AWS Security Series

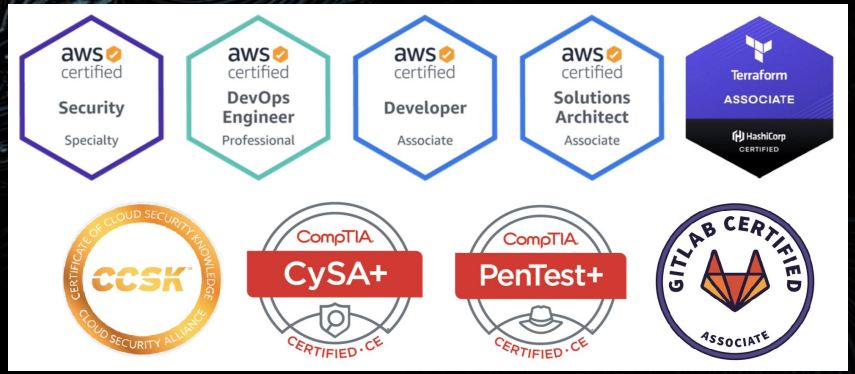
Part 4: AWS S3 Security: Fundamentals of Data Protection in Cloud

Nitin Sharma
CyberSecurity and DevSecOps Engineer
LinkedIn: linkedin.com/in/nitins87
Quora: quora.com/profile/NitinS-1
Blog: 4hathacker.in

Contents

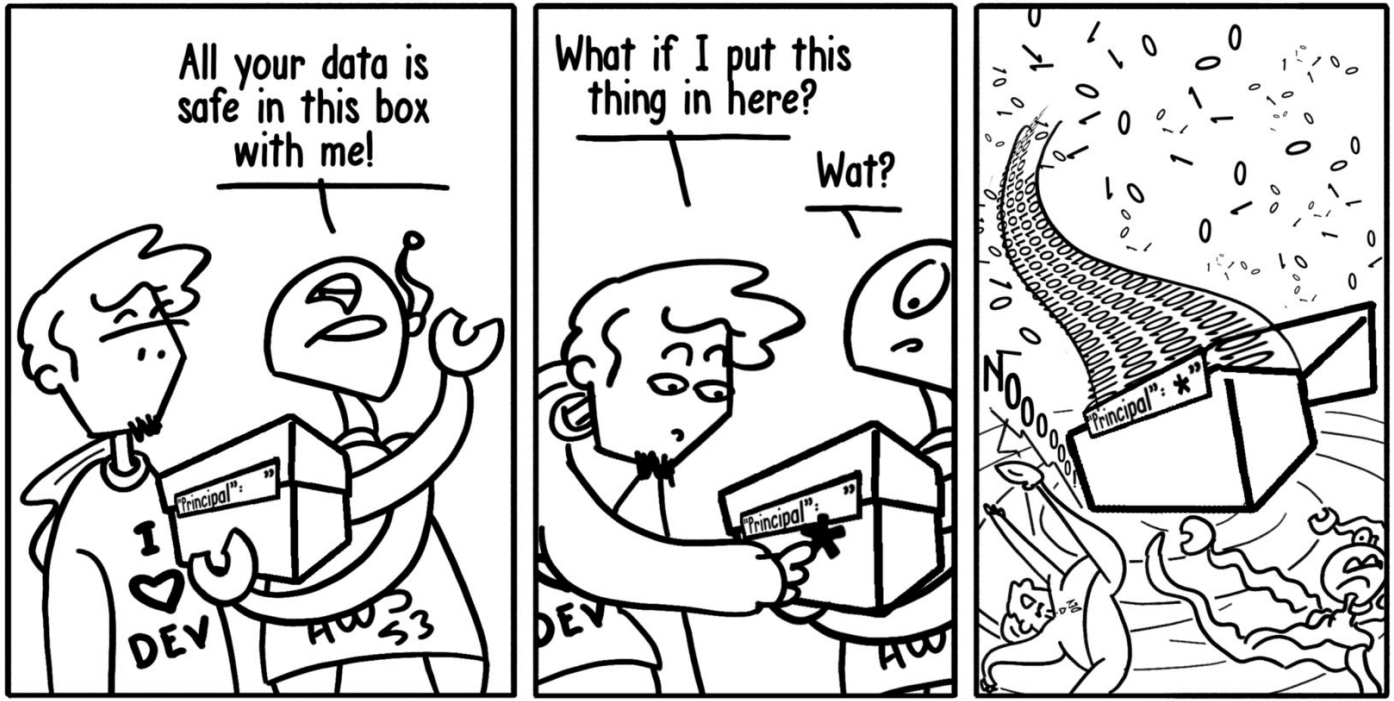
$ whoami

- Cybersecurity and DevSecOps professional experienced in Cloud Security, Container Security and DevOps Research
- Certifications:



