CyberWarFare Labs

Detection Techniques for Identifying

AWS S3 Targeted Attacks

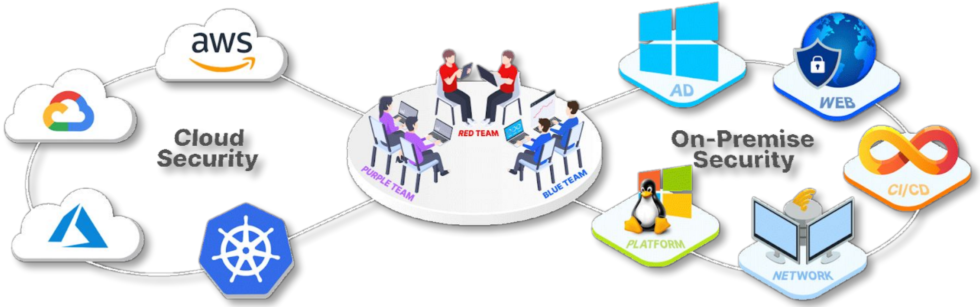
CWL
CyberWarFare Labs

About CyberWarFare Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has two primary divisions :

1. Cyber Range Labs

2. Up-Skilling Platform



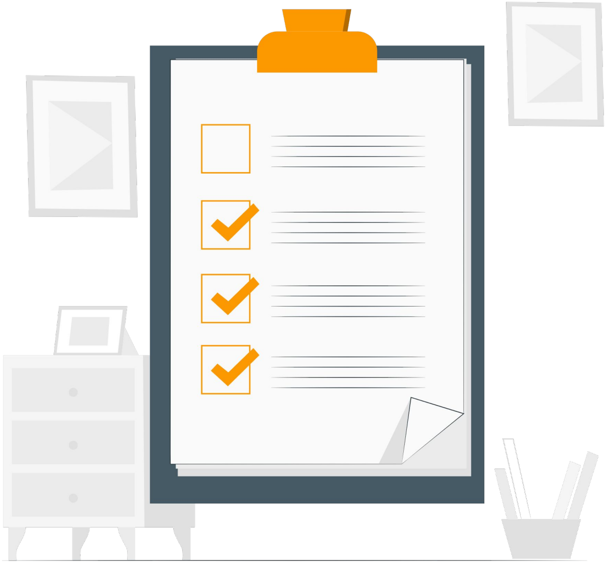
INFINITE LEARNING EXPERIENCE

About Speaker :

Harisuthan S

(Senior Security Engineer)

He Is a Blue Team Security researcher, bringing over 3+ years of experience in cyber defence. possesses a deep understanding of Blue Team methodologies including investigation and detection over cyber attacks,



Agenda

- Basic Introduction about S3 and S3 targeted attacks
- List of Essential AWS services for Safeguarding S3
- Detection Techniques for Identifying S3 Targeted Attacks
- Conclusion

Basic Introduction about AWS S3 Service

AWS S3 : Simple Storage Service

Amazon Simple Storage Service (**Amazon S3**) is a scalable, high-speed, web-based cloud storage service designed for various purposes including online backup and archiving of data, content storage and distribution and applications on Amazon Web Services (AWS).

List of AWS S3 Targeted Attacks

AWS S3 : Simple Storage Service

- Public Bucket Exposure
- Credential Leakage
- Privilege Escalation
- Ransomware Attacks
- Data exfiltration
- Exploiting Misconfigured Bucket Policies

