

# ThreatModel™ for Amazon Simple Storage Service (S3)

Extract from the [blog](#): The last S3 security document that you'll ever need, and how to use it

TrustOnCloud helps customers make sense of the shared responsibility model, and accelerates secure adoption of each Cloud Service. We use threat modeling to ensure that **Security Architects, DevOps, and Security Governance teams are able to make good and bias-free security decisions.**

With 70+ ThreatModels published for our customers, we decided to release the ThreatModel for Amazon S3 to all, in order to **clearly define customer responsibilities** and **reduce security bad days for the AWS community, now and in the future.**

## How to use the ThreatModel for Amazon S3

To get started, the document might feel overwhelming with its 170+ pages. With its 32 distinct features, Amazon S3, the Simple Storage Service, is no longer "Simple", but I digress. All pages of the ThreatModel are relevant for at least a use case; your use case might not need all the pages.

Common use cases we see from our customers are:

1. **Covering the "best practices" (e.g. best security/effort ratio)**
2. **Reviewing the service depending on your application(s), and implementing the controls based on your risk tolerance**
3. **Technology onboarding for large enterprises/agencies**
4. **Compliance mapping to demonstrate a risk-based approach and formulate an action plan**

For each use case, you will find below where to look, what to do, and for whom it typically makes sense.

### 1. Covering the "best practices" (e.g. best security/effort ratio)

Where to look in the ThreatModel: Go to page 144 [Appendix 1 - Prioritized list for control implementation]. You will have a list of all the controls ordered by priority. It is risk-based, without the hassle to go through all the risks. We built this priority using our list of threats, the impact of the controls on the threats, and the effort it takes to implement the controls.

What to do: review that you implemented the controls starting with the "Very High" priority (using the implementation column). Test your controls actually work (using the testing column). Note that some controls might not be relevant for your usage of the service, feel free to skip them.

Typically for: DevOps team, and/or not-too-sensitive workloads (or what I like to call it "if it gets owned, we will get a bad week, not a bad year")

### 2. Reviewing the service depending on your application(s), and implementing the controls based on your risk tolerance (e.g. high security but ad hoc)

Where to look in the ThreatModel: Go to page 6 [Feature Classes]. We call feature classes, the portion of the service you can enable (exposing you to risk on those APIs) while being able to disable the rest. You can then go deeper with each feature class page with its Data Flow Diagram, and its associated threats and controls.

What to do: Identify the feature classes you intend to use during a threat modeling session with the DevOps team. Review each threat (at least Medium and above) and their mitigating controls. Decide what controls (or levels of mitigation impact) is required for each threat to satisfy your risk tolerance.

Typically for: Security Architect, and/or for sensitive workloads (typically having reputational risks or regulatory risks)

### **3. Technology onboarding for large enterprises/agencies (if you are required to dive deep – or enjoying – like as if it were the Mariana Trench)**

Where to look in the ThreatModel: Everywhere. Typically at this point, there is a decision from the enterprise/agency to use the service or not. We typically walk our customers through the relevant sections with our Cloud Threat Researchers.

What to do: Once the whole document is reviewed, some of our customers decided not to use a service for the highest application criticality or block certain features (looking at you Torrent S3 Object); or to take an exception-based approach. For other cases, the service can progress to their internal next steps. For example, building infrastructure-as-code templates that application owners must use, or defining the use cases to configure as IOC events and in your CSPM (e.g. Config Rules).

Typically for: Cloud Enterprise Security and GRC, for mass adoption of Cloud Services

### **4. Compliance mapping to demonstrate a risk-based approach, gap analysis and formulating an action plan (where compliance comes in handy)**

Where to look in the ThreatModel: Go to page 137 [Compliance Mapping]. You will find a mapping from S3 controls to PCI DSS v3.2. The document supports over 100 Compliance frameworks and standards using the [Secure Control Framework](#). Our mappings are based on compliance requirements mapped to security objectives and their underlying security activities. The activities are prioritized using our risk-based approach anchored in identifying threats on the service.

What to do: Review how you address the compliance requirements to which you are subject. Request evidence of the implementation and testing of the controls. Track the completion of any gaps.

Typically for: Compliance specialists, auditors, regulators

#### **Document Structure**

- Overall data flow diagram of Amazon S3 (page 3)
- Overview of the Mitre ATT&CK matrix for Amazon S3 (page 4)
- List of S3 features (page 6)
- Prioritized list of all threat scenarios per S3 feature (page 8)
- List of all the control activities and testing procedures (page 113)
- Control mappings to PCI DSS (page 137)
- Risk-based prioritized list of control implementation (page 144)

#### **License Agreement and disclaimer**

This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](#). This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The license allows for commercial use. If you remix, adapt, or build upon the material, you must license the modified material under identical terms.



All trademarks not owned by TrustOnCloud that appear on this work are the property of their respective owners, and do not imply any affiliation with or endorsement by them.

#### **Source**

The latest version of this work is hosted on [GitHub](#).

#### **Contact**

If you have any questions, please contact [contact@trustoncloud.com](mailto:contact@trustoncloud.com).

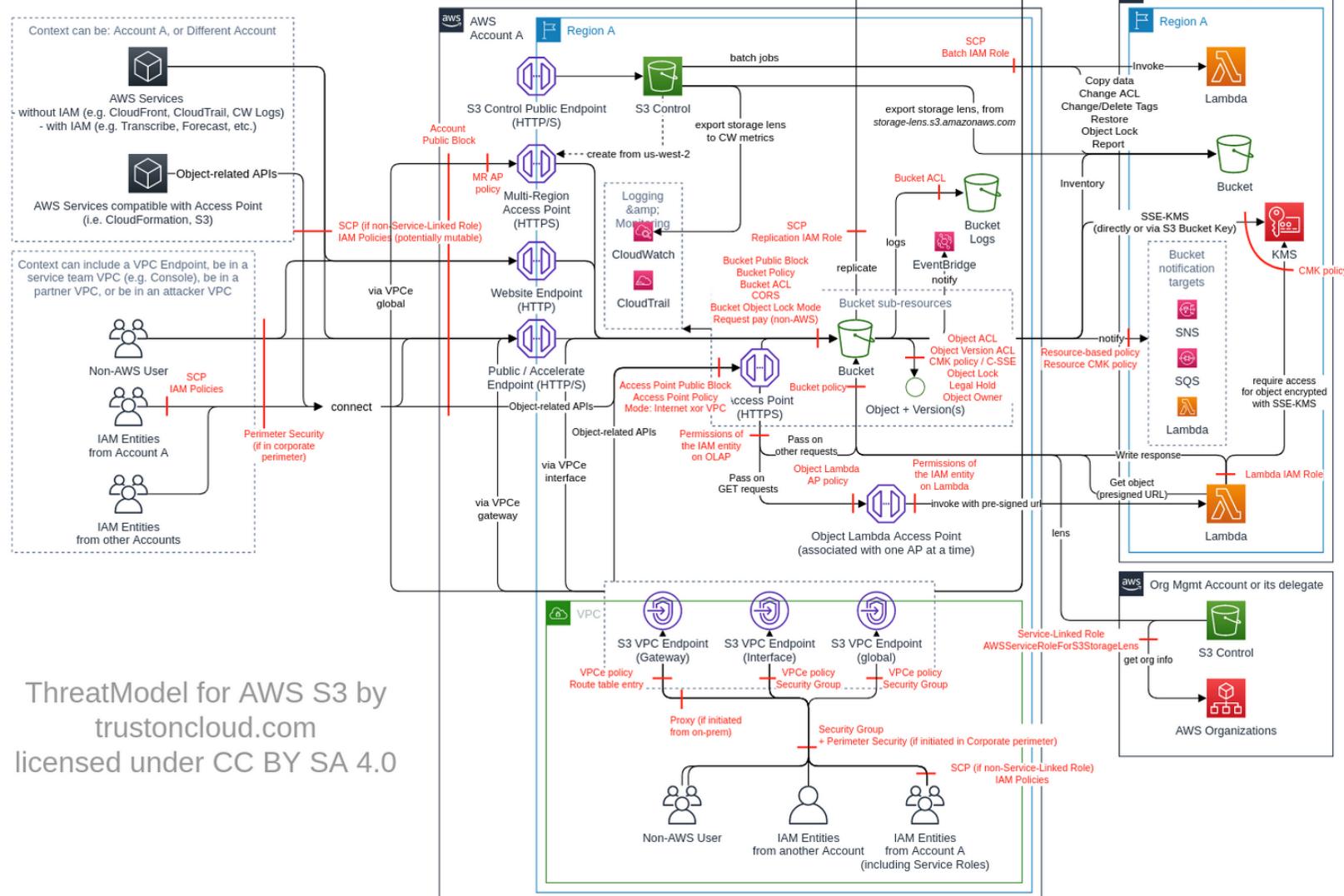


## Amazon Simple Storage Service (S3)

### Data Flow Diagram



Amazon  
S3



ThreatModel for AWS S3 by  
trustoncloud.com  
licensed under CC BY SA 4.0

## Security Scorecard

### Security of the Cloud

|  |              |
|--|--------------|
| Global Assurance Program Coverage (i.e. SOC, PCI, ISO)*        | 6 out of 6   |
| Specific Assurance Program Coverage (e.g. FedRAMP, HIPAA BAA)* | 16 out of 16 |

### Security in the Cloud

|  |                                 |
|--|---------------------------------|
| Number of Actions*                             | 182                             |
| Identity management                            | AWS IAM, bucket ACL, object ACL |
| Number of IAM permissions*                     | 153                             |
| Resource-level statement                       | Yes                             |
| Resource-based policy                          | Bucket                          |
| Tag-based ABAC                                 | Yes                             |
| CloudTrail Coverage for APIs                   | 99.3% (missing 1)               |
| Number of CloudTrail Event Names*              | 150                             |
| CloudWatch Events                              | via CloudTrail                  |
| VPC endpoint                                   | Yes (Interface + Gateway)       |
| VPC endpoint Policy                            | Yes                             |
| Network Filtering                              | No                              |
| Encryption-at-rest                             | Yes (SSE-KMS, SSE-S3, SSE-C)    |
| Encryption-in-transit (inc. Endpoint protocol) | Yes, but HTTP supported         |
| CloudFormation                                 | 6                               |

\* See details in Appendixes

## Mitre ATT&CK matrix for Amazon Simple Storage Service (S3)

| Initial Access | Execution | Persistence | Privilege Escalation  | Defense Evasion                                      | Credential Access | Discovery   | Lateral Movement   | Collection  | Exfiltration   | Impact   |
|----------------|-----------|-------------|---|--|-------------------|---|--|---|--|--|
|                |           |             | Gain access by modifying or deleting important object tags [S3.T33] | Exfiltrate data via ungoverned S3 endpoint [S3.T45]  |                   | Recon of AWS root account emails using email ACL grantee feature [S3.T19] | Reduce bucket security by modify the bucket public access block [S3.T52]                       | Move prod data in non-prod environment [S3.T11]                   | Bucket takeover to gather data [S3.T1]   | Grant unauthorized access to a private bucket by changing bucket ACL [S3.T4]     |
|                |           |             | Reduce bucket security by deleting the bucket policy [S3.T38]       | Evade detection by disabling S3 access logs [S3.T51] |                   |   | Reduce bucket security by modify the account public access block [S3.T53]                      | Unauthorized collection of data by swapping access point [S3.T28] | Unauthorized access to data via bucket replication [S3.T2]   | Use bucket to upload a malware or modify an object to include a malware [S3.T14] |
|                |           |             |   |  |                   |   | Grant unauthorized access to buckets by changing the Multi-Region Access Point policy [S3.T55] | Use AWS services to access data on S3 [S3.T30]                    | Exfiltrate your data hosted on an external bucket, by using of a compromised IAM access from Internet [S3.T3]  | Embed client-side script malware in bucket website [S3.T15]                      |
|                |           |             |   |  |                   |   |  |   | Unauthorized upload of a private object in an accessible bucket (e.g. public) you do not own [S3.T5]   | Files encrypted for ransomware [S3.T16]  |
|                |           |             |   |  |                   |   |  |   | Unauthorized modification of an object to become public or accessible in a private bucket you do not own by changing object ACL [S3.T6]                              | Destroy or modify primary data [S3.T17]  |
|                |           |             |   |  |                   |   |  |   | Exfiltrate data to an attacker bucket via public endpoint [S3.T7]  | Hotlinking content from S3 bucket [S3.T22]                                       |
|                |           |             |   |  |                   |   |  |   | Exfiltrate data by using a S3 VPC endpoint to upload data to an attacker bucket using an internal IAM entity [S3.T8]   | Abuse MD5 etag [S3.T27]  |
|                |           |             |   |  |                   |   |  |   | Exfiltrate data by uploading it to an attacker bucket using a non-authenticated user or an unauthorized external IAM entity via one of your S3 VPC endpoints [S3.T9] | Clickjacking on S3 website [S3.T29]  |
|                |           |             |   |  |                   |   |  |   | Exfiltrate data by using the public endpoint to upload data in an attacker bucket, using external credentials [S3.T10]   | Increase bill by creating incomplete uploads [S3.T40]                            |
|                |           |             |   |  |                   |   |  |   | Intercept data in transit to an external bucket [S3.T12]   | Loss of ownership of an object [S3.T43]  |
|                |           |             |   |  |                   |   |  |   | Intercept data in transit on the website endpoint [S3.T13]   | Exfiltrate, modify or delete objects using Batch [S3.T44]                        |
|                |           |             |   |  |                   |   |  |   | Exfiltrate data by using tags [S3.T18]   | Increase bill by restoring large amount of data [S3.T47]                         |
|                |           |             |   |  |                   |   |  |   | Use CloudFront to access private bucket [S3.T20]   | Affect data protection by removing versioning [S3.T48]                           |
|                |           |             |   |  |                   |   |  |   | Exfiltrate data stored on S3 via AWS services [S3.T21]   | Affect data protection by removing replication [S3.T49]                          |

|  |  |  |  |  |  |  |  |  |  |   |
|--|--|--|--|--|--|--|--|--|--|---|
|  |  |  |  |  |  |  |  |  | Phishing using trademarks [S3.T23]   | DoS by blocking traffic using bucket ACL [S3.T50] |
|  |  |  |  |  |  |  |  |  | Recon on valid AWS account or IAM principals [S3.T24]  |   |
|  |  |  |  |  |  |  |  |  | Delete objects by using lifecycle [S3.T25]   |   |
|  |  |  |  |  |  |  |  |  | Unauthorized object restore into an unauthorized bucket [S3.T26]                             |   |
|  |  |  |  |  |  |  |  |  | Upload in an authorized external bucket, but in an incorrect AWS account [S3.T31]            |   |
|  |  |  |  |  |  |  |  |  | Recon on information about a bucket [S3.T32]   |   |
|  |  |  |  |  |  |  |  |  | Intercept data in transit to an internal bucket [S3.T34]                                     |   |
|  |  |  |  |  |  |  |  |  | Use of less secure or old S3 features [S3.T35]   |   |
|  |  |  |  |  |  |  |  |  | Object made public or accessible in a private bucket you own by changing object ACL [S3.T36] |   |
|  |  |  |  |  |  |  |  |  | Grant unauthorized access to a private bucket by changing bucket policy [S3.T37]             |   |
|  |  |  |  |  |  |  |  |  | Exfiltrate data by using of a compromised IAM access from Internet [S3.T39]                  |   |
|  |  |  |  |  |  |  |  |  | Exfiltrate data via event notification [S3.T41]  |   |
|  |  |  |  |  |  |  |  |  | Exfiltrate data via inventory [S3.T42]   |   |
|  |  |  |  |  |  |  |  |  | Hijack connection with an Object Lambda [S3.T46]   |   |
|  |  |  |  |  |  |  |  |  | Grant unauthorized access to a bucket by changing/deleting access point policy [S3.T54]      |   |
|  |  |  |  |  |  |  |  |  | Gain unauthorized access to buckets trusting all Multi-Region Access Points [S3.T56]         |   |

## Feature Classes

Amazon Simple Storage Service (S3) has the following feature classes and subclasses (i.e. dependent on the usage of its class) that can be activated, restricted, or blocked using AWS Identity and Access Management.

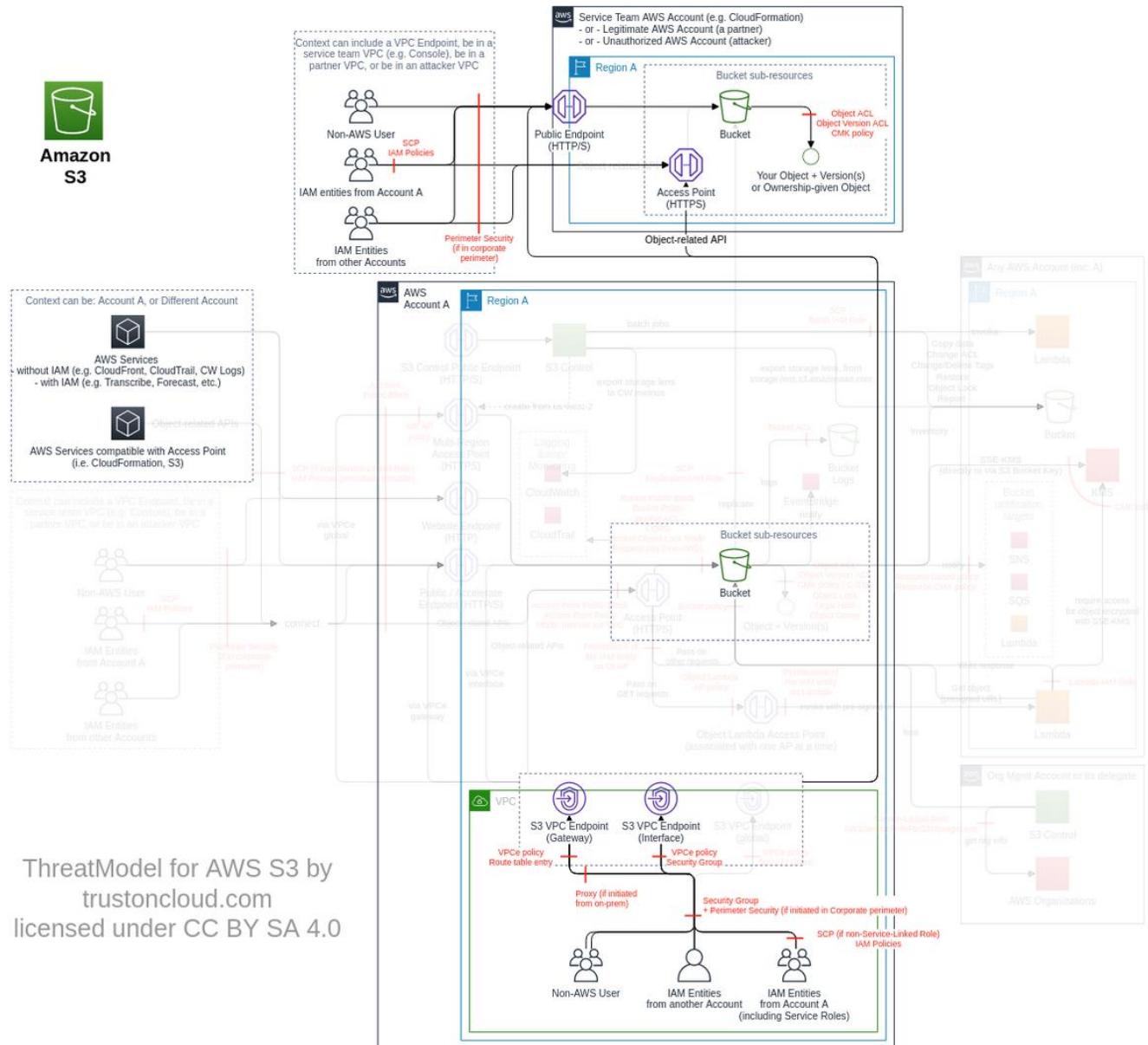
| Feature                  | Relation   | Description   |
|--------------------------|--|---|
| Object upload/download   | class  | You can upload and download virtually any number of objects to an external S3 bucket you authorized to.   |
| Bucket                   | subclass of Object upload/download                           | To upload your data into your AWS account, you must create an S3 bucket in one of the AWS Regions.  |
| Object tagging           | subclass of Object upload/download, used by Bucket           | You can tag objects ( <a href="#">ref</a> ).  |
| Torrent                  | subclass of Object upload/download, used by Bucket           | You can use the BitTorrent protocol to retrieve objects ( <a href="#">ref</a> ).  |
| Batch                    | subclass of Object upload/download, used by Bucket           | S3 Batch Operations performs large-scale Batch Operations on Amazon S3 objects.   |
| Object versioning        | subclass of Object upload/download, used by Bucket           | You can version your objects ( <a href="#">ref</a> ).   |
| Tag on versioned objects | subclass of Object tagging/Object versioning, used by Bucket | You can tag objects versions ( <a href="#">ref</a> ).   |
| ACL on versioned objects | subclass of Object versioning/ACL on versioned objects       | Amazon S3 access control lists (ACLs) enable you to manage access to object versions ( <a href="#">ref</a> ).   |
| Bucket versioning        | subclass of Object versioning/Bucket                         | Versioning is a means of keeping multiple variants of an object in the same bucket ( <a href="#">ref</a> ).   |
| Replication              | subclass of Bucket versioning                                | Replication enables automatic and asynchronous copying of objects of a bucket into another bucket ( <a href="#">ref</a> ).  |
| Bucket tag               | subclass of Bucket   | You can tag buckets ( <a href="#">ref</a> ).  |
| Bucket ACL               | subclass of Bucket   | Amazon S3 access control lists (ACLs) enable you to manage access to buckets ( <a href="#">ref</a> ).   |
| S3 access logging        | subclass of Bucket ACL                                       | Server access logging provides detailed records for the requests that are made to a bucket.   |
| Bucket policy            | subclass of Bucket   | For your bucket, you can add a bucket policy to grant other AWS accounts or IAM users permissions for the bucket and the objects in it. Any object permissions apply only to the objects that the bucket owner creates. |
| Analytics                | subclass of Bucket   | You can analyse storage access patterns to decide on the storage class ( <a href="#">ref</a> ).   |
| Inventory                | subclass of Bucket   | You can create a report on your storage, including object metadata, or versions ( <a href="#">ref</a> ).  |
| Lifecycle                | subclass of Bucket   | You can lifecycle your data to reduce the cost of storage ( <a href="#">ref</a> ).  |
| Metrics                  | subclass of Bucket   | You can configure metrics to get additional insights into your usage ( <a href="#">ref</a> ).   |
| S3 Storage Lens          | subclass of Bucket   | S3 Storage Lens provides a single view of object storage usage and activity across your entire S3 storage.  |
| Website                  | subclass of Bucket   | You can host a static website on Amazon S3. On a static website, individual web pages include static content. They might also contain client-side scripts ( <a href="#">ref</a> ).                                      |

|                               |  |   |
|-------------------------------|--|---|
| S3 Object Lock                | subclass of Bucket                                 | You can use S3 Object Lock to store objects using a write-once-read-many (WORM) model ( <a href="#">ref</a> ). Creating a bucket with S3 Object Lock will enable versioning even without permissions.                             |
| Legal hold                    | subclass of S3 Object Lock                         | A legal hold provides the same protection as a retention period, but it has no expiration date. S3 Object Lock must be activated on the bucket.   |
| Transfer Acceleration         | subclass of Bucket                                 | You can use Transfer Acceleration to improve the performance of long-distance transfers ( <a href="#">ref</a> ).  |
| Notification                  | subclass of Bucket                                 | You can receive notifications when certain events happen in your bucket.  |
| Access point                  | subclass of Bucket                                 | Access points are named network endpoints that are attached to buckets that you can use to perform S3 object operations.  |
| S3 Object Lambda              | subclass of Access point                           | S3 Object Lambda enables users to apply their own custom code to process the output of a standard S3 request by automatically invoking a Lambda function.   |
| Multi-Region Access Points    | subclass of Bucket                                 | S3 Multi-Region Access Points provide a single global endpoint to access a data set that spans multiple S3 buckets in different AWS Regions.  |
| CORS                          | subclass of Bucket                                 | You can create a CORS configuration with rules that identify the origins that you will allow to access your bucket and the operations (HTTP methods) that will support for each origin, and other operation-specific information. |
| Bucket default encryption     | subclass of Bucket                                 | You can set default encryption on a bucket so that all new objects are encrypted when they are stored in the bucket.  |
| S3 Object Ownership           | subclass of Bucket, used by Object upload/download | S3 Object Ownership enables bucket owners to automatically assume ownership of objects that are uploaded to their buckets by other AWS accounts.  |
| Public Access Block (bucket)  | subclass of Bucket                                 | S3 Block Public Access (bucket) provides controls across at the individual S3 bucket level to ensure objects never have public access.  |
| Public Access Block (account) | subclass of Bucket                                 | S3 Block Public Access (account) provides controls across an entire AWS account to ensure objects never have public access.   |
| Other uses                    | class  | Others can use their own S3 service to impact you in some ways.   |

# Object upload/download (class, FC1)

You can upload and download virtually any number of objects to an external S3 bucket you authorized to. Amazon S3 access control lists (ACLs) enable you to manage access to objects. Each object has an ACL attached to it as a sub-resource. It defines which AWS accounts or groups are granted access and the type of access. When a request is received against a resource, Amazon S3 checks the corresponding ACL to control that the requester has the necessary access permissions ([ref](#)).

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

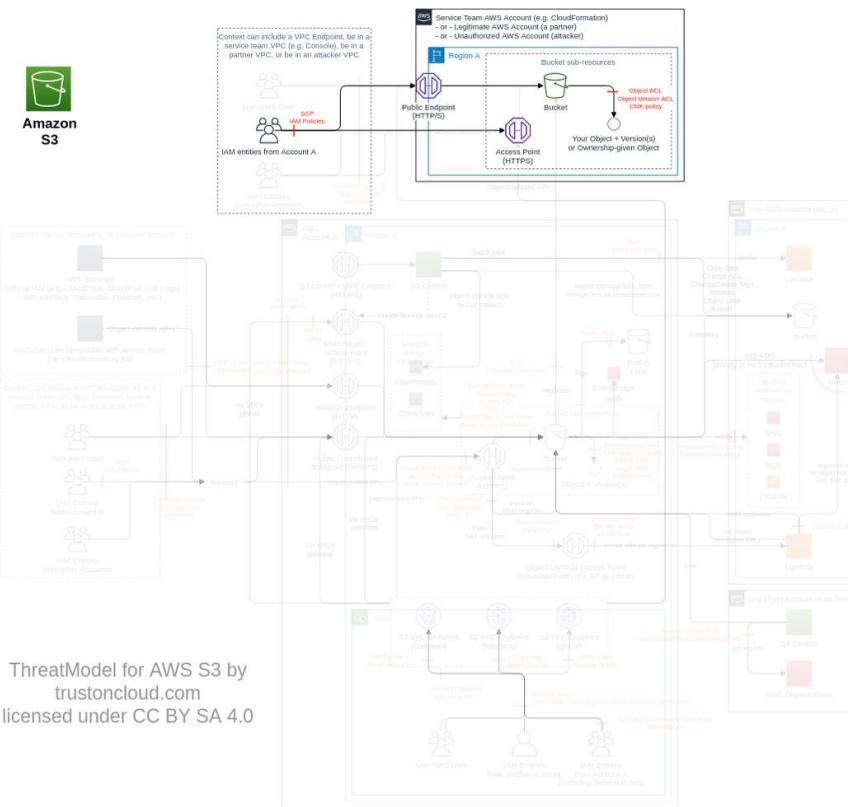
| Action  | IAM Permission  |
|---|-----------------|
| Retrieves an object from Amazon S3.   | s3:GetObject    |
| Adds an object to a bucket.   | s3:PutObject    |
| Sets the access control list (ACL) permissions for an object. You must have WRITE_ACP permission to set the ACL of an object. | s3:PutObjectAcl |

## Threat List

| Name   | CVSS                         |
|--|------------------------------|
| Exfiltrate your data hosted on an external bucket, by using of a compromised IAM access from Internet  | <a href="#">Medium (6.7)</a> |
| Loss of ownership of an object   | <a href="#">Medium (6.3)</a> |
| Exfiltrate data by uploading it to an attacker bucket using a non-authenticated user or an unauthorized external IAM entity via one of your S3 VPC endpoints | <a href="#">Medium (6.2)</a> |
| Exfiltrate data stored on S3 via AWS services  | <a href="#">Medium (5.8)</a> |
| Exfiltrate data to an attacker bucket via public endpoint  | <a href="#">Medium (5.7)</a> |
| Unauthorized upload of a private object in an accessible bucket (e.g. public) you do not own   | <a href="#">Medium (5.7)</a> |
| Exfiltrate data by using a S3 VPC endpoint to upload data to an attacker bucket using an internal IAM entity   | <a href="#">Medium (5.5)</a> |
| Unauthorized modification of an object to become public or accessible in a private bucket you do not own by changing object ACL                              | <a href="#">Medium (5.2)</a> |
| Intercept data in transit to an external bucket  | <a href="#">Medium (4.6)</a> |
| Unauthorized object restore into an unauthorized bucket  | <a href="#">Medium (4.5)</a> |
| Upload in an authorized external bucket, but in an incorrect AWS account   | <a href="#">Medium (4.0)</a> |
| Exfiltrate data via ungoverned S3 endpoint   | <a href="#">Low (1.9)</a>    |
| Use of less secure or old S3 features  | <a href="#">Low (1.9)</a>    |

## Exfiltrate your data hosted on an external bucket, by using of a compromised IAM access from Internet

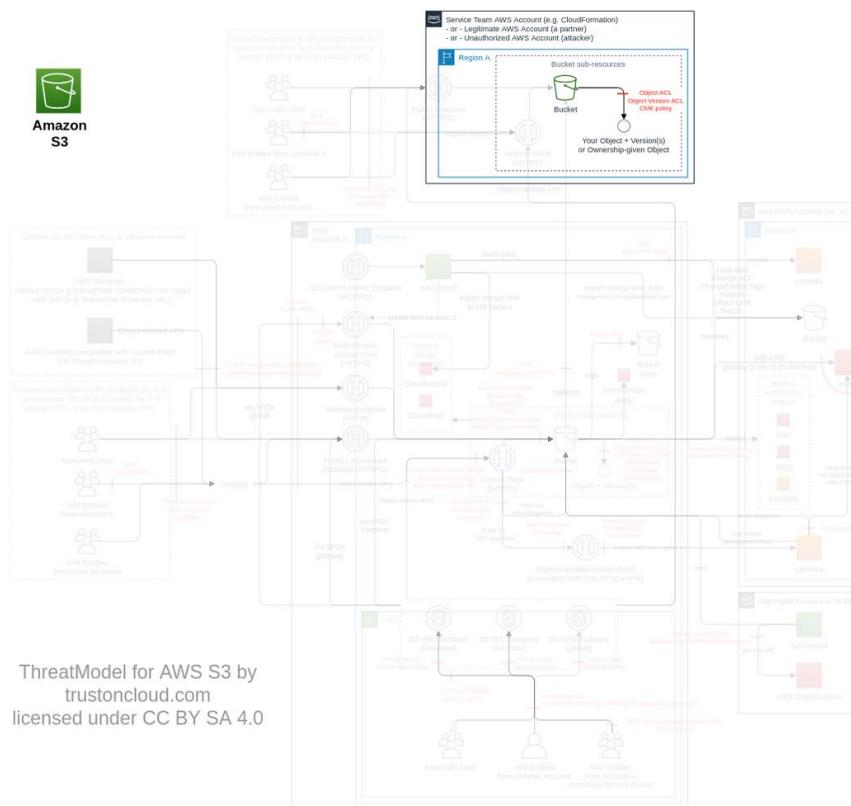
|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T3  |
| <b>Name</b>             | Exfiltrate your data hosted on an external bucket, by using of a compromised IAM access from Internet  |
| <b>Description</b>      | IAM credentials can be compromised. An attacker can use a compromised but authorized credential to download your object from an external bucket via the public endpoint (using or not their own VPC endpoint). |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">Medium (6.7)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:GetObject"<br>}   |



| Control Objectives   | Priority | # of associated Controls |              |           |
|--|----------|--------------------------|--------------|-----------|
|  |          | Directive                | Preventative | Detective |
| <b>Identify and ensure the protection all external buckets hosting your objects</b><br>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel). | High     | 1                        | -            | -         |
| <b>Enforce good coding practice</b><br>Ensure all S3 buckets interacted with are in the correct AWS account (e.g. using the condition in all compatible S3 requests: x-amz-expected-bucket-owner and x-amz-source-expected-bucket-owner)   | Medium   | 1                        | -            | -         |
| <b>Monitor S3 with Amazon GuardDuty and Macie</b><br>Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using GuardDuty ThreatModel. Ensure findings are investigated (e.g. using Amazon Detective).  | Low      | 1                        | -            | -         |
| <b>Encrypt or tokenize critical data</b><br>Aligned with your data governance, encrypt on the client side - or tokenize - appropriate data   | Very Low | 1                        | -            | -         |

## Loss of ownership of an object

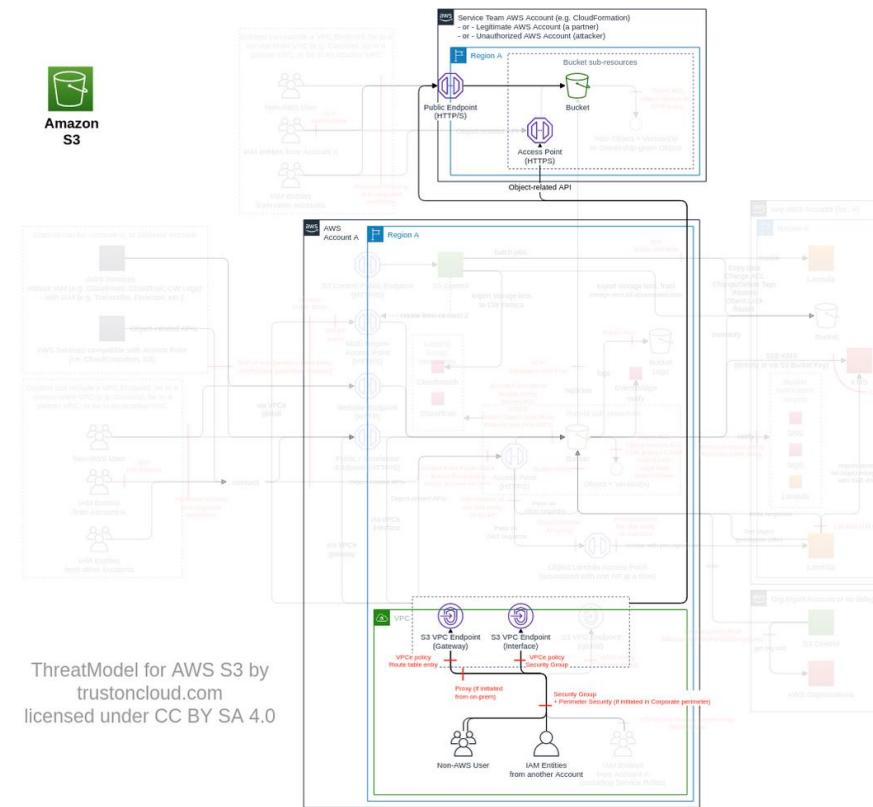
|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T43   |
| <b>Name</b>             | Loss of ownership of an object   |
| <b>Description</b>      | S3 Object Ownership enables a bucket receiver to convert a bucket-owner-full-control ACL into an ownership transfer (for new object); additionally a bucket can convert all the objects to be owned by the bucket owner. An attacker can modify the receiver bucket to remove your object ACL control on an object, and remove your access to this object. |
| <b>Goal</b>             | Data manipulation  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>   |
| <b>CVSS</b>             | <a href="#">Medium (6.3)</a>   |
| <b>IAM Access</b>       | {<br>"OPTIONAL": "s3:PutBucketOwnershipControls"<br>}  |



| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Disabling ACLs for all buckets</b><br>Ensure bucket ACL and object ACL are disabled on each bucket<br>Prevent the creation of buckets with ACL enabled (e.g. by using a SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note it does not block someone to enable ACL afterwards via PutPutBucketOwnershipControls.   | Very High | 1                        | 1            | -         |
| <b>Identify and ensure the protection all external buckets hosting your objects</b><br>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel).<br>For all external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover, block the PutObject with any ACL (e.g. using IAM or SCP and a deny on the condition "StringLike": {"s3:x-amz-acl": "*"}). It should be called via PutObjectAcl.<br>For all external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover, monitor that the PutObject do not include the ACL operation | Very High | 1                        | 1            | 1         |
| <b>Enforce good coding practice</b><br>When transmitting an object to an external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover, use 2 separate APIs (PutObject and PutObjectAcl), instead of the built-in object ACL operation in PutObject.   | High      | 1                        | -            | -         |

## Exfiltrate data by uploading it to an attacker bucket using a non-authenticated user or an unauthorized external IAM entity via one of your S3 VPC endpoints

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T9   |
| <b>Name</b>             | Exfiltrate data by uploading it to an attacker bucket using a non-authenticated user or an unauthorized external IAM entity via one of your S3 VPC endpoints  |
| <b>Description</b>      | VPC endpoints for S3 allow any entity to connect from a VPC to any S3 bucket without Internet Gateway. An attacker can exfiltrate data to an external S3 bucket via one of your VPC endpoints, using a non-authenticated user or its own external IAM entity. Note that some external IAM entities might be authorized, if provided by one of your business partners. |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Medium (6.2)</a>  |
| <b>IAM Access</b>       | 0   |

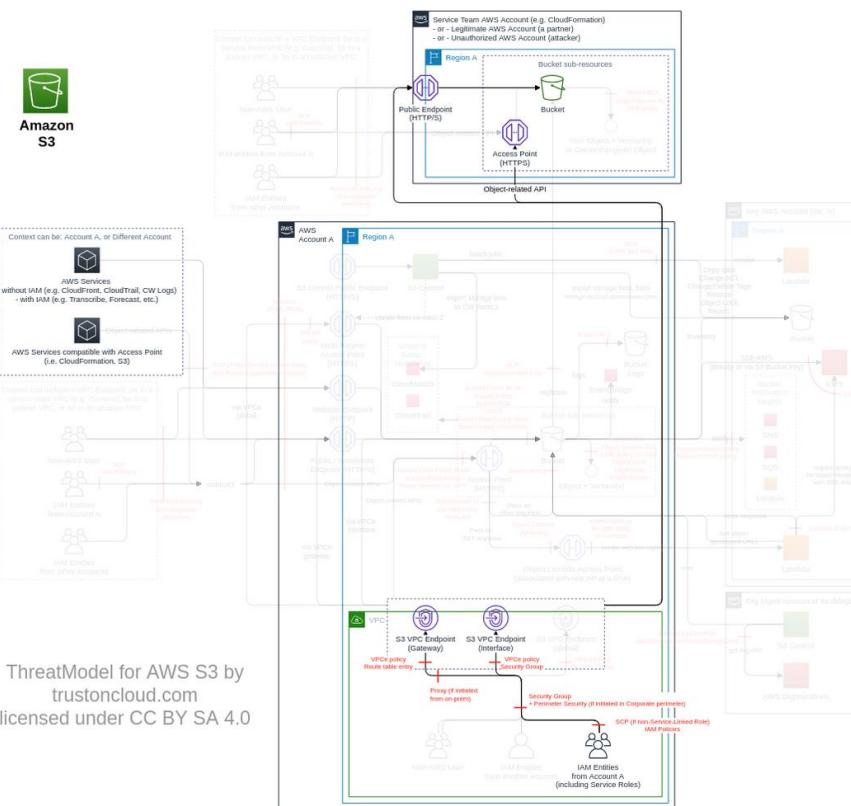


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Restrict access point access to VPC when in use</b><br><br>Maintain a list of authorized access between VPC, S3 access point and S3.<br>Limit access via the S3 access point by using in VPC endpoint and/or bucket policy the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of allowlist bucket name in VPC endpoint/bucket policy.   | Very High | 1                        | 1            | -         |
| <b>Limit and monitor access via S3 VPC endpoints</b><br><br>For each VPC, maintain a list of AWS Organizations, OU and/or AWS account(s), where IAM entities are authorized to access S3<br>For each VPC with an IAM entity allowed to use S3, secure them with the VPC ThreatModel (e.g. <a href="#">modification of VPC endpoints</a> , <a href="#">VPC endpoint policy</a> , <a href="#">routing table</a> , <a href="#">Security Groups</a> )<br>Block any IAM entity not belonging to an authorized AWS Organizations, OU and/or AWS account(s) to call S3 from your VPCs by adding a deny statement on S3 VPC endpoint policy of each VPC, with the condition using "aws:PrincipalOrgPaths" ( <a href="#">ref</a> ) including the full Org ID, as those are globally unique.<br>Enable <a href="#">VPC DNS query logging</a> in all VPC<br>Maintain a list of authorized S3 and S3 access point (and their respective AWS accounts) to be access for each VPC<br>Limit the access to only authorized S3 bucket(s) or their AWS account(s) from each VPC (e.g. using the condition key "s3:ResourceAccount" on the VPC endpoint policy, alternatively use specific resource-level statement for each bucket, or if the VPC endpoint policy size is beyond the limit and more granular control on VPC is required, use access points)<br>Monitor VPC DNS query logs that only authorized S3 bucket and S3 access points are being queried in each VPC (e.g. using VPC DNS query logging), and protect it using Route53 ThreatModel | Very High | 4                        | 2            | 1         |
| <b>Block requests with KMS keys from unauthorized AWS account(s)</b><br><br>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account<br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)<br>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <code>response.x-amz-server-side-encryption-aws-kms-key-id</code> )   | Very High | 1                        | 1            | 1         |

|   |        |   |   |   |
|---|--------|---|---|---|
| <b>Identify and ensure the protection all external buckets hosting your objects</b><br>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel).<br>Request access via S3 access point on bucket you don't own, if compatible with your interaction with the bucket (e.g. not through not-compatible AWS service) | High   | 2 | - | - |
| <b>Enable CloudTrail S3 data events</b><br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel  | Medium | 1 | - | - |