- Published author for "Securing Docker - The Attack & Defense Ways" book under CyberSecrets Publication
- Half Marathon runner, Cyclist and Fitness Enthusiast
- Helping out beginners in Cloud, DevOps and CyberSec at Quora

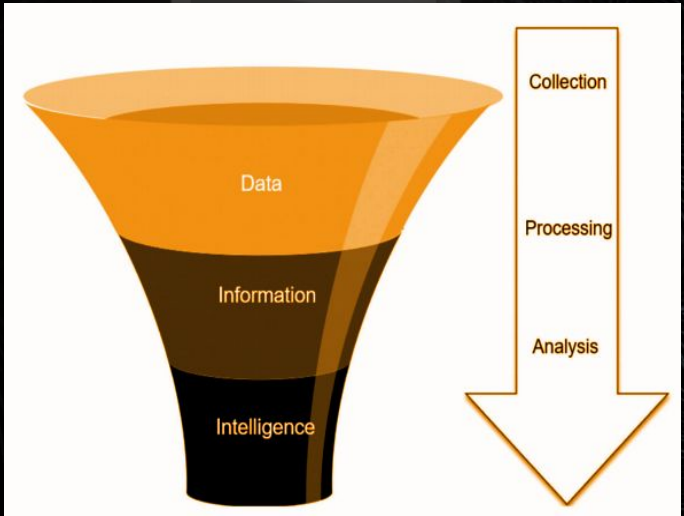
$ whoami (finding mistakes in the past)



© TotalCloud Inc. | https://TotalCloud.io

$ Data vs Information

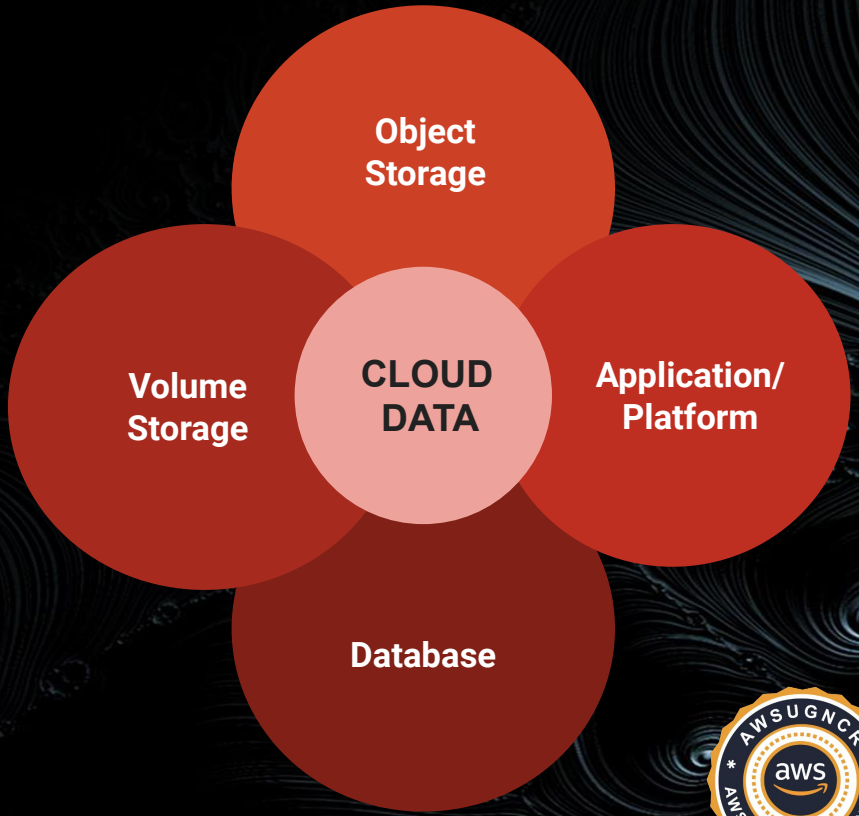
- **Data**: raw, unprocessed & plain facts.
- **Information**: processed, organised and structured form of data.
- **Knowledge/Intelligence**: processing and analysis of information that helps in business decisions.