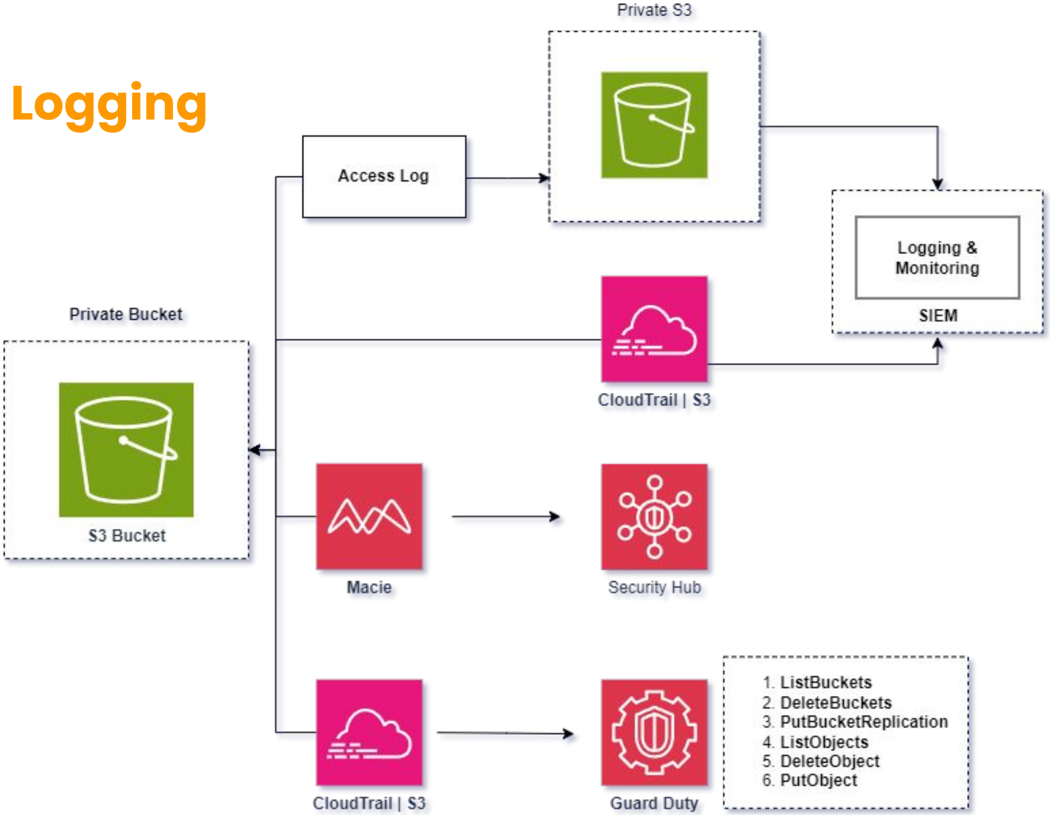
AWS S3 : Simple Storage Service

1. S3 enumeration
2. Suspicious bucket deletion activity
3. S3 data Exfiltration