## Exfiltrate data stored on S3 via AWS services

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T21  |
| <b>Name</b>             | Exfiltrate data stored on S3 via AWS services   |
| <b>Description</b>      | Number of AWS services are using S3 for storage, including storing in cross-account S3 buckets. Services with IAM roles (e.g. SageMaker) will give ownership to the target AWS account, hence removing the ownership protection. An attacker can use those services to exfiltrate data. |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Medium (5.8)</a>  |
| <b>IAM Access</b>       | {<br>"OPTIONAL": "s3:PutObjectAcl"<br>}   |

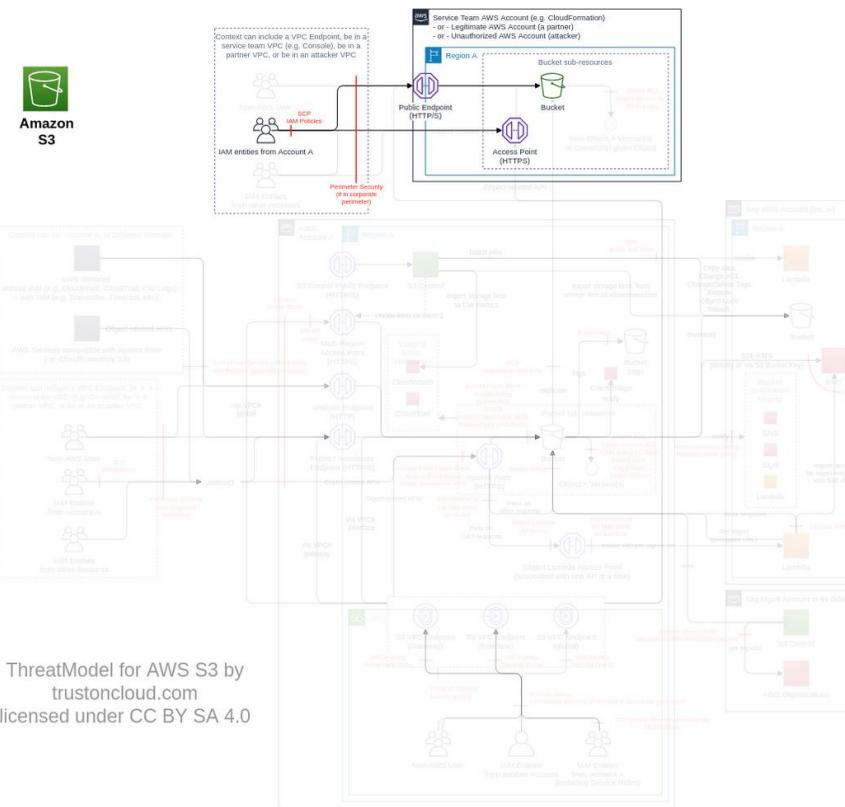


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Block requests with KMS keys from unauthorized AWS account(s)</b><br><br>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account<br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)<br>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <code>response.x-amz-server-side-encryption-aws-kms-key-id</code> )                               | Very High | 1                        | 1            | 1         |
| <b>Identify and ensure the protection all external buckets hosting your objects</b><br><br>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel).<br>Monitor that only authorized external buckets are used (e.g. via CloudTrail S3 data events in <code>resources[].accountId</code> and <code>resources[].ARN</code> ). Both account ID and bucket name must be verified. | High      | 1                        | -            | 1         |
| <b>Model the threats on all AWS services accessing S3</b><br><br>Analyse and protect all AWS services accessing S3 (e.g. via ThreatModel). Enforce usage in VPC only, whenever possible.   | High      | 1                        | -            | -         |
| <b>Enable CloudTrail S3 data events</b><br><br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel   | Medium    | 1                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.  | Low       | 2                        | -            | -         |

|  |  |  |  |  |
|--|--|--|--|--|
| In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. |  |  |  |  |
|--|--|--|--|--|

## Exfiltrate data to an attacker bucket via public endpoint

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T7  |
| <b>Name</b>             | Exfiltrate data to an attacker bucket via public endpoint  |
| <b>Description</b>      | S3 allows IAM entities to upload data in a bucket in other AWS accounts, if they have the IAM permissions. An attacker can use one of your IAM entities to upload data to one of their buckets. If the attacker does not control object ACL, it can use the name of objects (1KB). |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">Medium (5.7)</a>   |
| <b>IAM Access</b>       | {<br>"AND": ["s3:PutObject", {<br>"OPTIONAL": "s3:PutObjectAcl"<br>}<br>]}   |

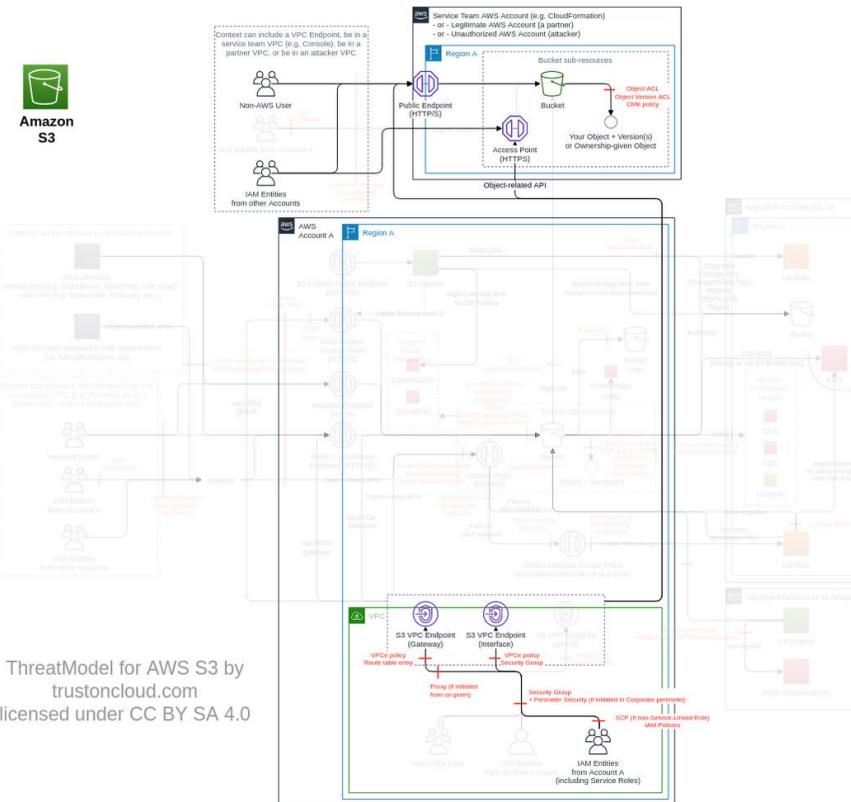


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Block S3 endpoints in your corporate perimeter security</b><br>Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g. firewalls, or cloud interception proxy like <a href="#">Kivera</a> ) including via Internet Gateway, to force usage of VPC endpoints. It will block data-plane transfer. Note: AWS console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com").  | Very High | 1                        | -            | -         |
| <b>Block requests with KMS keys from unauthorized AWS account(s)</b><br>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account<br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)<br>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <code>response.x-amz-server-side-encryption-aws-kms-key-id</code> )                               | Very High | 1                        | 1            | 1         |
| <b>Identify and ensure the protection all external buckets hosting your objects</b><br>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel).<br>Monitor that only authorized external buckets are used (e.g. via CloudTrail S3 data events in <code>resources[].accountId</code> and <code>resources[].ARN</code> ). Both account ID and bucket name must be verified. | High      | 1                        | -            | 1         |
| <b>Enable CloudTrail S3 data events</b><br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel   | Medium    | 1                        | -            | -         |
| <b>Restrict access point access to VPC when in use</b><br>Maintain a list of authorized access between VPC, S3 access point and S3.  | Medium    | 1                        | 5            | -         |

|  |        |   |   |   |
|--|--------|---|---|---|
| <p>Limit access via the S3 access point by using in VPC endpoint and/or bucket policy the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of allowlist bucket name in VPC endpoint/bucket policy.</p> <p>In S3 bucket policy, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn"</p> <p>Block the creation "s3&gt;CreateAccessPoint" of non-VPC S3 access point (e.g. using the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"})</p> <p>Block all traffic from Internet-configured S3 access point (e.g. on the bucket policy, using a deny statement with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"})</p> <p>Block any <a href="#">object-related operations</a> access to S3 bucket not through access point (i.e. using a deny IAM policy statement with the condition "ArnNotLike" {"s3:DataAccessPointArn": "arn:aws:s3:Region:AccountId:accesspoint/*"})</p> |        |   |   |   |
| <p><b>Limit the access to the IAM actions required to execute the threats</b></p> <p>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.</p> <p>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account.</p>   | Medium | 2 | - | - |
| <p><b>Encrypt or tokenize critical data</b></p> <p>Aligned with your data governance, encrypt on the client side - or tokenize - appropriate data</p>  | Low    | 1 | - | - |

## Unauthorized upload of a private object in an accessible bucket (e.g. public) you do not own

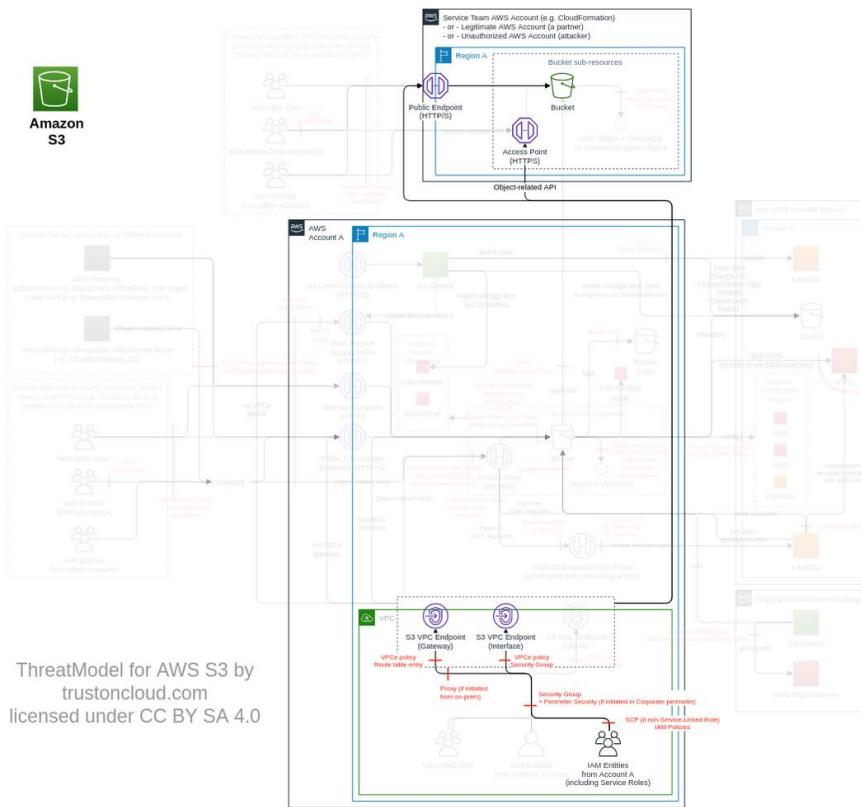
|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T5   |
| <b>Name</b>             | Unauthorized upload of a private object in an accessible bucket (e.g. public) you do not own  |
| <b>Description</b>      | S3 buckets can be public for a legitimate reason. An attacker (or someone by negligence) can upload sensitive data in an accessible bucket (e.g. public) you do not own to make it accessible to exfiltrate it. |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Medium (5.7)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutObject"<br>}  |



| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Block requests with KMS keys from unauthorized AWS account(s)</b><br>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account<br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)<br>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> )   | Very High | 1                        | 1            | 1         |
| <b>Identify and ensure the protection all external buckets hosting your objects</b><br>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel).<br>Allow only authorized ACL on objects for bucket you don't control (e.g. using IAM and VPC endpoint policy with the <a href="#">ACL conditions</a> )<br>Scan all data before uploading to an external bucket to ensure the classification of the data is aligned with the bucket classification (e.g. using Macie). | High      | 2                        | 1            | -         |
| <b>Enable CloudTrail S3 data events</b><br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel   | Medium    | 1                        | -            | -         |
| <b>Encrypt or tokenize critical data</b><br>Aligned with your data governance, encrypt on the client side - or tokenize - appropriate data   | Low       | 1                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.  | Very Low  | 1                        | -            | -         |

## Exfiltrate data by using a S3 VPC endpoint to upload data to an attacker bucket using an internal IAM entity

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T8   |
| <b>Name</b>             | Exfiltrate data by using a S3 VPC endpoint to upload data to an attacker bucket using an internal IAM entity  |
| <b>Description</b>      | VPC endpoints for S3 allow IAM entities to connect from a VPC to any S3 bucket without Internet Gateway. An attacker can exfiltrate pre-collected data to an external S3 bucket via a VPC endpoint, using an internal IAM entity they control. If the attacker does not control object ACL, it can use the name of objects (1KB). |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Medium (5.5)</a>  |
| <b>IAM Access</b>       | {<br>"AND": [{"s3:PutObject", {<br>"OPTIONAL": "s3:PutObjectAcl"<br>}}]<br>}  |

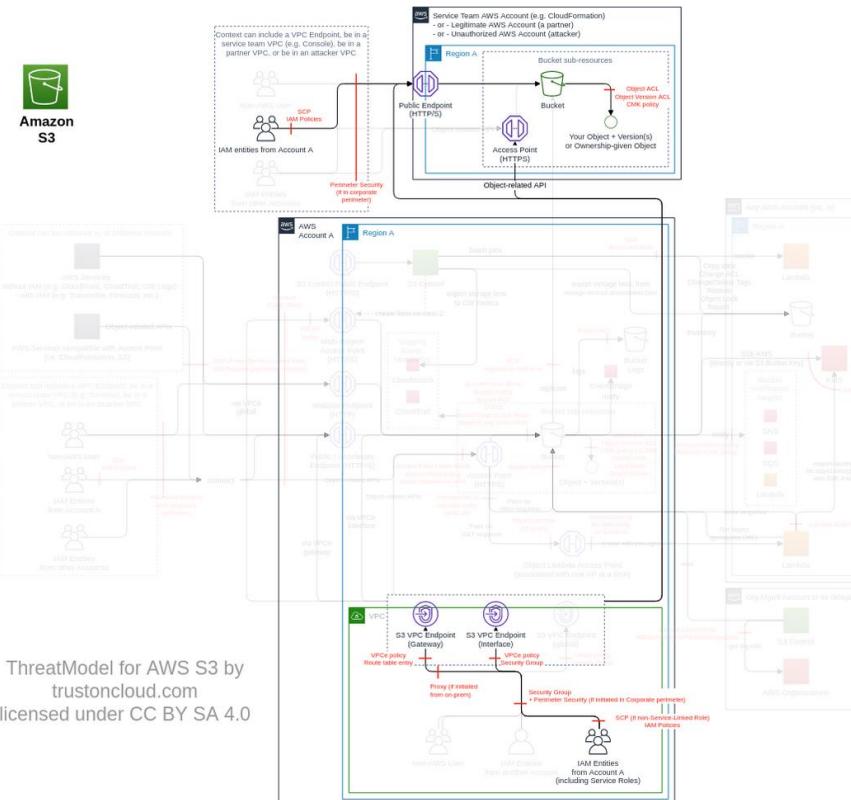


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Block requests with KMS keys from unauthorized AWS account(s)</b><br><br>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account<br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)<br>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> )   | Very High | 1                        | 1            | 1         |
| <b>Identify and ensure the protection all external buckets hosting your objects</b><br><br>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel).<br>Request access via S3 access point on bucket you don't own, if compatible with your interaction with the bucket (e.g. not through not-compatible AWS service)  | High      | 2                        | -            | -         |
| <b>Limit and monitor access via S3 VPC endpoints</b><br><br>Enable <a href="#">VPC DNS query logging</a> in all VPC<br>Maintain a list of authorized S3 and S3 access point (and their respective AWS accounts) to be access for each VPC<br>Limit the access to only authorized S3 bucket(s) or their AWS account(s) from each VPC (e.g. using the condition key "s3:ResourceAccount" on the VPC endpoint policy, alternatively use specific resource-level statement for each bucket, or if the VPC endpoint policy size is beyond the limit and more granular control on VPC is required, use access points)<br>Monitor VPC DNS query logs that only authorized S3 bucket and S3 access points are being queried in each VPC (e.g. using VPC DNS query logging), and protect it using Route53 ThreatModel | High      | 2                        | 1            | 1         |
| <b>Enable CloudTrail S3 data events</b><br><br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel   | Medium    | 1                        | -            | -         |

|  |        |   |   |   |
|--|--------|---|---|---|
| <p><b>Limit the access to the IAM actions required to execute the threats</b></p> <p>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.</p> <p>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account.</p> | Medium | 2 | - | - |
|--|--------|---|---|---|

## Unauthorized modification of an object to become public or accessible in a private bucket you do not own by changing object ACL

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T6  |
| <b>Name</b>             | Unauthorized modification of an object to become public or accessible in a private bucket you do not own by changing object ACL  |
| <b>Description</b>      | Bucket authority only prevails on object ACL when the object access is explicitly denied ( <a href="#">ref</a> ). An attacker (or someone by negligence) can change the object ACL to make it public or accessible for themselves. |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">Medium (5.2)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutObjectAcl"<br>}  |

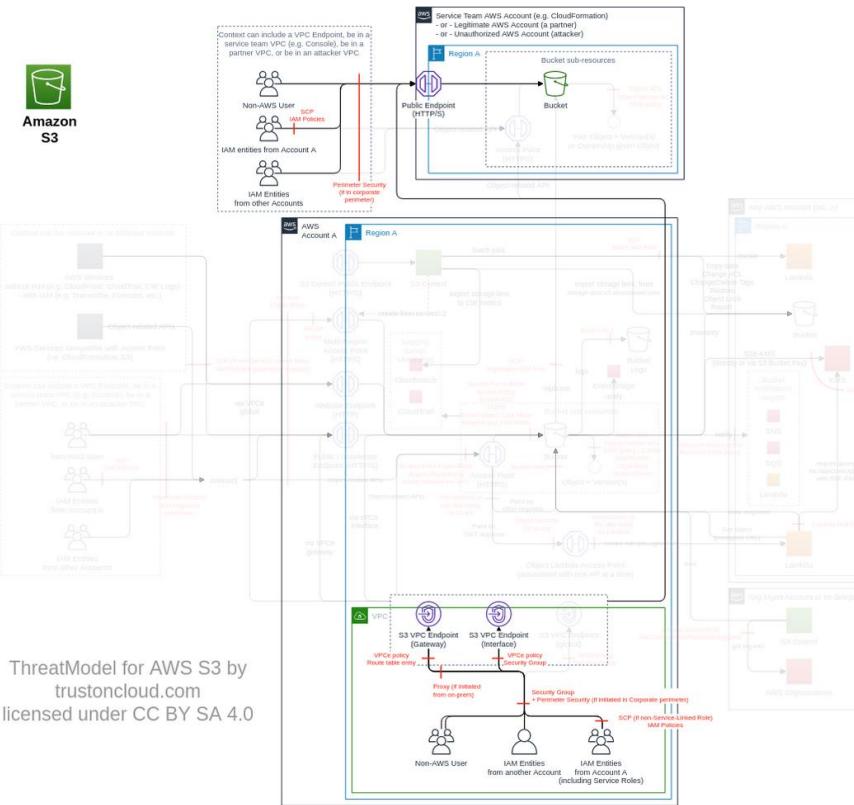


| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Block changes to make an object public via object ACL</b><br>Deny requests to change object ACL to public (e.g. using an SCP, S3 bucket policy and VPC endpoint policy blocking PutObjectAcl for "s3:x-amz-grant-read", "s3:x-amz-grant-read-acp", "s3:x-amz-grant-write-acp", "s3:x-amz-grant-full-control" on the following predefined groups " <a href="http://acs.amazonaws.com/groups/global/AllUsers">http://acs.amazonaws.com/groups/global/AllUsers</a> " and " <a href="http://acs.amazonaws.com/groups/global/AuthenticatedUsers">http://acs.amazonaws.com/groups/global/AuthenticatedUsers</a> ")<br>Monitor ObjectACL changed (or tentatively changed) to public using CloudTrail S3 data events | Very High | -                        | 1            | 1         |
| <b>Disabling ACLs for all buckets</b><br>Ensure bucket ACL and object ACL are disabled on each bucket<br>Prevent the creation of buckets with ACL enabled (e.g. by using a SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note it does not block someone to enable ACL afterwards via PutPutBucketOwnershipControls.  | Very High | 1                        | 1            | -         |
| <b>Identify and ensure the protection all external buckets hosting your objects</b><br>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel).<br>Allow only authorized ACL on objects for bucket you don't control (e.g. using IAM and VPC endpoint policy with the <a href="#">ACL conditions</a> )   | High      | 1                        | 1            | -         |
| <b>Enable CloudTrail S3 data events</b><br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel  | Medium    | 1                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b>  | Low       | 2                        | -            | -         |

|   |  |  |  |  |
|---|--|--|--|--|
| Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions. |  |  |  |  |
| In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account.  |  |  |  |  |

## Intercept data in transit to an external bucket

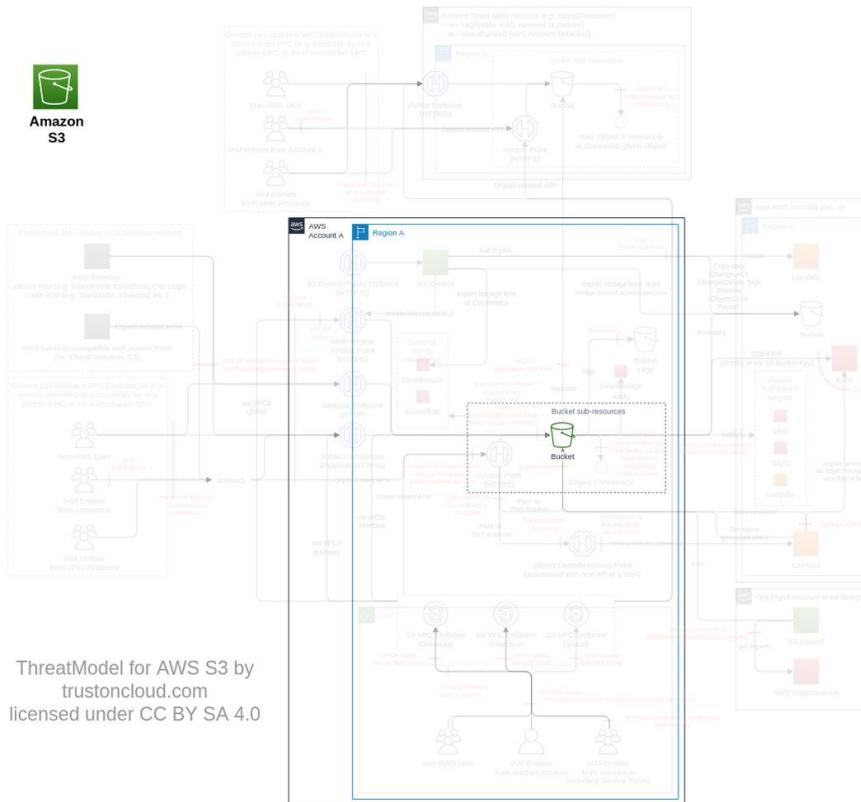
|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T12  |
| <b>Name</b>             | Intercept data in transit to an external bucket   |
| <b>Description</b>      | S3 allows communication over HTTP. An attacker can intercept the traffic you send on an external bucket, in order to read or modify the data. |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Medium (4.6)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:any"<br>}  |



| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Enforce encryption-in-transit</b><br><br>Block all unencrypted requests and unauthorized TLS version(s) from IAM entities you control (e.g. by denying all unencrypted request with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != "authorized TLS version(s)", using an SCP on your AWS Organization root node)<br>Block all unencrypted requests and unauthorized TLS version(s) from VPC endpoints you control (e.g. by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != "authorized TLS version(s)", on the VPC endpoint policy)<br>Monitor and investigate that all requests made with HTTP (e.g. via CloudTrail S3 data events with the lack of additionalEventData.CipherSuite)<br>Maintain a list of authorized version(s) of TLS/SSL per bucket (or per account/OU/Org) | Very High | 1                        | 2            | 1         |
| <b>Encrypt or tokenize critical data</b><br><br>Aligned with your data governance, encrypt on the client side - or tokenize - appropriate data  | Medium    | 1                        | -            | -         |
| <b>Enable CloudTrail S3 data events</b><br><br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel  | Medium    | 1                        | -            | -         |
| <b>Block S3 endpoints in your corporate perimeter security</b><br><br>Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g. firewalls, or cloud interception proxy like <a href="#">Kivera</a> ) including via Internet Gateway, to force usage of VPC endpoints. It will block data-plane transfer. Note: AWS console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com").   | Low       | 1                        | -            | -         |

## Unauthorized object restore into an unauthorized bucket

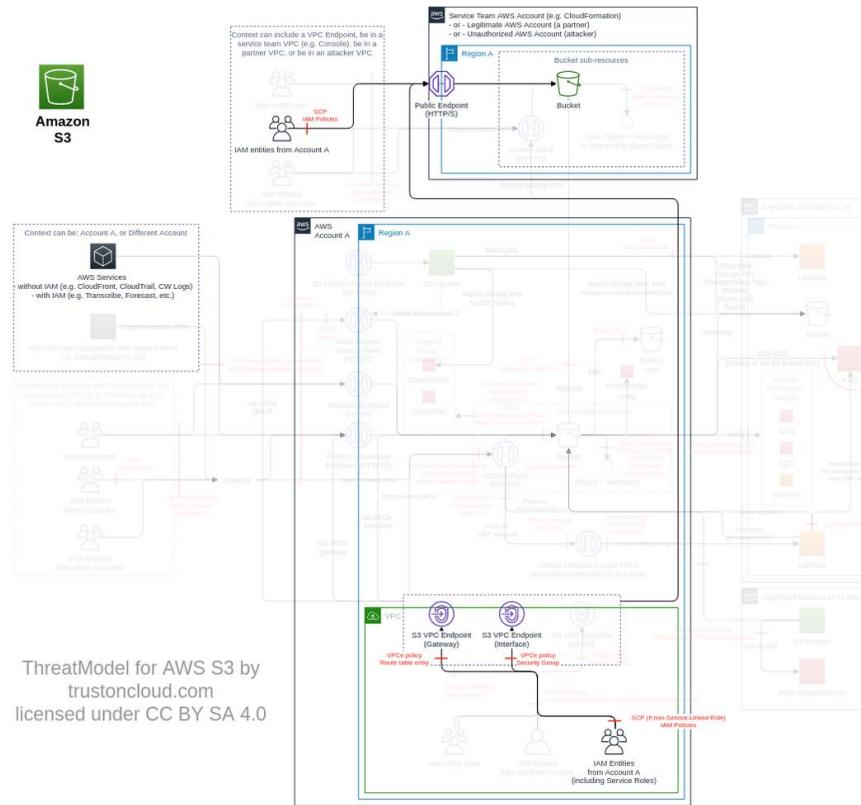
|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T26   |
| <b>Name</b>             | Unauthorized object restore into an unauthorized bucket  |
| <b>Description</b>      | Objects can be stored in S3 Glacier. An attacker can restore an object to an unauthorized S3 bucket to collect or exfiltrate data. |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">Medium (4.5)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:RestoreObject"<br>}   |



| Control Objectives  | Priority | # of associated Controls |              |           |
|---|----------|--------------------------|--------------|-----------|
|   |          | Directive                | Preventative | Detective |
| <b>Limit the access to the IAM actions required to execute the threats</b><br><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. | Medium   | 2                        | -            | -         |

## Upload in an authorized external bucket, but in an incorrect AWS account

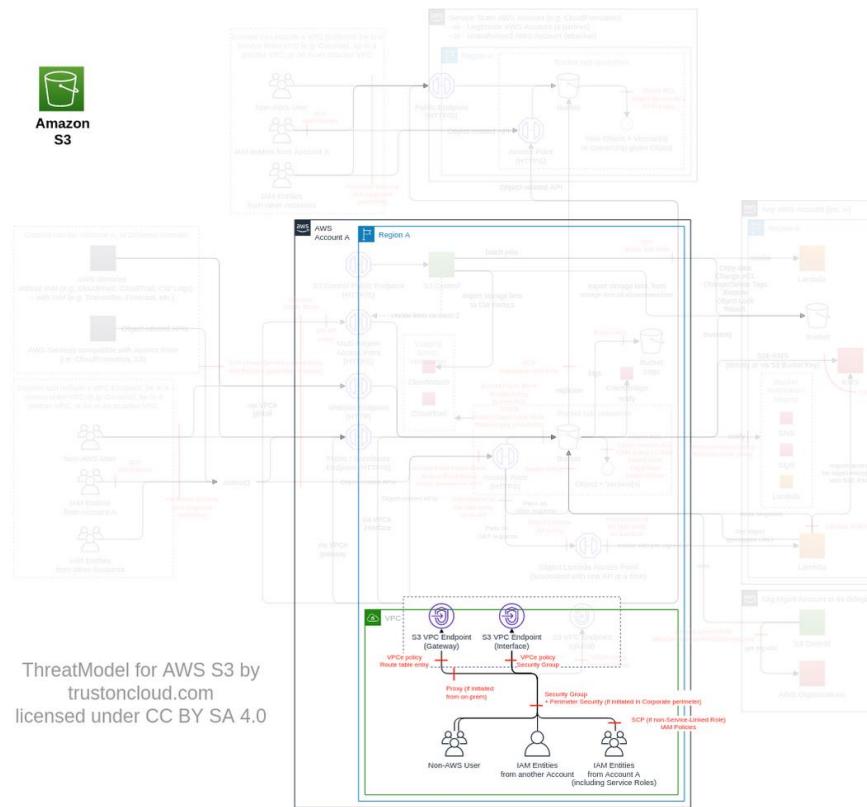
|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T31   |
| <b>Name</b>             | Upload in an authorized external bucket, but in an incorrect AWS account   |
| <b>Description</b>      | Bucket names are globally unique. An attacker can take over a legitimate external bucket, and deceive you into sending it to their bucket. |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">Medium (4.0)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutObject"<br>}   |



| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Identify and ensure the protection all external buckets hosting your objects</b><br>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel).<br>Monitor that only authorized external buckets are used (e.g. via CloudTrail S3 data events in resources[].accountId and resources[].ARN). Both account ID and bucket name must be verified.<br>Request access via S3 access point on bucket you don't own, if compatible with your interaction with the bucket (e.g. not through not-compatible AWS service) | Very High | 2                        | -            | 1         |
| <b>Block requests with KMS keys from unauthorized AWS account(s)</b><br>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account<br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)<br>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in response.x-amz-server-side-encryption-aws-kms-key-id)   | Very High | 1                        | 1            | 1         |
| <b>Enable CloudTrail S3 data events</b><br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel   | Medium    | 1                        | -            | -         |
| <b>Encrypt or tokenize critical data</b><br>Aligned with your data governance, encrypt on the client side - or tokenize - appropriate data   | Low       | 1                        | -            | -         |

## Exfiltrate data via ungoverned S3 endpoint

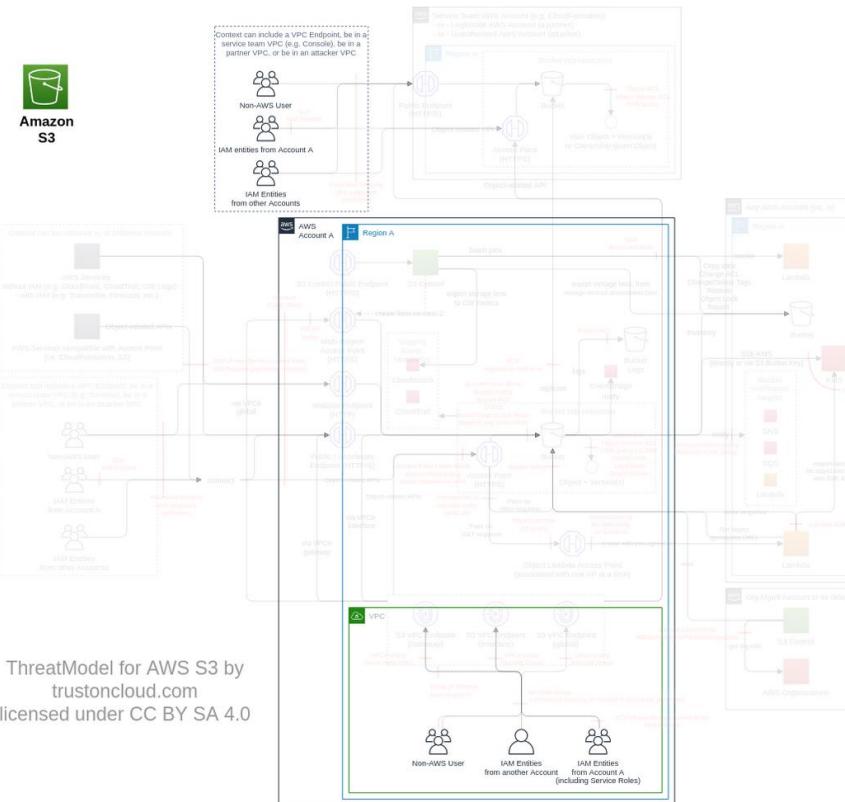
|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T45   |
| <b>Name</b>             | Exfiltrate data via ungoverned S3 endpoint   |
| <b>Description</b>      | S3 VPC endpoints can be either Interface or Gateway. An attacker can create a second endpoint to create an ungoverned exfiltration vector. |
| <b>Goal</b>             | Launch another attack  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0005</a>   |
| <b>CVSS</b>             | <a href="#">Low (1.9)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "ec2:CreateVpcEndpoint"<br>}  |



| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Limit and monitor access via S3 VPC endpoints</b><br>Ensure all S3 VPC endpoints (Interface and Gateway) are covered by the VPC endpoints controls | Very High | 1                        | -            | -         |

## Use of less secure or old S3 features

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T35  |
| <b>Name</b>             | Use of less secure or old S3 features   |
| <b>Description</b>      | S3 was launched in 2006, and its features have evolved. An attacker can use older features that have been proven less secure by AWS (e.g. certain API configuration, <a href="#">SigV2</a> , path-style model), but are still maintained for retro-compatibility. |
| <b>Goal</b>             | Launch another attack   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Low (1.9)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:deprecated"<br>}   |



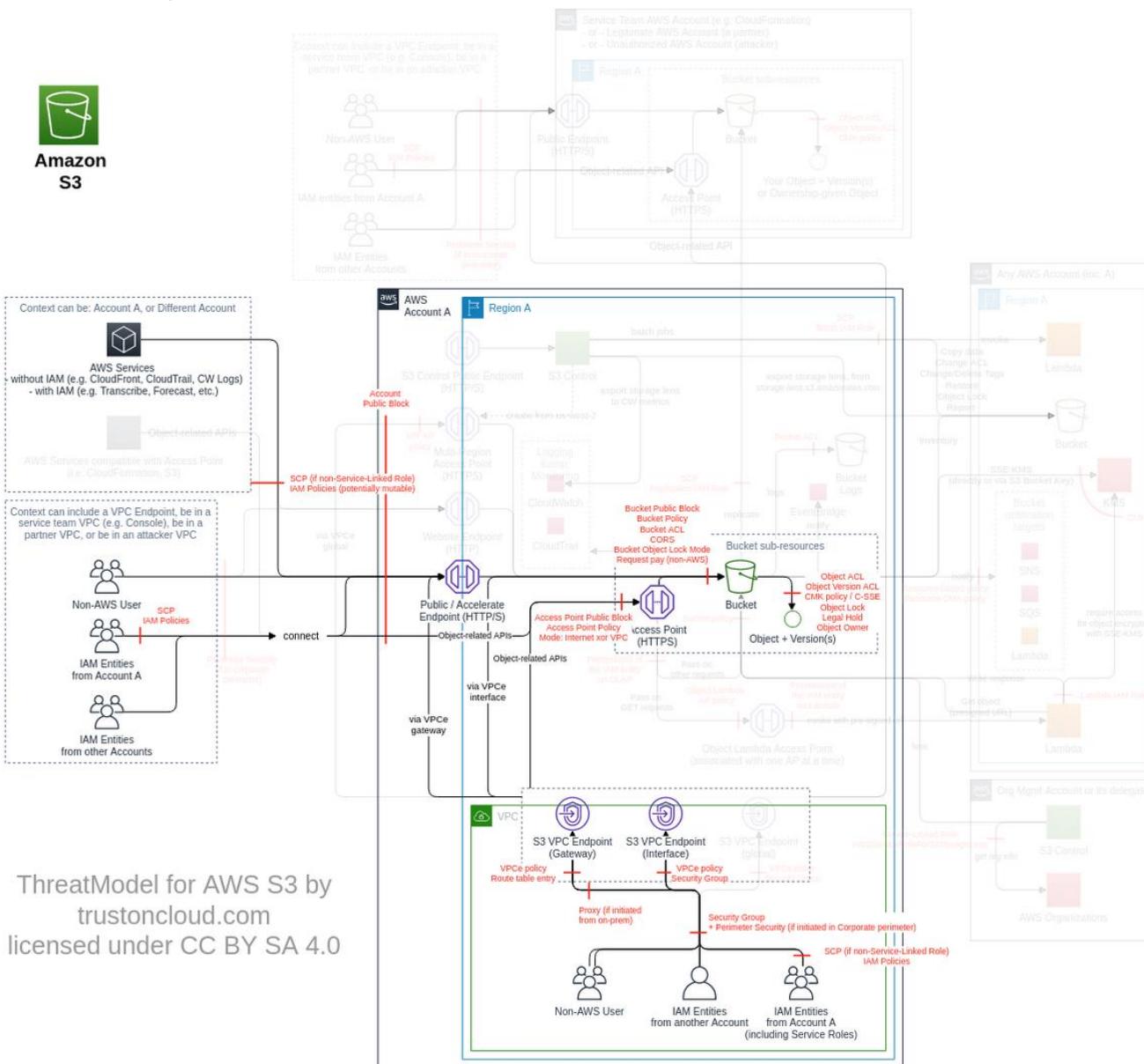
| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Enforce good coding practice</b><br>When connecting to S3 endpoints, use virtual-hosted model ("my-bucket-name.s3.amazonaws.com" or "my-bucket-name.my-s3-regional-endpoint.amazonaws.com") instead of path-style model ("s3.amazonaws.com/my-bucket-name" or "my-s3-regional-endpoint.amazonaws.com/my-bucket-name") (see <a href="#">ref</a> ). All the latest SDK make use of domain style, by default.<br>Monitor that all S3 connections are made with virtual-hosted model (e.g via CloudTrail S3 requestParameters.Host)                            | Very High | 1                        | -            | 1         |
| <b>Block direct public access</b><br>Use SDK with SigV4 enabled ( <a href="#">ref</a> )   | Very High | 1                        | -            | -         |
| <b>Block all requests not using SigV4</b><br>Block all requests not using SigV4 (e.g. using an SCP and S3 policy on all buckets with deny on "StringNotEquals": {"s3:signatureversion": "AWS4-HMAC-SHA256"})<br>Monitor and investigate that all requests not using SigV4 (e.g via CloudTrail S3 with the additionalEventData.SignatureVersion different from "SigV4")  | Very High | -                        | 1            | 1         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. | High      | 2                        | -            | -         |
| <b>Block deprecated actions</b><br>Block deprecated S3 actions, using IAM ThreatModel and the S3 actions list.  | Medium    | 1                        | -            | -         |
| <b>Enable CloudTrail S3 data events</b>   | Medium    | 1                        | -            | -         |

|   |  |  |  |  |
|---|--|--|--|--|
| Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel |  |  |  |  |
|---|--|--|--|--|

# Bucket (subclass of Object upload/download, FC5)

To upload your data into your AWS account, you must create an S3 bucket in one of the AWS Regions.