(Source: CREST Cyber Threat Intelligence)

$ Cloud Data Storage Fundamentals

- **Object Storage**: Objects are typically files which are then stored using a cloud platform specific mechanism and accessible through API calls.
- **Volume Storage**: This is essentially a virtual hard drive for instances/virtual machines.
- **Database**: Cloud Platforms and Providers may support variety of different kinds of databases.
- **Application/Platform**: Examples of these would be a content delivery network, files stored in SaaS, caching, etc.



$ Cloud Data Security LifeCycle

- **Create**: This is probably better named Create/Update because it applies to creating or changing a data/content element, not just a document or database.

- **Store**: Storing is the act committing the digital data to some sort of storage repository, and typically occurs nearly simultaneously with creation.

- **Use**: Data is viewed, processed, or otherwise used in some sort of activity.

- **Share**: Data is exchanged between users, customers, and partners.

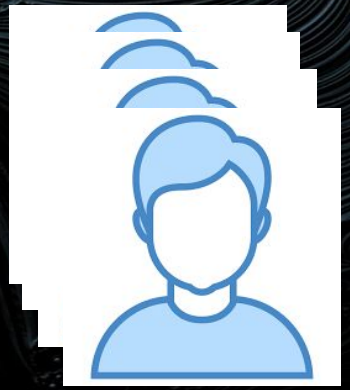
- **Archive**: Data leaves active use and enters long-term storage.

- **Destroy**: Data is permanently destroyed using physical or digital means (*e.g.*, crypto-shredding).

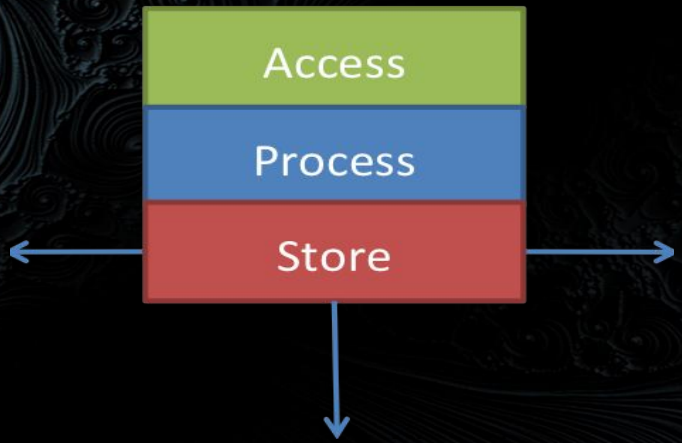
(Source: Securosis Blog)

$ Cloud Data Security Controls

Actors



Functions



Locations

Controls

	Create	Store	Use	Share	Archive	Destroy
Access	X	X	X	X	X	X
Process	X		X			
Store		X			X	

(Source: Securosis Blog)

$ AWS S3 Introduction - Level 100

- S3 stands for **Simple Storage Service**
- **S3 Bucket:** A container for uploaded data which must have a unique name.
- **S3 Object:** Item stored within a bucket which is identified by key and version ID.
- **S3 Policy:** JSON Based Access control statement.
- **S3 Bucket ACLs:** sub-resource that's attached to every S3 bucket and object. It defines which AWS accounts or groups are granted access and the type of access. When you create a bucket or an object, Amazon S3 creates a default ACL that grants the resource owner full control over the resource.

$ AWS S3 Introduction - Level 100

Let’s take a small trip to AWS S3...

- How to create an AWS S3 Bucket ?
- How to assign a Policy ?
- How to see security misconfigurations with S3 ?

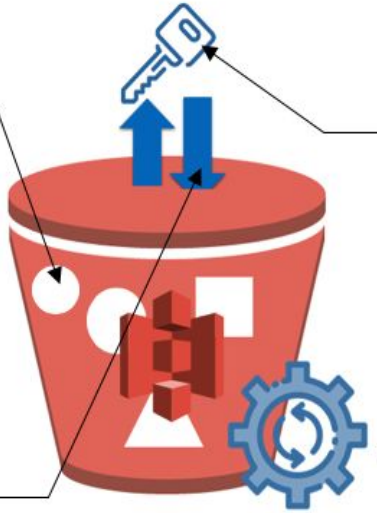
$ AWS S3 - Misconfigurations

Storehouse of Sensitive Data

- Lot of sensitive Data (PII, PCI, PHI, SPI) are stored in the S3 buckets
- Compliance (CCPA, GDPR , etc.) makes data security & integrity extremely critical

