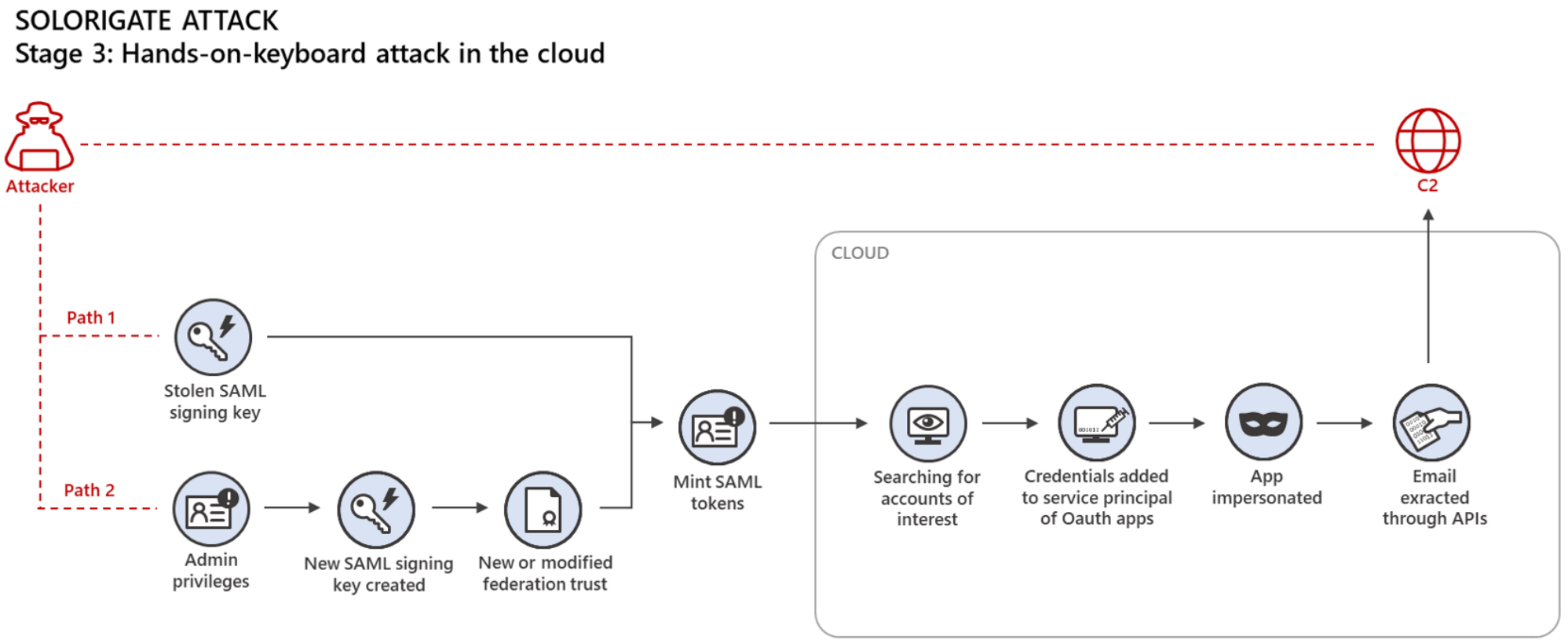
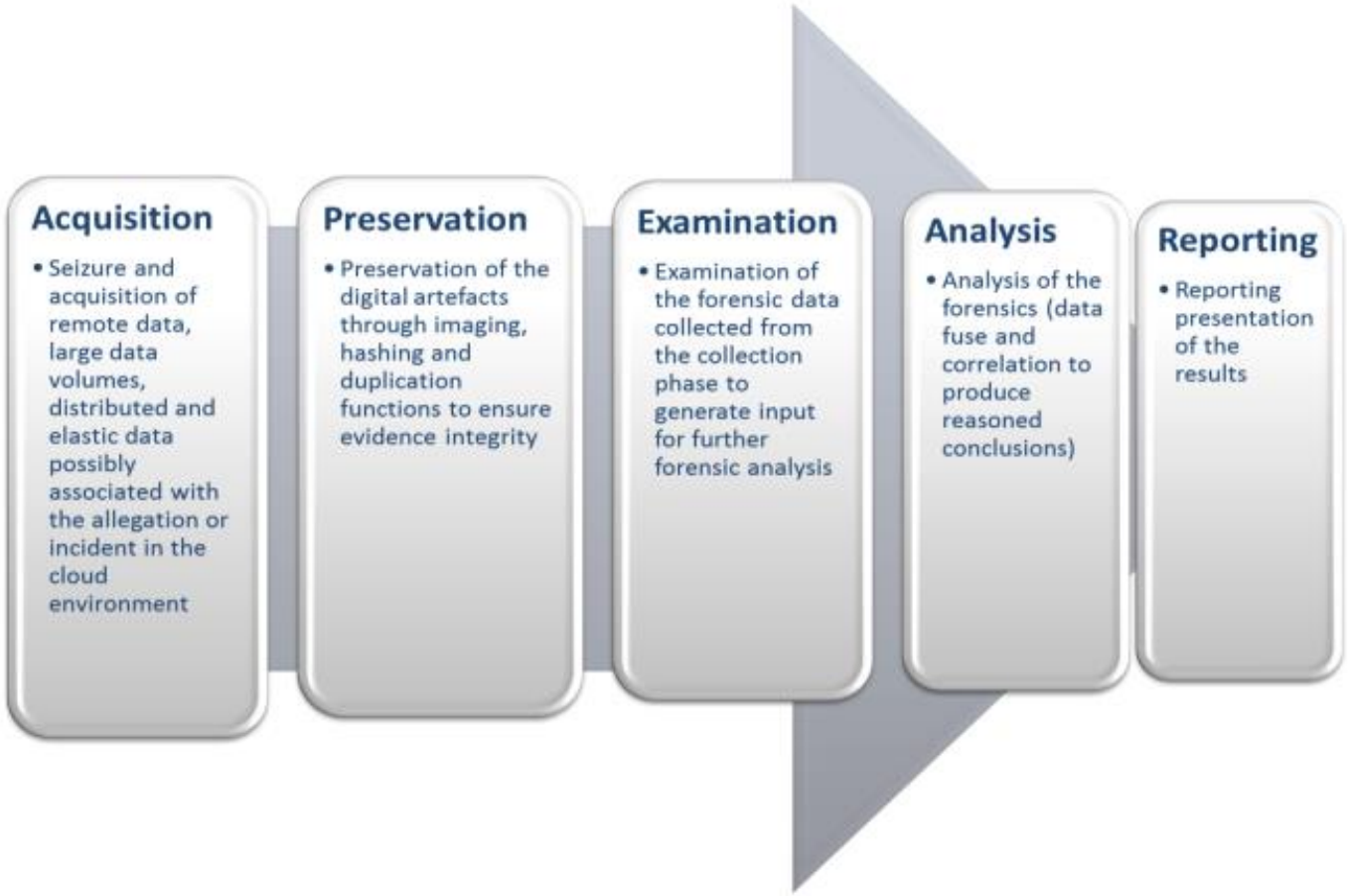
DEPARTMENT OF COMPUTER SCIENCE