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

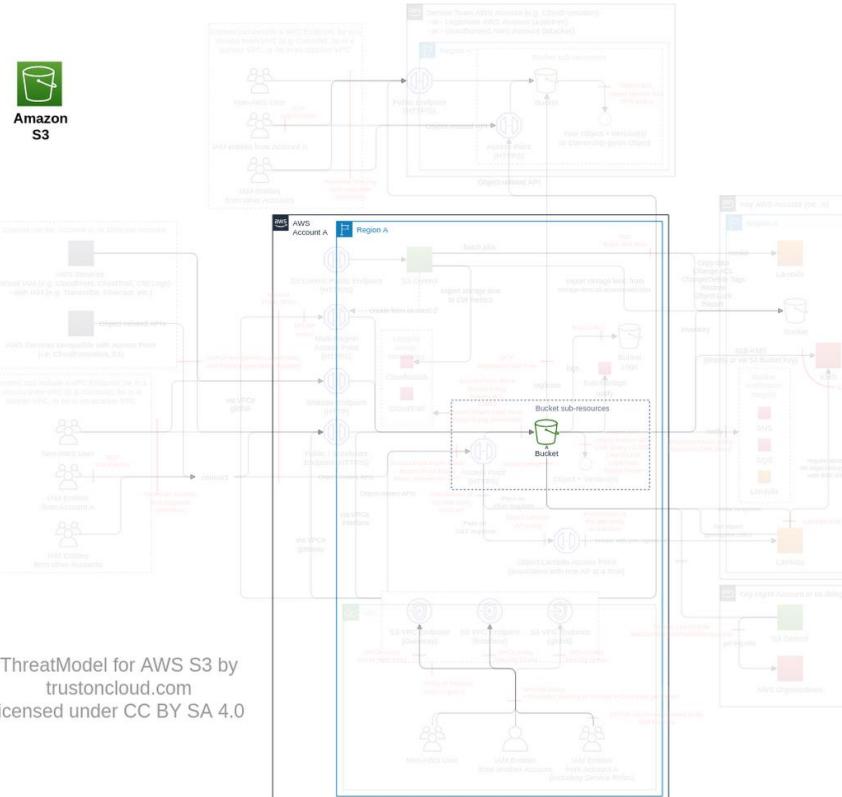
| Action               | IAM Permission  |
|----------------------|-----------------|
| Creates a new bucket | s3:CreateBucket |

## Threat List

| Name  | CVSS                         |
|---|------------------------------|
| Use bucket to upload a malware or modify an object to include a malware             | <a href="#">High (7.3)</a>   |
| Exfiltrate data by using of a compromised IAM access from Internet                  | <a href="#">Medium (6.5)</a> |
| Files encrypted for ransomware  | <a href="#">Medium (6.3)</a> |
| Destroy or modify primary data  | <a href="#">Medium (6.1)</a> |
| Object made public or accessible in a private bucket you own by changing object ACL | <a href="#">Medium (5.9)</a> |
| Bucket takeover to gather data  | <a href="#">Medium (5.2)</a> |
| Intercept data in transit to an internal bucket                                     | <a href="#">Medium (4.6)</a> |
| Use AWS services to access data on S3   | <a href="#">Medium (4.4)</a> |
| Move prod data in non-prod environment  | <a href="#">Medium (4.4)</a> |
| Hotlinking content from S3 bucket   | <a href="#">Low (3.5)</a>    |
| Increase bill by restoring large amount of data                                     | <a href="#">Low (2.7)</a>    |
| Increase bill by creating incomplete uploads  | <a href="#">Low (2.3)</a>    |
| Abuse MD5 etag  | <a href="#">Low (1.8)</a>    |

## Use bucket to upload a malware or modify an object to include a malware

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T14  |
| <b>Name</b>             | Use bucket to upload a malware or modify an object to include a malware   |
| <b>Description</b>      | S3 buckets are commonly used to distribute software. An attacker can upload malware in a bucket to better position it for later use, or directly change an object to include a malware ( <a href="#">example</a> ). |
| <b>Goal</b>             | Launch another attack   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>  |
| <b>CVSS</b>             | <a href="#">High (7.3)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutObject"<br>}  |

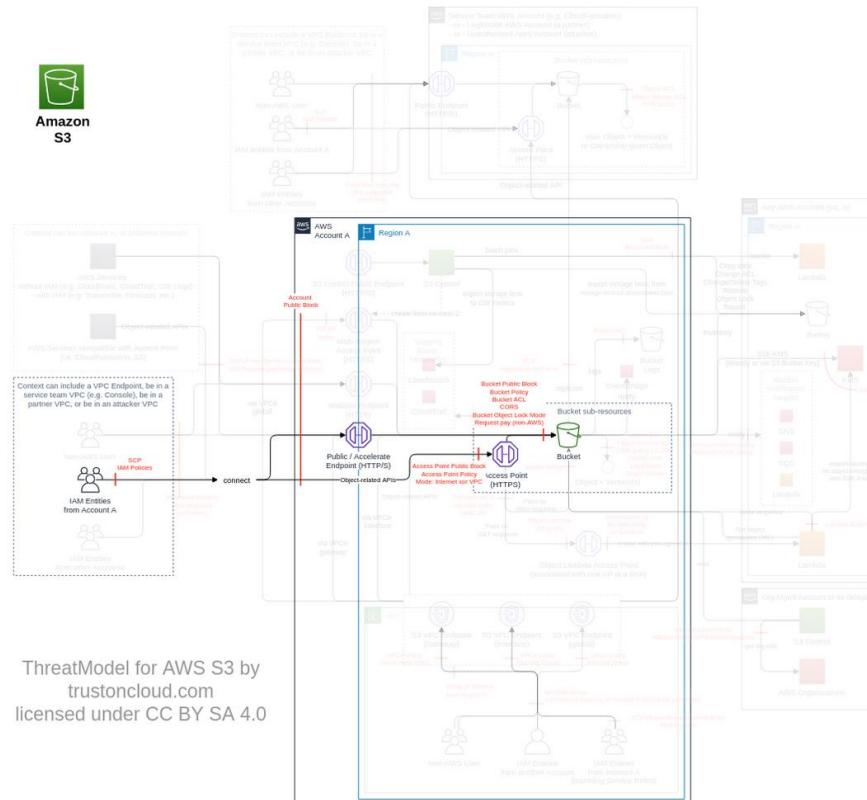


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Block direct public access</b><br><br>Front buckets required to be public, using authenticated CDN (e.g. CloudFront) or API Gateway, protected with WAF (e.g. for <a href="#">hotlinking</a> )<br>Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.<br>Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.<br>Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true. | Very High | 1                        | 3            | -         |
| <b>Limit access from only authorized VPCs</b><br><br>For each S3 bucket, maintain a list of VPC(s), authorized to access it.<br>Limit the access to only those VPC(s) (e.g. using S3 bucket statement, deny if the condition "aws:SourceVpc", or if the bucket policy size is beyond the limit, use this condition on access point)  | High      | 1                        | 1            | -         |
| <b>Identify and ensure the protection all external buckets hosting your objects</b><br><br>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel).<br>Scan all data before uploading to an external bucket to ensure the classification of the data is aligned with the bucket classification (e.g. using Macie).  | High      | 2                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account.  | High      | 2                        | -            | -         |
| <b>Scan input/output objects for malware</b>   | Medium    | -                        | -            | 1         |

If the bucket is used as an input or the output of a process, scan the objects for malware (e.g. using [VirusScan](#) or [Trend Micro Cloud One](#))

## Exfiltrate data by using of a compromised IAM access from Internet

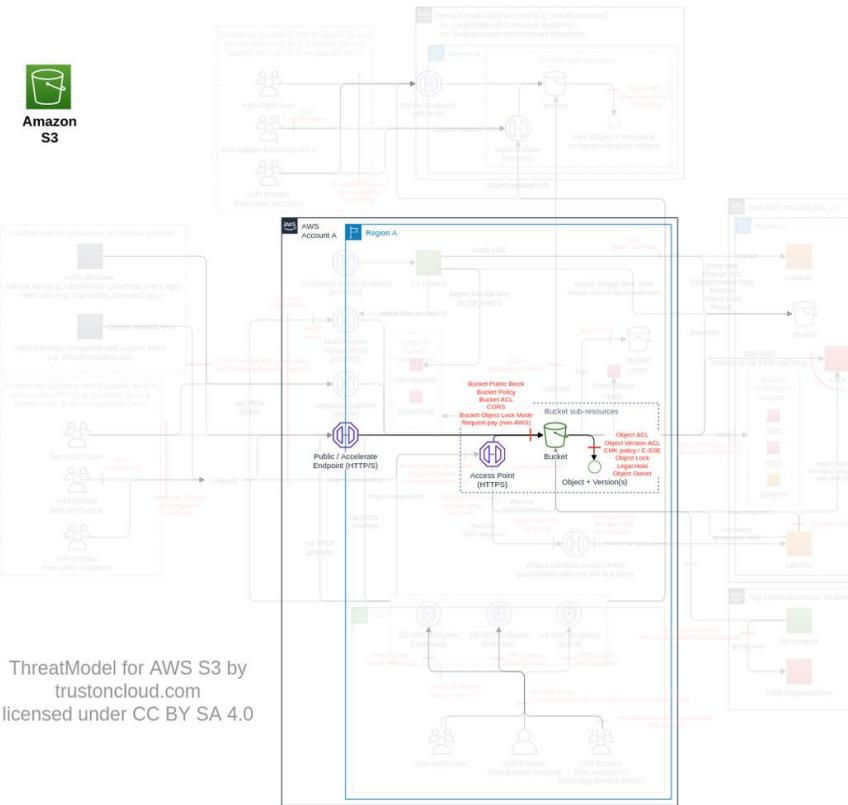
|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T39   |
| <b>Name</b>             | Exfiltrate data by using of a compromised IAM access from Internet   |
| <b>Description</b>      | IAM credentials can be compromised (directly or using <a href="#">pre-signed URL</a> ). An attacker can use a compromised but authorized IAM credential to download your object from an internal bucket via the public endpoint (using or not their own VPC endpoint). |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">Medium (6.5)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:GetObject"<br>}   |



| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Limit access from only authorized VPCs</b><br>For each S3 bucket, maintain a list of VPC(s), authorized to access it.<br>Limit the access to only those VPC(s) (e.g. using S3 bucket statement, deny if the condition "aws:SourceVpce", or if the bucket policy size is beyond the limit, use this condition on access point)   | Very High | 1                        | 1            | -         |
| <b>Block all requests not using HTTP authorization header, if not explicitly authorized</b><br>Block all requests not using HTTP authorization header, i.e. presign via query strings or POST ( <a href="#">ref</a> ) (e.g. using an SCP and S3 policy on all buckets with deny on "StringNotEquals": {"s3:authType": "REST-HEADER"}). Note it blocks uploads via the console, as well.<br>Monitor and investigate that all requests not using HTTP authorization header (e.g via CloudTrail S3 with the additionalEventData.AuthenticationMethod different from "AuthHeader") | Medium    | -                        | 1            | 1         |
| <b>Enable CloudTrail S3 data events</b><br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel   | Medium    | 1                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account.                  | Medium    | 2                        | -            | -         |

## Files encrypted for ransomware

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T16   |
| <b>Name</b>             | Files encrypted for ransomware   |
| <b>Description</b>      | S3 provides several types of encryption where the key is not operated by AWS (e.g. SSE-KMS with Bring Your Own Key). An attacker can encrypt all the data stored in S3 to ransom the data owner to get the decryption key ( <a href="#">blog</a> ). Alternatively, an attacker can change the default encryption key, for a similar effect on any new data uploaded. |
| <b>Goal</b>             | Direct Financial Gain  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>   |
| <b>CVSS</b>             | <a href="#">Medium (6.3)</a>   |
| <b>IAM Access</b>       | {<br>"AND": ["s3:GetObject", "s3:PutObject"]<br>}  |

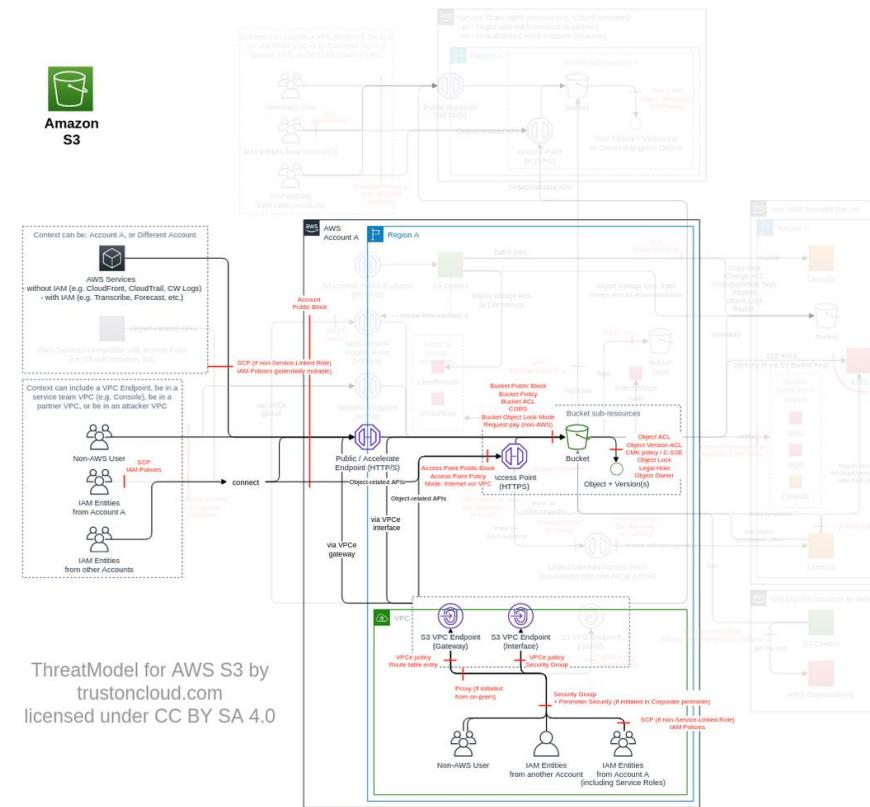


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Enforce encryption-at-rest</b><br><br>Maintain a list of authorized KMS key(s) for each bucket, and their default encryption key. You might simplify by using only 1 key per bucket, ideally dedicated. Note that S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ).<br><br>Ensure all objects on S3 buckets are encrypted with an authorized KMS key<br>Block PutObject requests with unauthorized KMS key on each bucket (e.g. using an S3 bucket policy deny statement on PutObject if the condition if exists "s3:x-amz-server-side-encryption-aws-kms-key-id" is not an authorized KMS key)<br>Monitor that only authorized KMS key(s) are used on each bucket (using CloudTrail S3 data events in <i>requestParameter.bucketName</i> and <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> )<br>Maintain a list of buckets (or paths) required to be encrypted with server-side encryption with customer-provided keys (SSE-C)<br>For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g. using an S3 bucket policy deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present)<br>For buckets (or paths) requiring SSE-C, monitor that only authorized encryption is used on each bucket or path (using CloudTrail S3 data events in <i>requestParameter.bucketName</i> and <i>response.x-amz-server-side-encryption-customer-algorithm</i> ) | Very High | 3                        | 2            | 2         |
| <b>Protect primary data against loss</b><br><br>Enable versioning on buckets holding primary data<br>Backup primary data in a secure location under a different security authority (e.g. in an <a href="#">AWS data bunker account</a> via replication)  | Very High | 2                        | -            | -         |
| <b>Use S3 Object Lock to protect data integrity</b><br><br>Implement the authorized default S3 Object Lock on each bucket (note: Amazon S3 evaluates and applies bucket policies before applying bucket default S3 Object Lock settings)<br>Block PutObject and PutObjectRetention requests with unauthorized S3 Object Lock on each bucket (e.g. using an S3 bucket policy deny statement on PutObject and PutObjectRetention if the condition if exists "s3:object-lock-mode" and "s3:object-lock-remaining-retention-days" is not the defined S3 Object Lock configuration)   | Very High | -                        | 2            | -         |

|  |           |   |   |   |
|--|-----------|---|---|---|
| <b>Block requests with KMS keys from unauthorized AWS account(s)</b><br>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account<br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)<br>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> ) | Very High | 1 | 1 | 1 |
| <b>Enable CloudTrail S3 data events</b><br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel   | Medium    | 1 | - | - |
| <b>Monitor S3 with Amazon GuardDuty and Macie</b><br>Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using GuardDuty ThreatModel. Ensure findings are investigated (e.g. using Amazon Detective).  | Medium    | 1 | - | - |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account.  | Medium    | 2 | - | - |
| <b>Have a process to apply legal hold</b><br>Create a process to apply legal hold to any S3 bucket, whenever required. The condition "s3:object-lock-legal-hold" can be used to restrict who can remove such a lock.   | Low       | 1 | - | - |

## Destroy or modify primary data

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T17  |
| <b>Name</b>             | Destroy or modify primary data  |
| <b>Description</b>      | S3 provides high durability by design (11 9s), however data can still be deleted by the customer. An attacker (or someone by negligence) can use its access to destroy (or modify) primary data located on S3, affecting the ability for the business to operate (for example, <a href="#">Code Spaces</a> ). |
| <b>Goal</b>             | Disruption of Service   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>  |
| <b>CVSS</b>             | <a href="#">Medium (6.1)</a>  |
| <b>IAM Access</b>       | {<br>"AND": ["s3>DeleteObject", {<br>"OPTIONAL": "S3>DeleteObjectVersion"<br>}, {<br>"OPTIONAL": "s3>BypassGovernanceMode"<br>}]  |

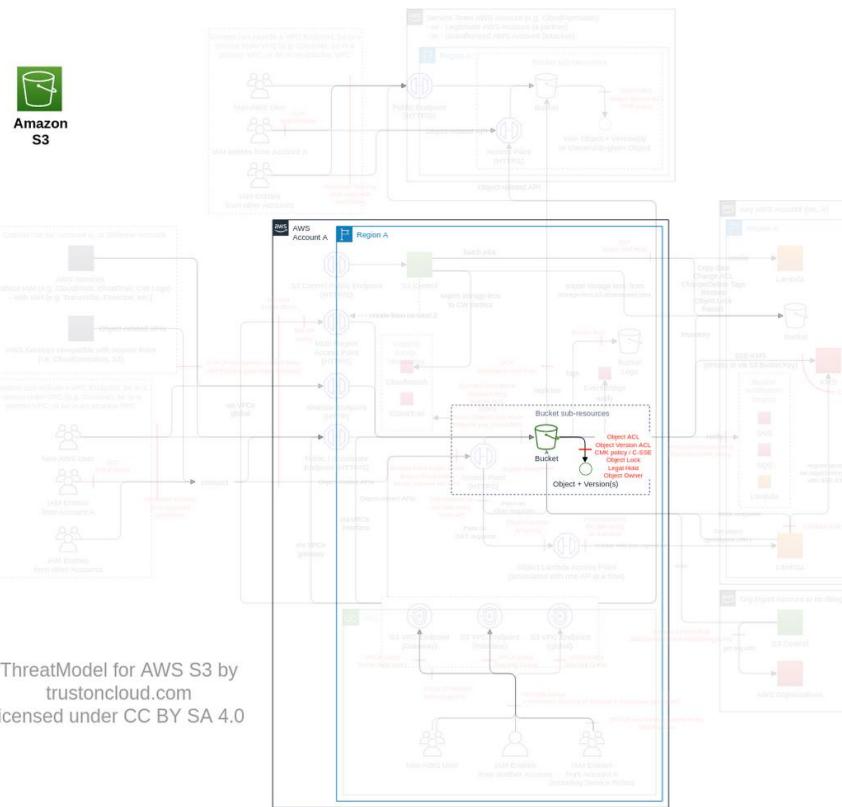


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Identify and ensure the protection all internal buckets hosting your objects</b><br><br>Track all buckets you control, define their authorized data classification, identify whether the hosted data is primary (i.e. source of truth, for example logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g. file-processing, software package, etc.), their WORM requirements (e.g. SEC 17a-4, CTCC, etc.), if they are production/non-production (preferably done at account-level), their storage class. You may use tags, Infra-as-code, AWS Glue Data Catalog or external management tool like <a href="#">FINRA herd</a> )  | Very High | 1                        | -            | -         |
| <b>Enforce encryption-at-rest</b><br><br>Maintain a list of authorized KMS key(s) for each bucket, and their default encryption key. You might simplify by using only 1 key per bucket, ideally dedicated. Note that S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ).<br><br>Ensure all objects on S3 buckets are encrypted with an authorized KMS key<br>Use KMS ThreatModel to protect the KMS keys used for S3 (e.g. using encryptionContext on the policy of each KMS key)<br>Implement an authorized default encryption key on each bucket and enable S3 Bucket Key (note: Amazon S3 evaluates and applies bucket policies before applying bucket default encryption settings)<br>Block PutObject requests with unauthorized KMS key on each bucket (e.g. using an S3 bucket policy deny statement on PutObject if the condition if exists "s3:x-amz-server-side-encryption-aws-kms-key-id" is not an authorized KMS key) | Very High | 4                        | 1            | -         |
| <b>Protect primary data against loss</b><br><br>Enable versioning on buckets holding primary data<br>Backup primary data in a secure location under a different security authority (e.g. in an <a href="#">AWS data bunker account</a> via replication)  | Very High | 2                        | -            | -         |
| <b>Use S3 Object Lock to protect data integrity</b><br><br>Implement the authorized default S3 Object Lock on each bucket (note: Amazon S3 evaluates and applies bucket policies before applying bucket default S3 Object Lock settings)   | Very High | -                        | 2            | -         |

|   |        |   |   |   |
|---|--------|---|---|---|
| Block PutObject and PutObjectRetention requests with unauthorized S3 Object Lock on each bucket (e.g. using an S3 bucket policy deny statement on PutObject and PutObjectRetention if the condition if exists "s3:object-lock-mode" and "s3:object-lock-remaining-retention-days" is not the defined S3 Object Lock configuration)  |        |   |   |   |
| <b>Limit access from only authorized VPCs</b><br>For each S3 bucket, maintain a list of VPC(s), authorized to access it.<br>Limit the access to only those VPC(s) (e.g. using S3 bucket statement, deny if the condition "aws:SourceVpce", or if the bucket policy size is beyond the limit, use this condition on access point)  | High   | 1 | 1 | - |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. | High   | 2 | - | - |
| <b>Have a process to apply legal hold</b><br>Create a process to apply legal hold to any S3 bucket, whenever required. The condition "s3:object-lock-legal-hold" can be used to restrict who can remove such a lock.  | Medium | 1 | - | - |
| <b>Encrypt or tokenize critical data</b><br>Aligned with your data governance, encrypt on the client side - or tokenize - appropriate data  | Low    | 1 | - | - |

## Object made public or accessible in a private bucket you own by changing object ACL

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T36   |
| <b>Name</b>             | Object made public or accessible in a private bucket you own by changing object ACL  |
| <b>Description</b>      | Bucket authority only prevails on object ACL when the object access is explicitly denied by the bucket authority ( <a href="#">ref</a> ). An attacker (or someone by negligence) can change the object ACL to make it public or accessible for themselves (to exfiltrate or modify). |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">Medium (5.9)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutObjectAcl"<br>}  |

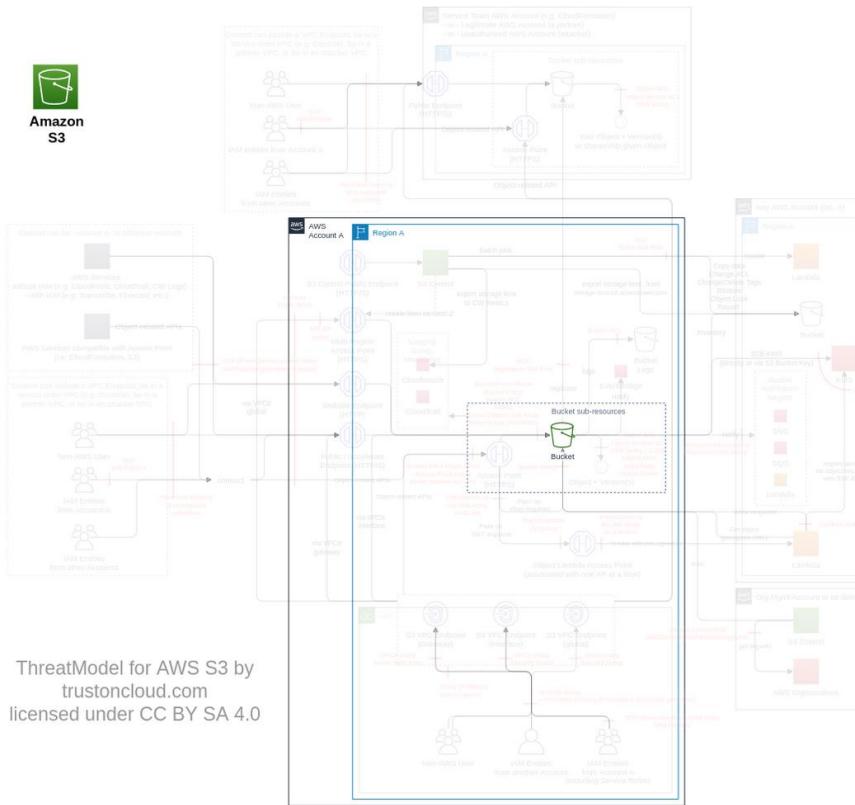


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Block changes to make an object public via object ACL</b><br><br>Deny requests to change object ACL to public (e.g. using an SCP, S3 bucket policy and VPC endpoint policy blocking PutObjectAcl for "s3:x-amz-grant-read", "s3:x-amz-grant-read-acp", "s3:x-amz-grant-write-acp", "s3:x-amz-grant-full-control" on the following predefined groups " <a href="http://acs.amazonaws.com/groups/global/AllUsers">http://acs.amazonaws.com/groups/global/AllUsers</a> " and " <a href="http://acs.amazonaws.com/groups/global/AuthenticatedUsers">http://acs.amazonaws.com/groups/global/AuthenticatedUsers</a> ")<br>Monitor ObjectACL changed (or tentatively changed) to public using CloudTrail S3 data events<br>Monitor and investigate anonymous requests to objects (e.g. using CloudTrail S3 data events with userIdentity.accountId=ANONYMOUS_PRINCIPAL)  | Very High | -                        | 1            | 2         |
| <b>Block direct public access</b><br><br>Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.<br>Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.<br>Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.   | Very High | -                        | 3            | -         |
| <b>Enforce encryption-at-rest</b><br><br>Maintain a list of authorized KMS key(s) for each bucket, and their default encryption key. You might simplify by using only 1 key per bucket, ideally dedicated. Note that S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ).<br>Ensure all objects on S3 buckets are encrypted with an authorized KMS key<br>Use KMS ThreatModel to protect the KMS keys used for S3 (e.g. using encryptionContext on the policy of each KMS key)<br>Implement an authorized default encryption key on each bucket and enable S3 Bucket Key (note: Amazon S3 evaluates and applies bucket policies before applying bucket default encryption settings)<br>Block PutObject requests with unauthorized KMS key on each bucket (e.g. using an S3 bucket policy deny statement on PutObject if the condition if exists "s3:x-amz-server-side-encryption-aws-kms-key-id" is not an authorized KMS key)<br>Monitor that only authorized KMS key(s) are used on each bucket (using CloudTrail S3 data events in <i>requestParameter.bucketName</i> and <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> ) | Very High | 5                        | 2            | 2         |

|   |           |   |   |   |
|---|-----------|---|---|---|
| Maintain a list of buckets (or paths) required to be encrypted with server-side encryption with customer-provided keys (SSE-C)<br>For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g. using an S3 bucket policy deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present)<br>For buckets (or paths) requiring SSE-C, monitor that only authorized encryption is used on each bucket or path (using CloudTrail S3 data events in <i>requestParameter.bucketName</i> and <i>response.x-amz-server-side-encryption-customer-algorithm</i> ) |           |   |   |   |
| <b>Limit access from only authorized VPCs</b><br>For each S3 bucket, maintain a list of VPC(s), authorized to access it.<br>Limit the access to only those VPC(s) (e.g. using S3 bucket statement, deny if the condition "aws:SourceVpce", or if the bucket policy size is beyond the limit, use this condition on access point)  | Very High | 1 | 1 | - |
| <b>Disabling ACLs for all buckets</b><br>Ensure bucket ACL and object ACL are disabled on each bucket<br>Prevent the creation of buckets with ACL enabled (e.g. by using a SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note it does not block someone to enable ACL afterwards via PutPutBucketOwnershipControls.  | Very High | 1 | 1 | - |
| <b>Monitor S3 with Amazon GuardDuty and Macie</b><br>Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect it using Macie ThreatModel   | High      | 1 | - | - |
| <b>Enable CloudTrail S3 data events</b><br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel  | Medium    | 1 | - | - |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account.   | Low       | 2 | - | - |

## Bucket takeover to gather data

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T1  |
| <b>Name</b>             | Bucket takeover to gather data   |
| <b>Description</b>      | Bucket names are globally unique. An attacker can recreate the same bucket name of a deleted bucket you used to own to collect any new data being uploaded by a non-updated party, do a DNS takeover (using a non-deleted CNAME / CloudFront origin to the bucket) or to use remaining permissions to exfiltrate data. |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">Medium (5.2)</a>   |
| <b>IAM Access</b>       | {<br>"OPTIONAL": "s3>DeleteBucket"<br>}  |

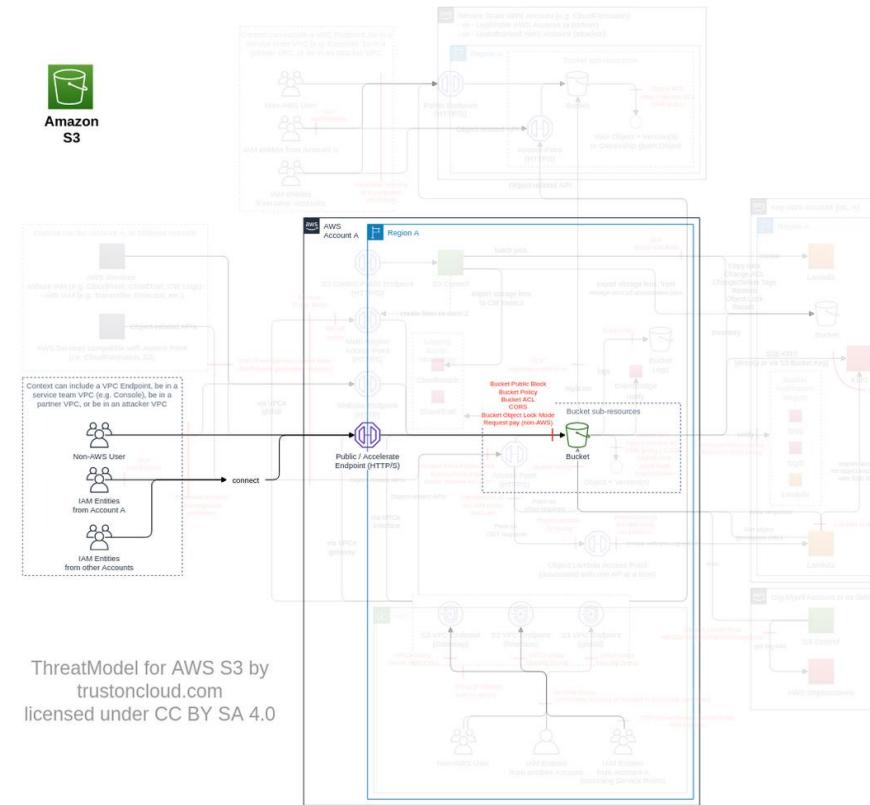


| Control Objectives   |  | Priority  | # of associated Controls |              |           |
|--|--|-----------|--------------------------|--------------|-----------|
|  |  |           | Directive                | Preventative | Detective |
| <b>Prevent deletion of buckets</b>   | Block the action "s3:DeleteBucket" (e.g. via SCP, exemption can be managed by authorizing a SuperAdmin to delete buckets with a certain tag, and with bucket owners able to tag bucket)<br>Scan your CNAME records (e.g. in Route53) and CloudFront origin for deleted buckets   | Very High | -                        | 1            | 1         |
| <b>Block requests with KMS keys from unauthorized AWS account(s)</b>       | Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account<br><br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)<br><br>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> ) | Very High | 1                        | 1            | 1         |
| <b>Enforce good coding practice</b>  | Parameterize S3 bucket name or S3 access point in your code (no hardcoding)<br><br>Ensure all S3 buckets interacted with are in the correct AWS account (e.g. using the condition in all compatible S3 requests: x-amz-expected-bucket-owner and x-amz-source-expected-bucket-owner)   | Medium    | 2                        | -            | -         |
| <b>Enable CloudTrail S3 data events</b>                                    | Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel  | Medium    | 1                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b> | Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.  | Medium    | 2                        | -            | -         |

|  |          |   |   |   |
|--|----------|---|---|---|
| In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account.   |          |   |   |   |
| <b>Identify and ensure the protection all external buckets hosting your objects</b><br>Monitor that only authorized external buckets are used (e.g. via CloudTrail S3 data events in resources[], accountId and resources[], ARN). Both account ID and bucket name must be verified. | Low      | - | - | 1 |
| <b>Encrypt or tokenize critical data</b><br>Aligned with your data governance, encrypt on the client side - or tokenize - appropriate data   | Very Low | 1 | - | - |

## Intercept data in transit to an internal bucket

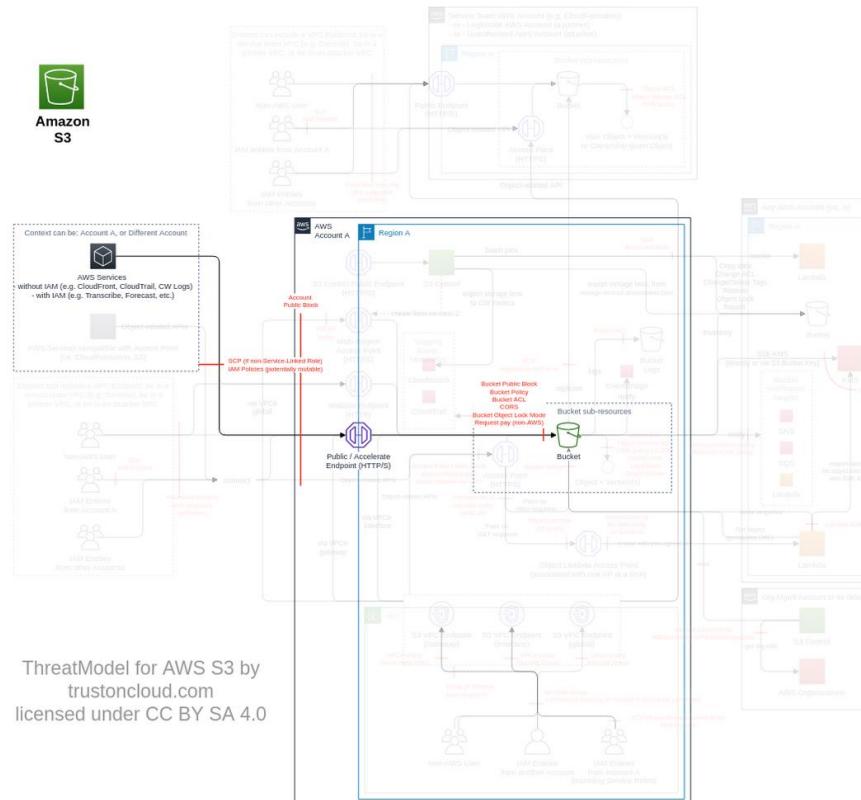
|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T34  |
| <b>Name</b>             | Intercept data in transit to an internal bucket   |
| <b>Description</b>      | S3 allows communication over HTTP. An attacker can intercept the traffic you send on an internal bucket, in order to read or modify the data. |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Medium (4.6)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:any"<br>}  |



| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Enforce encryption-in-transit</b><br><br>Block all unencrypted requests and unauthorized TLS version(s) from IAM entities you control (e.g. by denying all unencrypted request with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != <i>authorized TLS version(s)</i> , using an SCP on your AWS Organization root node)<br><br>Block all unencrypted requests and unauthorized TLS version(s) from VPC endpoints you control (e.g. by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != <i>authorized TLS version(s)</i> , on the VPC endpoint policy)<br><br>Monitor and investigate that all requests made with HTTP (e.g. via CloudTrail S3 data events with the lack of additionalEventData.CipherSuite)<br><br>Block all unencrypted requests to S3 bucket you control (e.g. by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != <i>authorized TLS version(s)</i> , on the S3 bucket policy) | Very High | -                        | 3            | 1         |
| <b>Block S3 endpoints in your corporate perimeter security</b><br><br>Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g. firewalls, or cloud interception proxy like <a href="#">Kivera</a> ) including via Internet Gateway, to force usage of VPC endpoints. It will block data-plane transfer. Note: AWS console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com").   | Very High | 1                        | -            | -         |
| <b>Enable CloudTrail S3 data events</b><br><br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel  | Medium    | 1                        | -            | -         |

## Use AWS services to access data on S3

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T30   |
| <b>Name</b>             | Use AWS services to access data on S3  |
| <b>Description</b>      | Number of AWS services can access S3 to execute their own functions. An attacker can use them to collect data, using their service role or service-linked roles. |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0009</a>   |
| <b>CVSS</b>             | <a href="#">Medium (4.4)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "iam:PassRole"<br>}   |

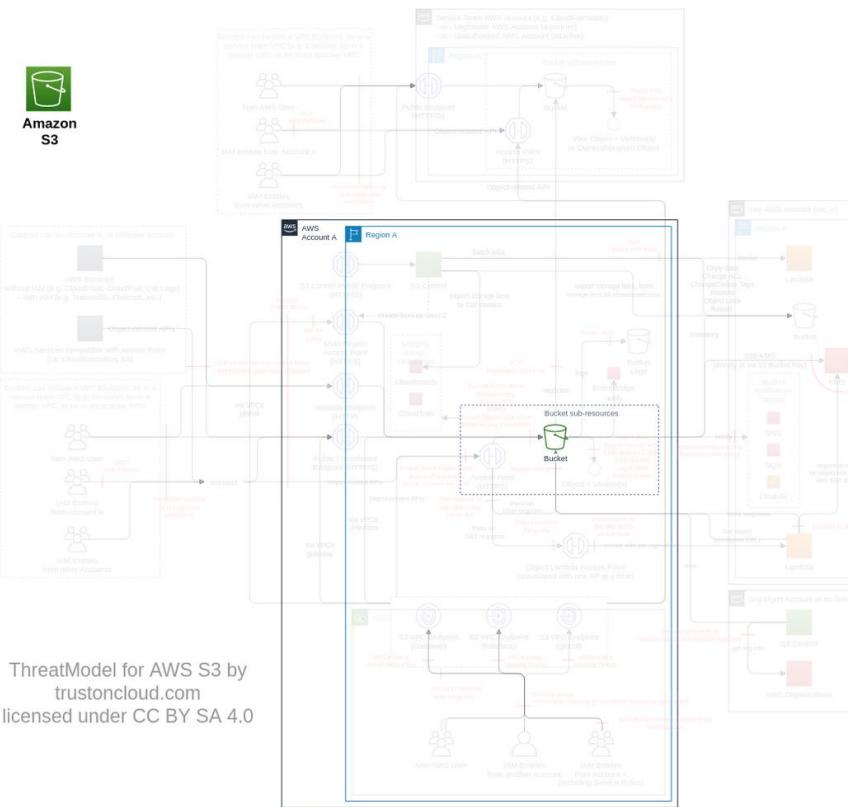


| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Enforce encryption-at-rest</b> <p>Maintain a list of authorized KMS key(s) for each bucket, and their default encryption key. You might simplify by using only 1 key per bucket, ideally dedicated. Note that S3 server access log bucket does not support KMS encryption (<a href="#">ref</a>).</p> <p>Ensure all objects on S3 buckets are encrypted with an authorized KMS key</p> <p>Block PutObject requests with unauthorized KMS key on each bucket (e.g. using an S3 bucket policy deny statement on PutObject if the condition if exists "s3:x-amz-server-side-encryption-aws-kms-key-id" is not an authorized KMS key)</p> <p>Monitor that only authorized KMS key(s) are used on each bucket (using CloudTrail S3 data events in <i>requestParameter.bucketName</i> and <i>response.x-amz-server-side-encryption-aws-kms-key-id</i>)</p> <p>Maintain a list of buckets (or paths) required to be encrypted with server-side encryption with customer-provided keys (SSE-C)</p> <p>For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g. using an S3 bucket policy deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"!="AES256" is not present)</p> <p>For buckets (or paths) requiring SSE-C, monitor that only authorized encryption is used on each bucket or path (using CloudTrail S3 data events in <i>requestParameter.bucketName</i> and <i>response.x-amz-server-side-encryption-customer-algorithm</i>)</p> | Very High | 3                        | 2            | 2         |
| <b>Limit access from only authorized VPCs</b> <p>For each S3 bucket, maintain a list of VPC(s), authorized to access it.</p> <p>Limit the access to only those VPC(s) (e.g. using S3 bucket statement, deny if the condition "aws:SourceVpc", or if the bucket policy size is beyond the limit, use this condition on access point)</p>   | Very High | 1                        | 1            | -         |
| <b>Block requests with KMS keys from unauthorized AWS account(s)</b> <p>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account</p> <p>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)</p> <p>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <i>response.x-amz-server-side-encryption-aws-kms-key-id</i>)</p>   | Very High | 1                        | 1            | 1         |

|   |        |   |   |   |
|---|--------|---|---|---|
| <b>Model the threats on all AWS services accessing S3</b><br>Analyse and protect all AWS services accessing S3 (e.g. via ThreatModel). Enforce usage in VPC only, whenever possible.  | High   | 1 | - | - |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. | Medium | 2 | - | - |
| <b>Encrypt or tokenize critical data</b><br>Aligned with your data governance, encrypt on the client side - or tokenize - appropriate data  | Low    | 1 | - | - |

## Move prod data in non-prod environment

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T11   |
| <b>Name</b>             | Move prod data in non-prod environment   |
| <b>Description</b>      | Multiple types of environments are usually operated in AWS. An attacker can move the data from a secure location (e.g. production) to a less secure location (e.g. dev). |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0009</a>   |
| <b>CVSS</b>             | <a href="#">Medium (4.4)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:GetObject"<br>}   |