List of AWS services to protect S3

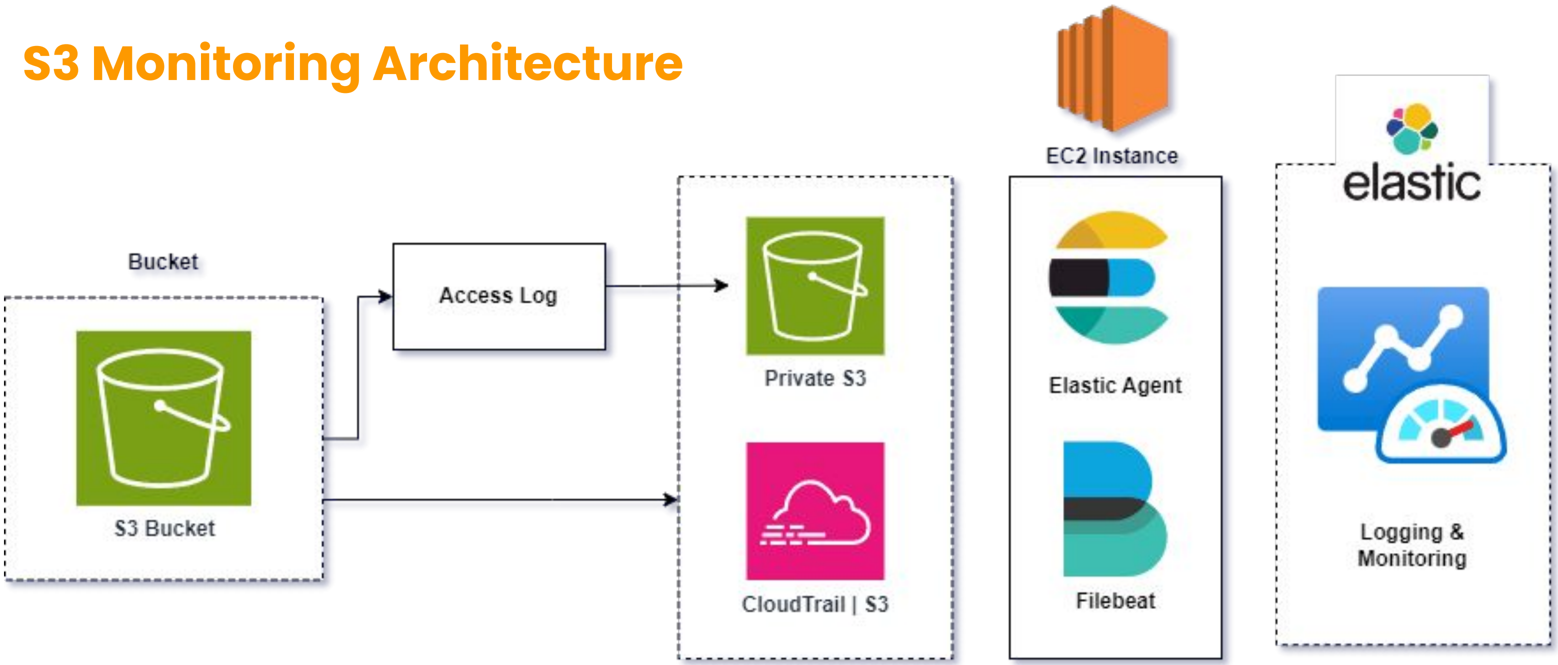
- CloudTrail
- Guard Duty
- CloudWatch
- AWS Macie
- SIEM