CLOUD FORENSIC READINESS

Cloud Related Case



CLOUD FORENSIC STAGES



CLOUD FORENSIC CHALLENGES (NIST IR 8006)

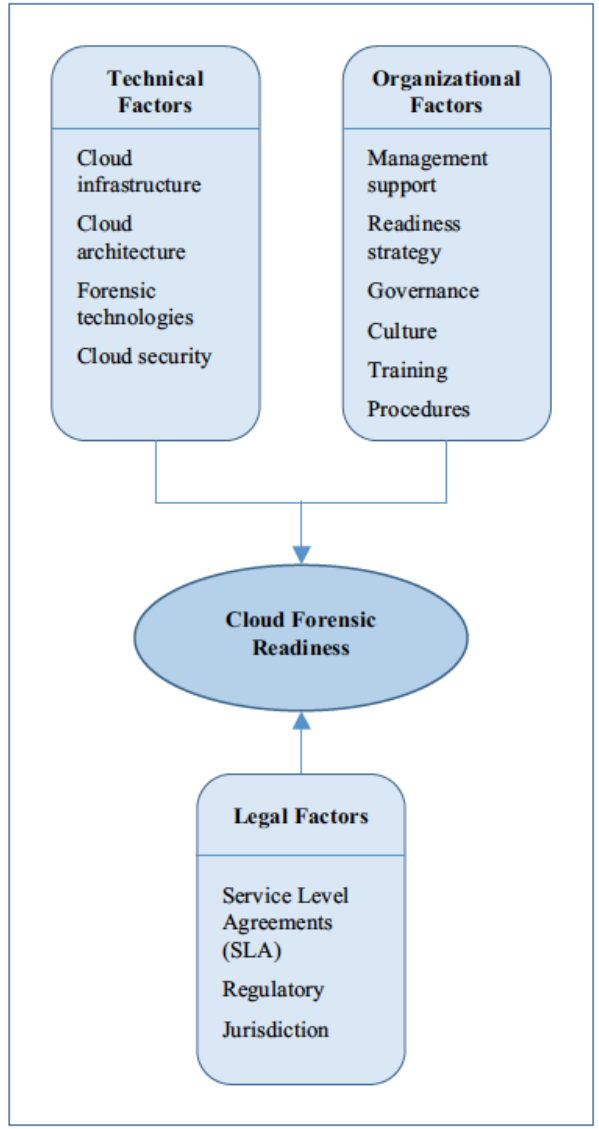
- Architecture
- Data Collection
- Analysis
- Anti-Forensic
- Incident first responders
- Role Management
- Legal
- Standards
- Training

LOUD FORENSIC
IR 8006)

FC ID	Short Title	Challenge	Description	Result of Overcoming Challenge
FC-01	Deletion in the cloud	Recovering data deleted from the cloud (by either the Provider, Consumer, or attacker) and attributing that data to a specific user	Deletion in the cloud is often based on the deletion of nodes pointing to information in virtual instances. Pathways for retrieval of the deleted information are dependent on cloud Providers offering sufficiently sophisticated mechanisms for access. Once the data is recovered, it remains a challenge to attribute specific data items to an individual user given the fact that cloud-based storage is a shared service in a multi-tenant environment.	If this challenge were overcome, it would be easier to recover deleted data and to attribute that recovered data to a specific user.
FC-02	Recovering overwritten data	Recovery of deleted data that has been overwritten by another user in a shared virtual environment	Recovery of data marked as deleted (i.e., for which the nodes pointing to it are deleted) is difficult if the data is overwritten by another user in a shared virtual environment. Note: Data can be overwritten by the same user or another user. If the latter, attributing ownership is difficult.	If this challenge were overcome, it would be easier to recover deleted data that has been overwritten and to attribute that recovered data to a specific user.