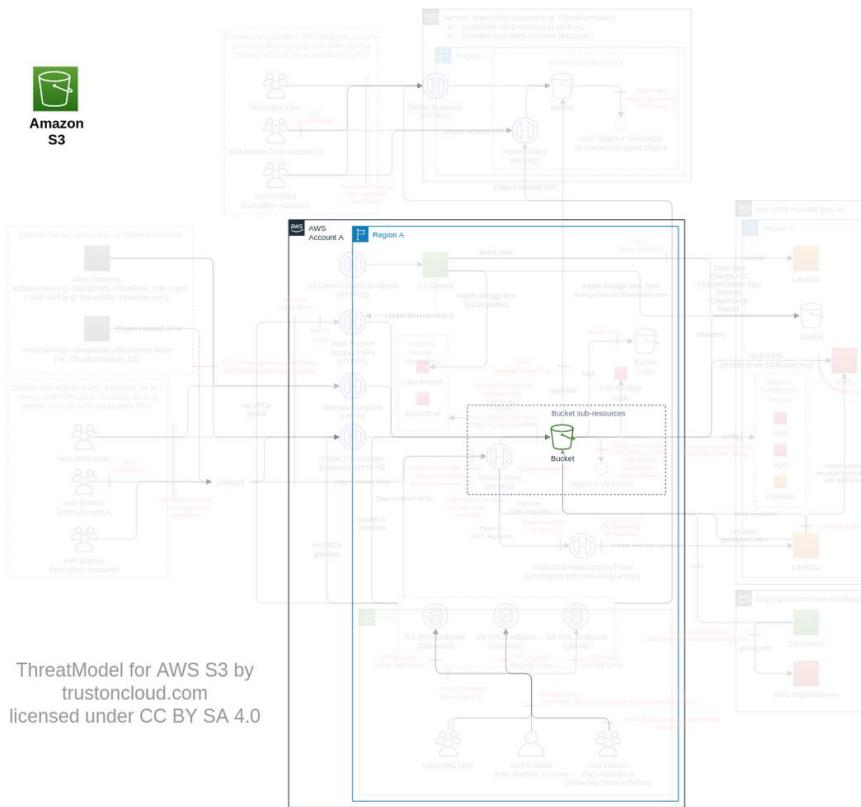


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Identify and ensure the protection all internal buckets hosting your objects</b><br><br>Track all buckets you control, define their authorized data classification, identify whether the hosted data is primary (i.e. source of truth, for example logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g. file-processing, software package, etc.), their WORM requirements (e.g. SEC 17a-4, CTCC, etc.), if they are production/non-production (preferably done at account-level), their storage class. You may use tags, Infra-as-code, AWS Glue Data Catalog or external management tool like <a href="#">FINRA herd</a> )<br>Use a data discovery tool (e.g. Amazon Macie) to control that no sensitive data are stored in unauthorized bucket<br>Use a data discovery tool (e.g. Amazon Macie) to ensure the bucket names, object names, tags and metadata do not contain sensitive data  | Very High | 1                        | -            | 2         |
| <b>Enforce encryption-at-rest</b><br><br>Maintain a list of authorized KMS key(s) for each bucket, and their default encryption key. You might simplify by using only 1 key per bucket, ideally dedicated. Note that S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ).<br>Ensure all objects on S3 buckets are encrypted with an authorized KMS key<br>Block PutObject requests with unauthorized KMS key on each bucket (e.g. using an S3 bucket policy deny statement on PutObject if the condition if exists "s3:x-amz-server-side-encryption-aws-kms-key-id" is not an authorized KMS key)<br>Monitor that only authorized KMS key(s) are used on each bucket (using CloudTrail S3 data events in <i>requestParameter.bucketName</i> and <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> )<br>Maintain a list of buckets (or paths) required to be encrypted with server-side encryption with customer-provided keys (SSE-C)<br>For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g. using an S3 bucket policy deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present)<br>For buckets (or paths) requiring SSE-C, monitor that only authorized encryption is used on each bucket or path (using CloudTrail S3 data events in <i>requestParameter.bucketName</i> and <i>response.x-amz-server-side-encryption-customer-algorithm</i> ) | Very High | 3                        | 2            | 2         |
| <b>Restrict access point access to VPC when in use</b><br><br>Maintain a list of authorized access between VPC, S3 access point and S3.  | Very High | 1                        | 2            | -         |

|   |           |   |   |   |
|---|-----------|---|---|---|
| <p>Limit access via the S3 access point by using in VPC endpoint and/or bucket policy the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of allowlist bucket name in VPC endpoint/bucket policy.</p> <p>Block any <a href="#">object-related operations</a> access to S3 bucket not through access point (i.e. using a deny IAM policy statement with the condition "ArnNotLike" {"s3:DataAccessPointArn": "arn:aws:s3:Region:AccountId:accesspoint/*"})</p>  |           |   |   |   |
| <p><b>Limit and monitor access via S3 VPC endpoints</b></p> <p>For each VPC, maintain a list of AWS Organizations, OU and/or AWS account(s), where IAM entities are authorized to access S3</p> <p>For each VPC with an IAM entity allowed to use S3, secure them with the VPC ThreatModel (e.g. <a href="#">modification of VPC endpoints</a>, <a href="#">VPC endpoint policy</a>, <a href="#">routing table</a>, <a href="#">Security Groups</a>)</p> <p>Block any IAM entity not belonging to an authorized AWS Organizations, OU and/or AWS account(s) to call S3 from your VPCs by adding a deny statement on S3 VPC endpoint policy of each VPC, with the condition using "aws:PrincipalOrgPaths" (<a href="#">ref</a>) including the full Org ID, as those are globally unique.</p> <p>Enable <a href="#">VPC DNS query logging</a> in all VPC</p> <p>Maintain a list of authorized S3 and S3 access point (and their respective AWS accounts) to be access for each VPC</p> <p>Limit the access to only authorized S3 bucket(s) or their AWS account(s) from each VPC (e.g. using the condition key "s3:ResourceAccount" on the VPC endpoint policy, alternatively use specific resource-level statement for each bucket, or if the VPC endpoint policy size is beyond the limit and more granular control on VPC is required, use access points)</p> <p>Monitor VPC DNS query logs that only authorized S3 bucket and S3 access points are being queried in each VPC (e.g. using VPC DNS query logging), and protect it using Route53 ThreatModel</p> | Very High | 4 | 2 | 1 |
| <p><b>Block requests with KMS keys from unauthorized AWS account(s)</b></p> <p>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account</p> <p>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)</p> <p>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <i>response.x-amz-server-side-encryption-aws-kms-key-id</i>)</p>  | Very High | 1 | 1 | 1 |
| <p><b>Limit access from only authorized VPCs</b></p> <p>For each S3 bucket, maintain a list of VPC(s), authorized to access it.</p> <p>Limit the access to only those VPC(s) (e.g. using S3 bucket statement, deny if the condition "aws:SourceVpce", or if the bucket policy size is beyond the limit, use this condition on access point)</p>   | High      | 1 | 1 | - |
| <p><b>Identify and ensure the protection all external buckets hosting your objects</b></p> <p>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel).</p> <p>Monitor that only authorized external buckets are used (e.g. via CloudTrail S3 data events in <i>resources[].accountId</i> and <i>resources[].ARN</i>). Both account ID and bucket name must be verified.</p>  | High      | 1 | - | 1 |
| <p><b>Encrypt or tokenize critical data</b></p> <p>Aligned with your data governance, encrypt on the client side - or tokenize - appropriate data</p>   | Medium    | 1 | - | - |
| <p><b>Enable CloudTrail S3 data events</b></p> <p>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel</p>   | Medium    | 1 | - | - |
| <p><b>Limit the access to the IAM actions required to execute the threats</b></p> <p>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.</p> <p>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account.</p>  | Medium    | 2 | - | - |

## Hotlinking content from S3 bucket

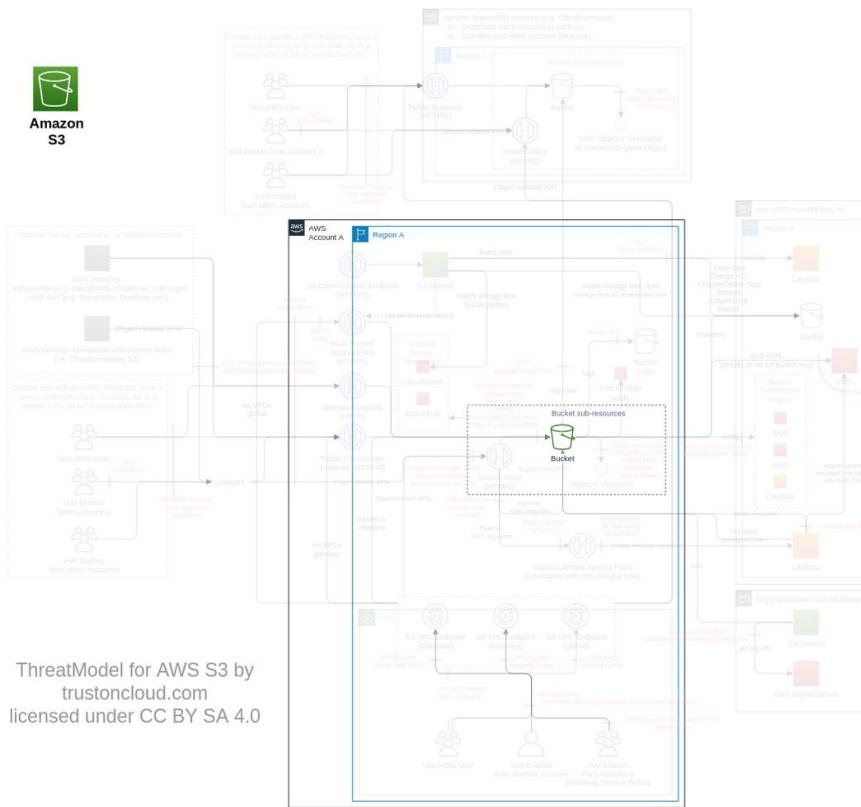
|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T22  |
| <b>Name</b>             | Hotlinking content from S3 bucket   |
| <b>Description</b>      | S3 charges for hosting and data transfer out. An attacker can hotlink your content hosted on S3 on another page to avoid paying the S3 charges ( <a href="#">ref</a> ). |
| <b>Goal</b>             | Financial Drain   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>  |
| <b>CVSS</b>             | <a href="#">Low (3.5)</a>   |
| <b>IAM Access</b>       | 0   |



| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Block direct public access</b><br>Front buckets required to be public, using authenticated CDN (e.g. CloudFront) or API Gateway, protected with WAF (e.g. for <a href="#">hotlinking</a> )             | Very High | 1                        | -            | -         |
| <b>Monitor S3 with Amazon GuardDuty and Macie</b><br>Enable <a href="#">S3 policy findings</a> in <a href="#">Amazon Macie</a> in all AWS accounts in all Regions, and protect it using Macie ThreatModel | High      | 1                        | -            | -         |

## Increase bill by restoring large amount of data

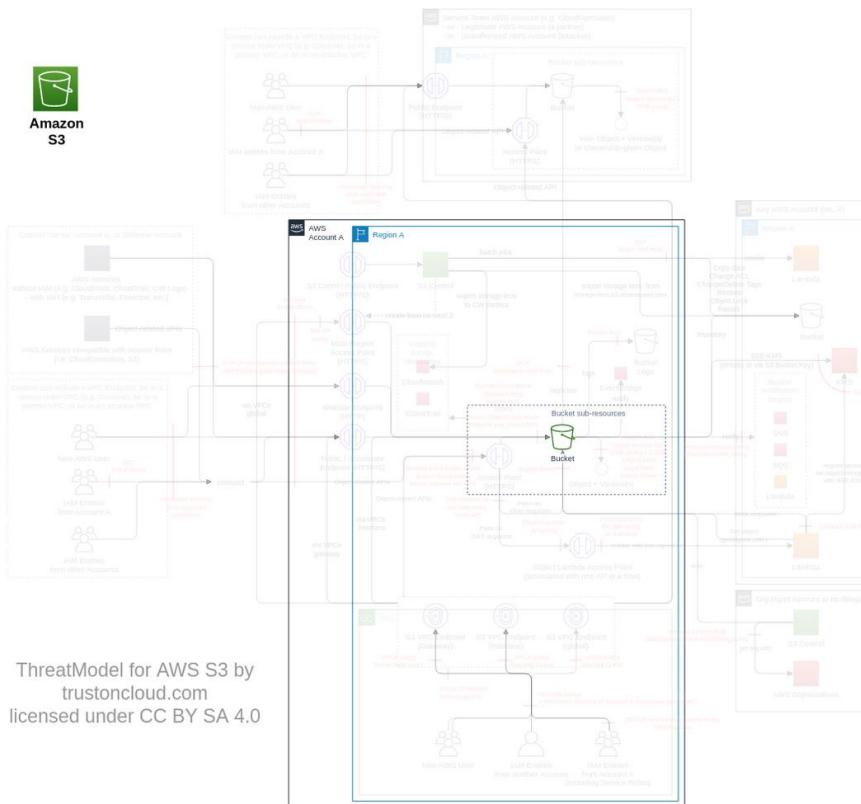
|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T47   |
| <b>Name</b>             | Increase bill by restoring large amount of data  |
| <b>Description</b>      | Restore cost can be amplified by the size and the type (i.e. expedited). An attacker can restore lots of data to generate costs. |
| <b>Goal</b>             | Financial Drain  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>   |
| <b>CVSS</b>             | <a href="#">Low (2.7)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:RestoreObject"<br>}   |



| Control Objectives   | Priority | # of associated Controls |              |           |
|--|----------|--------------------------|--------------|-----------|
|  |          | Directive                | Preventative | Detective |
| <b>Limit the access to the IAM actions required to execute the threats</b><br><small>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.</small> | Medium   | 1                        | -            | -         |

## Increase bill by creating incomplete uploads

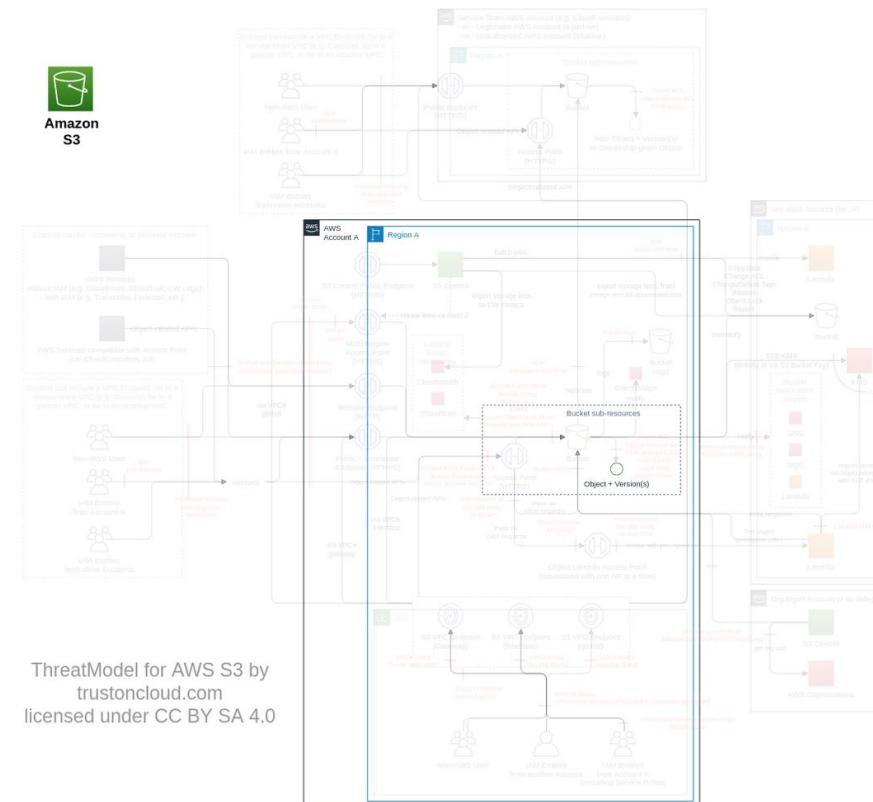
|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T40   |
| <b>Name</b>             | Increase bill by creating incomplete uploads   |
| <b>Description</b>      | By default, when a multiple upload is initiated but not completed, S3 will keep it ( <a href="#">ref</a> ). An attacker can upload a large amount of data without completing it, while being hard to detect. |
| <b>Goal</b>             | Financial Drain  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>   |
| <b>CVSS</b>             | <a href="#">Low (2.3)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutObject"<br>}   |



| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Remove incomplete multipart uploads</b><br>Reduce costs related to incomplete multipart upload by creating a lifecycle policy to remove them after an agreed length of time (e.g. 7 days) ( <a href="#">blog</a> ) | Very High | -                        | 1            | -         |

## Abuse MD5 etag

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T27  |
| <b>Name</b>             | Abuse MD5 etag  |
| <b>Description</b>      | Etags includes the MD5 of the file but not consistently and can be used by developers to verify the integrity of a file. An attacker can affect an upload function to change the etag of a file, in order to disrupt a workflow downstream. |
| <b>Goal</b>             | Data manipulation   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>  |
| <b>CVSS</b>             | <a href="#">Low (1.8)</a>   |
| <b>IAM Access</b>       | 0   |

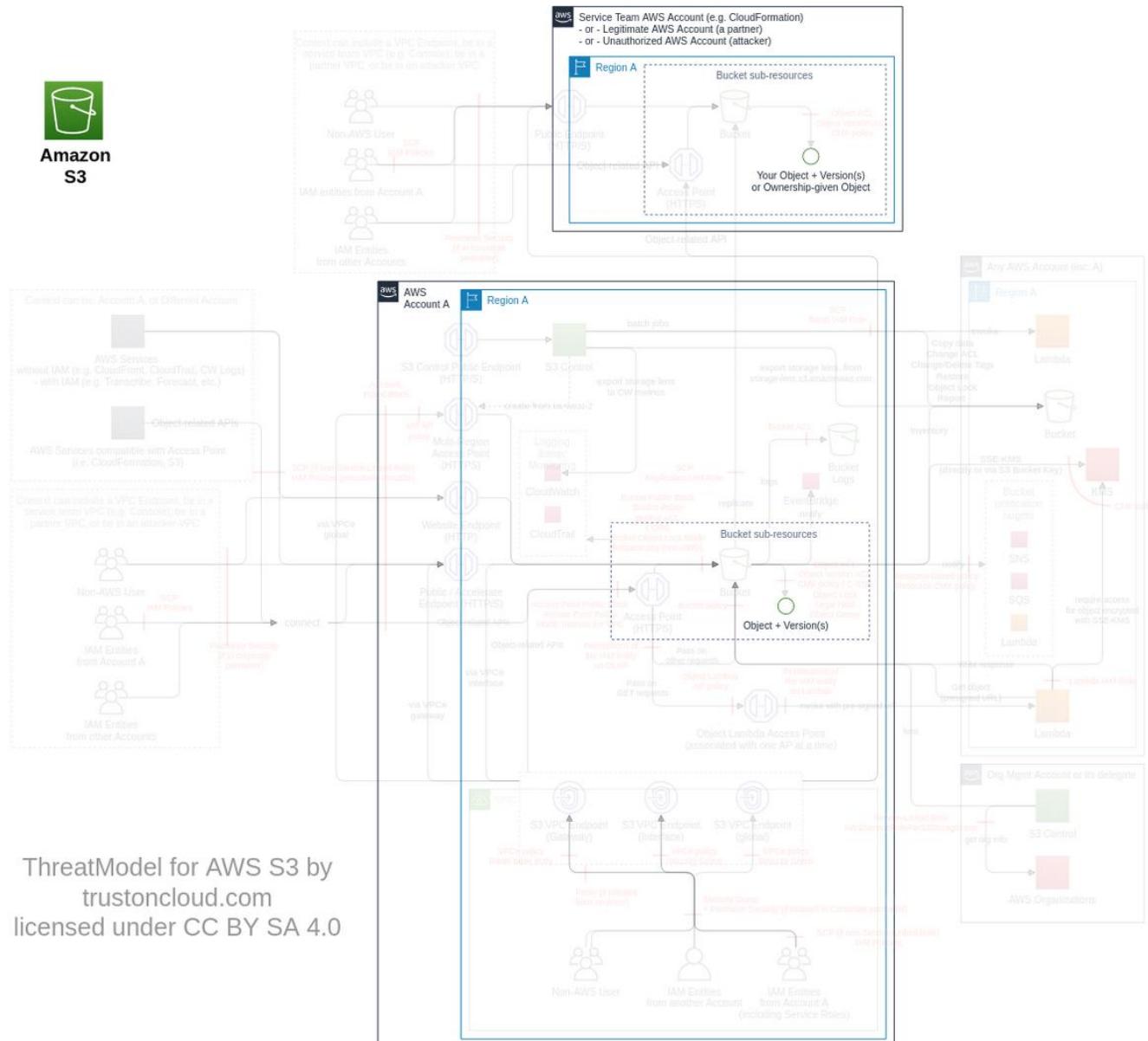


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Enforce good coding practice</b><br>If etag is used, make sure properly account for its different definitions ( <a href="#">ref</a> )   | Very High | 1                        | -            | -         |
| <b>Block requests with KMS keys from unauthorized AWS account(s)</b><br>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account<br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)<br>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> ) | Very High | 1                        | 1            | 1         |

**Object tagging** (*subclass of Object upload/download, used by Bucket, FC2*)

You can tag objects ([ref](#)).

# **Data Flow Diagram (DFD)**



#### ***Actions and IAM Permissions to deny the feature***

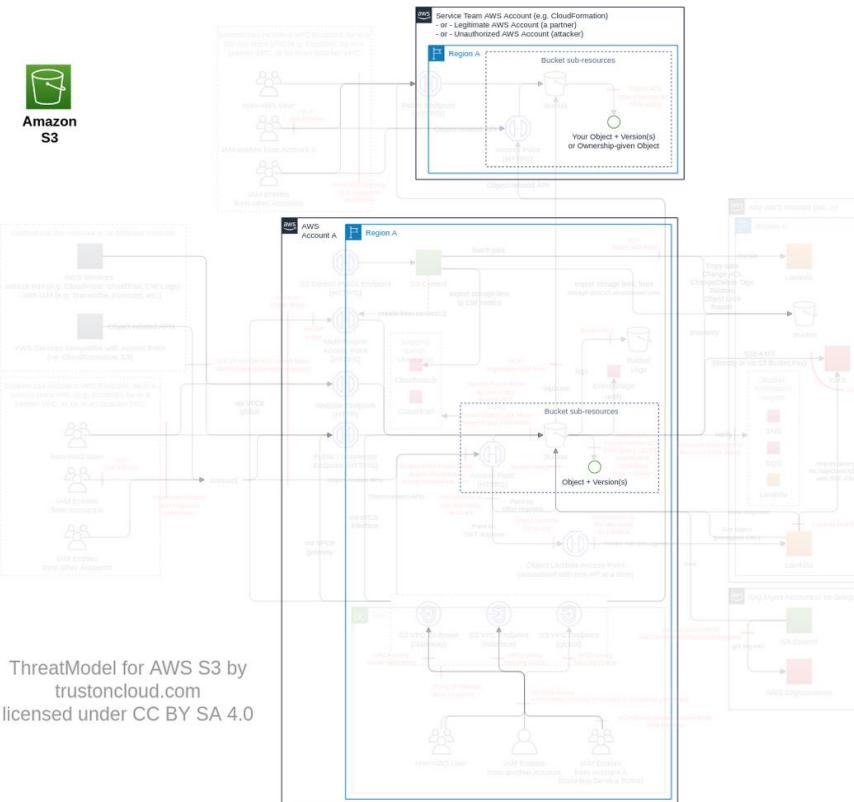
| Action                                    | IAM Permission      |
|---|---------------------|
| Adds a set of tags to an existing object. | s3:PutObjectTagging |

## ***Threat List***

| Name   | CVSS                         |
|--|------------------------------|
| Gain access by modifying or deleting important object tags | <a href="#">Medium (4.4)</a> |

## Gain access by modifying or deleting important object tags

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T33   |
| <b>Name</b>             | Gain access by modifying or deleting important object tags   |
| <b>Description</b>      | Tags can be used for various reasons, including security classification or access management (via ABAC). An attacker can change the tagging of an object to another value enabling them to execute another attack. |
| <b>Goal</b>             | Launch another attack  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0004</a>   |
| <b>CVSS</b>             | <a href="#">Medium (4.4)</a>   |
| <b>IAM Access</b>       | {<br>"OR": ["s3:PutObjectTagging", "s3>DeleteObjectTagging"]<br>}  |

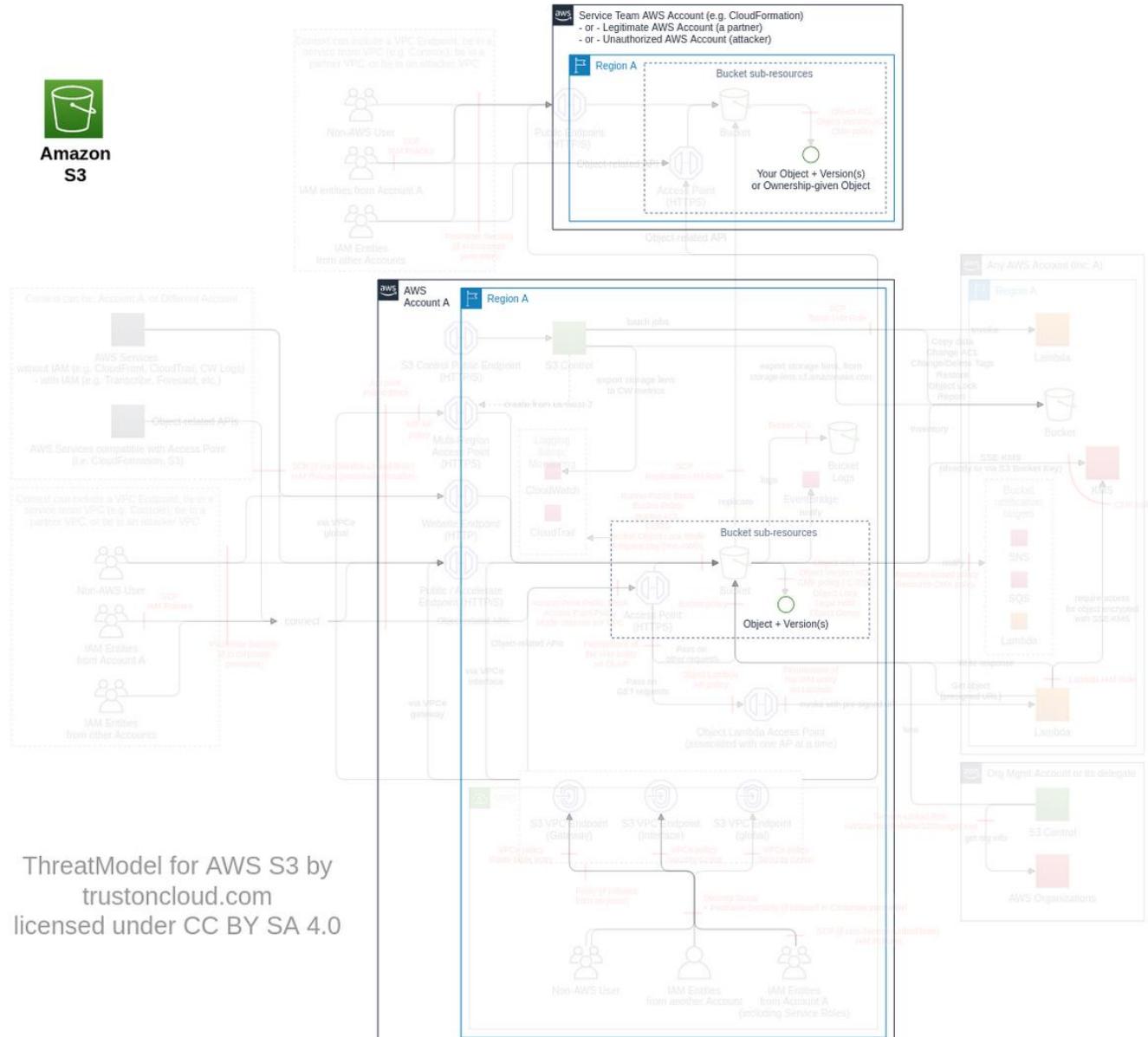


| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Limit access from only authorized VPCs</b><br>For each S3 bucket, maintain a list of VPC(s), authorized to access it.<br>Limit the access to only those VPC(s) (e.g. using S3 bucket statement, deny if the condition "aws:SourceVpce", or if the bucket policy size is beyond the limit, use this condition on access point)  | Very High | 1                        | 1            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. | High      | 2                        | -            | -         |

**Torrent** (*subclass of Object upload/download, used by Bucket, FC21*)

**[NOT RECOMMENDED]** You can use the BitTorrent protocol to retrieve objects ([ref](#)). Only available in the AWS Regions launched before May 30, 2016. The seed rate is 100KB.

## **Data Flow Diagram (DFD)**



### ***Actions and IAM Permissions to deny the feature***

| Action                                | IAM Permission      |
|---------------------------------------|---------------------|
| Returns torrent files from an object. | s3:GetObjectTorrent |

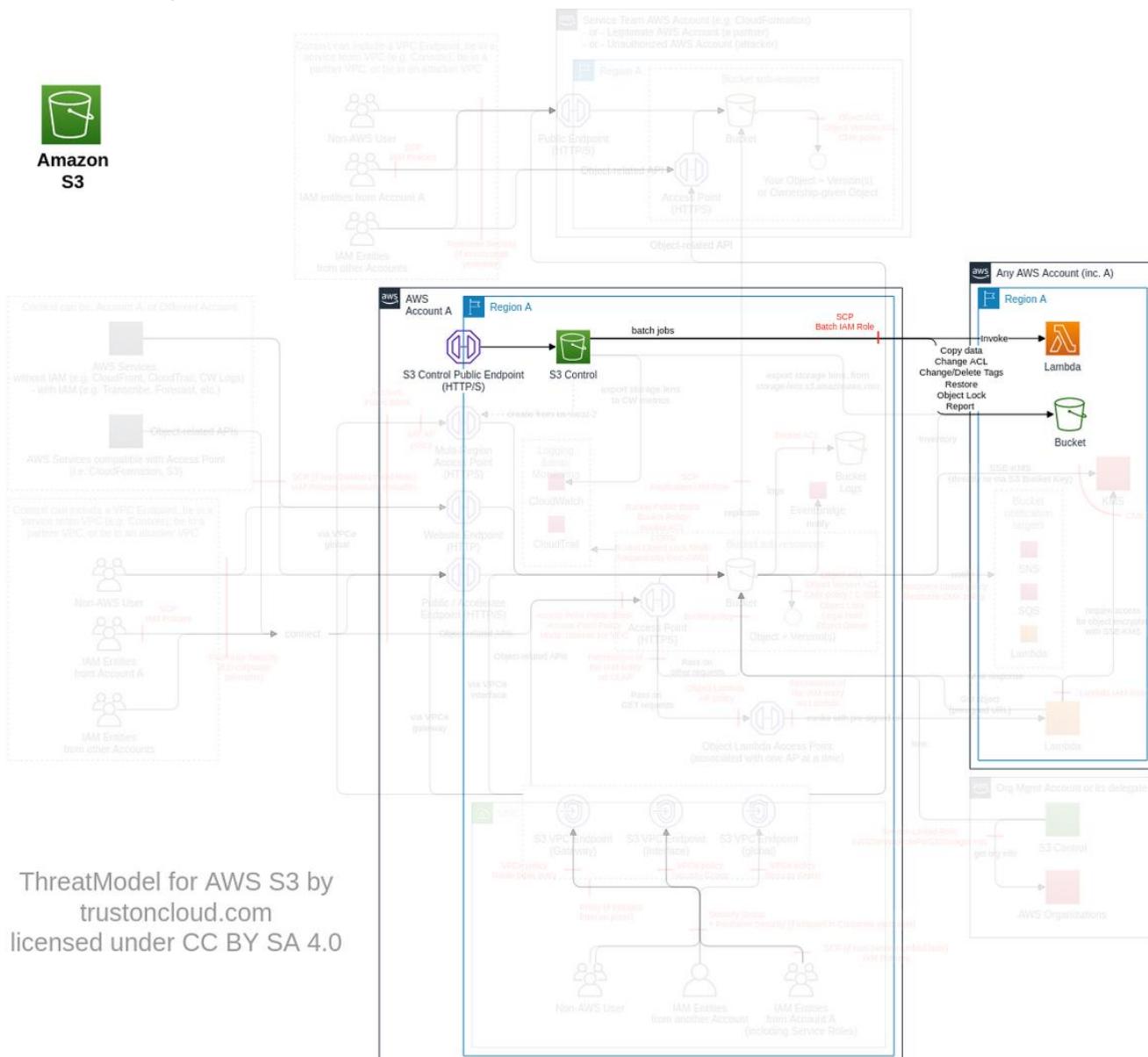
## ***Threat List***

| Name | CVSS |
|------|------|
| None | None |

**Batch** (*subclass of Object upload/download, used by Bucket, FC27*)

*S3 Batch Operations performs large-scale Batch Operations on Amazon S3 objects.*

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

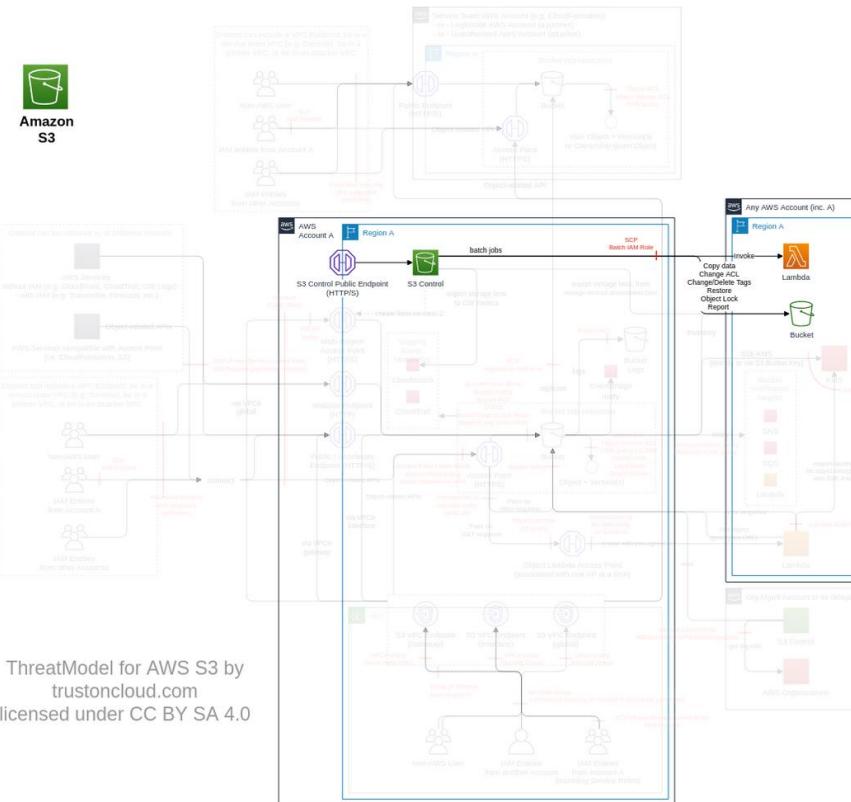
| Action  | IAM Permission |
|---|----------------|
| Creates a new Amazon S3 Batch Operations job. | s3:CreateJob   |

## ***Threat List***

| Name   | CVSS                         |
|--|------------------------------|
| Exfiltrate, modify or delete objects using Batch | <a href="#">Medium (6.2)</a> |

## Exfiltrate, modify or delete objects using Batch

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T44  |
| <b>Name</b>             | Exfiltrate, modify or delete objects using Batch  |
| <b>Description</b>      | S3 Batch Operations require an IAM role (with proper trust policy), then can run operations including copy, or replace/delete object tags. An attacker can use Batch copy or modify objects to exfiltrate or change the access management of an object (if relying on tag). |
| <b>Goal</b>             | Data manipulation   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>  |
| <b>CVSS</b>             | <a href="#">Medium (6.2)</a>  |
| <b>IAM Access</b>       | {<br>"AND": ["s3:CreateJob", "iam:PassRole"]<br>}   |



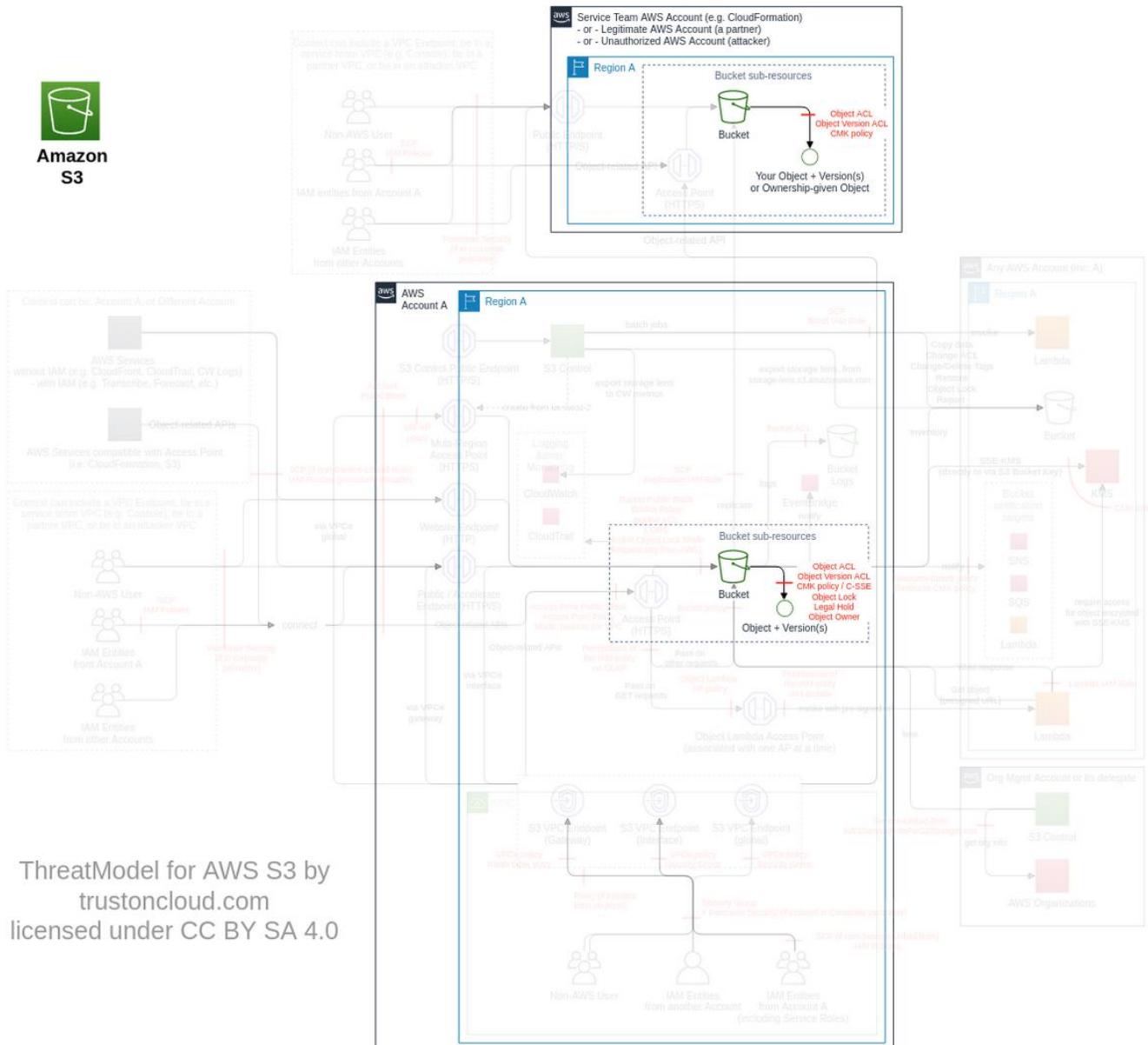
| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Control IAM roles used for Batch</b><br><br>Maintain a list of IAM roles used for Batch job, ideally dedicated (e.g. using change management process on infrastructure-as-code)<br>Ensure only an authorized IAM role is attached on each Batch job<br>Limit the access to only required resources/permissions (e.g. source/destination bucket, Lambda functions) of each authorized IAM role configured for Batch jobs<br>Limit access to authorized IAM roles used for Batch job, using the IAM ThreatModel (e.g. trust policy, and "iam:PassRole")          | Very High | 4                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. | Medium    | 2                        | -            | -         |

# Object versioning (subclass of Object upload/download, used by

*Bucket, FC3)*

You can version your objects ([ref](#)).