Monitoring & Logging AWS S3



1. ListBuckets
2. DeleteBuckets
3. PutBucketReplication
4. ListObjects
5. DeleteObject
6. PutObject

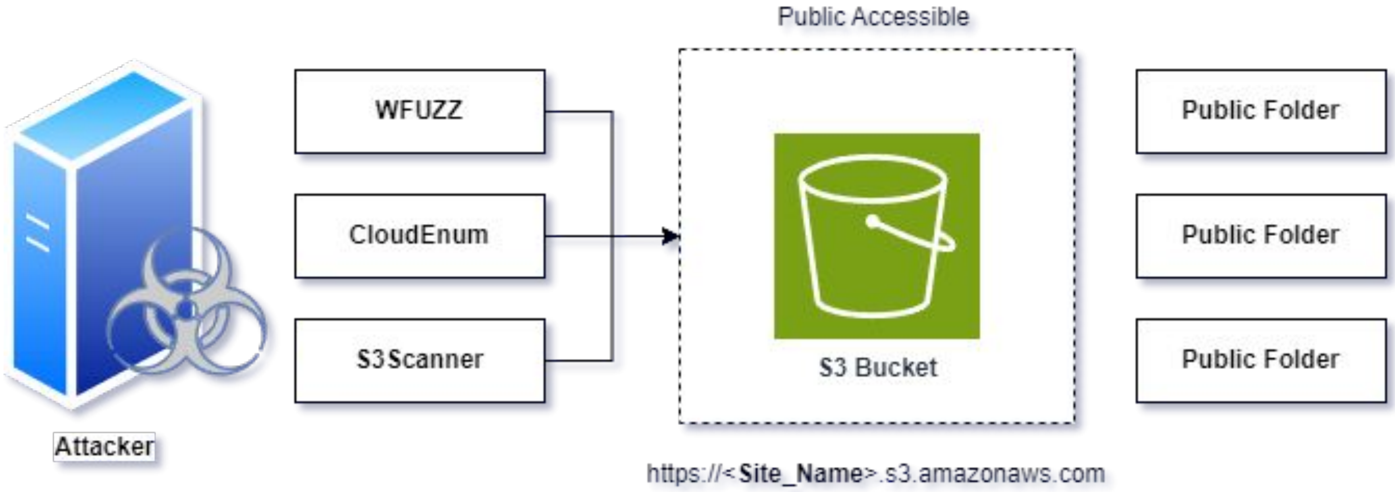
S3 Monitoring Architecture



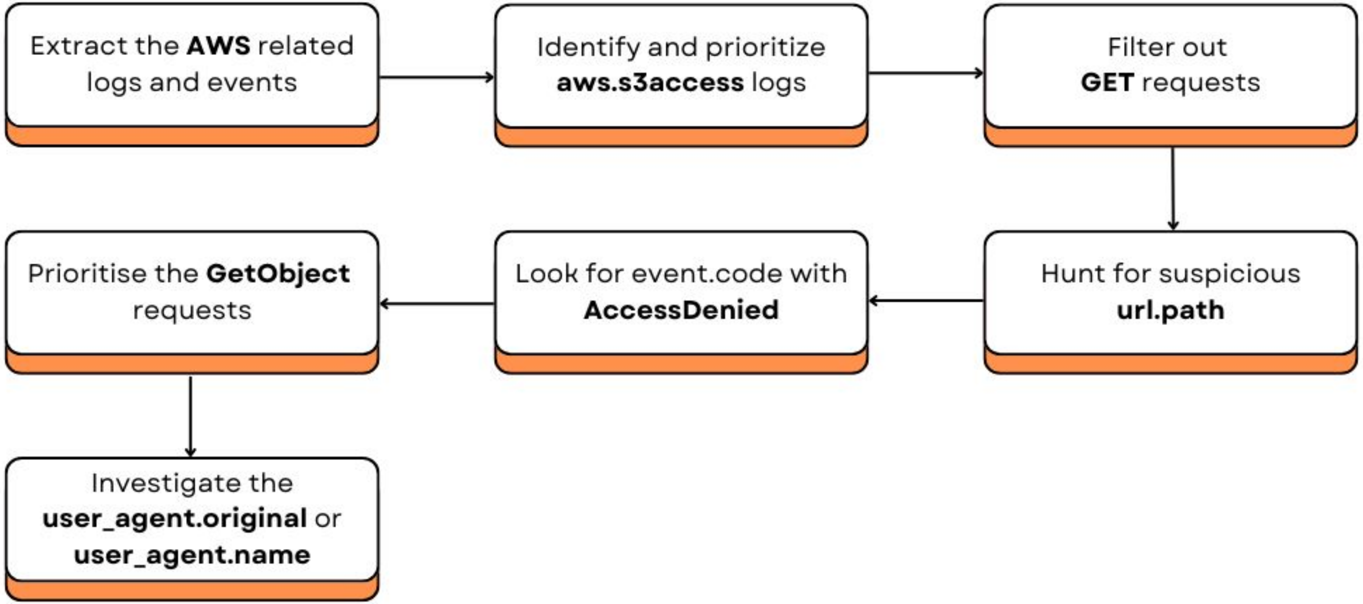
CWL
CyberWarFare Labs

Sub-domain S3 Enumeration

Working of S3 enumeration



Investigative Mind-Map for Sub-domain S3 enumeration



Extract the **AWS** related logs and events

Identify and prioritize **aws.s3access** logs

Filter out **GET** requests

