Preparation

### Develop incident management plans

The first document to develop for incident response is the incident response plan. The incident response plan is designed to be the foundation for your incident response program and strategy.

The incident response plan should be in a formal document. An incident response plan typically includes these sections:

- **An incident response team overview**: Outlines the goals and functions of the incident response team.
- **Roles and responsibilities**: Lists the incident response stakeholders and details their roles when an incident occurs.
- **A communication plan**: Details contact information and how you communicate during an incident.
- **Backup communication methods**: It's a best practice to have out-of-band communication as a backup for incident communication. An example of an

application that provides a secure out-of-band communications channel is AWS Wickr.

- **Phases of incident response and actions to take**: Enumerates the phases of incident response (for example, detect, analyze, eradicate, contain, and recover), including high-level actions to take within those phases.
- **Incident severity and prioritization definitions**: Details how to classify the severity of an incident, how to prioritize the incident, and then how the severity definitions affect escalation procedures.

While these sections are common throughout companies of different sizes and industries, each organization's incident response plan is unique. You need to build an incident response plan that works best for your organization.

**Prepare forensic capabilities**

For key information to start building forensics capabilities in the AWS Cloud, see Forensic investigation environment strategies in the AWS Cloud.

Once you have your environment and AWS account structure set up for forensics, define the technologies required to effectively perform forensically sound methodologies across the four phases:

- **Collection**: Collect relevant AWS logs, such as AWS CloudTrail, AWS Config, VPC Flow Logs, and host-level logs. Collect snapshots, backups, and memory dumps of impacted AWS resources where available.
- **Examination**: Examine the data collected by extracting and assessing the relevant information.
- **Analysis**: Analyze the data collected in order to understand the incident and draw conclusions from it.
- **Reporting**: Present the information resulting from the analysis phase.

**Develop and test security incident response playbooks**

*Details are in separate document.*

**Run simulations**

As organizations grow and evolve over time, so does the threat landscape, making it important to continually review your incident response capabilities. Running simulations (also known as game days) is one method that can be used to perform this assessment. Simulations use real-world security event scenarios designed to mimic a threat actor's tactics, techniques, and procedures (TTPs) and allow an organization to exercise and evaluate their incident response capabilities by responding to these mock cyber events as they might occur in reality.

Further information about this topic, with implementation guidance: link

## 2. Operations

Operations is the core of performing incident response. This is where the actions of responding and remediating security incidents occur. Operations includes the following five phases: *detection*, *analysis*, *containment*, *eradication*, and *recovery*.

## 3. Post-incident activity

**Establish a framework for learning from incidents**

Guidance and steps are here: link

## Confluence templates

Post incident review: link
Incident communication: link

Sources:
https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/incident-response.html

Cloud Guru Security Specialty