Opportunities to break into the bucket

- Leaked / Stolen credentials through GitHub, etc.
- Rogue employees misuse credentials
- Rogue workloads piggybacking on connections, go undetected
- Lateral spread within a VPC



Ease of Accessibility

- No hidden resource
- Everything is visible (using a URL)

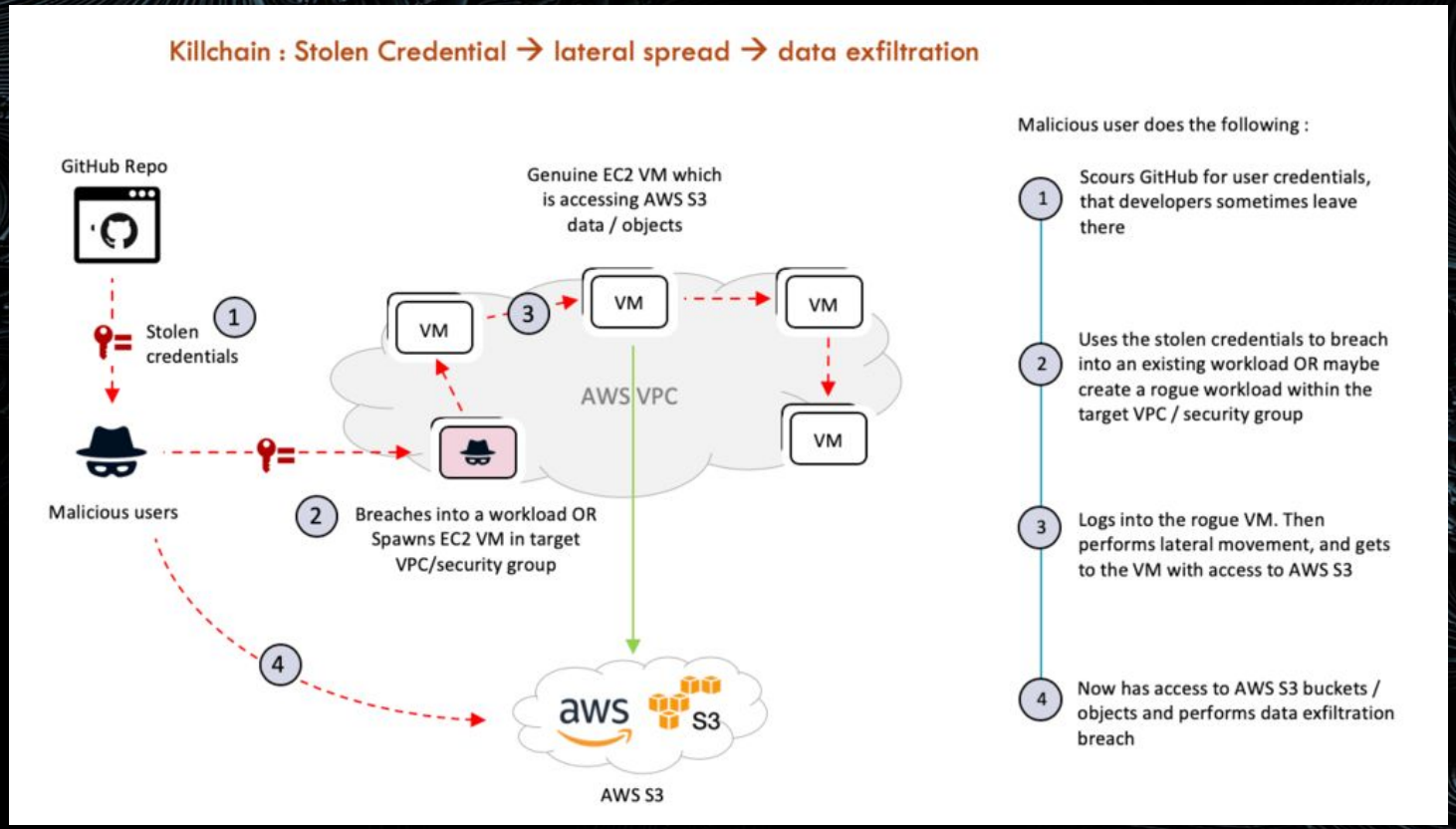
Opportunities for Human Error

- Incorrect bucket / object permissions
- Policy error or Misconfigurations (undetectable)
- Adding sensitive content/object in wrong bucket
- Buckets sometimes unintentionally open to public access

