GitHub @deezombiedude612

VIII. CLOUD FORENSICS

Cloud Forensics

may mean performing computer forensics:
↳ of VMs hosted in the cloud
↳ on cloud environment hosted by cloud service providers (CSPs)

Forensics on Cloud Environment

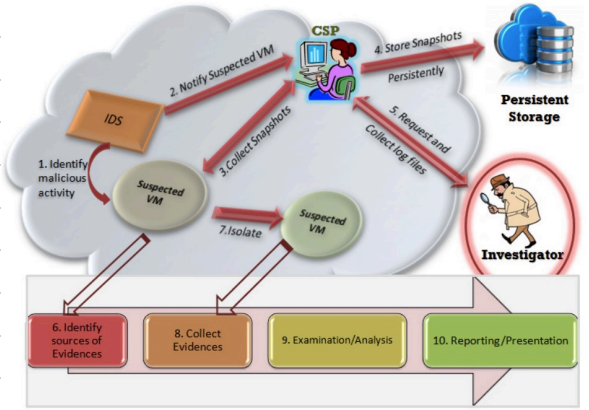
1. establish asset inventory
   ↳ know what you have (ex. # VMs)
2. enable logging & send logs to SIEM
   ↳ ↗ logs, ↗ forensic investigations
   ↳ just right amt of logging (↘ too much, ↘ too little — bandwidth & storage overhead vs info extensivity)
3. deploy & integrate SIEM infra.
   ↳ SIEM for data collection, aggregation, analysis
4. secure SIEM — define & apply secure environment (safety box) for SIEM
5. set up preset creds (only for forensic investigators) to access cloud VMs
6. engineers to build up skills & capabilities — knowledge of cloud tech, etc.
7. continuous improvement - be better & repeat

Forensics in Cloud VM

↗ good if VM & workstation in 2 diff. regions (copying VM internationally ⇒ high cost)

APPLY WHAT YOU KNOW FM COMPUTER FORENSICS

* take snapshots of VMs (instead of imaging in computer forensics)
* prepare forensics workstation (ex., Kali, SIFT)
* attach cloud VM snapshot as read-only
* perform forensics as usual



Rani & Geethakumari. (2015). An Efficient Approach to Forensic Investigation in Cloud using VM snapshots

SOF-ELK

* big data analytics platform tailored for computer forensic investigators & infosec personnel
* customized ver. of open-src Elastic stack, enhancing UX & efficiency
  ↳ incls.: Elasticsearch, Logstash, Kibana, Elastic Beats (filebeat)
* benefit: significant customizations & active development
  ↳ bypass Elastic ELK stack setup (complex!)
* feats:
  ↳ supports various data types (multiple log formats, Netflow)
  ↳ focuses on crucial data parsing & visualization
  ↳ offers numerous predefined dashboards; allows for creating & sharing custom visualizations

SIEM (Security Information & Event Management)

security solution that helps orgs recognize & addr. potential threats & vulns. before they can disrupt business ops. (IBM)

* fn components:
  1. Data Collection: collect log data fm users, endpoints, apps, security hardware\software, etc.
  2. Data Aggregation & Processing: identify & understand intricate data patterns
     ↳ insights impt for locating & mitigating threats
  3. Indexing & Storage: collected logs indexed & stored in efficient format
  4. Analysis & Visualization: consolidate analysis into 1 central dashboard (visualize analysis w UI)
     ↳ to monitor activity, triage alerts, identify threats, & initiate response or remediation
* ELK stack:

Beats (Data Collection) ← logs fm VMs
↓
Logstash (Data Aggregation & Processing)
↓
Elasticsearch (Indexing & Storage)
↑
Kibana (Analysis & Visualization)