CLOUD FORENSIC READIN

- Technical Factors
  - Cloud Infrastructure
  - Cloud Architecture
  - Forensic Technologies
  - Cloud Security
- Legal Factors
  - SLA
  - Regulatory
  - Jurisdiction
- Organisational Factors
  - Management Support
  - Readiness strategy
  - Governance
  - Culture

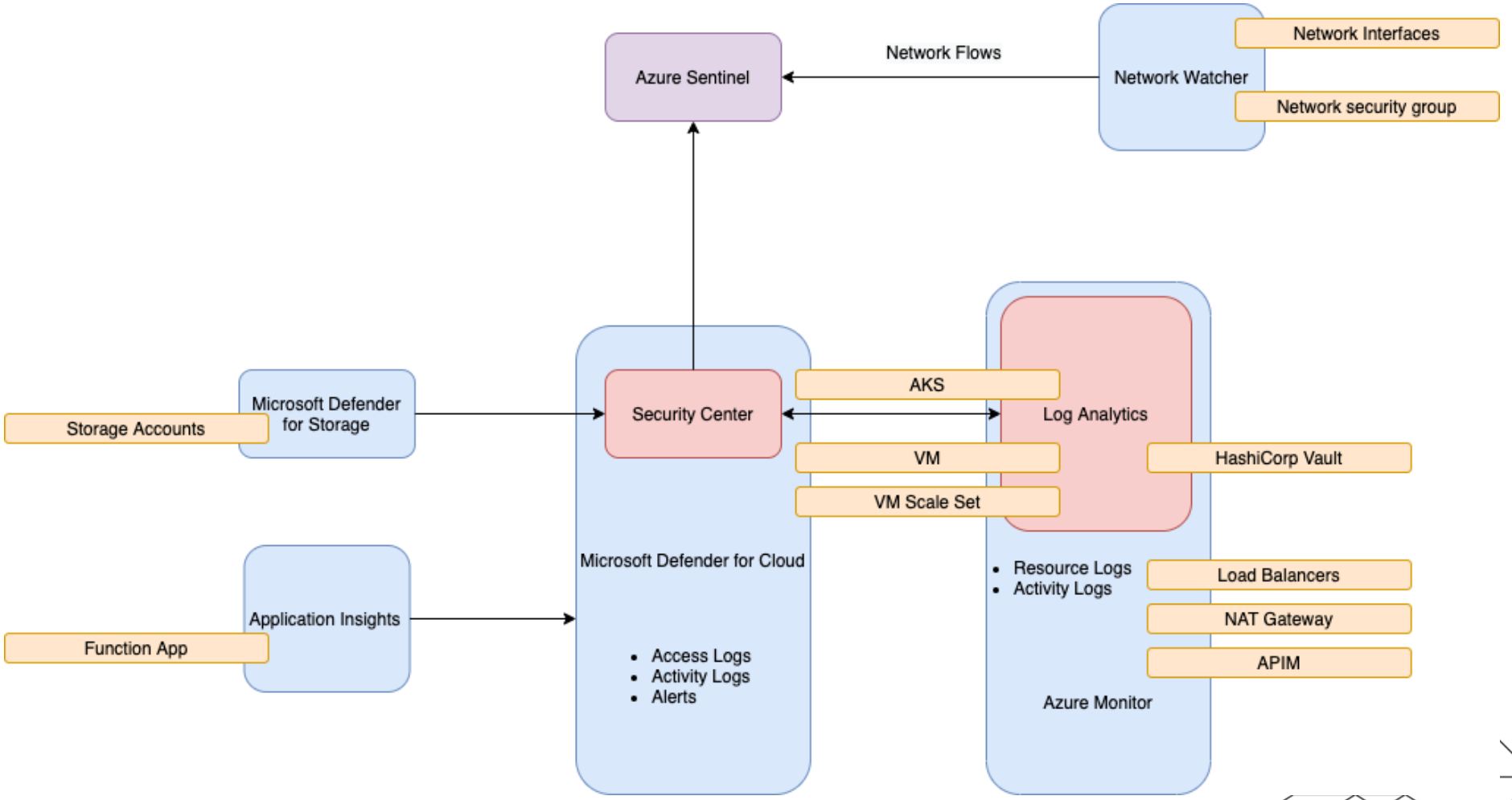


FORENSIC READINESS MODELS

Study	Forensics Readiness Factors												
	Technical Factors				Legal Factors			Organizational Factors					
	Infrastructure	Architecture	Technologies	Security	SLA	Regulatory	Jurisdiction	Management support	Strategy	Governance	Culture	Training	procedure
Grobler et al. [19]	√		√			√	√			√	√	√	√
Elyas et al [20]		√	√			√		√		√	√	√	
Elyas et al. [21]	√	√	√			√		√		√	√	√	
Sibiya et al. [25]	√		√	√									
Makutsoane & Leonard [27]			√		√		√		√				√
Kebande & Venter [28]		√	√	√			√						
Moussa et al. [29]			√	√			√		√	√		√	√
Ab Rahman et al. [30]	√		√	√		√	√		√				
ACPO [31]												√	√
CSA [32]		√		√	√	√	√						√
ENISA [33]			√		√		√						√
ISO [34]		√		√			√						√