All these issues are hard to detect except at runtime

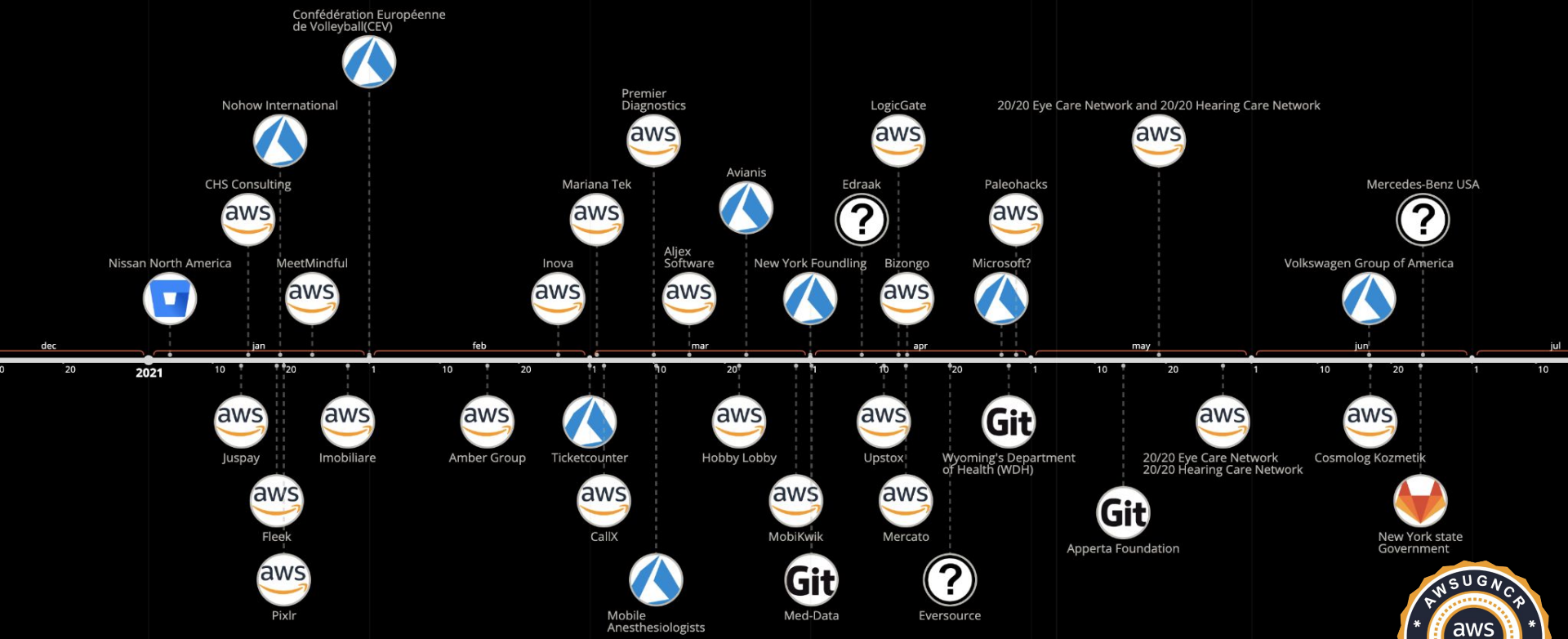
(Source: Mesh7 Blog)