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

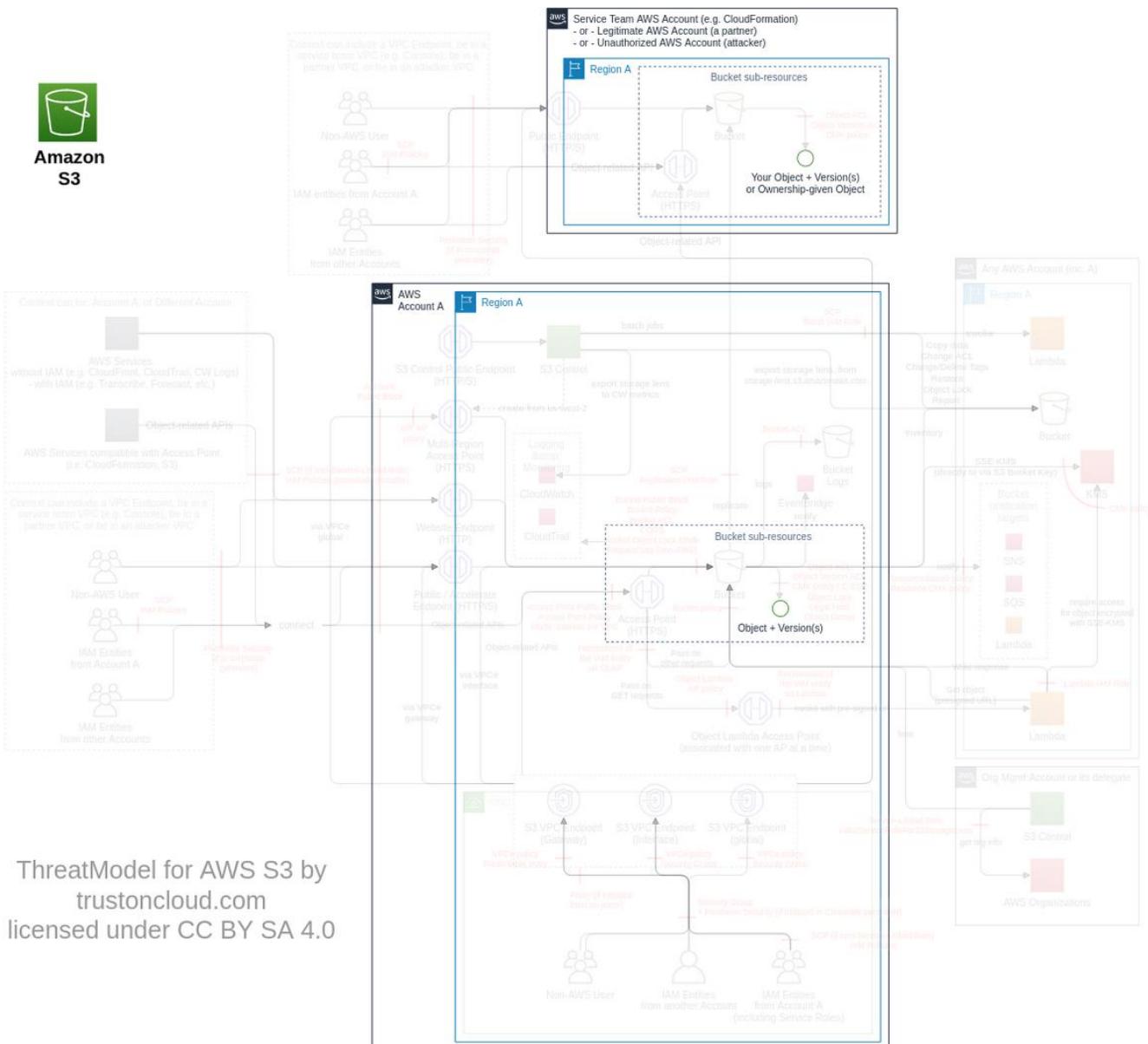
| Action                                      | IAM Permission      |
|---|---------------------|
| Retrieves an object version from Amazon S3. | s3:GetObjectVersion |

## ***Threat List***

| Name | CVSS |
|------|------|
| None | None |

**Tag on versioned objects** (*subclass of Object tagging/Object versioning, used by Bucket, FC4*)  
 You can tag objects versions ([ref](#)).

### Data Flow Diagram (DFD)



### Actions and IAM Permissions to deny the feature

| Action   | IAM Permission             |
|--|----------------------------|
| Adds a set of tags to an existing object version | s3:PutObjectVersionTagging |

### Threat List

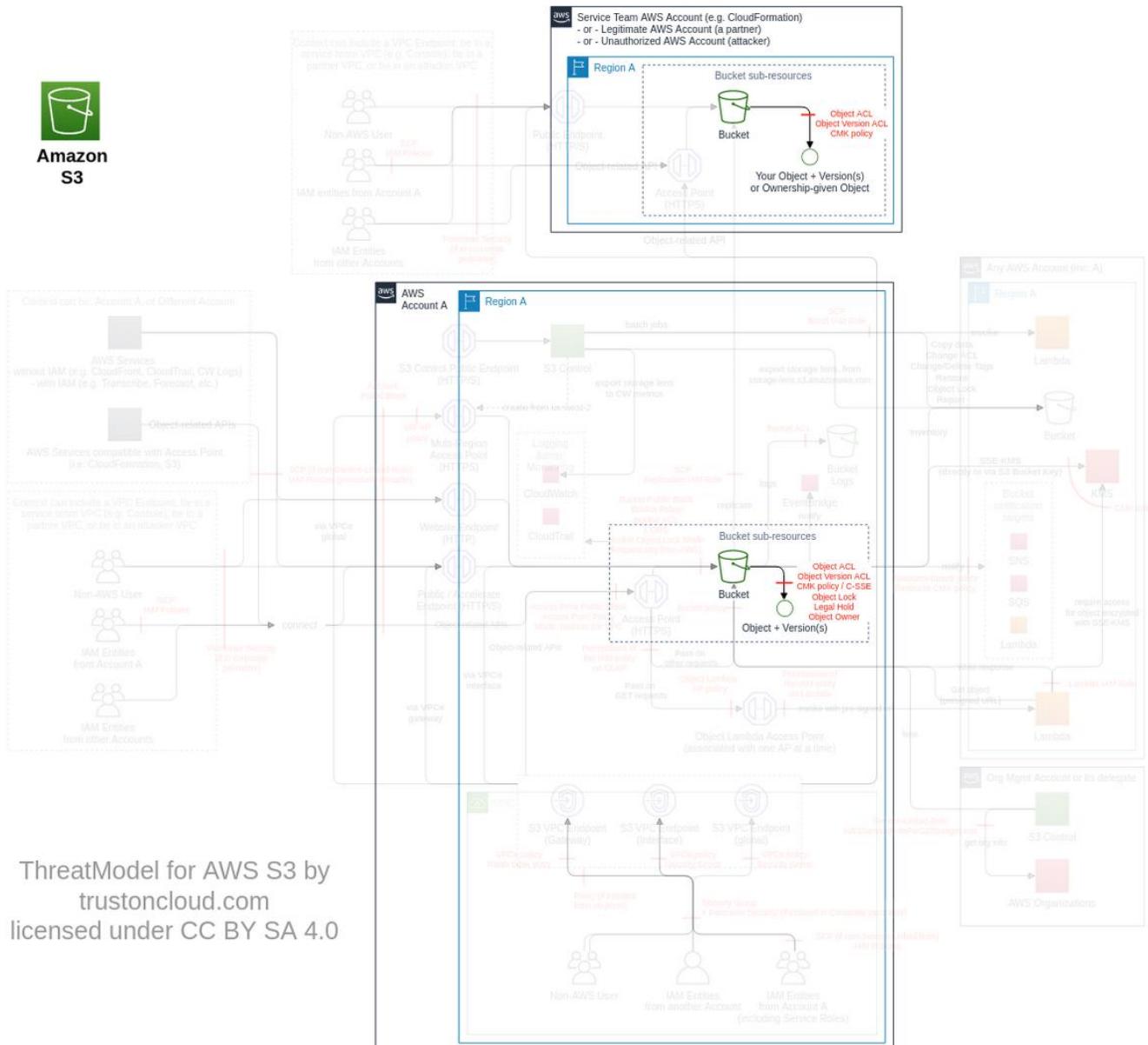
| Name | CVSS |
|------|------|
| None | None |

# ACL on versioned objects *(subclass of Object versioning/ACL on*

## *versioned objects, FC9)*

*Amazon S3 access control lists (ACLs) enable you to manage access to object versions ([ref](#)).*

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

| Action  | IAM Permission         |
|---|------------------------|
| Sets the access control list (ACL) permissions for an object version. You must have WRITE_ACP permission to set the ACL of an object version. | s3:PutObjectVersionAcl |

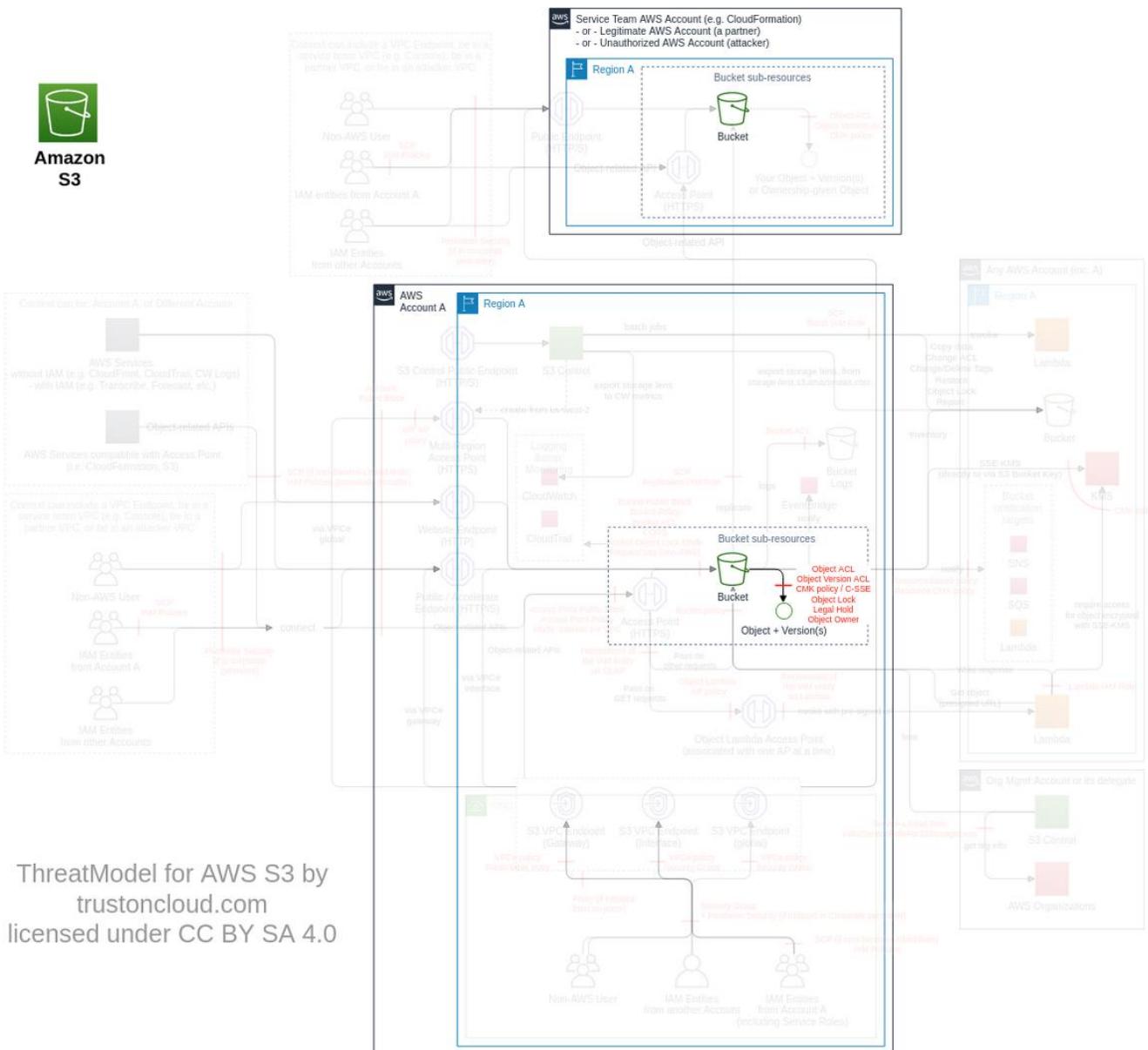
## ***Threat List***

| Name | CVSS |
|------|------|
| None | None |

# Bucket versioning (*subclass of Object versioning/Bucket, FC6*)

*Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures ([ref](#)).*

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

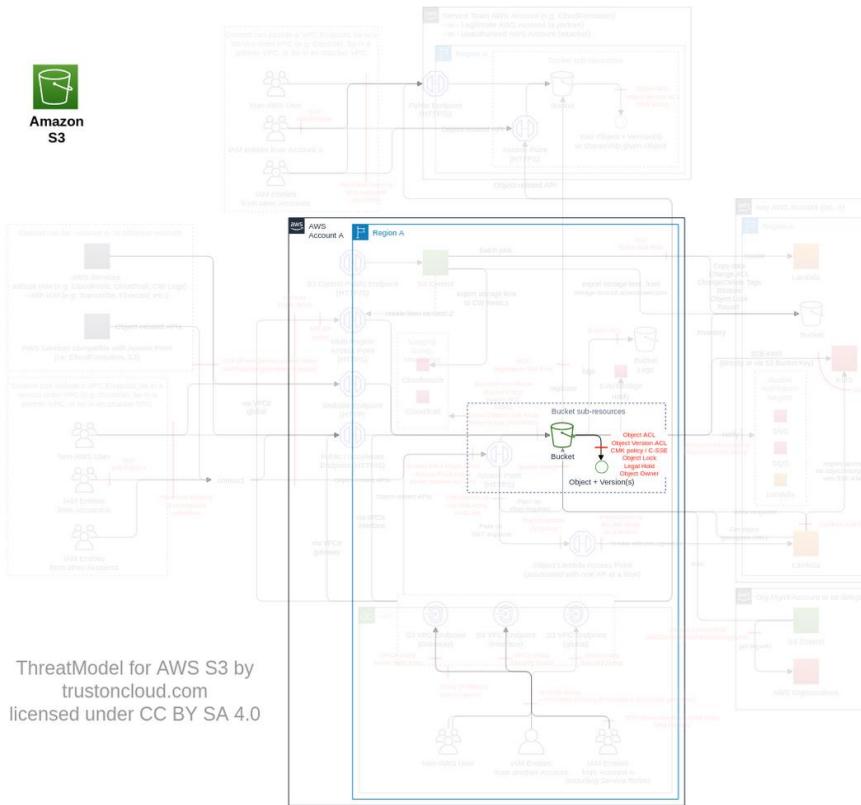
| Action   | IAM Permission         |
|--|------------------------|
| Sets the versioning state of an existing bucket. | s3:PutBucketVersioning |

## ***Threat List***

| Name  | CVSS                      |
|---|---------------------------|
| Affect data protection by removing versioning | <a href="#">Low (2.7)</a> |

## Affect data protection by removing versioning

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T48   |
| <b>Name</b>             | Affect data protection by removing versioning  |
| <b>Description</b>      | Versioning can be used as a first level of integrity protection. An attacker can suspend versioning to affect data protection of a bucket. |
| <b>Goal</b>             | Data manipulation  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>   |
| <b>CVSS</b>             | <a href="#">Low (2.7)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutBucketVersioning"<br>}   |

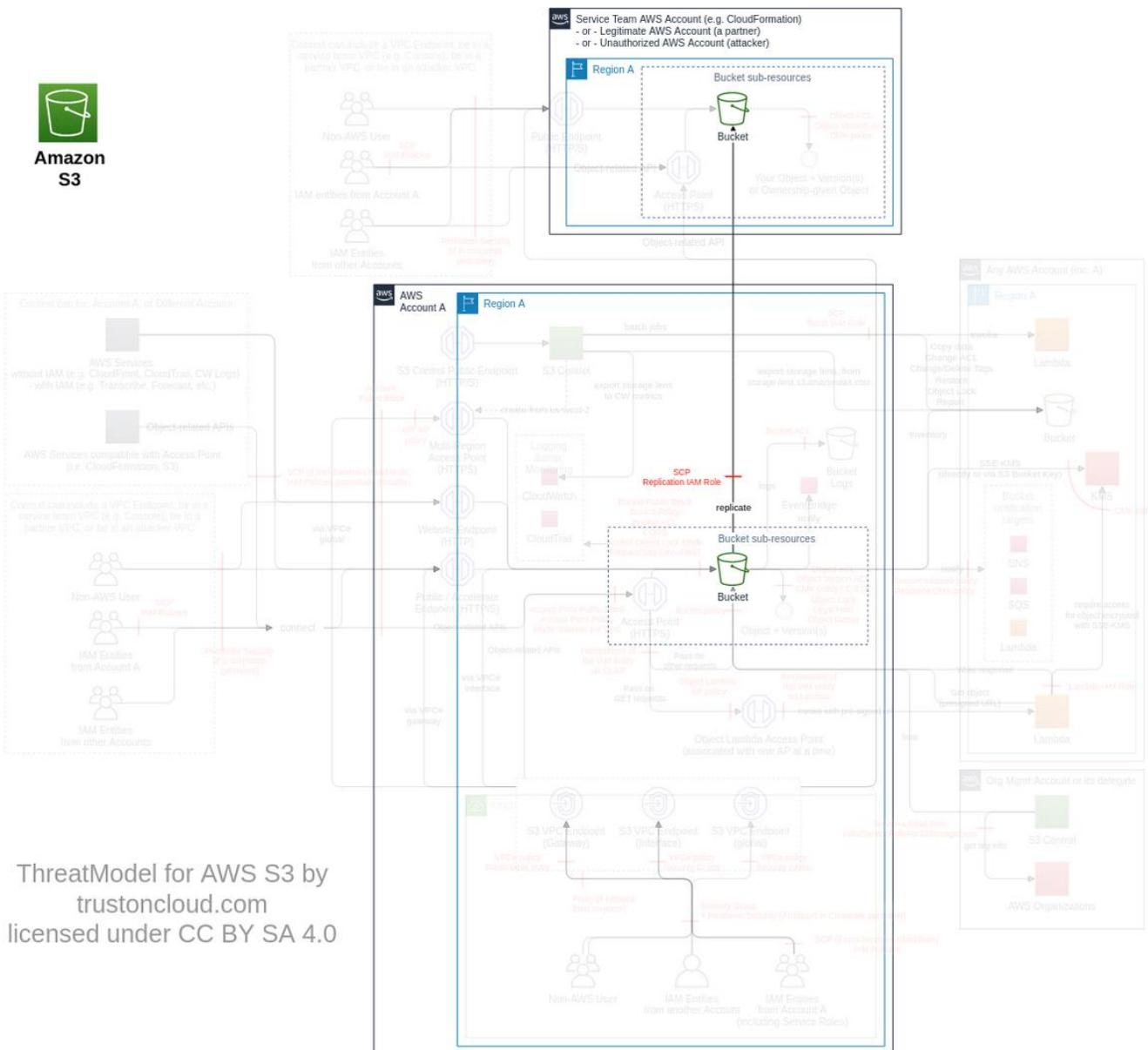


| Control Objectives  | Priority | # of associated Controls |              |           |
|---|----------|--------------------------|--------------|-----------|
|   |          | Directive                | Preventative | Detective |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions. | Medium   | 1                        | -            | -         |

# Replication (subclass of Bucket versioning, FC15)

Replication enables automatic and asynchronous copying of objects of a bucket into another bucket. It can be cross-region or in the same region. Buckets configured for replication can be in the same AWS account or by different accounts. It is usually to backup S3 data, data centralization, or multi-region applications.

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

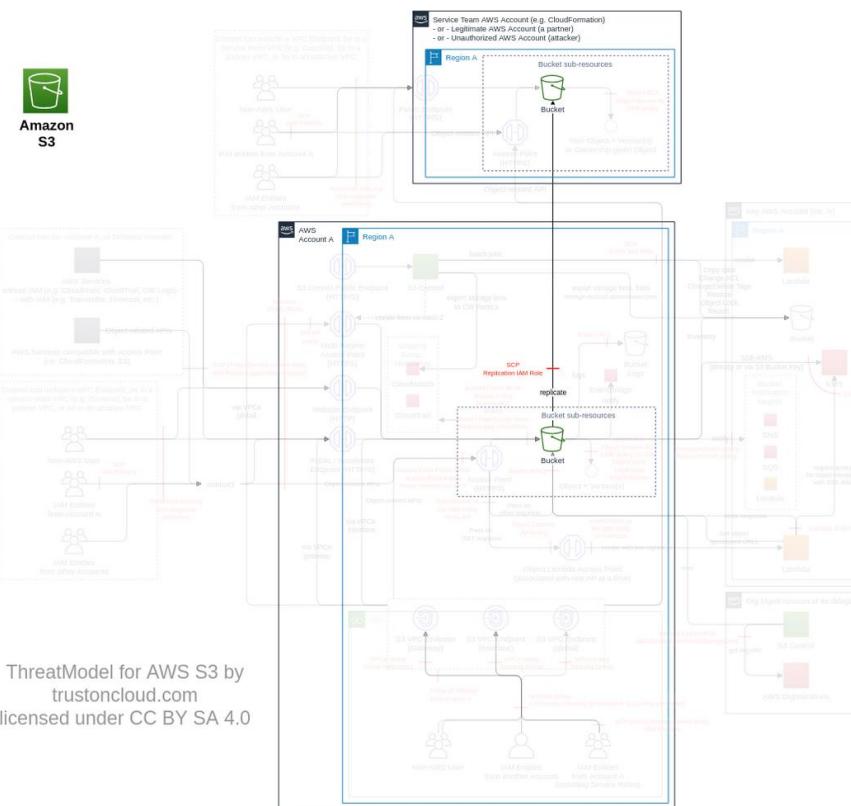
| Action   | IAM Permission                 |
|--|--------------------------------|
| Creates a new replication configuration (or replaces an existing one, if present). | s3:PutReplicationConfiguration |

## Threat List

| Name   | CVSS                         |
|--|------------------------------|
| Unauthorized access to data via bucket replication | <a href="#">Medium (4.5)</a> |
| Affect data protection by removing replication     | <a href="#">Low (2.7)</a>    |

## Unauthorized access to data via bucket replication

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T2   |
| <b>Name</b>             | Unauthorized access to data via bucket replication  |
| <b>Description</b>      | Replication allows you to replicate objects, their metadata and change ownership. The configuration focuses on new objects only (old objects replication requires <a href="#">a ticket to AWS Support</a> ). An attacker can configure replication on a bucket to replicate objects (or its metadata or tagging) in a bucket they control to exfiltrate data. |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Medium (4.5)</a>  |
| <b>IAM Access</b>       | {<br>"AND": ["s3:PutReplicationConfiguration", "iam:PassRole"]<br>}   |

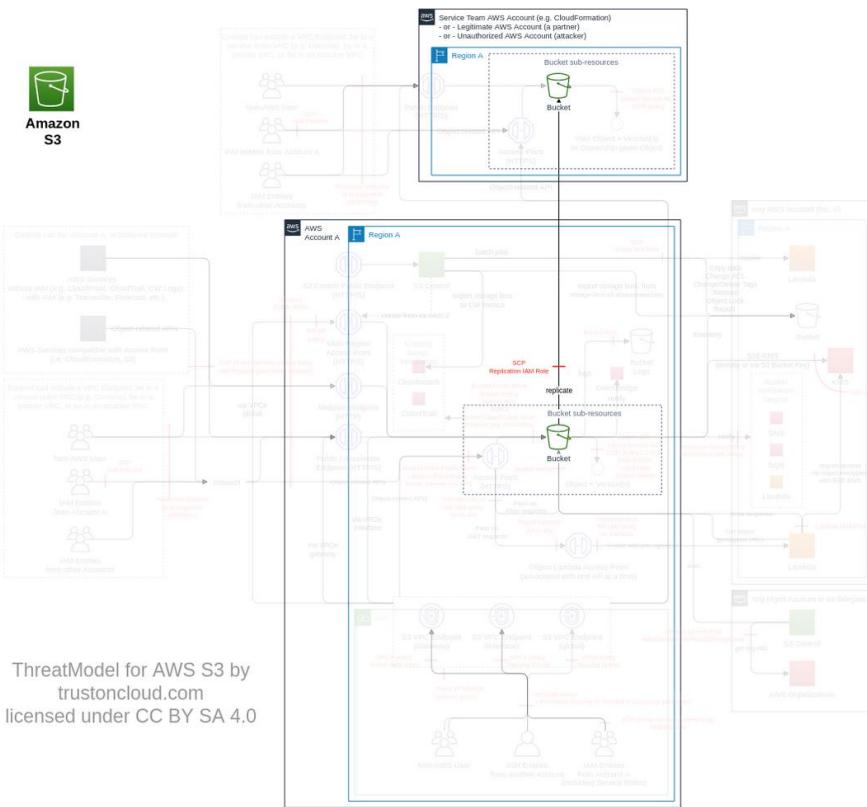


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Block requests with KMS keys from unauthorized AWS account(s)</b><br><br>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account<br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)<br>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> )   | Very High | 1                        | 1            | 1         |
| <b>Restrict bucket replication</b><br><br>Maintain a list of authorized buckets to have replication enabled, their target bucket and replication type (i.e. ownership, RTC, etc.) ( <a href="#">ref</a> ).<br>Ensure only authorized buckets have replication enabled and with correct configuration are configured<br>Maintain a list of IAM roles used for replication, ideally dedicated (e.g. using change management process on infrastructure-as-code)<br>Ensure only authorized IAM roles are attached for each replication, ideally dedicated<br>Limit the S3 access to the source/destination bucket and replication rights of each authorized IAM role configured for replication<br>Limit access to authorized IAM roles used for replication, using the IAM ThreatModel (e.g. trust policy, and "iam:PassRole")<br>Monitor abnormal behaviour on replication CloudWatch metrics (i.e. <i>BytesPendingReplication</i> and <i>OperationsPendingReplication</i> ) | High      | 6                        | -            | 1         |
| <b>Monitor S3 with Amazon GuardDuty and Macie</b><br><br>Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect it using Macie ThreatModel  | High      | 1                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.  | Medium    | 2                        | -            | -         |

|  |  |  |  |  |  |
|--|--|--|--|--|--|
| In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. |  |  |  |  |  |
|--|--|--|--|--|--|

## Affect data protection by removing replication

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T49   |
| <b>Name</b>             | Affect data protection by removing replication   |
| <b>Description</b>      | Replication can be used as a level of integrity protection and backup. An attacker can remove replication to affect the data protection. |
| <b>Goal</b>             | Data manipulation  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>   |
| <b>CVSS</b>             | <a href="#">Low (2.7)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutReplicationConfiguration"<br>}   |

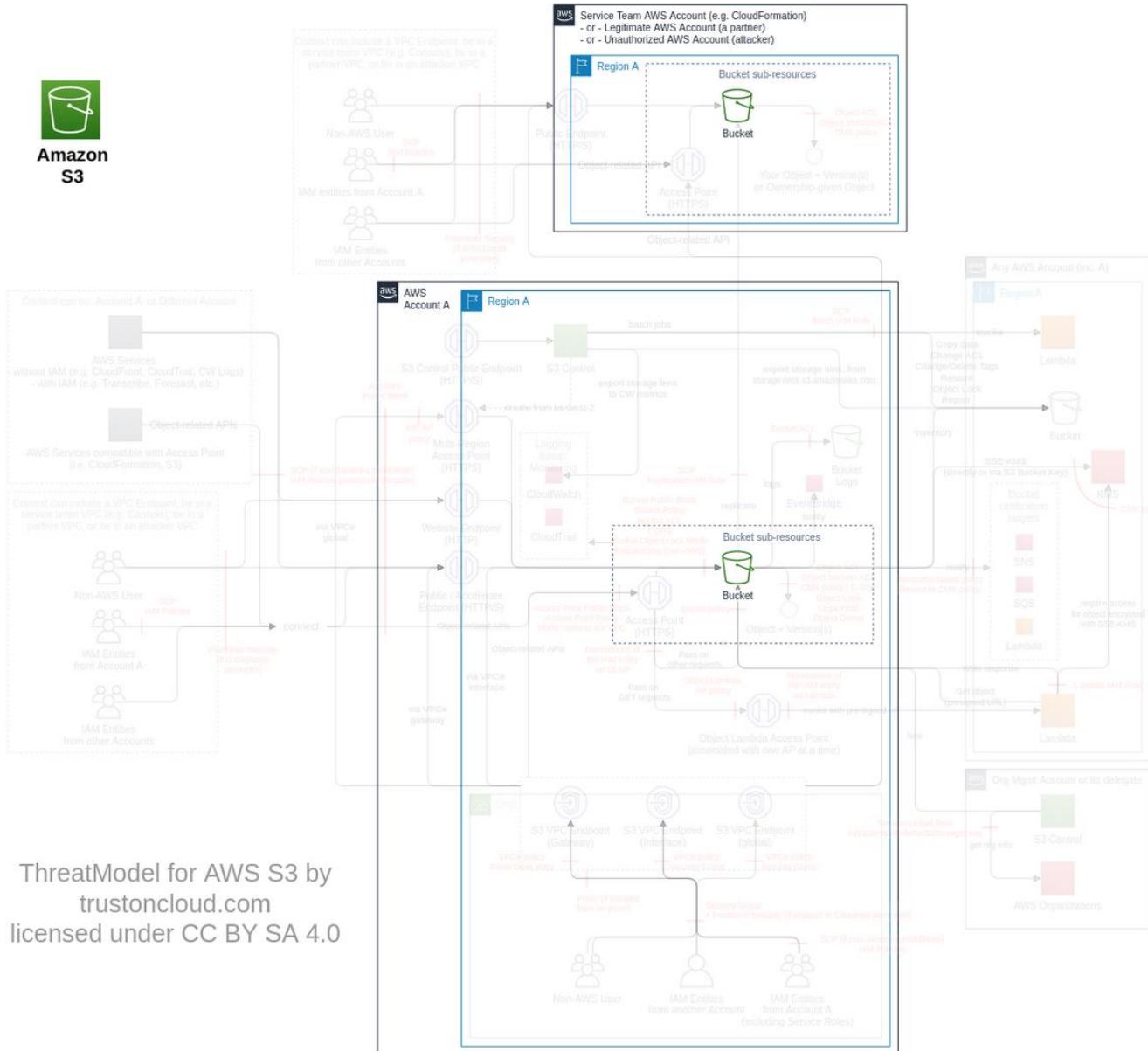


| Control Objectives  | Priority | # of associated Controls |              |           |
|---|----------|--------------------------|--------------|-----------|
|   |          | Directive                | Preventative | Detective |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions. | Medium   | 1                        | -            | -         |

# Bucket tag (subclass of Bucket, FC7)

You can tag buckets ([ref](#)).

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

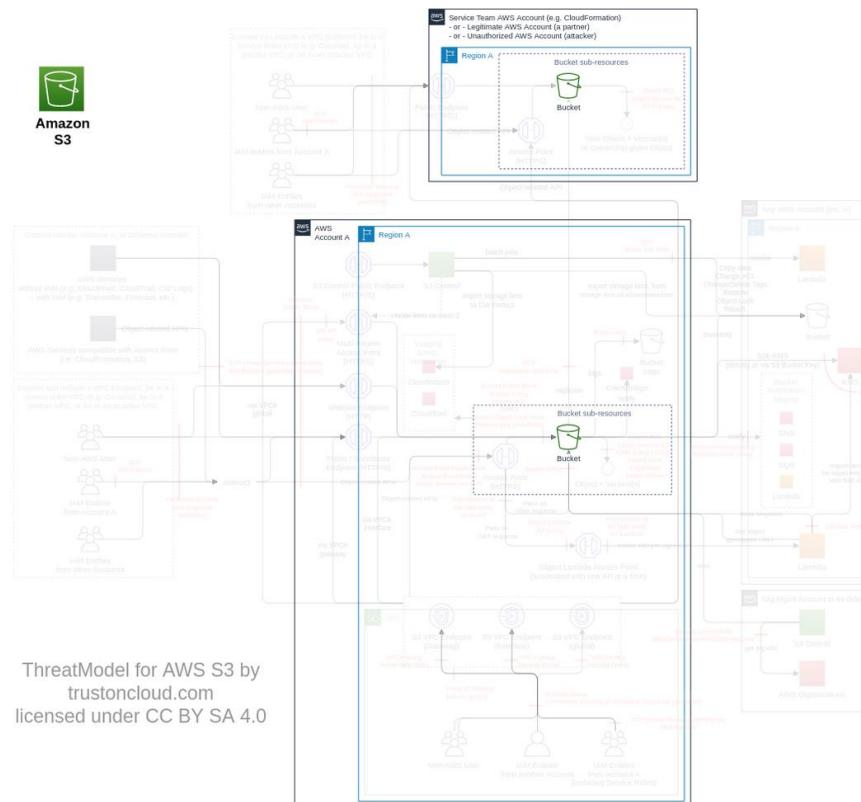
| Action                                    | IAM Permission      |
|---|---------------------|
| Adds a set of tags to an existing bucket. | s3:PutBucketTagging |

## Threat List

| Name                          | CVSS                      |
|-------------------------------|---------------------------|
| Exfiltrate data by using tags | <a href="#">Low (3.3)</a> |

## Exfiltrate data by using tags

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T18  |
| <b>Name</b>             | Exfiltrate data by using tags   |
| <b>Description</b>      | Objects and buckets can have tags. An attacker can use those features to exfiltrate data.   |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Low (3.3)</a>   |
| <b>IAM Access</b>       | <pre>{   "AND": [     {       "OR": ["GetObjectTagging", "s3:GetObjectVersionTagging"]     },     {       "OR": ["s3:PutObjectTagging", "s3:PutObjectVersionTagging"]     }   ] }</pre> |

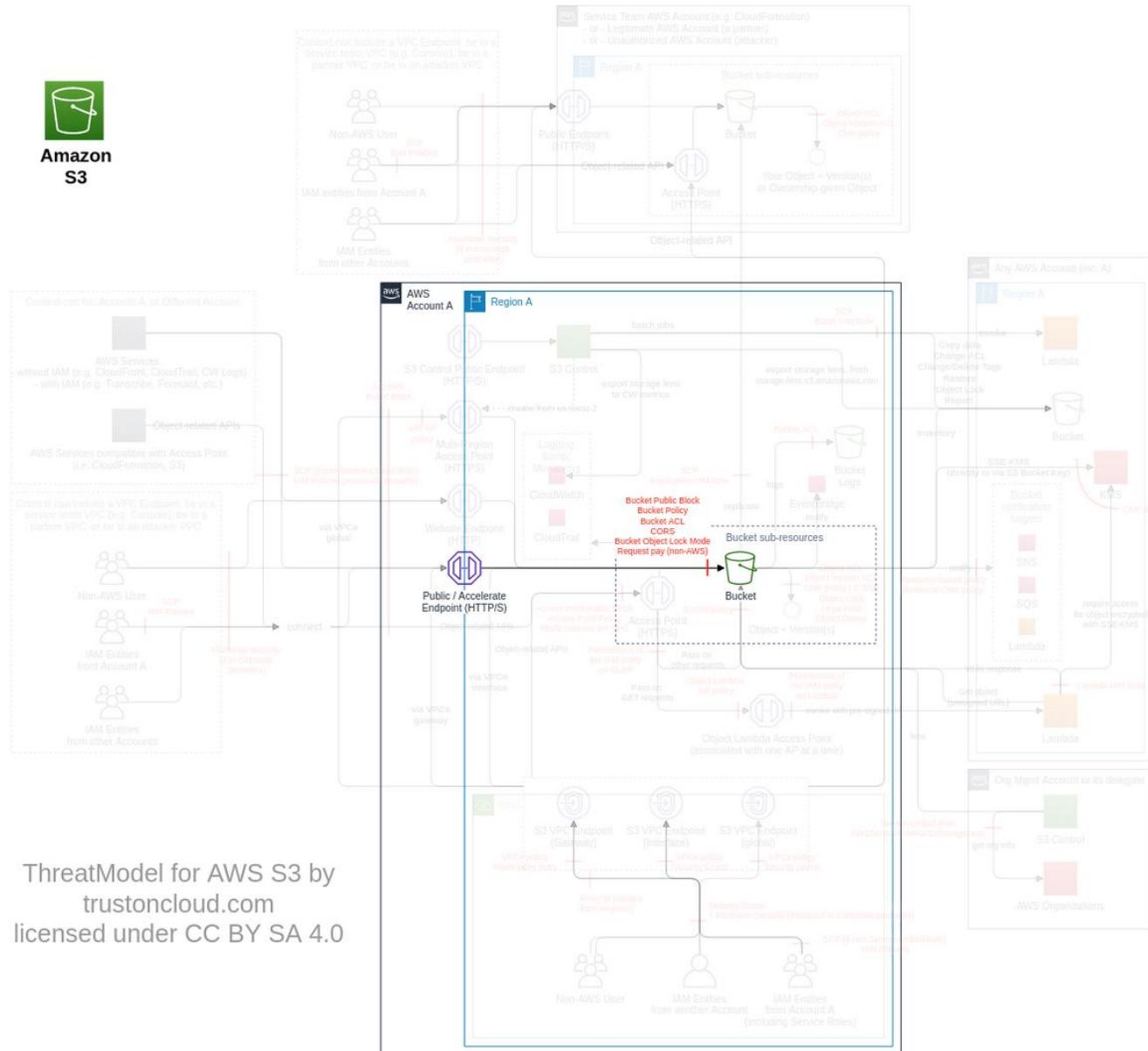


| Control Objectives  | Priority | # of associated Controls |              |           |
|---|----------|--------------------------|--------------|-----------|
|   |          | Directive                | Preventative | Detective |
| <b>Block S3 endpoints in your corporate perimeter security</b><br>Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g. firewalls, or cloud interception proxy like <a href="#">Kivera</a> ) including via Internet Gateway, to force usage of VPC endpoints. Note: AWS console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com").  | Medium   | 1                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. | Medium   | 2                        | -            | -         |

# Bucket ACL (subclass of Bucket, FC8)

**[NOT RECOMMENDED]** Amazon S3 access control lists (ACLs) enable you to manage access to buckets. Each bucket has an ACL attached to it as a sub-resource. It defines which AWS accounts or groups are granted access and the type of access. When a request is received against a resource, Amazon S3 checks the corresponding ACL to control that the requester has the necessary access permissions ([ref](#)).