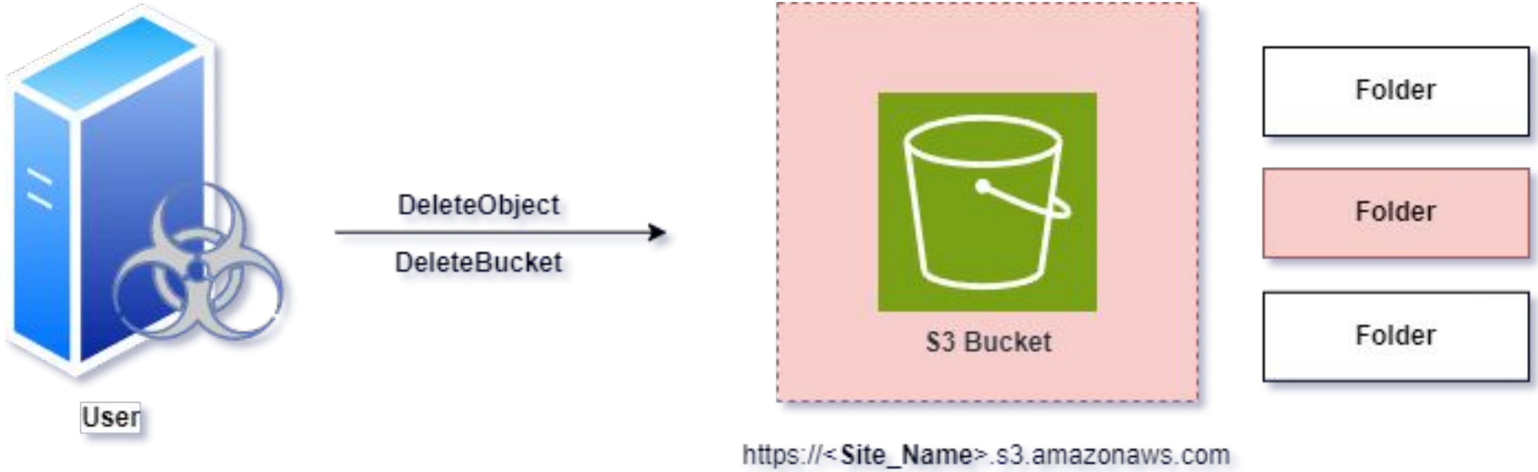
Hunt for suspicious **url.path**

Look for event.code with **AccessDenied**

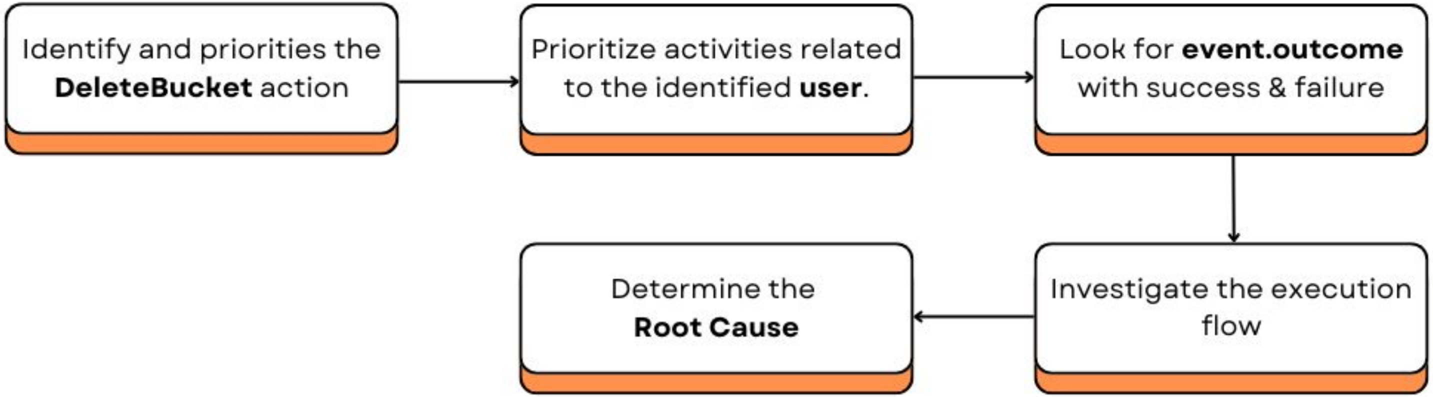
Prioritise the **GetObject** requests

Investigate the **user_agent.original** or **user_agent.name**

Bucket Deletion Activity



Investigative Mind-Map for Bucket Deletion Activity



Identify and priorities the **DeleteBucket** action

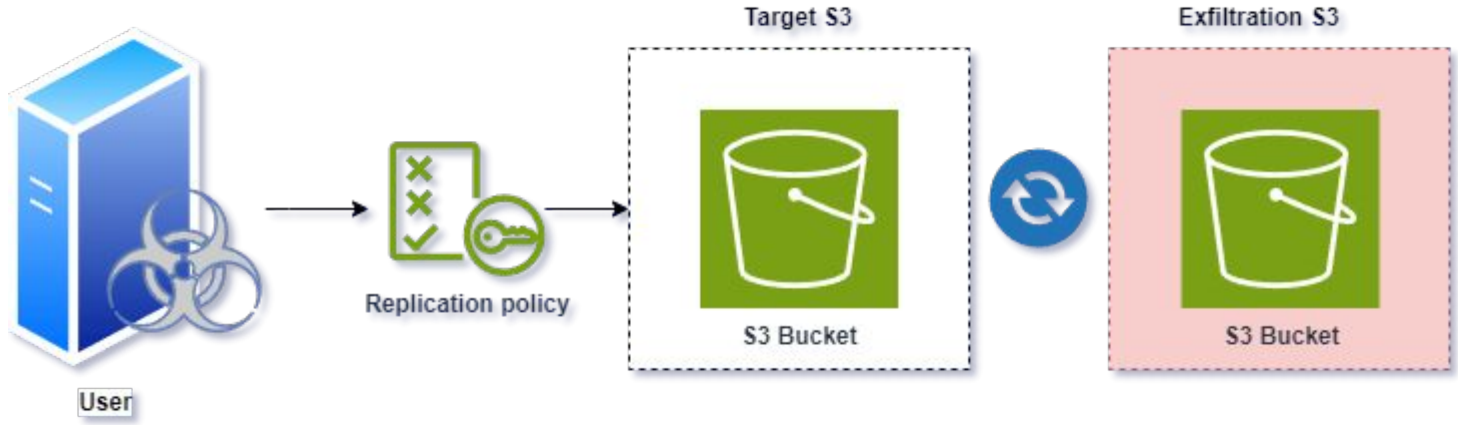
Prioritize activities related to the identified **user**.