AZURE

MAIN POINTS / EXAMPLE



- Architecture
- Licensing
- Technologies

TECHNICAL FACTORS

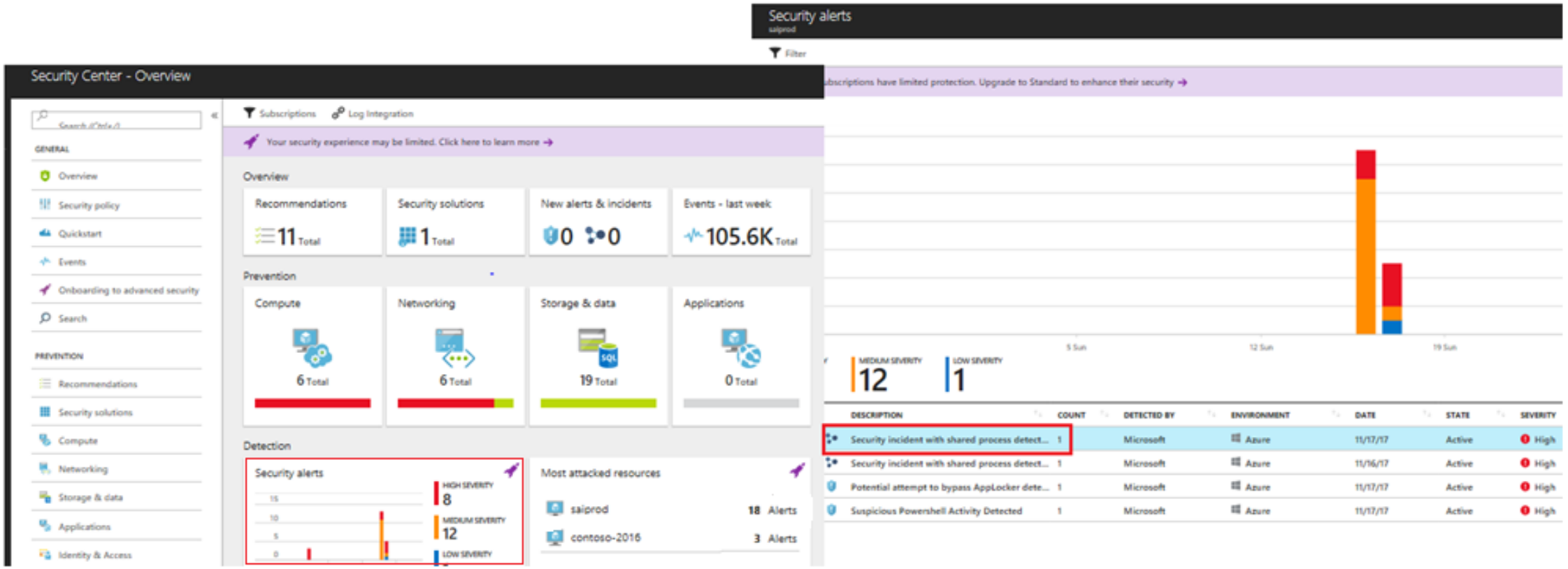
LICENSING

CURITY MONITORIN

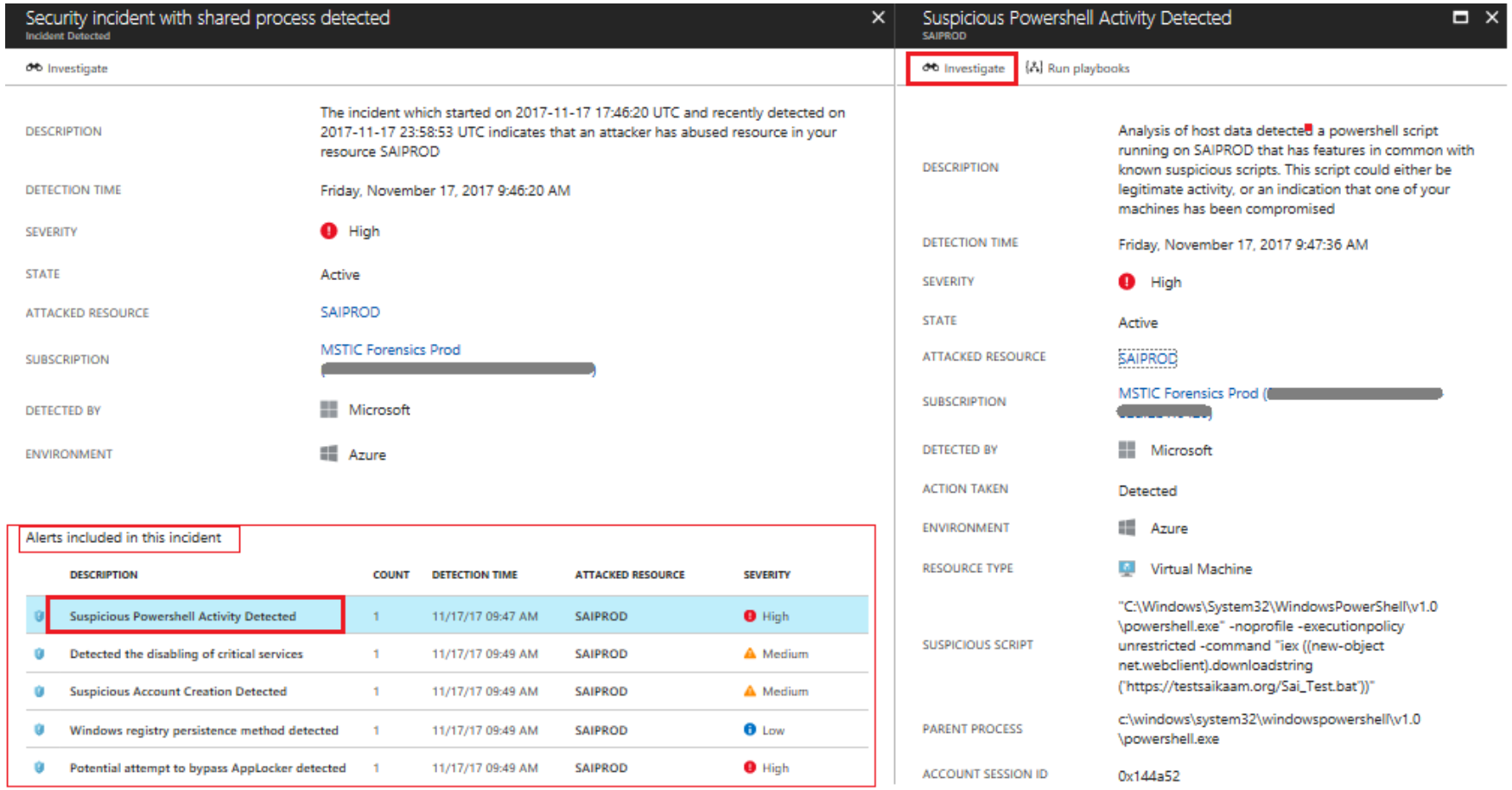
- Security Center
- Defender for Cloud - $0.02/Server/hour
- Defender for Storage - $0.02/10K transactions
- Network Watcher
- Monitor – Data Retention - $0.143 per GB/m
- Log Analytics - $3.28 per GB
- Sentinel