$ AWS S3 - Misconfigurations

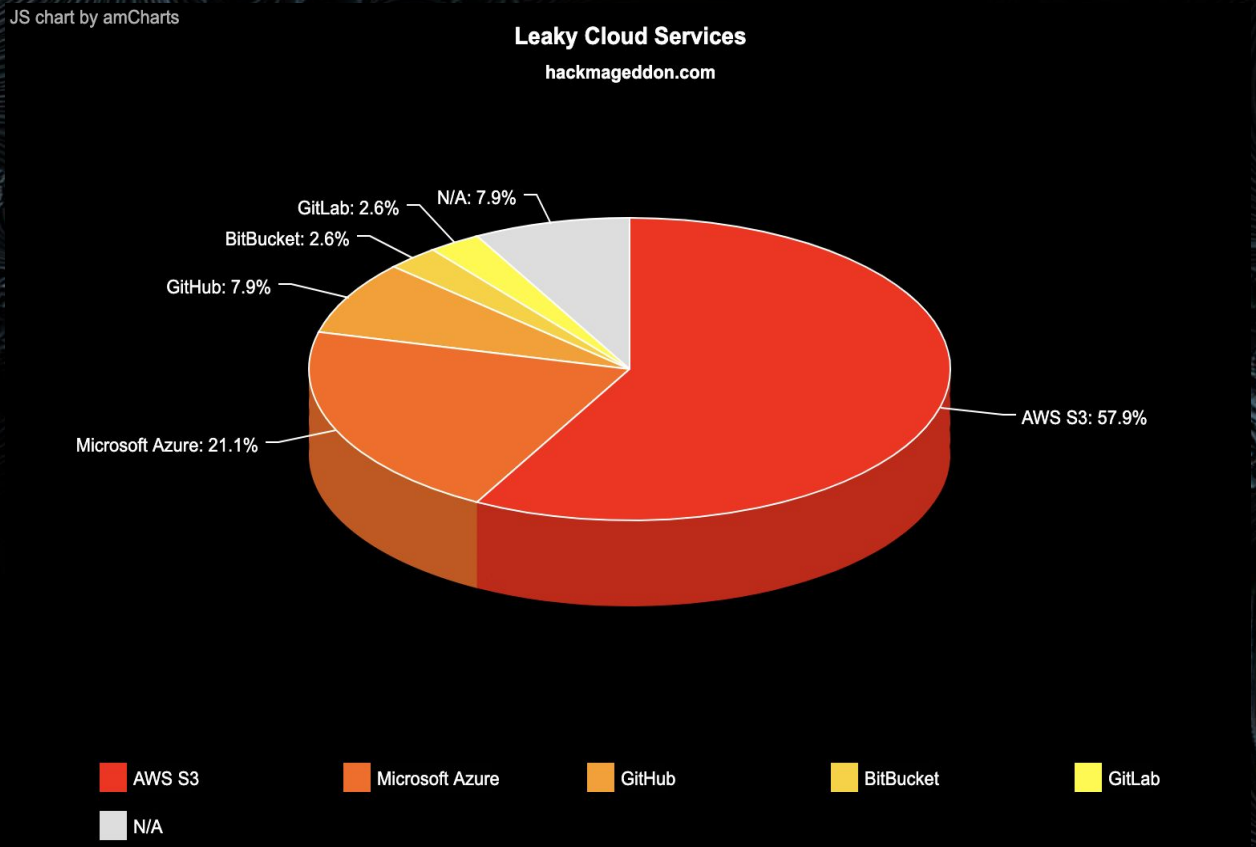


(Source: Mesh7 Blog)

$ Breaches in 2021 (Courtesy: Hackmageddon)



$ AWS S3 Breaches in 2021

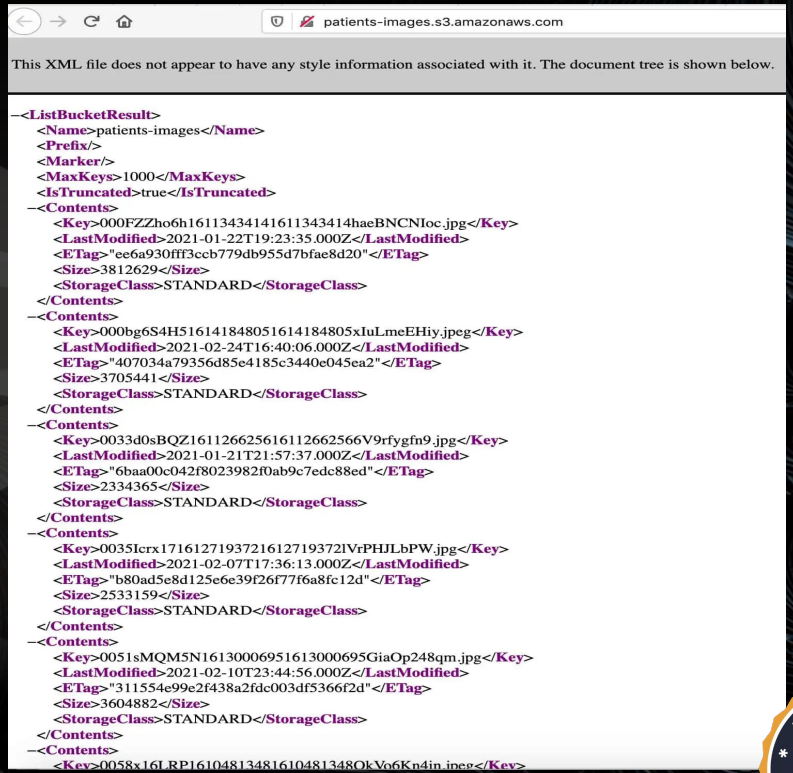


$ AWS S3 Breaches in 2021 - Scenario #1

A coronavirus testing company in Utah exposed more than 50,000 patients' scanned IDs and thousands of COVID-19 test results. [Timeline: Jan-Mar, 2021]