Look for **event.outcome** with success & failure

Investigate the execution flow

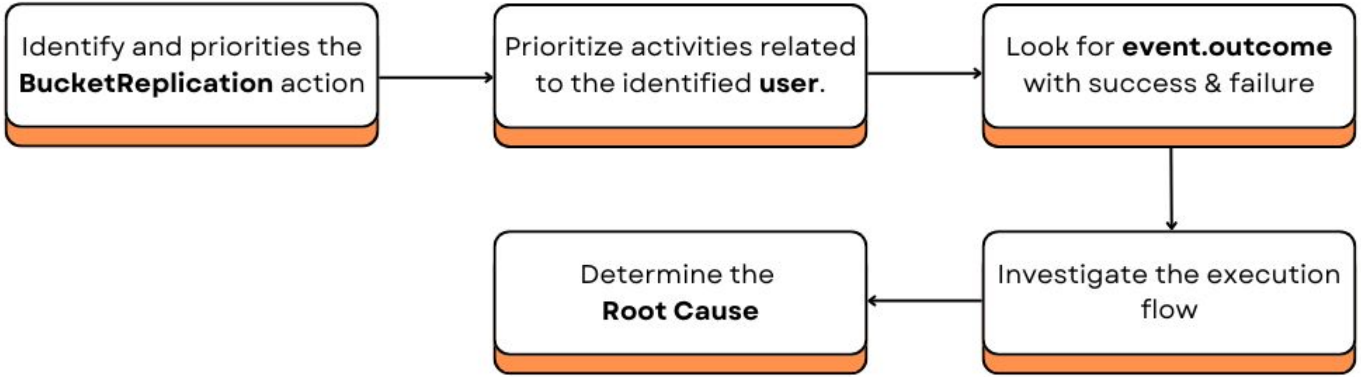
Determine the **Root Cause**

Data Exfiltration : Bucket-Replication



CWL
CyberWarFare Labs

Investigative Mind-Map for Bucket-Replication



Identify and priorities the **BucketReplication** action

Prioritize activities related to the identified **user**.

Look for **event.outcome** with success & failure

Investigate the execution flow

Determine the **Root Cause**

Thank You