Feature	Free units included	Price
Network Logs Collected[1]	5 GB per month	**$0.50** per GB
Network Diagnostic Tools[2]	1,000 checks per month	**$0.001** per 1,000 checks
Connection Monitor[5]	10 tests per month	0-10 tests - Included 10-240,010 tests - **$0.30** per test per month 240,010-750,010 tests - **$0.10** per test per month 750,010-1,000,010 tests - **$0.05** per test per month 1,000,010+ tests - **$0.02** per test per month
Network Performance Monitor – Service Connectivity Monitor	- -	**$3** per connection per month
Network Performance Monitor – Performance Monitor	10 per connection per month	0-10 connections - Included 10-240,010 connections - **$0.30** per connection metric per month 240,010-750,010 connections - **$0.10** per connection metric per month 750,010-1,000,010 connections - **$0.05** per connection metric per month 1,000,010+ connections - **$0.02** per connection metric per month
Network Analytics[3]	- -	See Azure Monitor Log Analytics pricing
Traffic Analytics	- -	Accelerated processing at 10-min intervals: **$3.50** per GB-processed[4] Standard processing at 60-min intervals: **$2.30** per GB-processed[4]

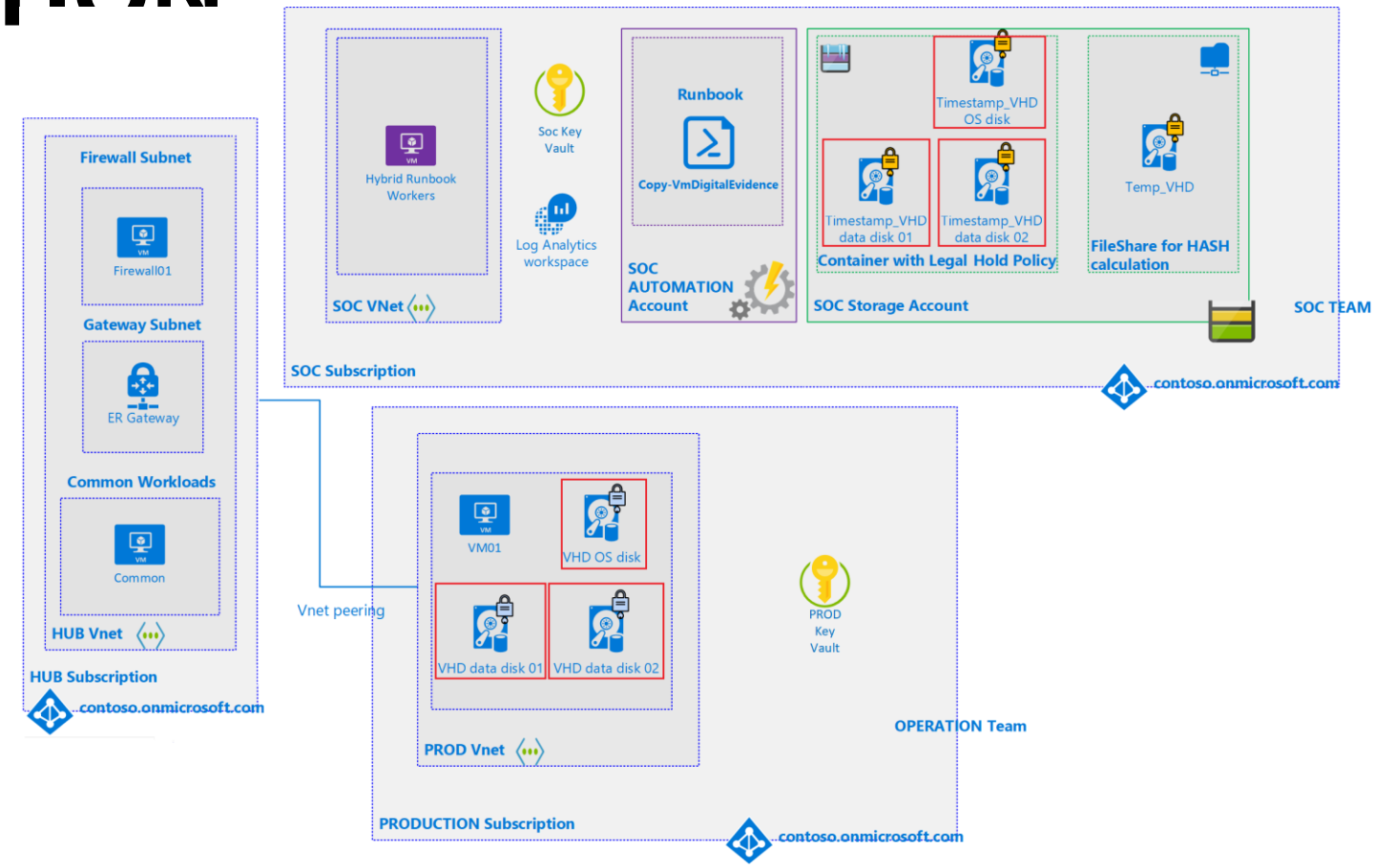
AZURE SECURITY MONITORING EXAMPLE



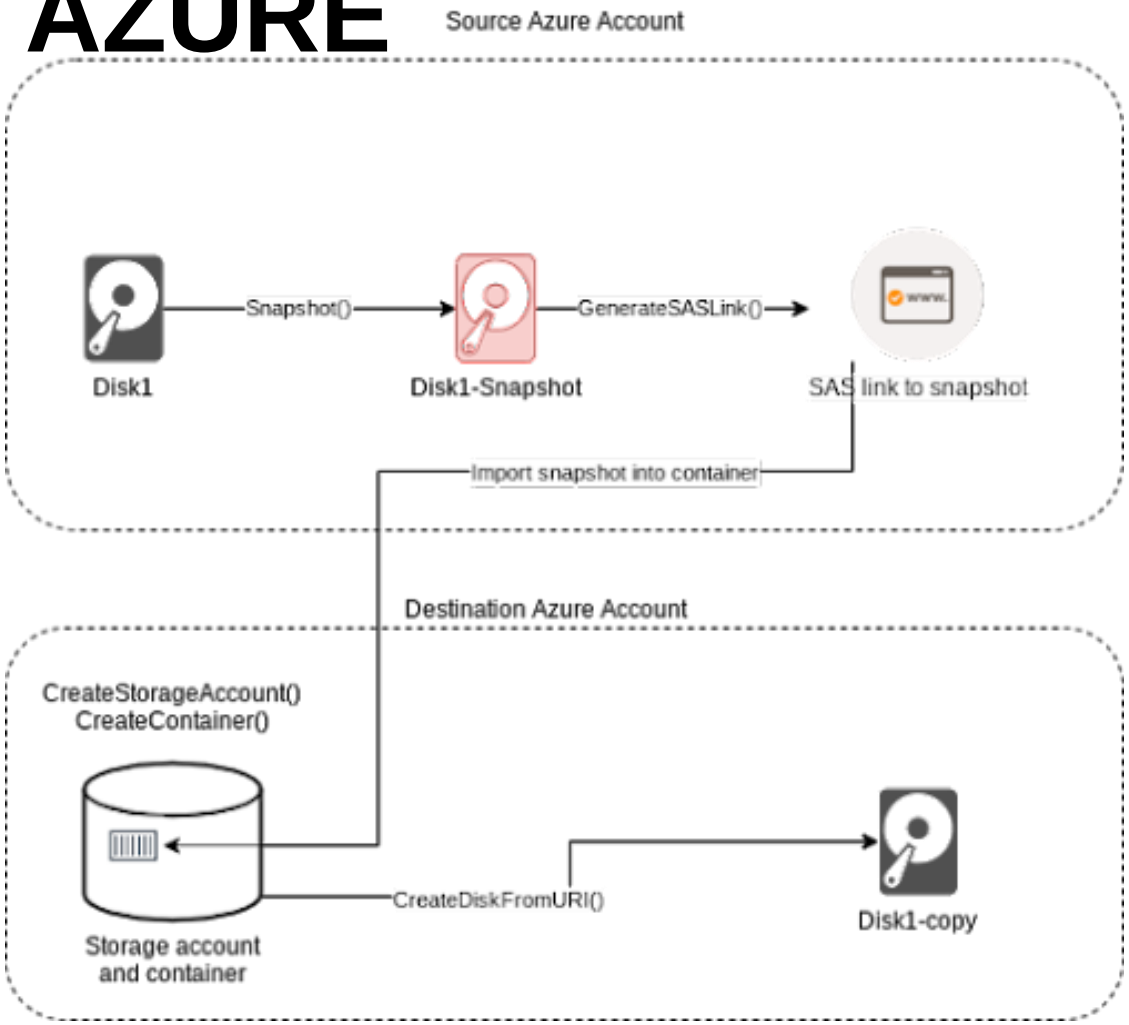
ALERT EXAMPLE



EXAMPLE OF SUGGESTED SOLUTION



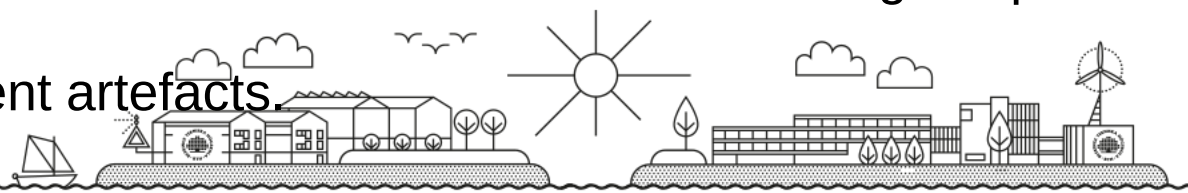
SNAPSHOTTING DISKS IN THE AZURE



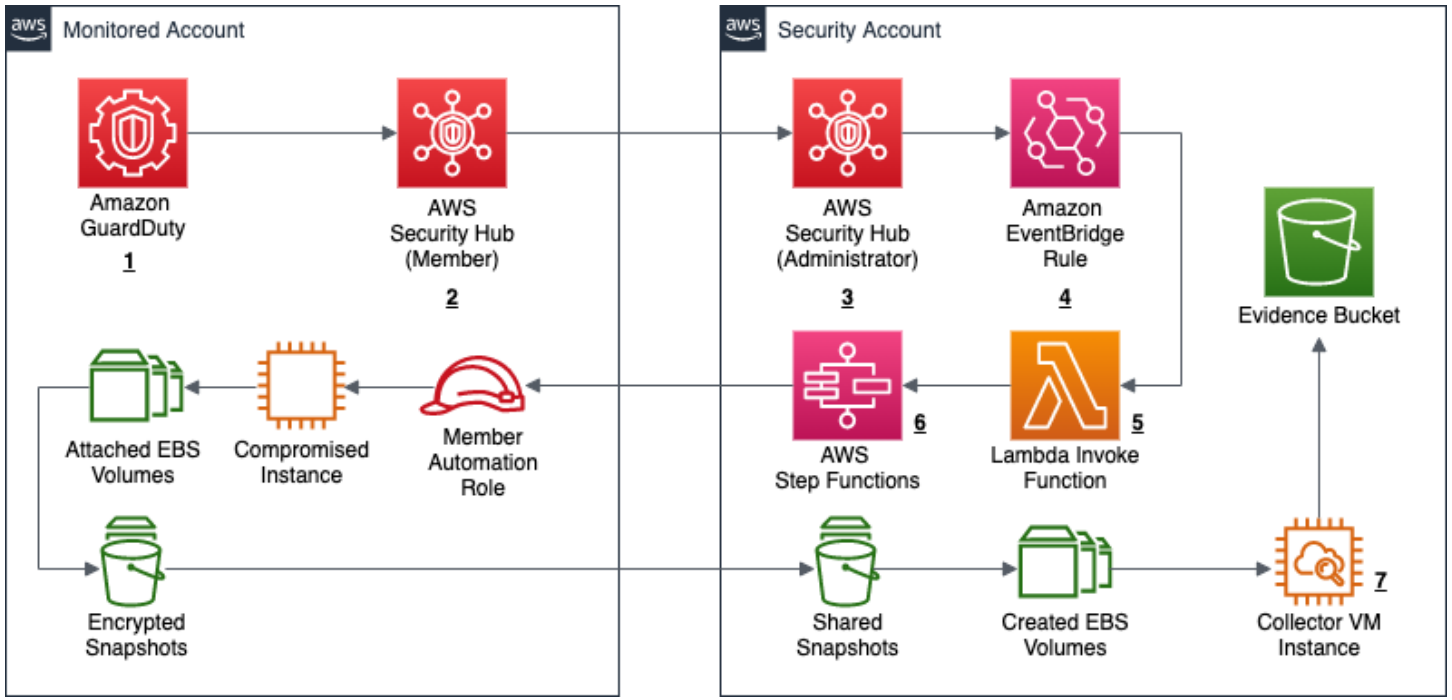
AWS

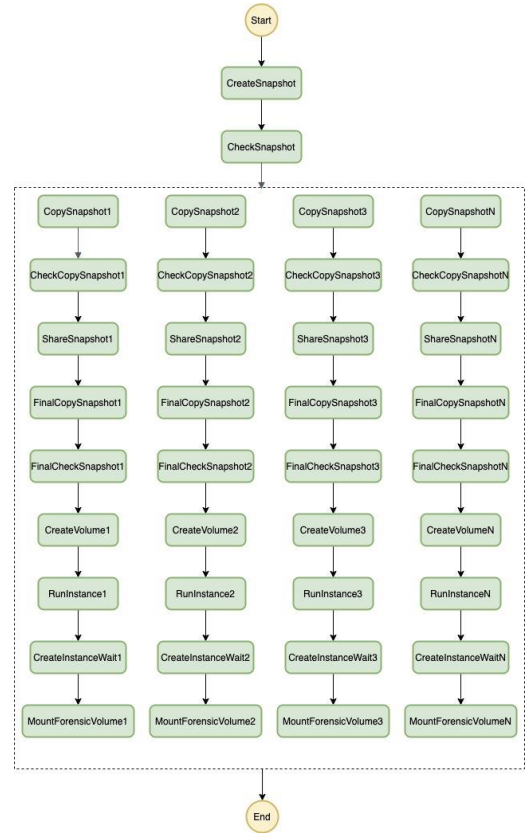
AWS TOOLS

- **AWS Organisations** allows you to create separate accounts along business lines or mission areas which also limits the “blast radius” should a breach occur; for governance, you can apply policies to each of those sub accounts from the AWS master account.
- **Security Groups** enables isolation of Amazon EC2 instances.
- **AWS CloudTrail** provides a history of AWS API calls that can assist in response and trigger automated detection and response systems.
- **VPC Flow Logs** enables you to capture information about the IP traffic going to and from network interfaces in your VPC.
- **Amazon GuardDuty** is a managed threat detection service that continuously monitors for malicious or unauthorised behaviour.
- **Amazon CloudWatch Events** triggers different automated actions from changes in AWS resources including CloudTrail.
- **AWS Step Functions** coordinates a sequence of steps to automate an incident response process.
- **AWS Cloud Formation** automates the creation of trusted environments for conducting deeper investigations.
- **Amazon S3** stores snapshots and related incident artefacts.