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

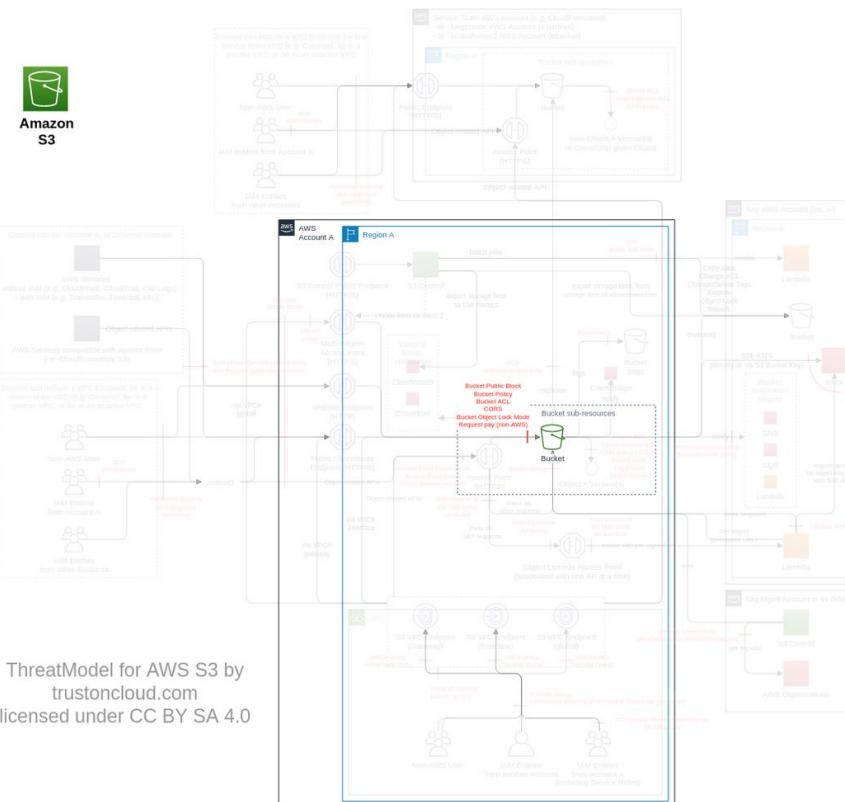
| Action   | IAM Permission  |
|--|-----------------|
| Sets the permissions on an existing bucket using access control lists (ACL). | s3:PutBucketAcl |

## Threat List

| Name   | CVSS                         |
|--|------------------------------|
| Grant unauthorized access to a private bucket by changing bucket ACL | <a href="#">Medium (5.2)</a> |
| DoS by blocking traffic using bucket ACL                             | <a href="#">Low (2.4)</a>    |

## Grant unauthorized access to a private bucket by changing bucket ACL

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T4   |
| <b>Name</b>             | Grant unauthorized access to a private bucket by changing bucket ACL  |
| <b>Description</b>      | Bucket ACL can be used to give access to the bucket information, list the objects, and overwrite/delete objects. An attacker can change the bucket ACL to destroy or modify data, or exfiltrate data via the object name (1KB). |
| <b>Goal</b>             | Data manipulation   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>  |
| <b>CVSS</b>             | <a href="#">Medium (5.2)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutBucketAcl"<br>}   |

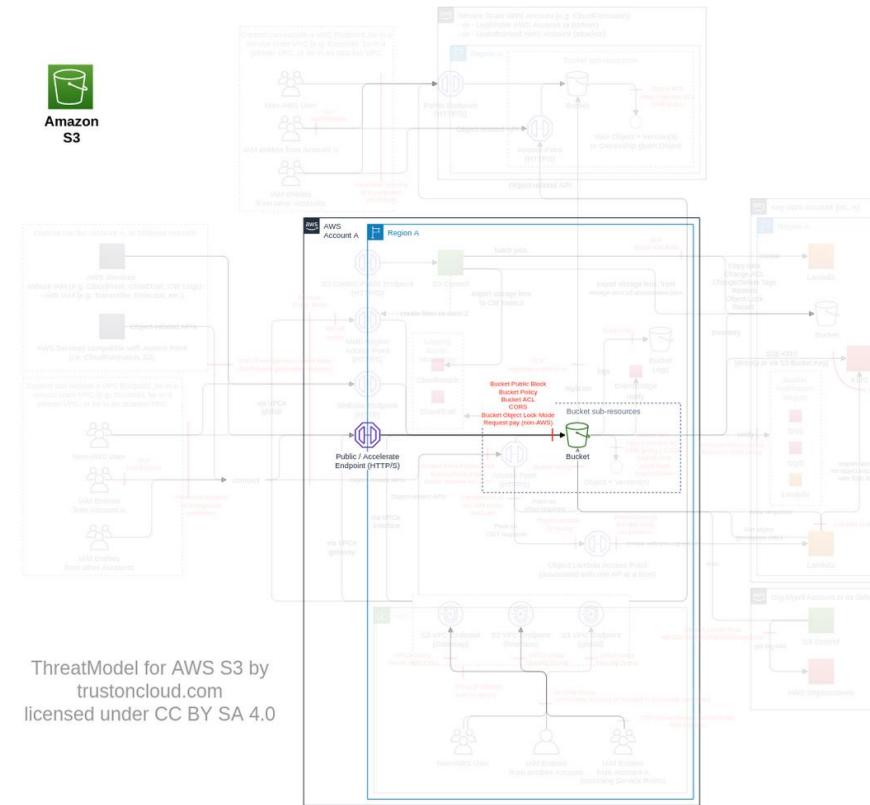


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Block direct public access</b><br>Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.<br>Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.  | Very High | -                        | 2            | -         |
| <b>Block bucket ACL except for server access logging</b><br>Deny requests to add bucket ACL other than for server access logging (e.g. using an SCP, bucket policy and VPC endpoint policy blocking PutBucketAcl for all but the following predefined group "http://acs.amazonaws.com/groups/s3/LogDelivery" using the IAM condition x-amz-acl: "log-delivery-write")<br>Monitor changes on bucket ACL other than for server access logging (e.g. using CloudTrail, 1) if the CloudTrail PutBucketAcl log indicates requestParameters.AccessControlPolicy.AccessControlList.Grant[] Grantee.xsi:type: "Group", then the URI should be "http://acs.amazonaws.com/groups/s3/LogDelivery", and 2) if the requestParameters.AccessControlPolicy.AccessControlList.Grant[] Grantee.xsi:type: "CanonicalUser" then the ID should be the same than "AccessControlPolicy.Owner.ID", and 3) requestParameters.x-amz-acl should be either "private", "log-delivery-write" or not existing) | Very High | -                        | 1            | 1         |
| <b>Disabling ACLs for all buckets</b><br>Ensure bucket ACL and object ACL are disabled on each bucket<br>Prevent the creation of buckets with ACL enabled (e.g. by using a SCP and/or an IAM policy on "s3>CreateBucket" with a deny statement on "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note it does not block someone to enable ACL afterwards via PutPutBucketOwnershipControls.   | Very High | 1                        | 1            | -         |
| <b>Block requests with KMS keys from unauthorized AWS account(s)</b><br>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account<br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)<br>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in response.x-amz-server-side-encryption-aws-kms-key-id)   | Very High | 1                        | 1            | 1         |

|  |        |   |   |   |
|--|--------|---|---|---|
| <p><b>Monitor S3 with Amazon GuardDuty and Macie</b></p> <p>Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using GuardDuty ThreatModel. Ensure findings are investigated (e.g. using Amazon Detective).</p> <p>Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect it using Macie ThreatModel</p> | High   | 2 | - | - |
| <p><b>Enable CloudTrail S3 data events</b></p> <p>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel</p>  | Medium | 1 | - | - |

## DoS by blocking traffic using bucket ACL

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T50   |
| <b>Name</b>             | DoS by blocking traffic using bucket ACL   |
| <b>Description</b>      | Bucket ACL can allow access (e.g. for server access logging). An attacker can remove an existing permission to deny legitimate access to the bucket. |
| <b>Goal</b>             | Disruption of Service  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>   |
| <b>CVSS</b>             | <a href="#">Low (2.4)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutBucketAcl"<br>}  |

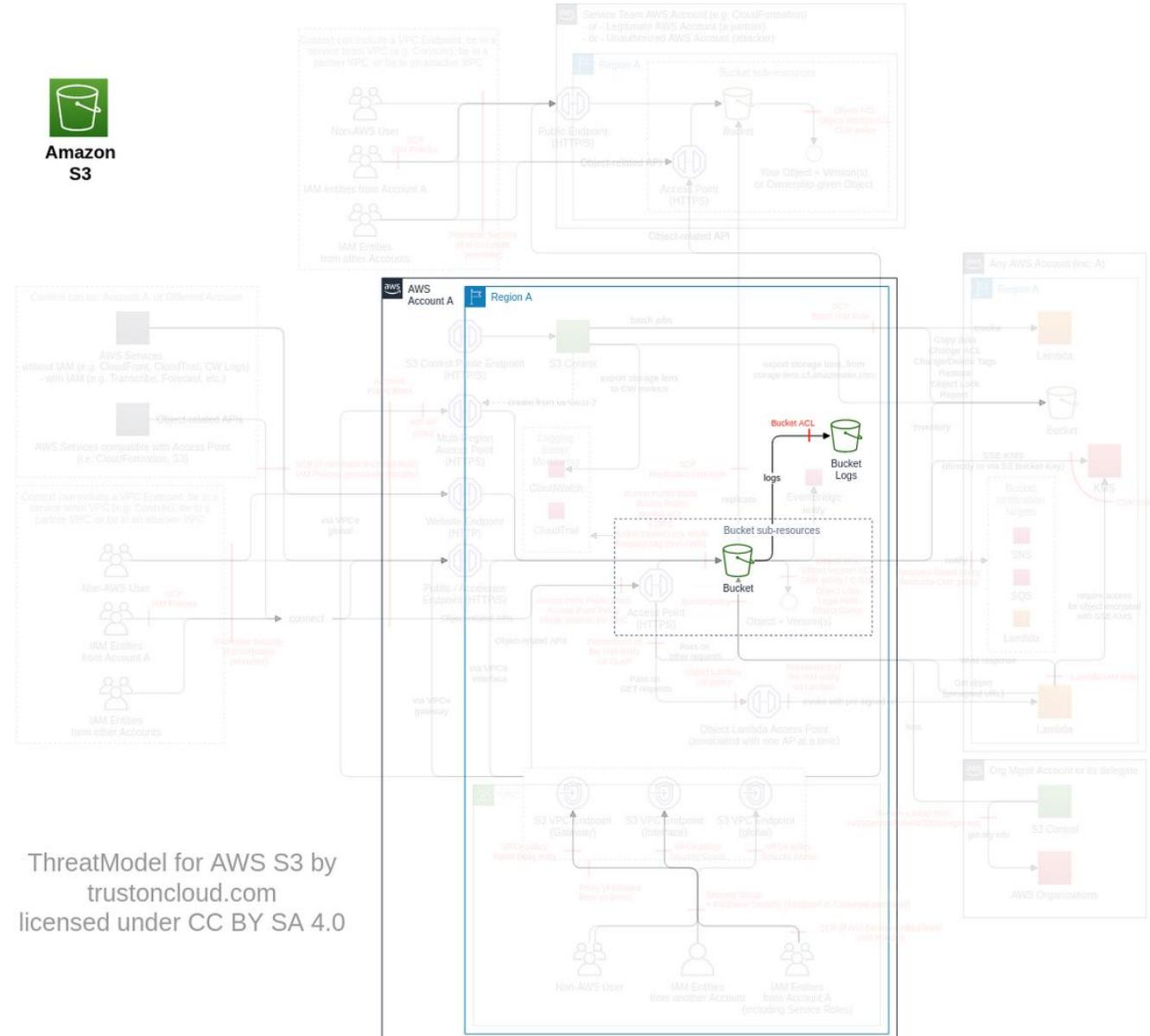


| Control Objectives  | Priority | # of associated Controls |              |           |
|---|----------|--------------------------|--------------|-----------|
|   |          | Directive                | Preventative | Detective |
| <b>Limit the access to the IAM actions required to execute the threats</b><br><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions. | Medium   | 1                        | -            | -         |

# S3 access logging (subclass of Bucket ACL, FC19)

Server access logging provides detailed records for the requests that are made to a bucket. CloudTrail S3 data events are preferred, due to the more reliable delivery timing, consistency, supporting KMS encryption and S3 Object Lock ([full comparison](#)), however website endpoint is not recorded on S3 data events, some SIEM modules might be more featured with S3 access logs, and access logging is free beside storage.

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

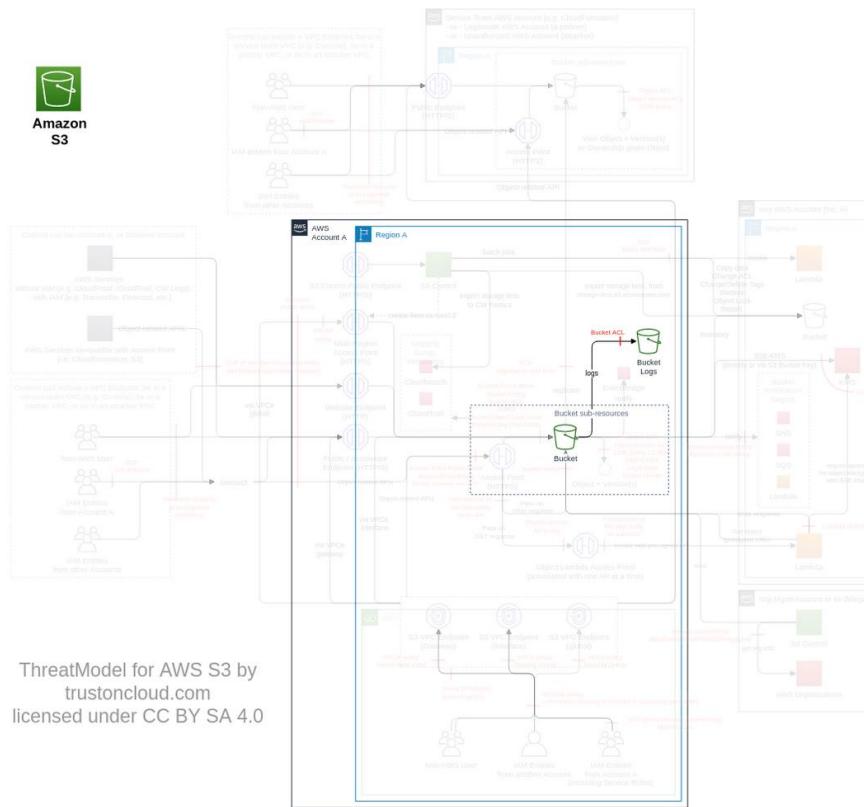
| Action                                    | IAM Permission      |
|---|---------------------|
| Sets the logging parameters for a bucket. | s3:PutBucketLogging |

## Threat List

| Name  | CVSS                      |
|---|---------------------------|
| Evide detection by disabling S3 access logs | <a href="#">Low (2.7)</a> |

## Evade detection by disabling S3 access logs

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T51   |
| <b>Name</b>             | Evade detection by disabling S3 access logs  |
| <b>Description</b>      | S3 access logs can be used by SIEM to detect abnormal behaviors. An attacker can disable S3 access log on a bucket to evade detection. |
| <b>Goal</b>             | Launch another attack  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0005</a>   |
| <b>CVSS</b>             | <a href="#">Low (2.7)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutBucketAcl"<br>}  |

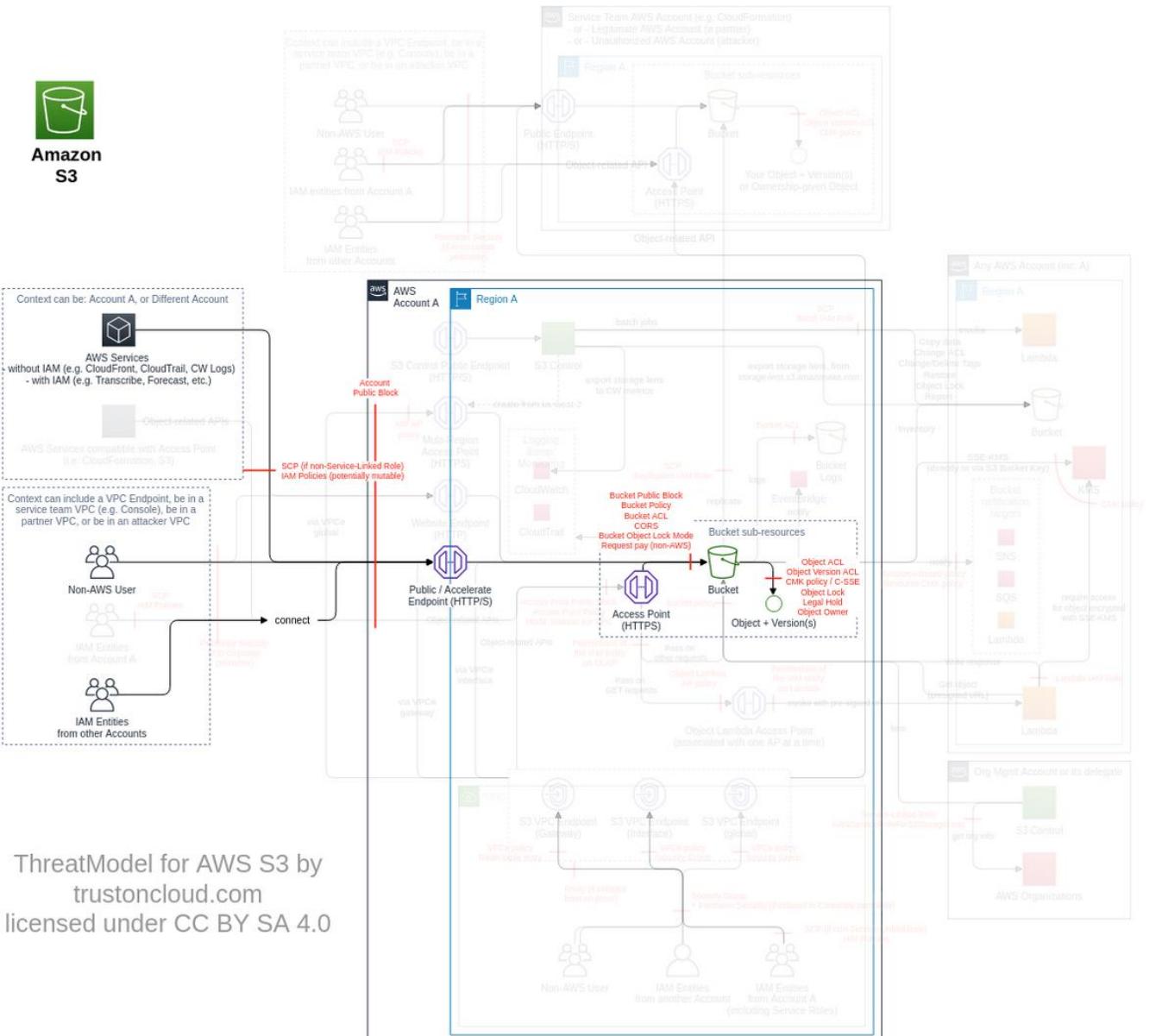


| Control Objectives  | Priority | # of associated Controls |              |           |
|---|----------|--------------------------|--------------|-----------|
|   |          | Directive                | Preventative | Detective |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions. | Medium   | 1                        | -            | -         |

# Bucket policy (subclass of Bucket, FC10)

For your bucket, you can add a bucket policy to grant other AWS accounts or IAM users permissions for the bucket and the objects in it. Any object permissions apply only to the objects that the bucket owner creates.

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

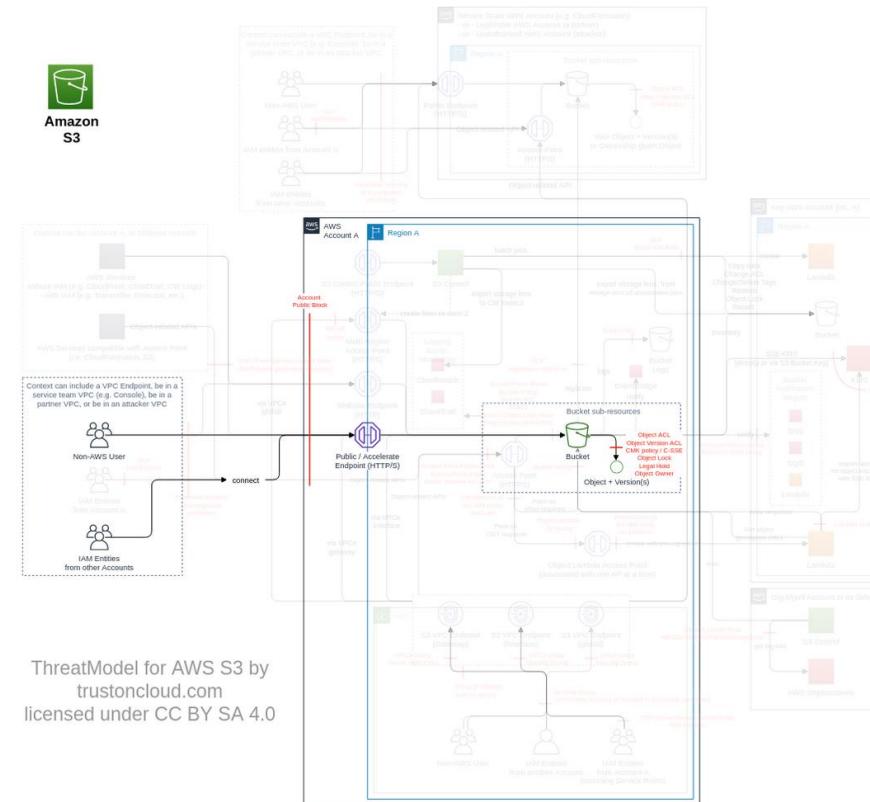
| Action                                    | IAM Permission     |
|---|--------------------|
| Adds to or replaces a policy on a bucket. | s3:PutBucketPolicy |

## Threat List

| Name  | CVSS                         |
|---|------------------------------|
| Grant unauthorized access to a private bucket by changing bucket policy | <a href="#">High (7.2)</a>   |
| Reduce bucket security by deleting the bucket policy                    | <a href="#">Medium (6.4)</a> |
| Use CloudFront to access private bucket                                 | <a href="#">Medium (5.5)</a> |

## Grant unauthorized access to a private bucket by changing bucket policy

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T37   |
| <b>Name</b>             | Grant unauthorized access to a private bucket by changing bucket policy  |
| <b>Description</b>      | Bucket policy can enable access to objects owned by the bucket. An attacker (or someone by negligence) can change the bucket policy and make the content accessible. |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">High (7.2)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutBucketPolicy"<br>}   |

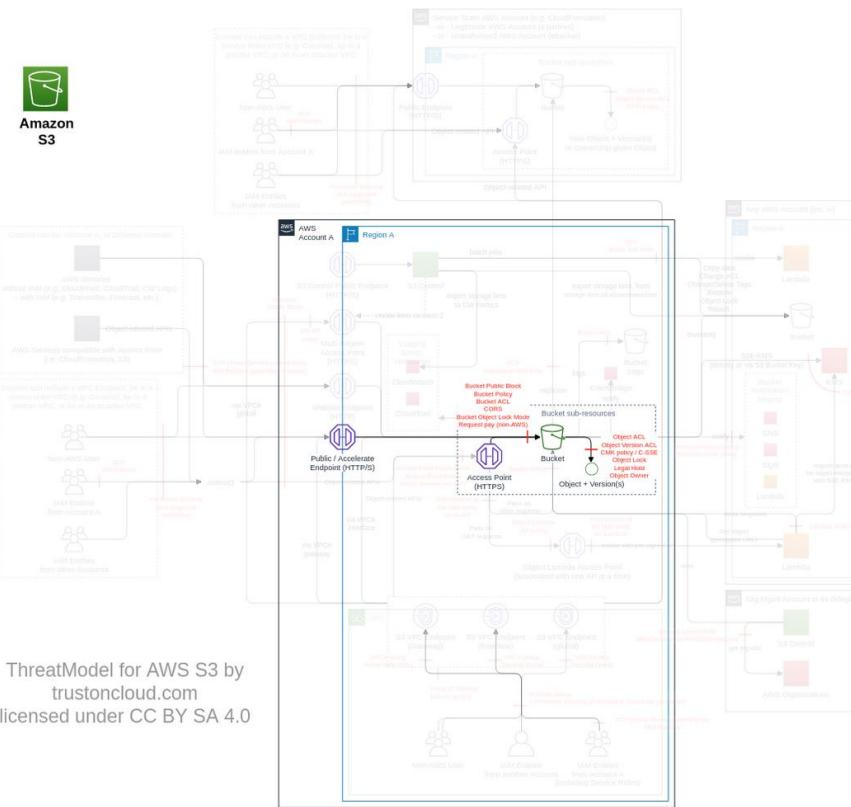


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Block direct public access</b><br><br>Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.<br>Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.<br>Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.   | Very High | -                        | 3            | -         |
| <b>Enforce encryption-at-rest</b><br><br>Maintain a list of authorized KMS key(s) for each bucket, and their default encryption key. You might simplify by using only 1 key per bucket, ideally dedicated. Note that S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ).<br>Ensure all objects on S3 buckets are encrypted with an authorized KMS key<br>Use KMS ThreatModel to protect the KMS keys used for S3 (e.g. using encryptionContext on the policy of each KMS key)<br>Implement an authorized default encryption key on each bucket and enable S3 Bucket Key (note: Amazon S3 evaluates and applies bucket policies before applying bucket default encryption settings)<br>Block PutObject requests with unauthorized KMS key on each bucket (e.g. using an S3 bucket policy deny statement on PutObject if the condition if exists "s3:x-amz-server-side-encryption-aws-kms-key-id" is not an authorized KMS key)<br>Maintain a list of buckets (or paths) required to be encrypted with server-side encryption with customer-provided keys (SSE-C)<br>For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g. using an S3 bucket policy deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present) | Very High | 5                        | 2            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.  | Very High | 4                        | -            | -         |

|  |      |   |   |   |
|--|------|---|---|---|
| In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account.<br>For each bucket, maintain a list of authorized IAM principals allowed to access via bucket policy<br>Ensure only authorized a list of authorized IAM principals allowed to access via bucket policy are configured (e.g. using IAM Access Analyzer for the reconciliation) |      |   |   |   |
| <b>Monitor S3 with Amazon GuardDuty and Macie</b><br>Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect it using Macie ThreatModel  | High | 1 | - | - |

## Reduce bucket security by deleting the bucket policy

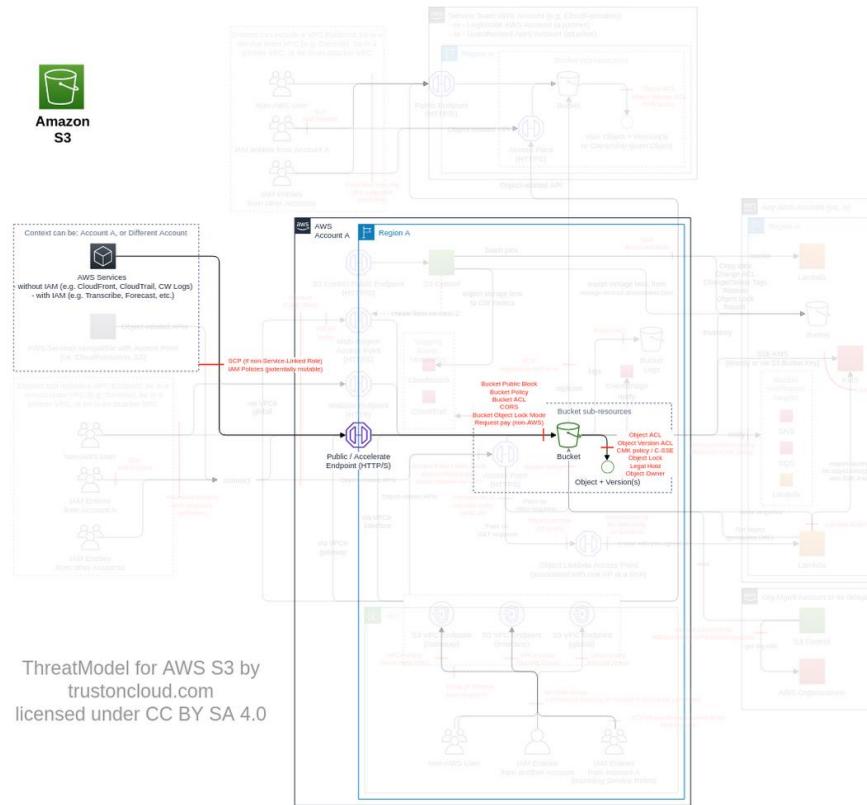
|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T38   |
| <b>Name</b>             | Reduce bucket security by deleting the bucket policy   |
| <b>Description</b>      | Bucket policy can deny access to objects, as it supersedes the object authority. An attacker (or someone by negligence) can delete the bucket policy and make the content less secure. |
| <b>Goal</b>             | Launch another attack  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0004</a>   |
| <b>CVSS</b>             | <a href="#">Medium (6.4)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3>DeleteBucketPolicy"<br>}  |



| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Limit access from only authorized VPCs</b><br>For each S3 bucket, maintain a list of VPC(s), authorized to access it.<br>Limit the access to only those VPC(s) (e.g. using S3 bucket statement, deny if the condition "aws:SourceVpce", or if the bucket policy size is beyond the limit, use this condition on access point)  | Very High | 1                        | 1            | -         |
| <b>Block direct public access</b><br>Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.<br>Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.<br>Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.            | High      | -                        | 3            | -         |
| <b>Monitor S3 with Amazon GuardDuty and Macie</b><br>Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect it using Macie ThreatModel   | High      | 1                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. | High      | 2                        | -            | -         |

## Use CloudFront to access private bucket

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T20   |
| <b>Name</b>             | Use CloudFront to access private bucket  |
| <b>Description</b>      | CloudFront distributions can use S3 as their origin. An attacker can connect a CloudFront distribution to a private S3 bucket to get access to it. |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">Medium (5.5)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutBucketPolicy"<br>}   |

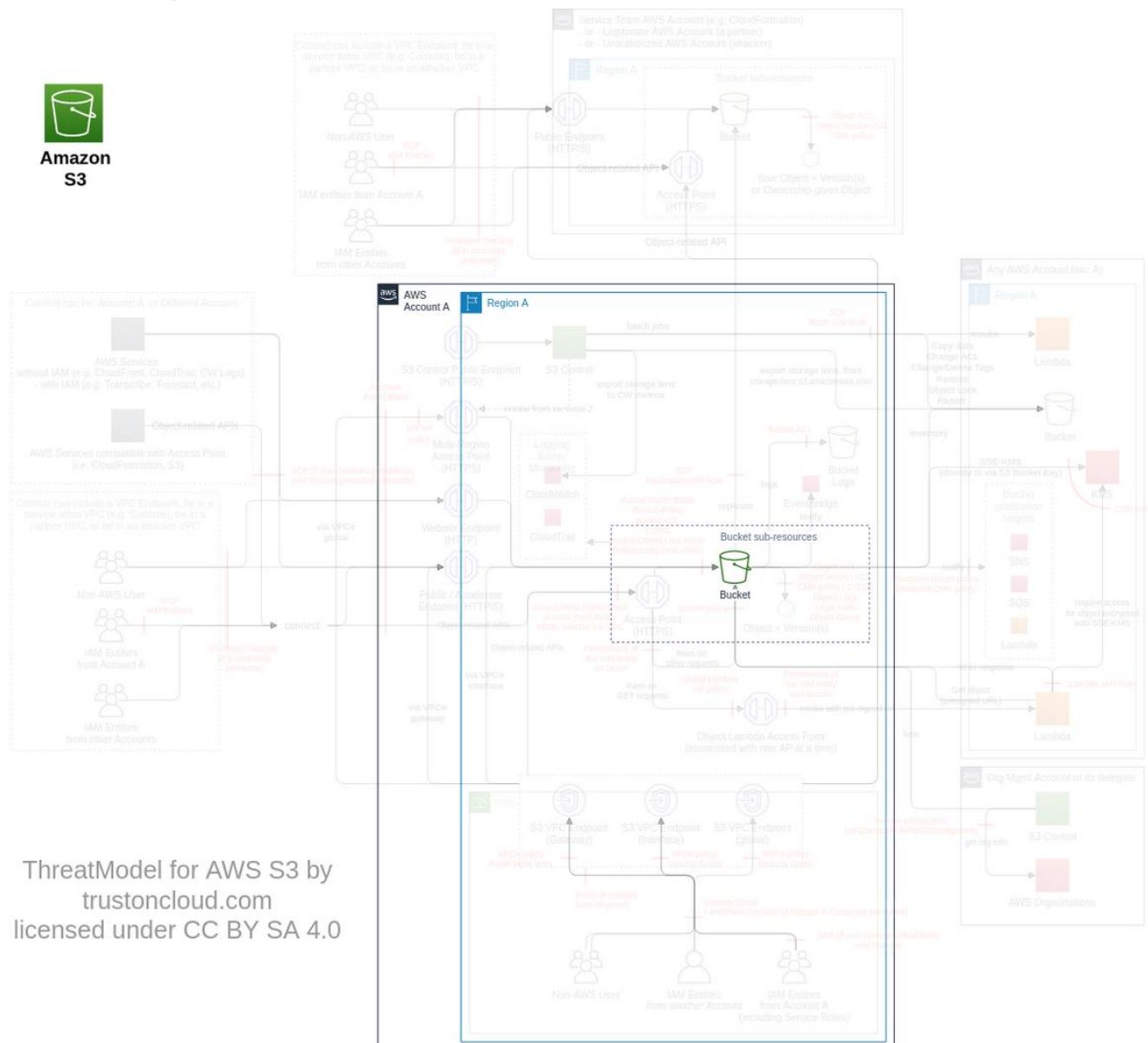


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Enforce encryption-at-rest</b><br><br>Maintain a list of authorized KMS key(s) for each bucket, and their default encryption key. You might simplify by using only 1 key per bucket, ideally dedicated. Note that S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ).<br>Ensure all objects on S3 buckets are encrypted with an authorized KMS key<br>Implement an authorized default encryption key on each bucket and enable S3 Bucket Key (note: Amazon S3 evaluates and applies bucket policies before applying bucket default encryption settings)<br>Block PutObject requests with unauthorized KMS key on each bucket (e.g. using an S3 bucket policy deny statement on PutObject if the condition if exists "s3:x-amz-server-side-encryption-aws-kms-key-id" is not an authorized KMS key)<br>Maintain a list of buckets (or paths) required to be encrypted with server-side encryption with customer-provided keys (SSE-C)<br>For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g. using an S3 bucket policy deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present) | Very High | 4                        | 2            | -         |
| <b>Control CloudFront access</b><br><br>Maintain a list of authorized CloudFront distribution (via origin access identity) and associated bucket<br>Ensure only authorized CloudFront distributions are associated with their authorized bucket, and vice versa.   | High      | 2                        | -            | -         |
| <b>Encrypt or tokenize critical data</b><br><br>Aligned with your data governance, encrypt on the client side - or tokenize - appropriate data   | Low       | 1                        | -            | -         |

## Analytics (*subclass of Bucket, FC11*)

You can analyse storage access patterns to decide on the storage class ([ref](#)).

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

| Action  | IAM Permission               |
|---|------------------------------|
| Adds an analytics configuration (identified by the analytics ID) to the bucket. | s3:PutAnalyticsConfiguration |

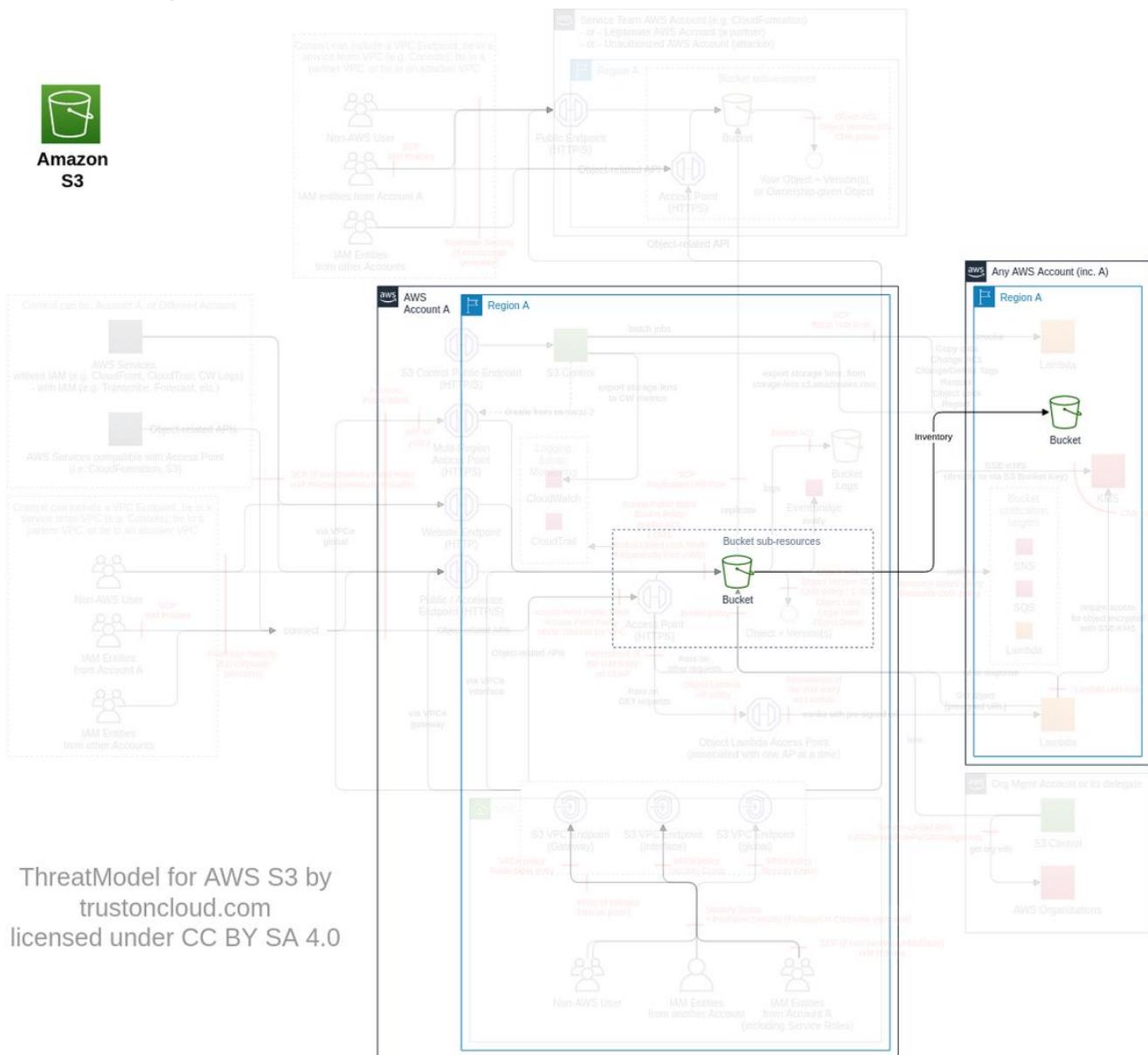
## ***Threat List***

| Name | CVSS |
|------|------|
| None | None |

# Inventory (subclass of Bucket, FC12)

You can create a report on your storage, including object metadata, or versions ([ref](#)).

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

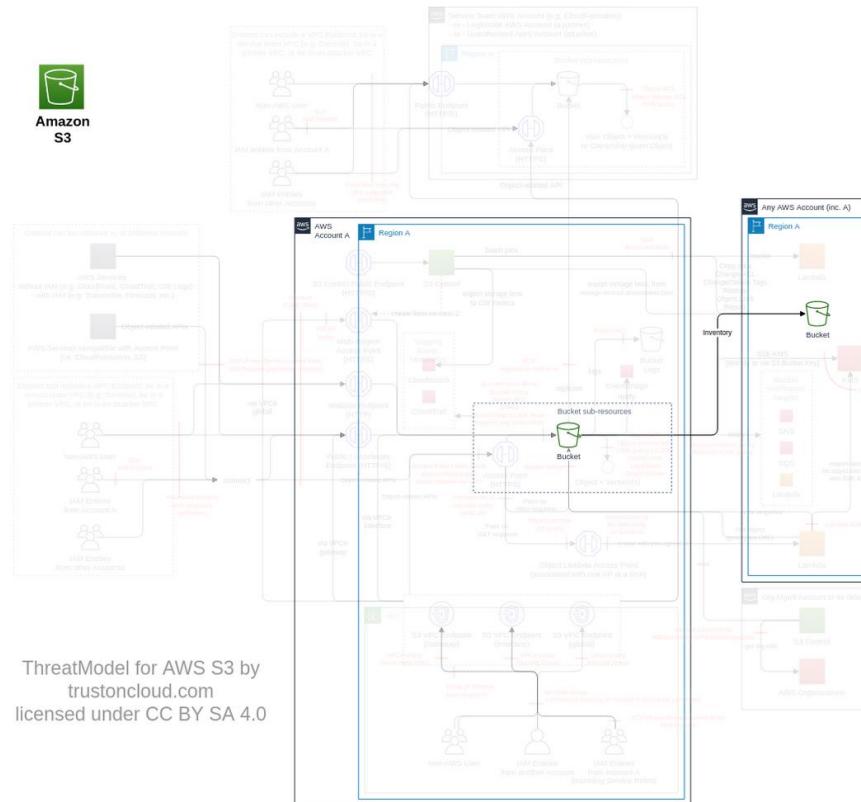
| Action   | IAM Permission               |
|--|------------------------------|
| Adds an inventory configuration (identified by the inventory ID) to the bucket | s3:PutInventoryConfiguration |

## ***Threat List***

| Name                          | CVSS                      |
|-------------------------------|---------------------------|
| Exfiltrate data via inventory | <a href="#">Low (2.4)</a> |

## Exfiltrate data via inventory

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T42  |
| <b>Name</b>             | Exfiltrate data via inventory   |
| <b>Description</b>      | Inventory sends the object names (i.e. keys) to any configured S3 bucket. An attacker can use the name of objects (1KB) to exfiltrate data. |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Low (2.4)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutBucketInventory"<br>}   |

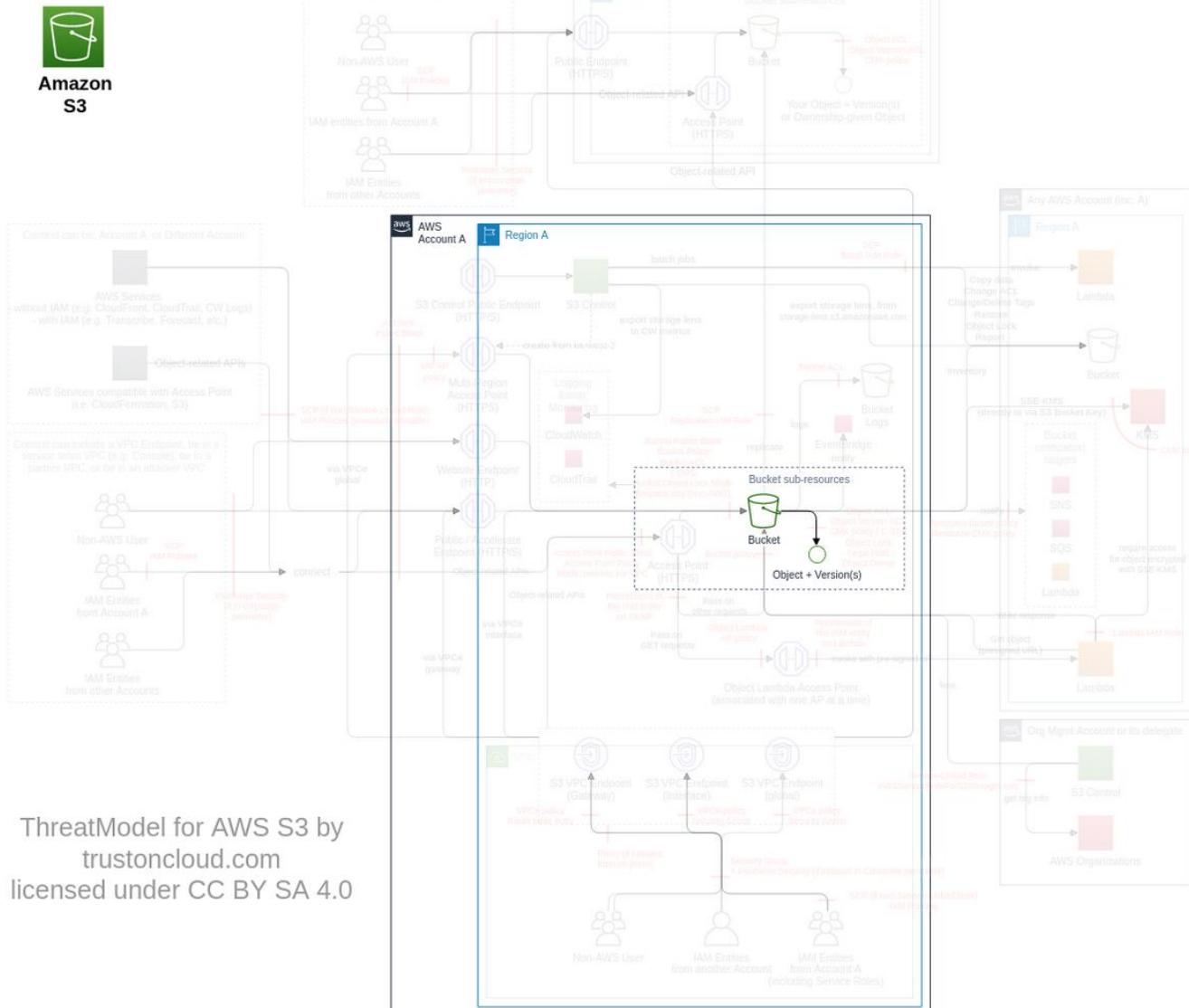


| Control Objectives  | Priority | # of associated Controls |              |           |
|---|----------|--------------------------|--------------|-----------|
|   |          | Directive                | Preventative | Detective |
| <b>Enforce good coding practice</b><br>Do not include sensitive data in bucket names, access point names, object names, object metadata and tags.   | Medium   | 1                        | -            | -         |
| <b>Control where the inventory is stored</b><br>Maintain a list of authorized S3 buckets to receive S3 inventory of each bucket<br>Ensure only authorized S3 buckets are configured to receive S3 inventory for each bucket   | Medium   | 2                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. | Medium   | 2                        | -            | -         |

# Lifecycle (*subclass of Bucket, FC13*)

You can lifecycle your data to reduce the cost of storage ([ref](#)).

