SWIMLANE

Getting Started with DFIR for the Cloud

Typical digital forensics procedures and incident response plans (IRPs) generally assume traditional physical systems architecture and physical access to systems under investigation.

To address workloads running in the cloud, modern digital forensics and incident response (DFIR) plans must account for systems that are virtual and located off premises.

The Incident Response Plan

Preparation

Ensures readiness for the DFIR plan phases: Detection, Containment, Eradication and Recovery

- DFIR plan is prepared for all situations.
- Personnel are trained and practiced.
- Infrastructure, software and other resources are ready.

Detection

Handles the initial identification and triage of an incident and establishes detailed investigation and documentation.

- Monitor configuration management, usage and costs, API usage and all user policy changes.
- Leverage your cloud provider for SIEM-like logging and threat detection services.
- Know what's available for memory collection in your cloud environment.

Containment

Protects the organization by preventing the incident from increasing in severity or scope

- Expect network modifications to be primarily based on access control lists (ACLs) instead of physical network changes or network routing modifications
- Create security groups that are ready for just-in-time deployment to limit universal access to all users at all times.

Eradication

Eliminates the root cause of the incident, both to secure affected assets and to prevent further breaches.

- Redeploy, update and patch affected containers and any serverless applications.
- Restrict network connections and mapped storage to prevent spreading the infection if the asset is compromised again.
- Enable enhanced monitoring to ensure the asset's usage, costs and logs fall within acceptable parameters.

Recovery

Restores pre-incident functionality to affected systems.

- Restore virtual systems from snapshots or backup.
- Review MAC and/or IP addresses to ensure they are returned to their previous configuration after restoring.
- Review account roles and policies as these could have been restored to an outdated configuration.

Lessons Learned

Reviews the incident and focuses on improving processes and procedures.

- Create an incident report based on the timeline of the incident and collate all documentation obtained during incident response.
- Gather the DFIR team and analyze the incident as a group to discover what worked well and what could be improved.
- Document everything to make it easier to do comparisons, identify gaps and enact changes.
- Drill regularly to evaluate the IR plan from start-to-finish in a controlled setting and to prepare the team for actual incidents.