The exposed data was stored in two large Amazon S3 buckets. One bucket named *patient-images* contained 207,524 images of patients' photo ID scans:

- Driver's licenses
- Medical insurance cards
- Passports
- Other forms of ID



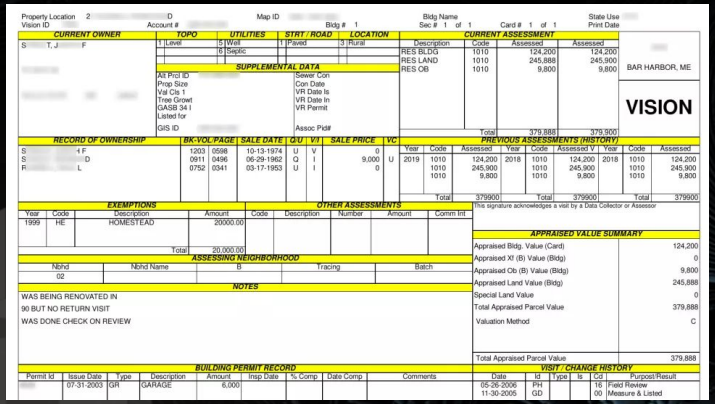
(Source: Comparitech Blog)

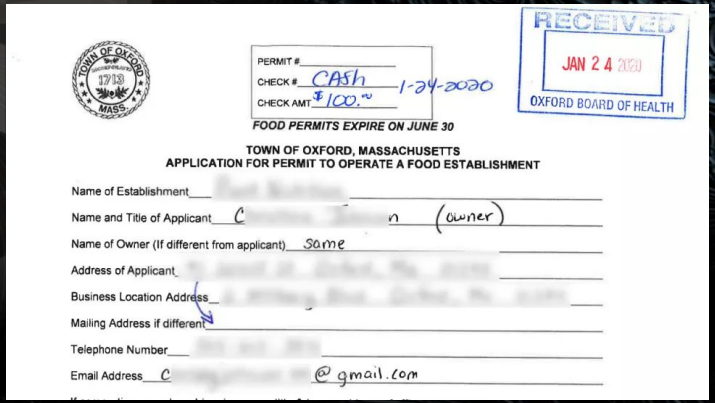
$ AWS S3 Breaches in 2021 - Scenario #2

US municipalities suffer data breach due to misconfigured Amazon S3 buckets. [Timeline - July, 2021]

PeopleGIS had reportedly stored the data of users in several misconfigured Amazon S3 buckets without proper encryption, exposing it to open access.

Out of 114 buckets, 28 appeared to be properly configured, and 86 were accessible without any authentication, accounting for 1000 GB of data and over 1.6 million files.





(Source: TechRadar Blog)

$ AWS S3 Security Best Practices

S3 Security Best Practices

Preventative

- Correct Policies and no Public Access
- Least Privilege Access
- Use of IAM Roles to access S3 Buckets
- Enable MFA Delete
- Encryption at Rest
- Encryption at Transit
- Use S3 Object Lock
- Use S3 Cross Region Replication for backups
- Use VPC endpoints for S3 Access

Monitoring & Auditing

- Identify and Audit all your S3 buckets
- Monitoring S3 Bucket Activity (S3 API calls)
- Enable S3 Server Access Logging
- Use AWS Cloudtrail to record S3 Data Events
- Enable AWS Config to simplify auditing for misconfigurations
- Use AWS Macie to protect sensitive info.
- Check Trusted Advisor

AWSUGNCR * AWS USER GROUP NCR *

Thank You...

For queries feel free to connect with AWS Delhi User Group at:

1. AWS Delhi User Group (MeetUp) - Learn Together, Grow Together
2. AWS User Group Delhi NCR (Follow us on LinkedIn Page)