## **Data Flow Diagram (DFD)**



### ***Actions and IAM Permissions to deny the feature***

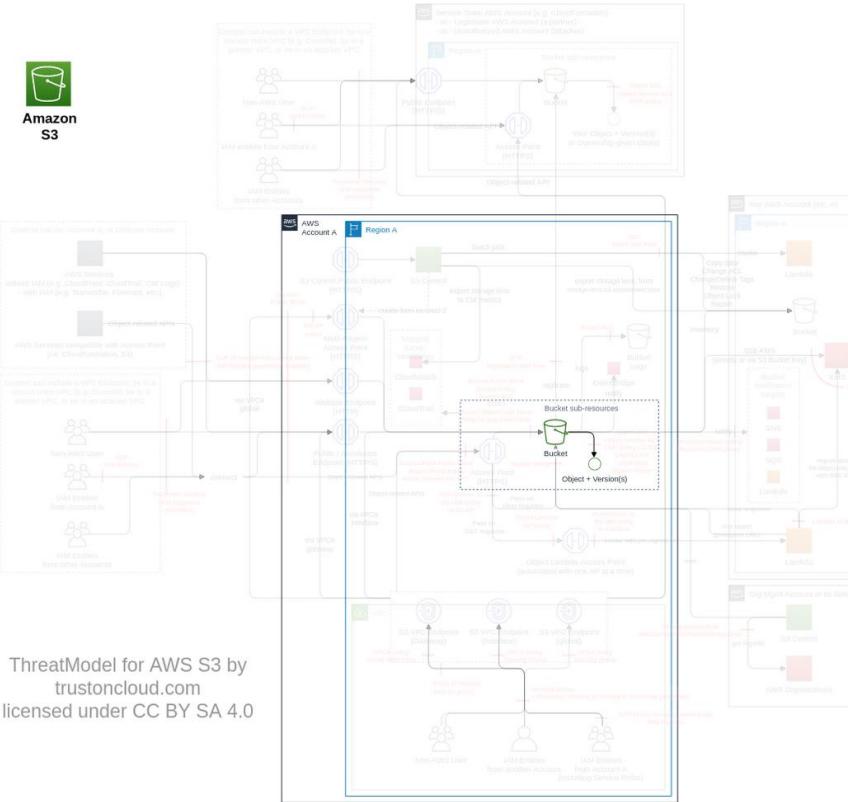
| Action  | IAM Permission                        |
|---|---------------------------------------|
| Creates a new lifecycle configuration for the bucket or replaces an existing lifecycle configuration. | s3:PutLifecycleConfiguration          |
| Puts a S3 Intelligent-Tiering configuration to the specified bucket                                   | s3:PutIntelligentTieringConfiguration |

## ***Threat List***

| Name                              | CVSS                         |
|-----------------------------------|------------------------------|
| Delete objects by using lifecycle | <a href="#">Medium (5.5)</a> |

## Delete objects by using lifecycle

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T25   |
| <b>Name</b>             | Delete objects by using lifecycle  |
| <b>Description</b>      | Lifecycle allows you to delete objects after its configured expiry. An attacker can use a lifecycle configuration to destroy data. |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">Medium (5.5)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutLifecycleConfiguration"<br>}   |

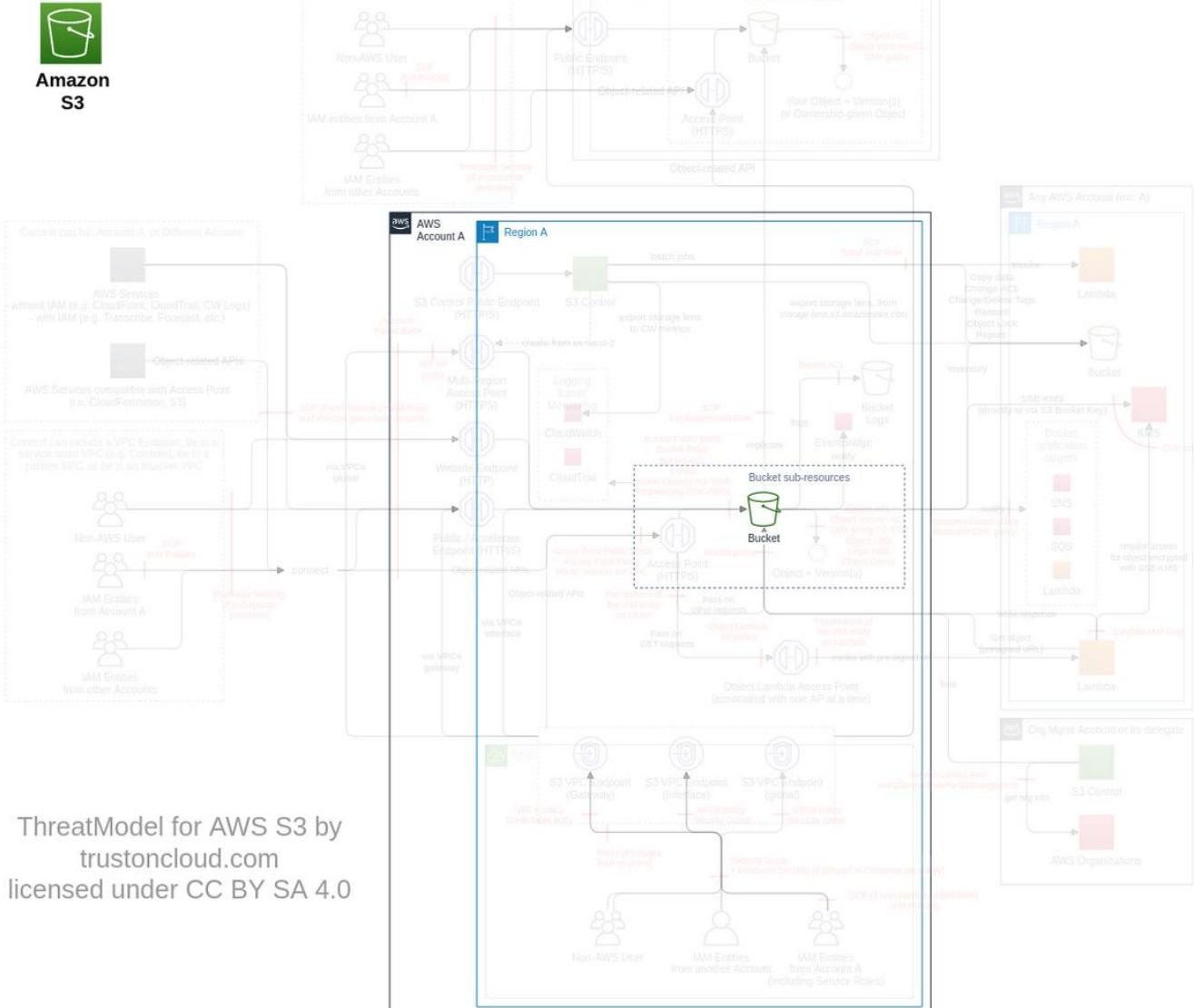


| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Identify and ensure the protection all internal buckets hosting your objects</b><br>Track all buckets you control, define their authorized data classification, identify whether the hosted data is primary (i.e. source of truth, for example logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g. file-processing, software package, etc.), their WORM requirements (e.g. SEC 17a-4, CTCC, etc.), if they are production/non-production (preferably done at account-level), their storage class. You may use tags, Infra-as-code, AWS Glue Data Catalog or external management tool like <a href="#">FINRA herd</a> ) | Very High | 1                        | -            | -         |
| <b>Use S3 Object Lock to protect data integrity</b><br>Implement the authorized default S3 Object Lock on each bucket (note: Amazon S3 evaluates and applies bucket policies before applying bucket default S3 Object Lock settings)  | Very High | -                        | 1            | -         |
| <b>Protect primary data against loss</b><br>Backup primary data in a secure location under a different security authority (e.g. in an <a href="#">AWS data bunker account</a> via replication)  | High      | 1                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account.   | Medium    | 2                        | -            | -         |

# Metrics (subclass of Bucket, FC14)

You can configure metrics to get additional insights into your usage ([ref](#)).

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

| Action  | IAM Permission                          |
|---|---|
| Sets or updates a metrics configuration for the CloudWatch request metrics (specified by the metrics configuration ID) from the bucket. | <code>s3:PutMetricsConfiguration</code> |

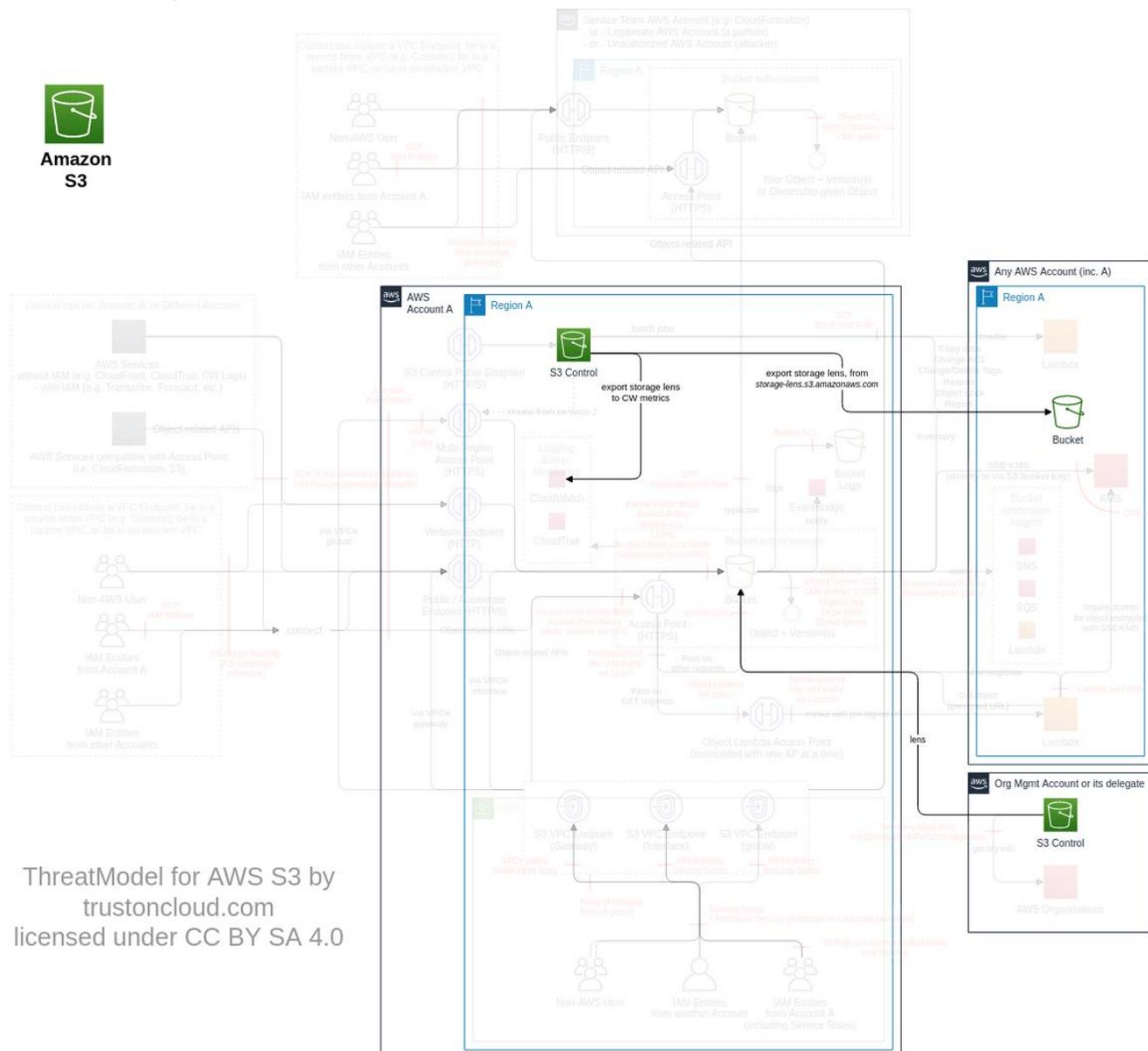
## Threat List

| Name | CVSS |
|------|------|
| None | None |

# S3 Storage Lens (*subclass of Bucket, FC31*)

*S3 Storage Lens provides a single view of object storage usage and activity across your entire S3 storage.*

## **Data Flow Diagram (DFD)**



### ***Actions and IAM Permissions to deny the feature***

| Action                                       | IAM Permission                 |
|--|--------------------------------|
| Puts an Amazon S3 Storage Lens configuration | s3:PutStorageLensConfiguration |

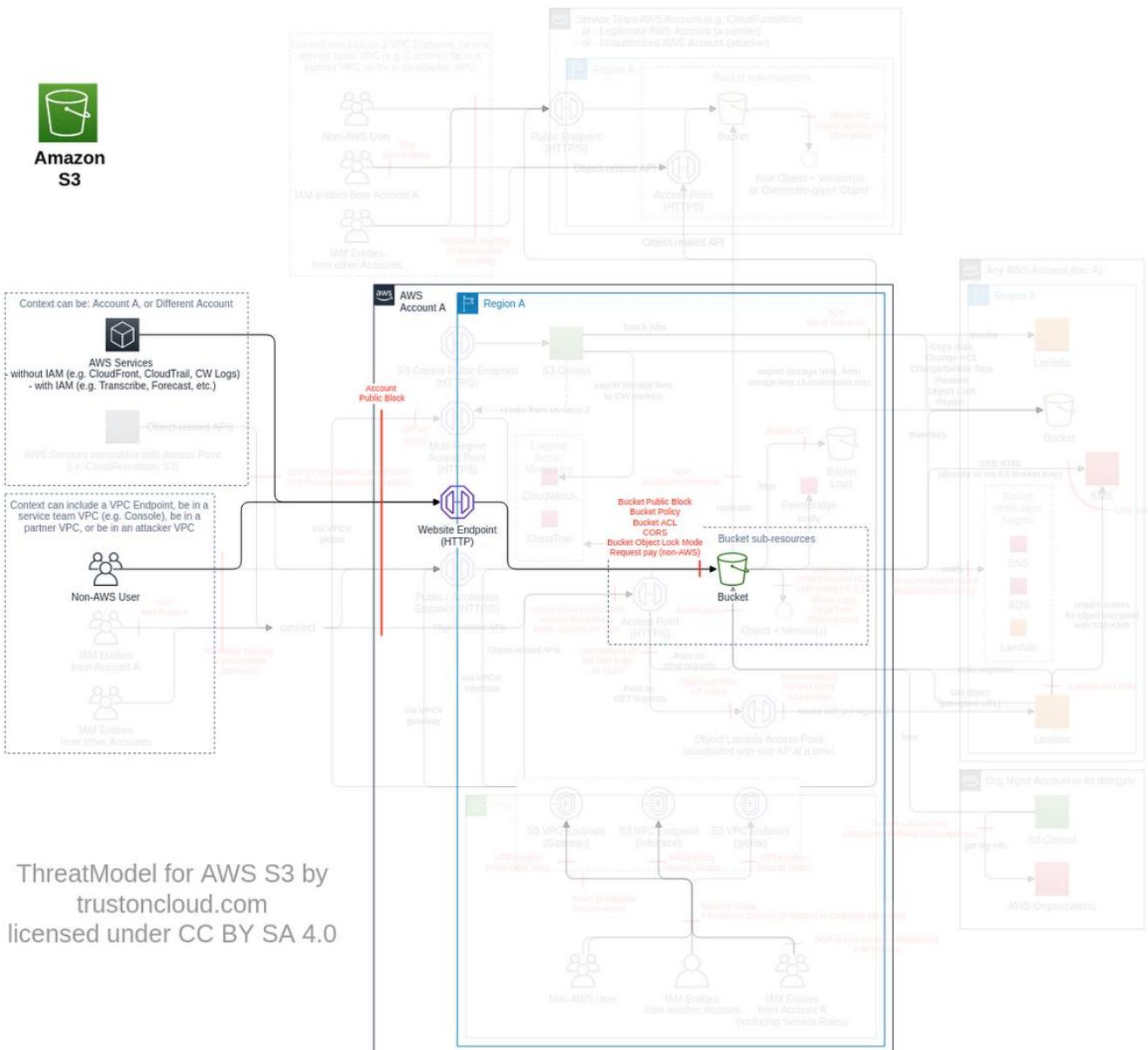
## ***Threat List***

| Name | CVSS |
|------|------|
| None | None |

# Website (subclass of Bucket, FC16)

You can host a static website on Amazon S3. On a static website, individual web pages include static content. They might also contain client-side scripts ([ref](#)).

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

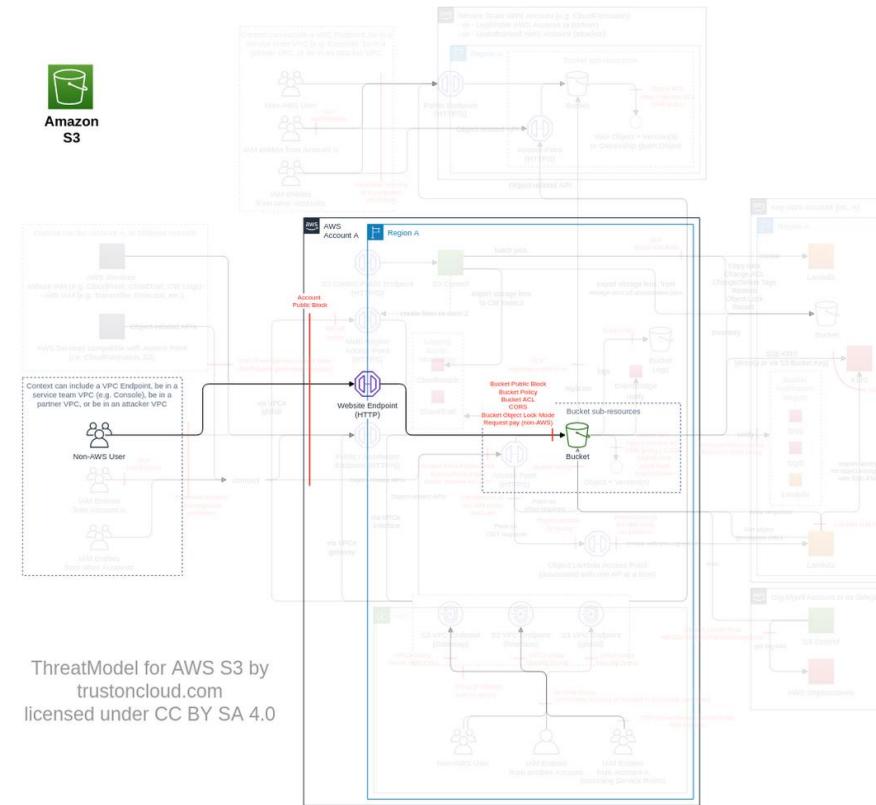
| Action  | IAM Permission      |
|---|---------------------|
| Sets the configuration of the website that is specified in the website subresource. | s3:PutBucketWebsite |

## Threat List

| Name   | CVSS                         |
|--|------------------------------|
| Embed client-side script malware in bucket website | <a href="#">Medium (5.5)</a> |
| Clickjacking on S3 website                         | <a href="#">Medium (4.2)</a> |
| Intercept data in transit on the website endpoint  | <a href="#">Low (3.1)</a>    |

## Embed client-side script malware in bucket website

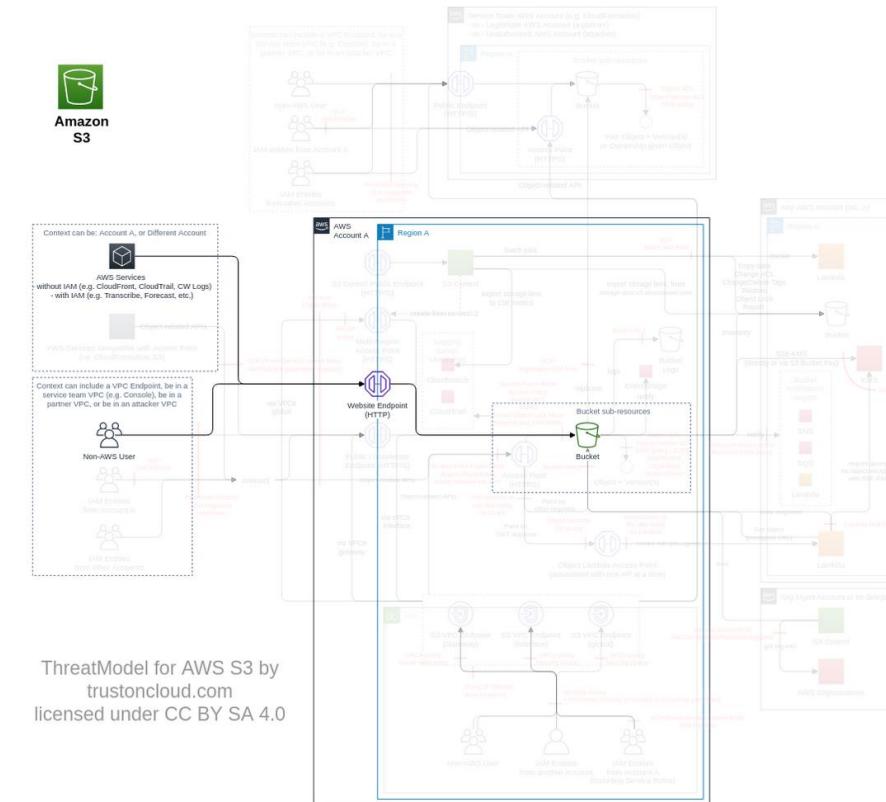
|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T15  |
| <b>Name</b>             | Embed client-side script malware in bucket website  |
| <b>Description</b>      | S3 website enables users to be served client-side scripts (e.g. JavaScript). An attacker can upload a client-side script with a malware (e.g. cryptomining) on the visitor. |
| <b>Goal</b>             | Direct Financial Gain   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>  |
| <b>CVSS</b>             | <a href="#">Medium (5.5)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutObject"<br>}  |



| Control Objectives  | Priority | # of associated Controls |              |           |
|---|----------|--------------------------|--------------|-----------|
|   |          | Directive                | Preventative | Detective |
| <b>Identify and ensure the protection all external buckets hosting your objects</b><br>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel).<br>Scan all data before uploading to an external bucket to ensure the classification of the data is aligned with the bucket classification (e.g. using Macie). | High     | 2                        | -            | -         |
| <b>Scan input/output objects for malware</b><br>If the bucket is used as an input or the output of a process, scan the objects for malware (e.g. using <a href="#">VirusScan</a> or <a href="#">Trend Micro Cloud One</a> )   | Low      | -                        | -            | 1         |

## Clickjacking on S3 website

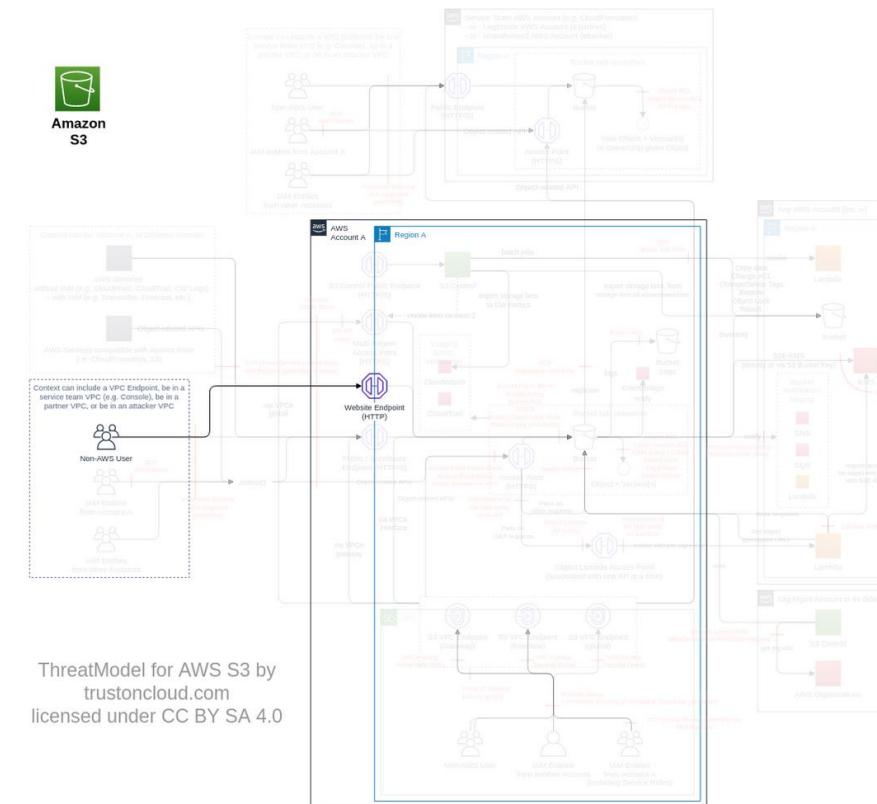
|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T29  |
| <b>Name</b>             | Clickjacking on S3 website  |
| <b>Description</b>      | S3 does not enforce certain security headers by default. An attacker can use an iFrame on your website to trick users to interact with their own scripts. |
| <b>Goal</b>             | Launch another attack   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0040</a>  |
| <b>CVSS</b>             | <a href="#">Medium (4.2)</a>  |
| <b>IAM Access</b>       | 0   |



| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Deploy only authorized S3 website and behind a CDN</b><br>Maintain a list of authorized buckets to be configured as website<br>Ensure only authorized buckets are configured as website<br>Ensure S3 websites are protected with HTTP headers ( <a href="#">ref</a> ) using a CDN (e.g. CloudFront) | Very High | 3                        | -            | -         |

## Intercept data in transit on the website endpoint

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T13  |
| <b>Name</b>             | Intercept data in transit on the website endpoint   |
| <b>Description</b>      | S3 website endpoint is serving HTTP only. An attacker can intercept HTTP traffic to steal data. |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Low (3.1)</a>   |
| <b>IAM Access</b>       | 0   |

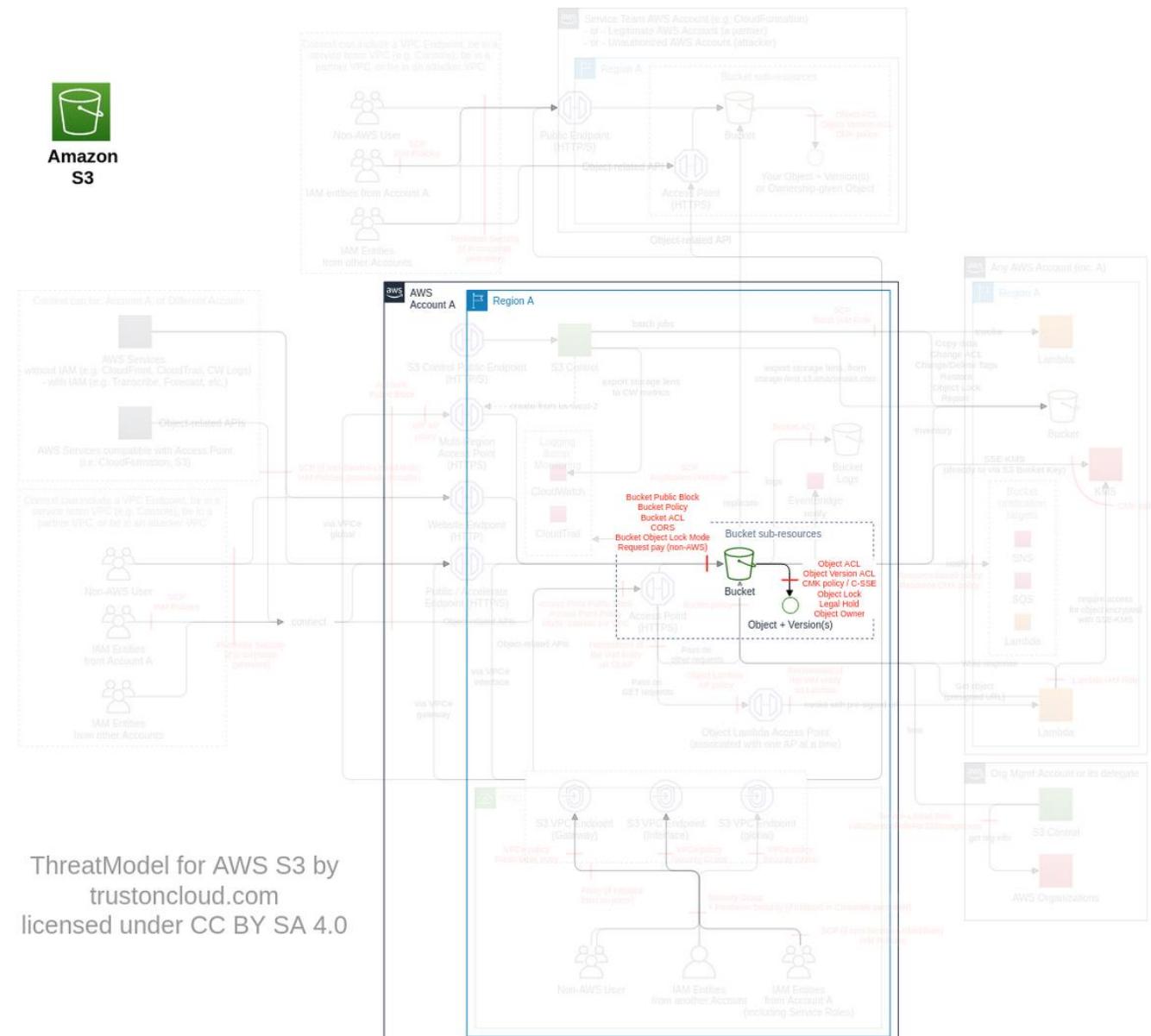


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Block direct public access</b><br>Front buckets required to be public, using authenticated CDN (e.g. CloudFront) or API Gateway, protected with WAF (e.g. for <a href="#">hotlinking</a> )  | Very High | 1                        | -            | -         |
| <b>Deploy only authorized S3 website and behind a CDN</b><br>Maintain a list of authorized buckets to be configured as website<br>Ensure only authorized buckets are configured as website<br>Ensure S3 websites are protected with HTTP headers ( <a href="#">ref</a> ) using a CDN (e.g. CloudFront) | High      | 3                        | -            | -         |
| <b>Encrypt or tokenize critical data</b><br>Aligned with your data governance, encrypt on the client side - or tokenize - appropriate data   | Medium    | 1                        | -            | -         |

# S3 Object Lock (subclass of Bucket, FC17)

You can use S3 Object Lock to store objects using a write-once-read-many (WORM) model ([ref](#)). Creating a bucket with S3 Object Lock will enable versioning even without permissions.

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

| Action  | IAM Permission                |
|---|-------------------------------|
| Grants permission to allow circumvention of governance-mode object retention settings (for DeleteObject, DeleteObjects and PutObjectRetention)  | s3:BypassGovernanceRetention  |
| Allows to place a default S3 Object Lock configuration at bucket creation (AWS Support needs to be contacted for existing buckets). It automatically enables versioning, even without the permission. | s3:PutObjectLockConfiguration |
| Puts object retention on a specific object  | s3:PutObjectRetention         |

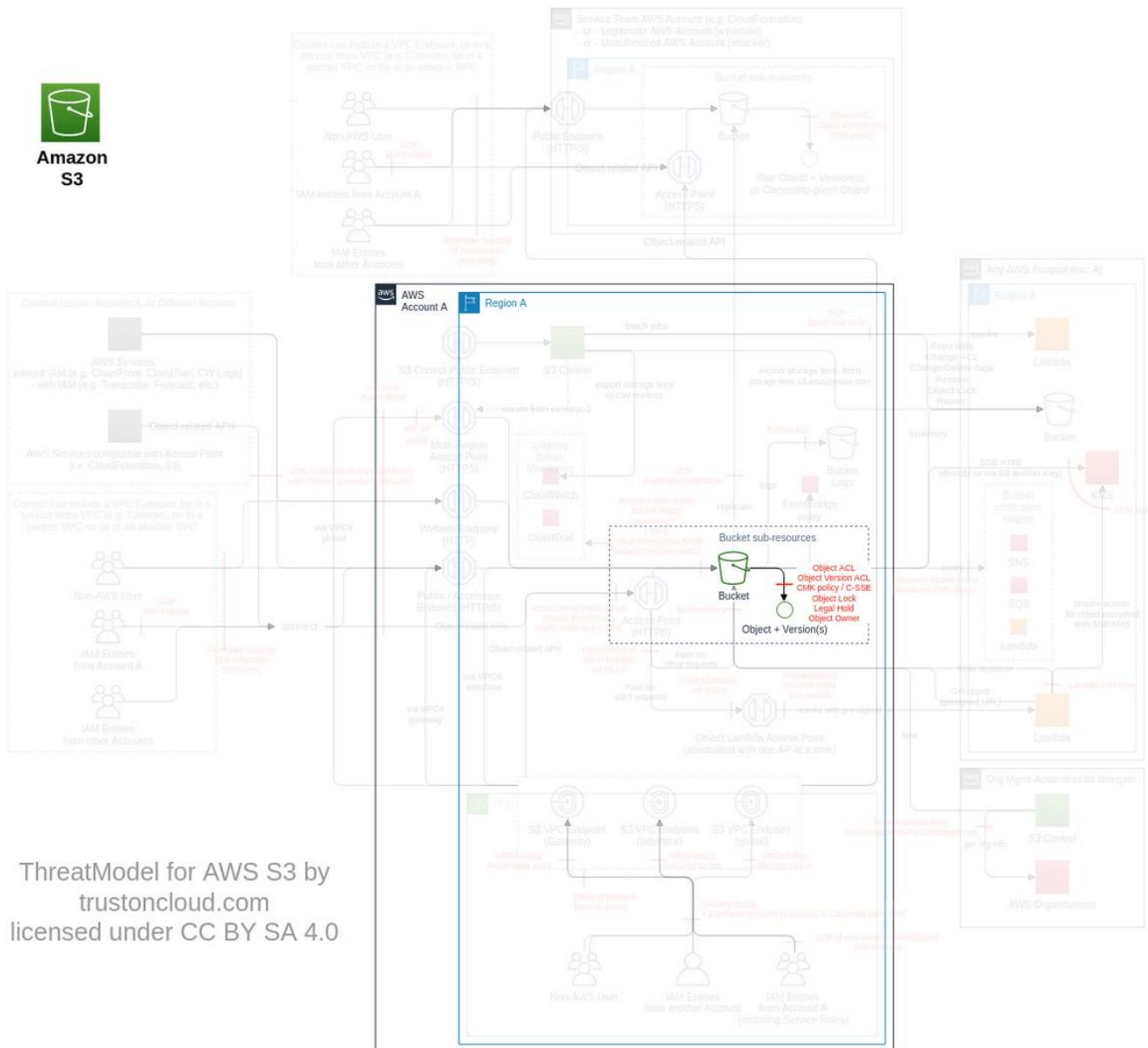
## Threat List

| Name | CVSS |
|------|------|
| None | None |

# Legal hold (subclass of S3 Object Lock, FC29)

A legal hold provides the same protection as a retention period, but it has no expiration date. Instead, a legal hold remains in place until you explicitly remove it. Legal holds are independent from retention periods.

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

| Action   | IAM Permission        |
|--|-----------------------|
| Puts Object Lock legal hold on a specific object | s3:PutObjectLegalHold |

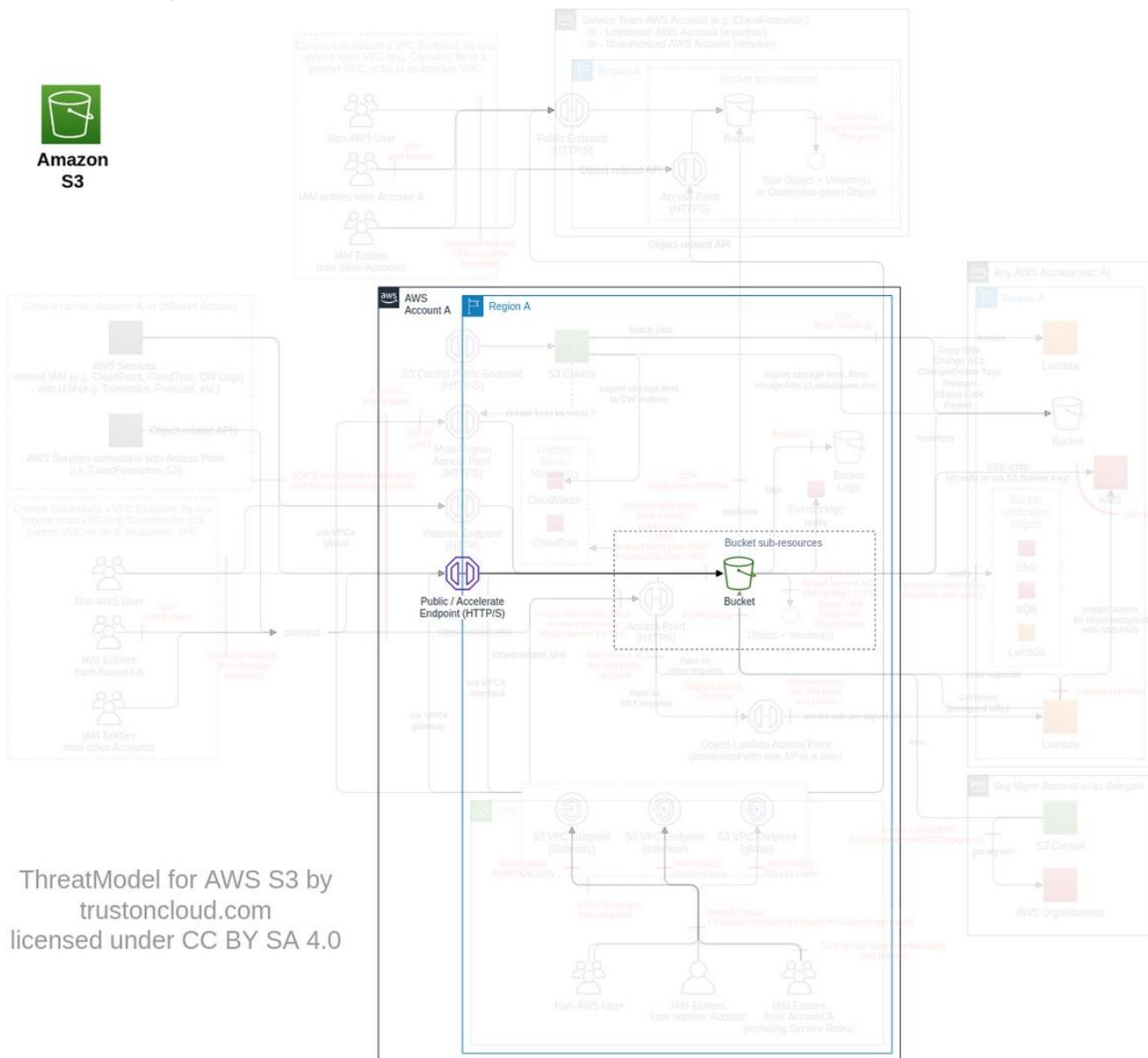
## Threat List

| Name | CVSS |
|------|------|
| None | None |

# Transfer Acceleration (subclass of Bucket, FC18)

You can use Transfer Acceleration to improve the performance of long-distance transfers ([ref](#)).