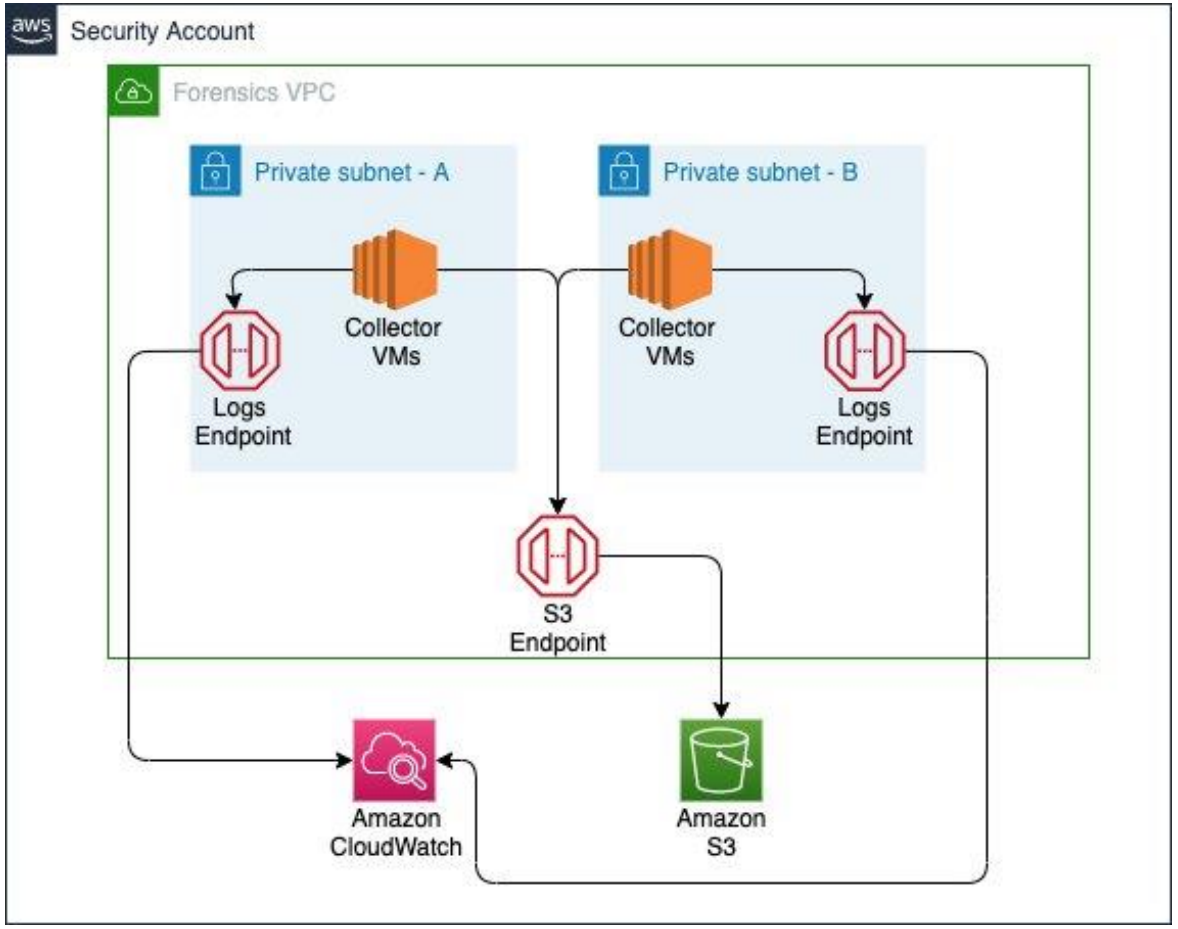


SNAPSHOTTING DISKS IN THE AWS



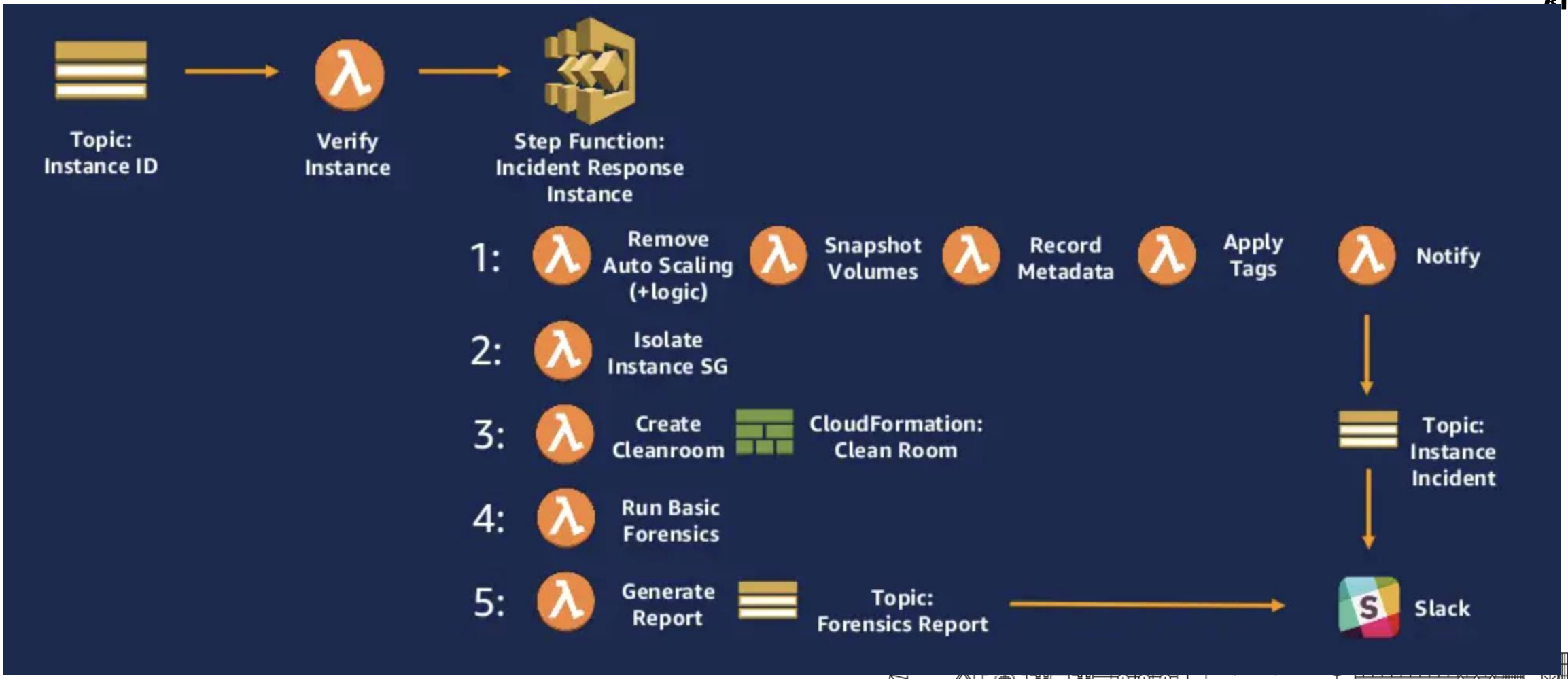


DISK FORENSIC AUTOMATION



https://aws.amazon.com/blogs/security/how-to-automate-forensic-disk-collection-in-aws/

EC2 AUTO CLEAN ROOM FORENSIC



OUR TRAINERSUR EXPERIENCE

- BlackEnergy
- LockerGoga
- NotPetya
- …

Dr. Anders Carlsson is an expert with more than 30-years of experience in cybersecurity, forensic investigations, and network security.

Dr. Oleksii Baranovskyi is an experienced cyber security expert with a demonstrated history of working in the academic as well as the financial industry.