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

| Action  | IAM Permission                |
|---|-------------------------------|
| Sets the Transfer Acceleration state of an existing bucket. | s3:PutAccelerateConfiguration |

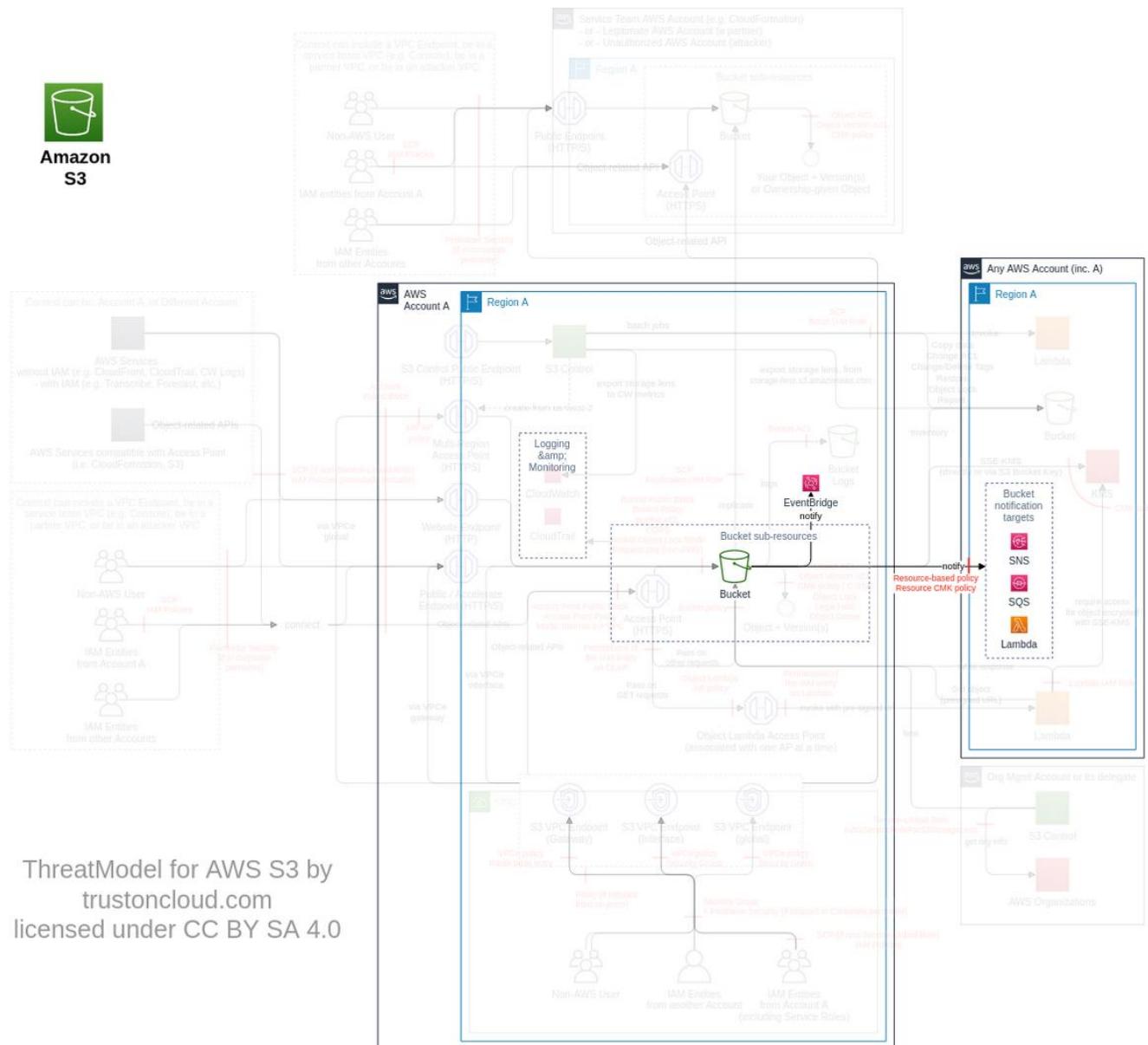
## Threat List

| Name | CVSS |
|------|------|
| None | None |

# Notification (*subclass of Bucket, FC20*)

You can receive notifications when certain events happen in your bucket. Notifications can be sent cross-account ([ref](#)).

# ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

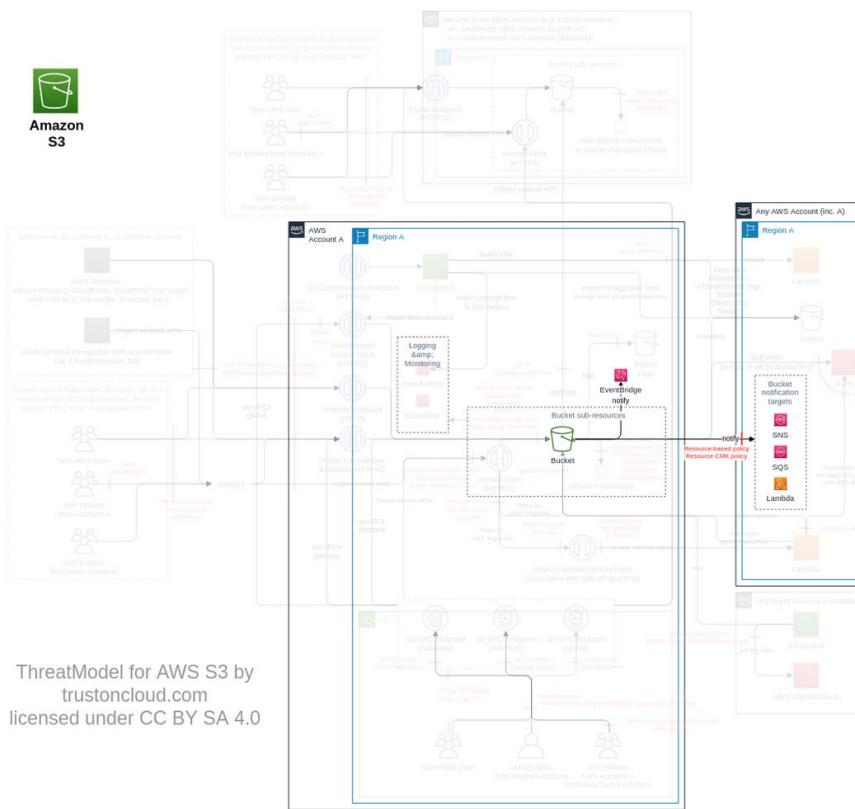
| Action  | IAM Permission           |
|---|--------------------------|
| Enables you to receive notifications when certain events happen in your bucket. | s3:PutBucketNotification |

## ***Threat List***

| Name                                   | CVSS                      |
|--|---------------------------|
| Exfiltrate data via event notification | <a href="#">Low (2.4)</a> |

## **Exfiltrate data via event notification**

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T41  |
| <b>Name</b>             | Exfiltrate data via event notification  |
| <b>Description</b>      | Event notification sends the key to any configured SQS, SNS or Lambda (cross-account), or EventBridge (same account). An attacker can use the name of objects (1KB) to exfiltrate data. |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Low (2.4)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutBucketNotification"<br>}  |

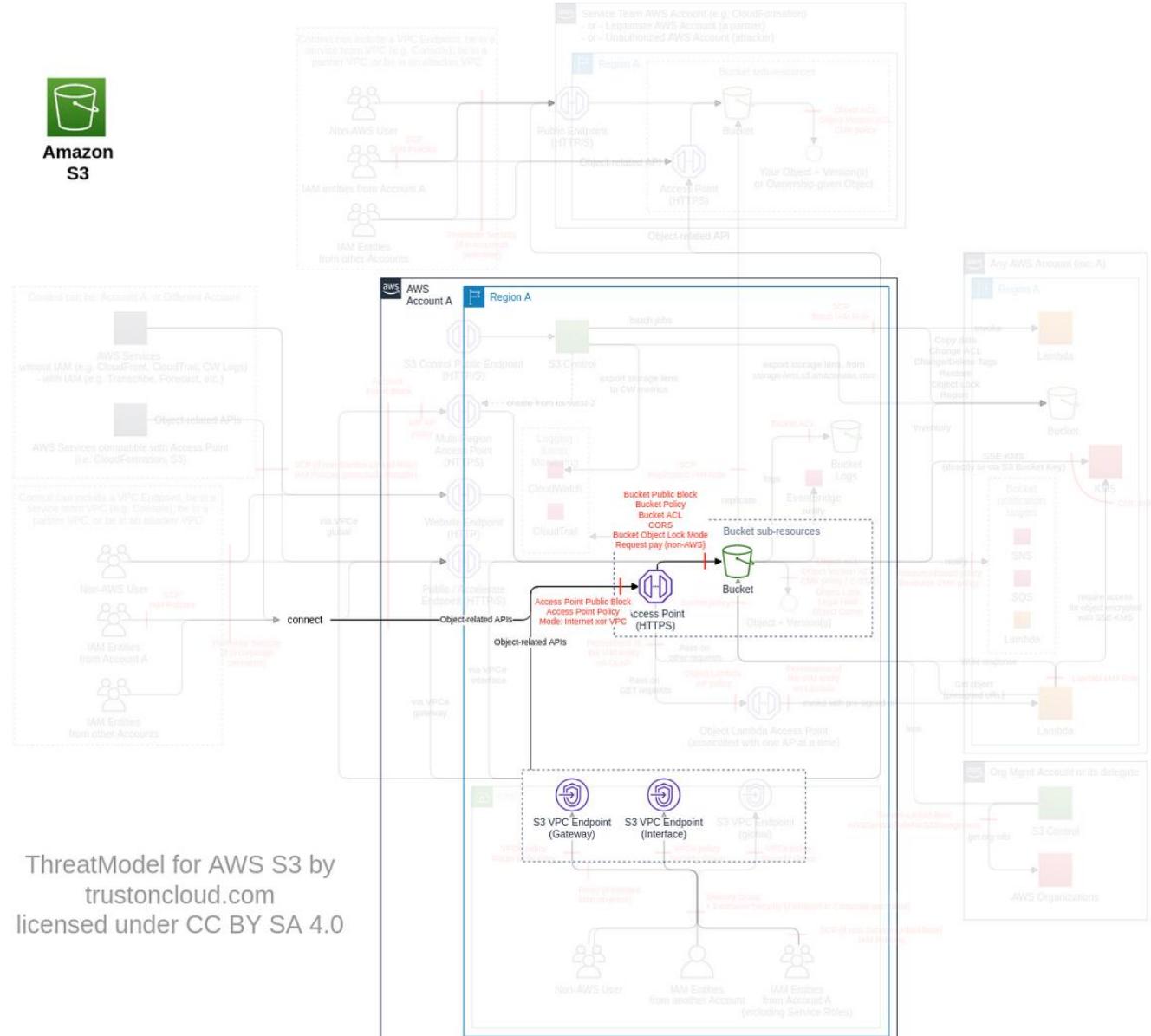


| Control Objectives   |   | Priority | # of associated Controls |              |           |
|--|---|----------|--------------------------|--------------|-----------|
|  |   |          | Directive                | Preventative | Detective |
| <b>Control event receivers</b>   | Maintain a list of authorized notification receiver(s) (e.g. SNS Topic, Lambda, etc.) for each bucket. You might use a simpler approach by using authorized account ID(s) to ensure all your receivers are in authorized AWS account(s).<br>Ensure only authorized notification receiver(s) (e.g. SNS Topic, Lambda, etc.) for each bucket are configured   | High     | 2                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b> | Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. | Medium   | 2                        | -            | -         |
| <b>Enforce good coding practice</b>  | Do not include sensitive data in bucket names, access point names, object names, object metadata and tags.  | Low      | 1                        | -            | -         |

# Access point (*subclass of Bucket, FC26*)

Access points are named network endpoints that are attached to buckets that you can use to perform S3 object operations. Only certain operations and AWS services are compatible (

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

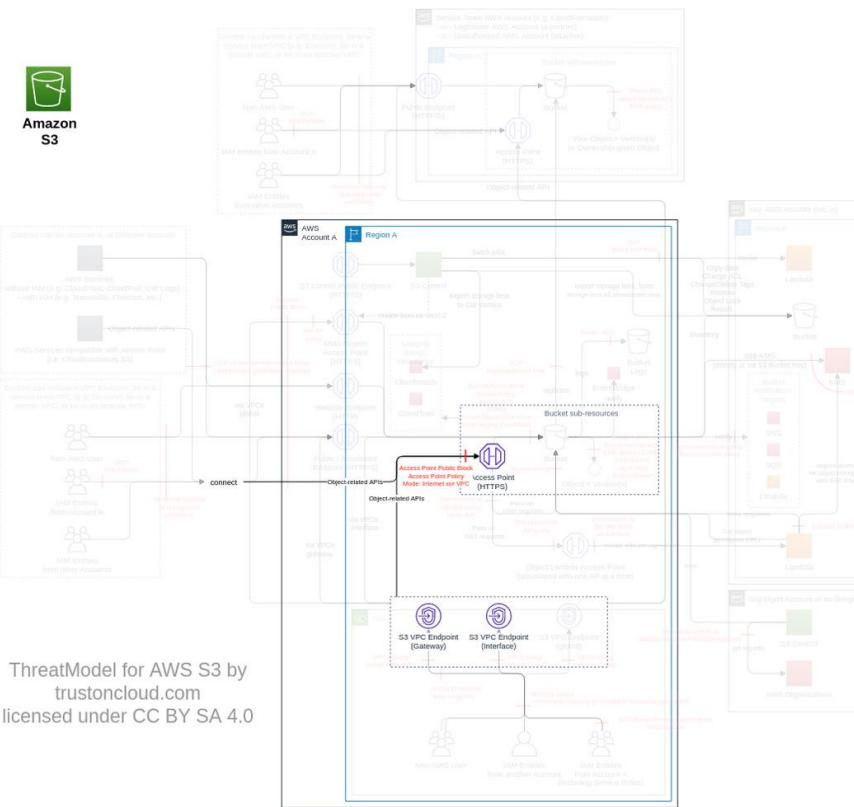
| Action                      | IAM Permission       |
|-----------------------------|----------------------|
| Creates a new access point. | s3>CreateAccessPoint |

## ***Threat List***

| Name   | CVSS                         |
|--|------------------------------|
| Grant unauthorized access to a bucket by changing/deleting access point policy | <a href="#">Medium (6.8)</a> |
| Unauthorized collection of data by swapping access point                       | <a href="#">Medium (4.6)</a> |

## Grant unauthorized access to a bucket by changing/deleting access point policy

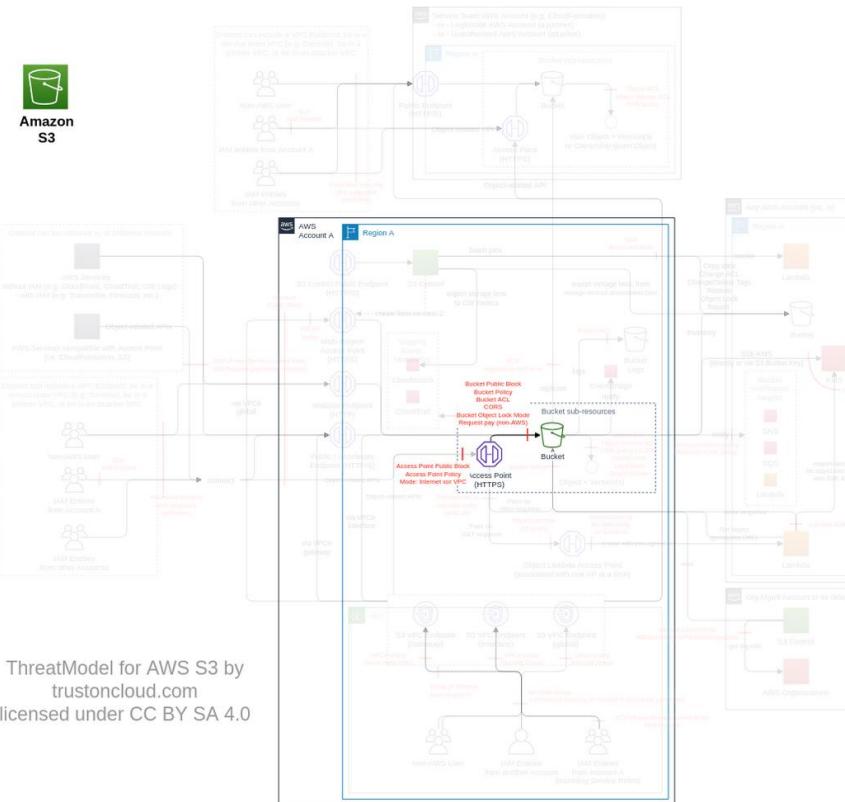
|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T54   |
| <b>Name</b>             | Grant unauthorized access to a bucket by changing/deleting access point policy   |
| <b>Description</b>      | Access point policy can enable access to objects owned by the bucket. An attacker (or someone by negligence) can change the access point policy and make the content accessible. |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">Medium (6.8)</a>   |
| <b>IAM Access</b>       | {<br>"OR": ["s3:PutAccessPointPolicy", "s3>DeleteAccessPointPolicy"]<br>}  |



| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Block direct public access</b><br>Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.  | Very High | -                        | 1            | -         |
| <b>Restrict access point access to VPC when in use</b><br>Limit access via the S3 access point by using in VPC endpoint and/or bucket policy the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of allowlist bucket name in VPC endpoint/bucket policy.   | Medium    | -                        | 1            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. | Medium    | 2                        | -            | -         |

## Unauthorized collection of data by swapping access point

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T28  |
| <b>Name</b>             | Unauthorized collection of data by swapping access point  |
| <b>Description</b>      | Access points can be deleted and recreated with the same name, and therefore the same ARN. An attacker can delete an access point and recreate the same, on a bucket (in the same account) it controls to collect/modify data; or making it accessible from the Internet. |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0009</a>  |
| <b>CVSS</b>             | <a href="#">Medium (4.6)</a>  |
| <b>IAM Access</b>       | {<br>"AND": ["s3>CreateAccessPoint", "s3>DeleteAccessPoint"]<br>}   |

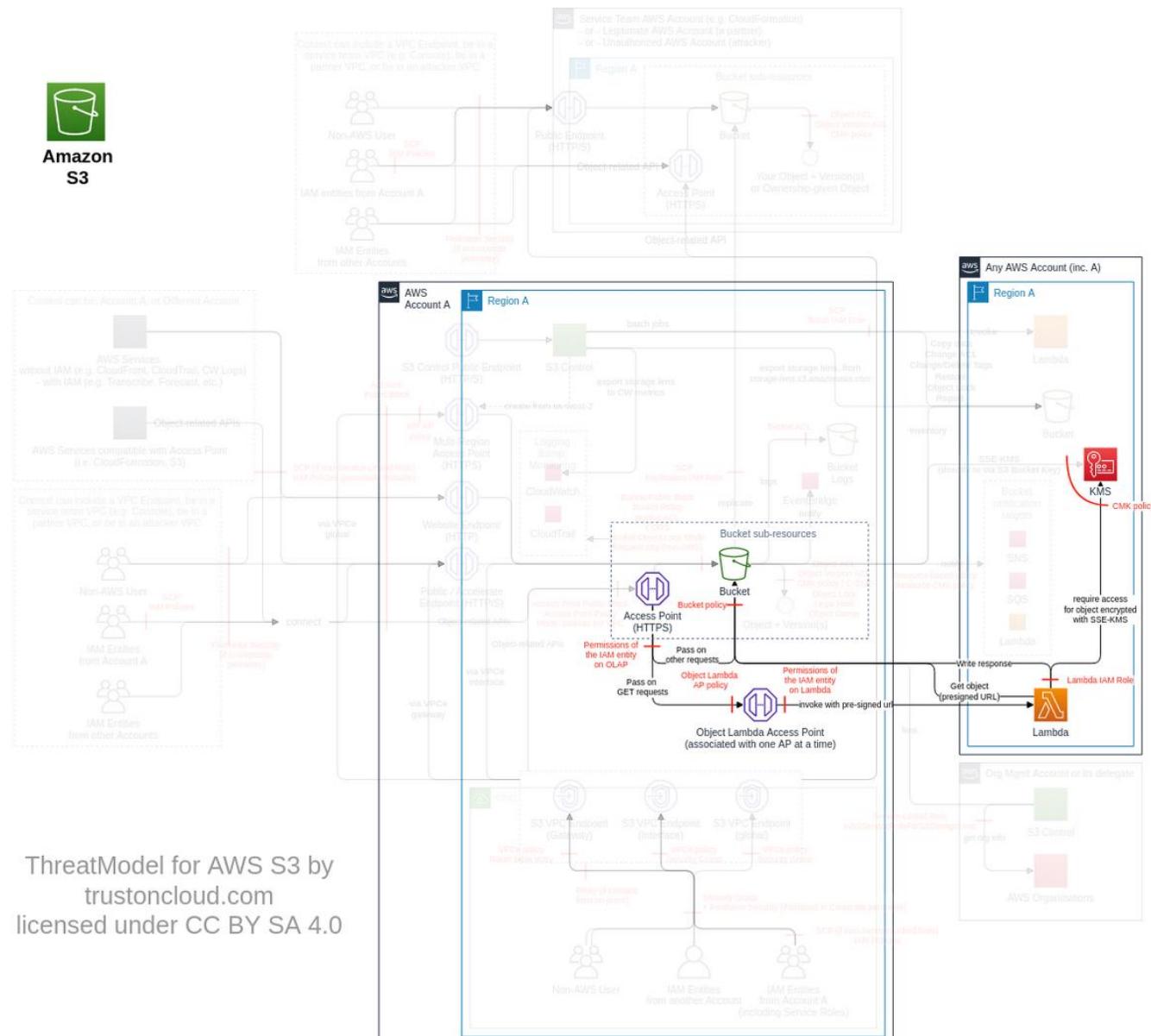


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Restrict access point access to VPC when in use</b><br><br>Maintain a list of authorized access between VPC, S3 access point and S3.<br>In S3 bucket policy, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn"<br>Block the creation "s3>CreateAccessPoint" of non-VPC S3 access point (e.g. using the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"})<br>Block all traffic from Internet-configured S3 access point (e.g. on the bucket policy, using a deny statement with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}) | Very High | 1                        | 3            | -         |
| <b>Block requests with KMS keys from unauthorized AWS account(s)</b><br><br>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account<br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts)<br>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> )                                     | Very High | 1                        | 1            | 1         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.  | Medium    | 1                        | -            | -         |

# S3 Object Lambda (*subclass of Access point, FC32*)

*S3 Object Lambda enables users to apply their own custom code to process the output of a standard S3 request by automatically invoking a Lambda function.*

## **Data Flow Diagram (DFD)**



### ***Actions and IAM Permissions to deny the feature***

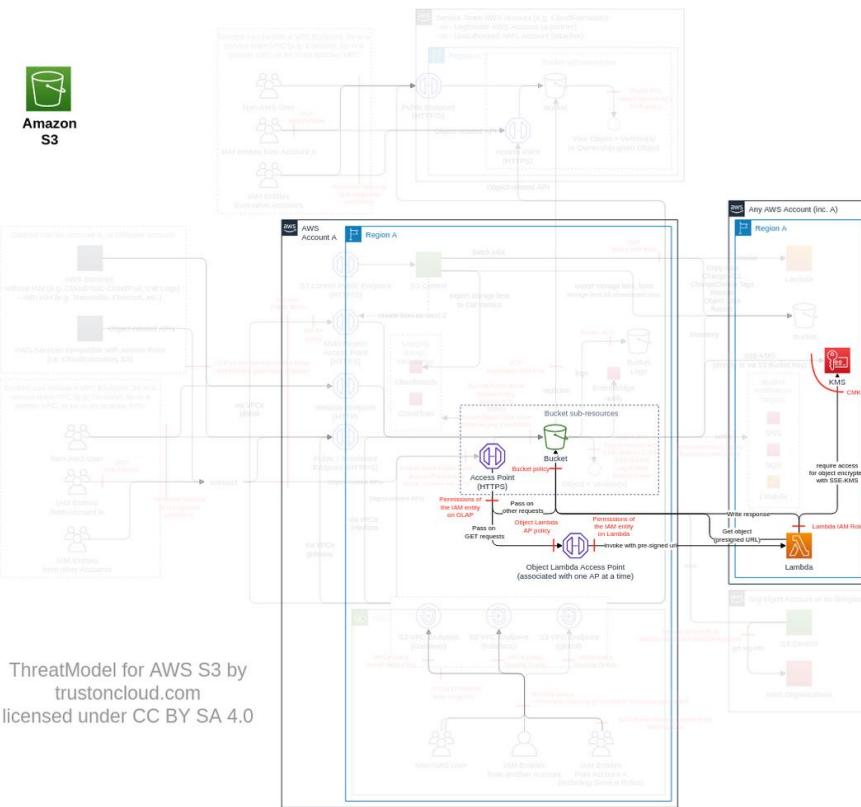
| Action   | IAM Permission                      |
|--|-------------------------------------|
| Creates an Object Lambda access point                | s3>CreateAccessPointForObjectLambda |
| Grants permission to retrieve objects from Amazon S3 | s3-object-lambda:GetObject          |
| Grants permission to add an object to a bucket       | s3-object-lambda:PutObject          |

## ***Threat List***

| Name                                    | CVSS                         |
|---|------------------------------|
| Hijack connection with an Object Lambda | <a href="#">Medium (5.7)</a> |

## Hijack connection with an Object Lambda

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T46   |
| <b>Name</b>             | Hijack connection with an Object Lambda  |
| <b>Description</b>      | Object Lambda are invoked between the access point and the object. An attacker can configure a Lambda to modify, snoop or exfiltrate data. |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">Medium (5.7)</a>   |
| <b>IAM Access</b>       | {<br>"OR": ["s3>CreateAccessPointForObjectLambda", "s3:PutAccessPointConfigurationForObjectLambda"]<br>}                                   |

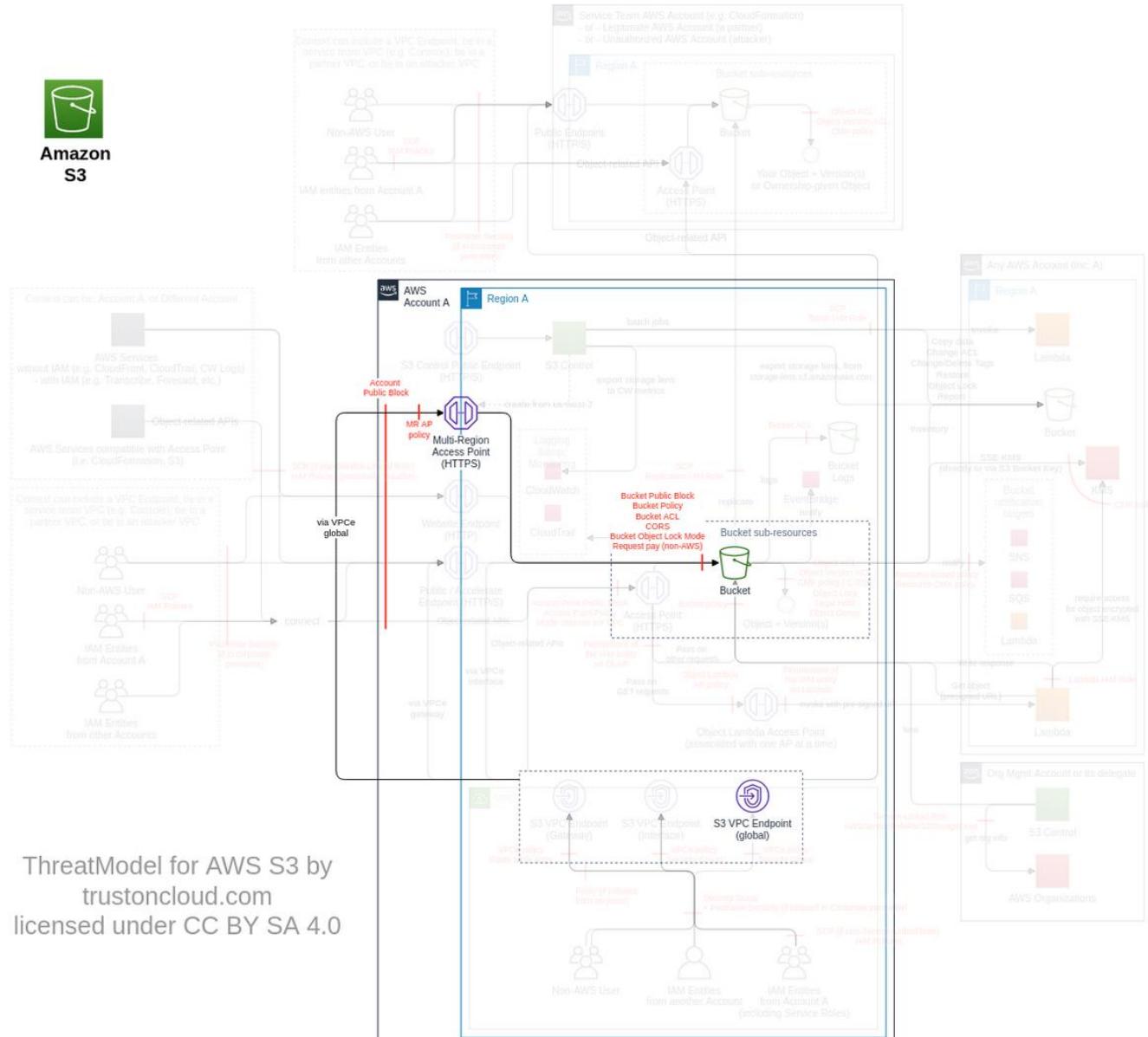


| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Enforce only authorized Object Lambda access point and associated access</b><br><br>Maintain a list of authorized Lambda function for each Object Lambda access point, its associated access point, its associated GET request(s), and payload<br>Ensure only authorized Lambda function for each Object Lambda access point, its associated access point, its associated GET request(s), and payload are created<br>Ensure Lambda functions configured on Object Lambda access point are secured using Lambda ThreatModel<br>Maintain a list of cross-account access on each Object Lambda access point<br>Ensure only authorized cross-account IAM entities are allowed in the Object Lambda access point policy<br>Ensure CloudWatch is enabled for all Object Lambda access points | Very High | 6                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account.   | Medium    | 2                        | -            | -         |

# Multi-Region Access Points (*subclass of Bucket, FC33*)

*S3 Multi-Region Access Points provide a single global endpoint to access a data set that spans multiple S3 buckets in different AWS Regions.*

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

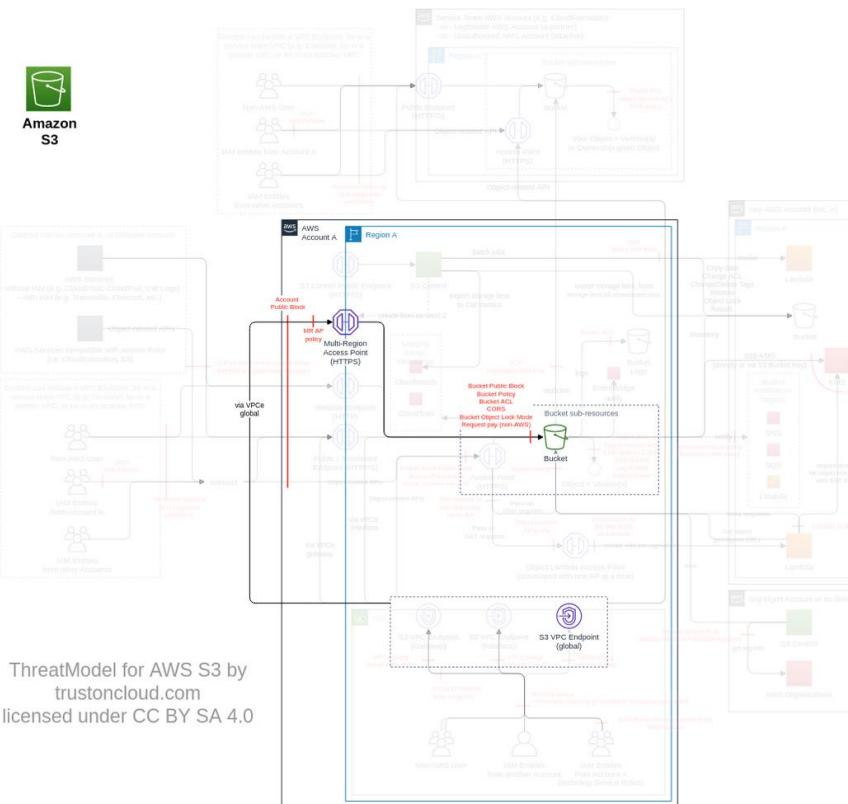
| Action  | IAM Permission                  |
|---|---------------------------------|
| Creates a Multi-Region Access Point and associates it with the specified buckets. | s3>CreateMultiRegionAccessPoint |

## ***Threat List***

| Name  | CVSS                         |
|---|------------------------------|
| Grant unauthorized access to buckets by changing the Multi-Region Access Point policy | <a href="#">Medium (6.8)</a> |
| Gain unauthorized access to buckets trusting all Multi-Region Access Points           | <a href="#">Medium (5.7)</a> |

## Grant unauthorized access to buckets by changing the Multi-Region Access Point policy

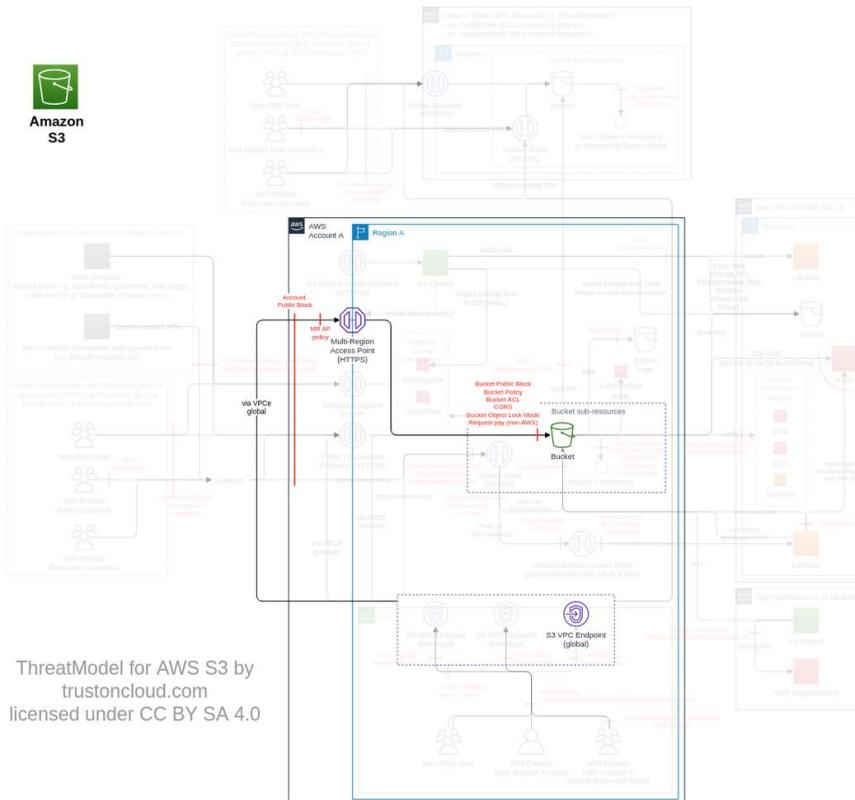
|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T55   |
| <b>Name</b>             | Grant unauthorized access to buckets by changing the Multi-Region Access Point policy  |
| <b>Description</b>      | Multi-Region Access Point policy can enable access to objects owned by the bucket. An attacker (or someone by negligence) can change the Multi-Region Access Point policy and make the content accessible. |
| <b>Goal</b>             | Launch another attack  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0008</a>   |
| <b>CVSS</b>             | <a href="#">Medium (6.8)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutMultiRegionAccessPointPolicy"<br>}   |



| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Block direct public access</b><br>Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.  | Very High | -                        | 1            | -         |
| <b>Restrict access point access to VPC when in use</b><br>Limit access via the S3 access point by using in VPC endpoint and/or bucket policy the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of allowlist bucket name in VPC endpoint/bucket policy.<br>In S3 bucket policy, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn"  | Medium    | -                        | 2            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. | Medium    | 2                        | -            | -         |

**Gain unauthorized access to buckets trusting all Multi-Region Access Points**

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T56  |
| <b>Name</b>             | Gain unauthorized access to buckets trusting all Multi-Region Access Points   |
| <b>Description</b>      | Buckets used by Multi-Region Access Points can be configured to delegate their access to any MRAP using the condition "s3:DataAccessPointAccount". An attacker can create a MRAP, add any misconfigured bucket and gain access to it. |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Medium (5.7)</a>  |
| <b>IAM Access</b>       | {<br>"AND": ["s3>CreateMultiRegionAccessPoint", "s3:PutMultiRegionAccessPointPolicy"]<br>}  |

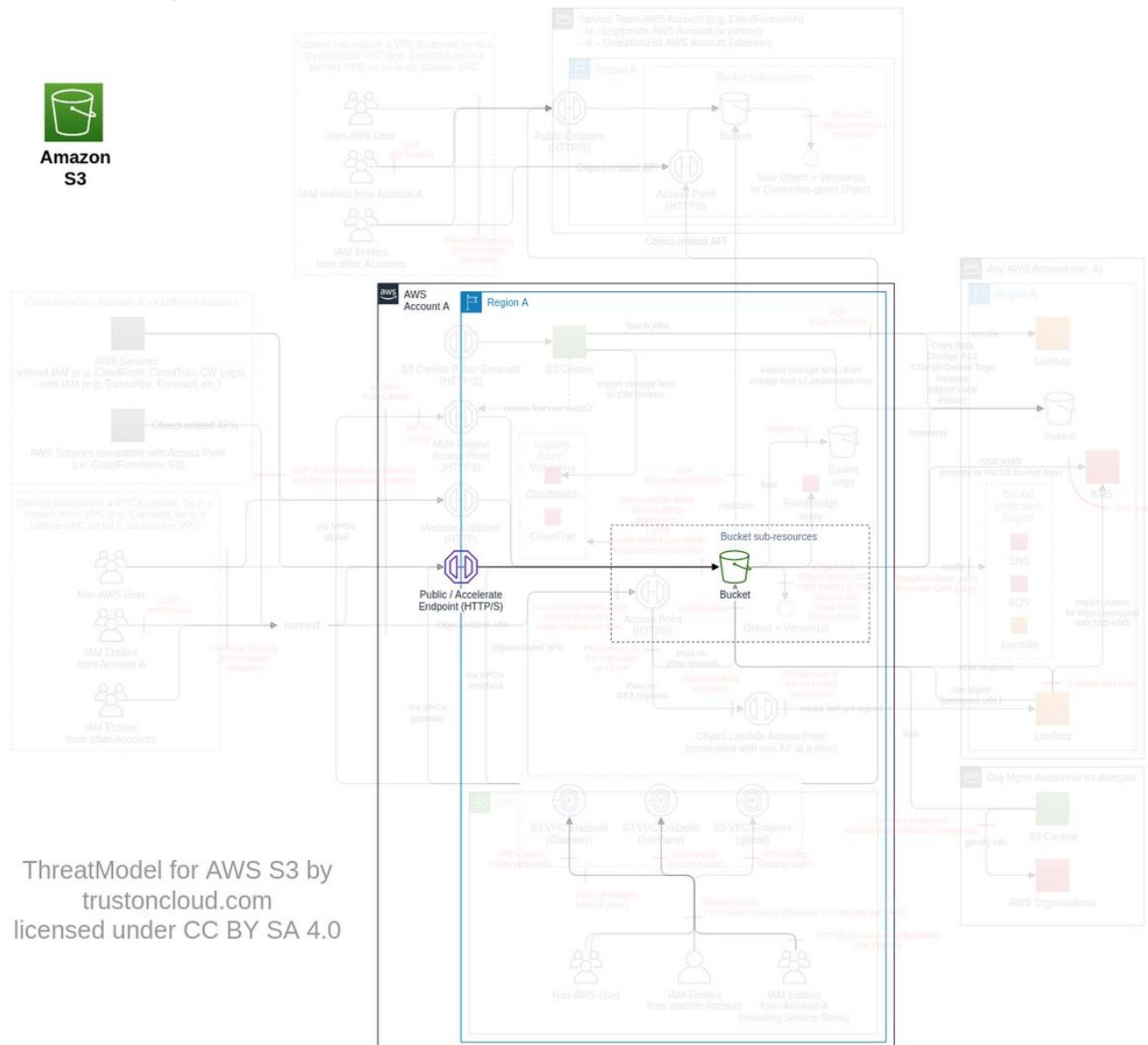


| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Restrict access point access to VPC when in use</b><br>In S3 bucket policy, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn"   | Very High | -                        | 1            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions. | Medium    | 1                        | -            | -         |

## CORS (*subclass of Bucket, FC22*)

**[NOT RECOMMENDED]** To configure your bucket to allow cross-origin requests, you create a CORS configuration, which is an XML document with rules that identify the origins that you will allow to access your bucket, the operations (HTTP methods) that will support for each origin, and other operation-specific information. This feature class is not recommended to be activated since it is all HTTP. Prefer the usage of CDN (e.g. CloudFront), API Gateway, and/or WAF fronting S3 buckets.

## **Data Flow Diagram (DFD)**



#### ***Actions and IAM Permissions to deny the feature***

| Action                                       | IAM Permission   |
|--|------------------|
| Sets the CORS configuration for your bucket. | s3:PutBucketCORS |

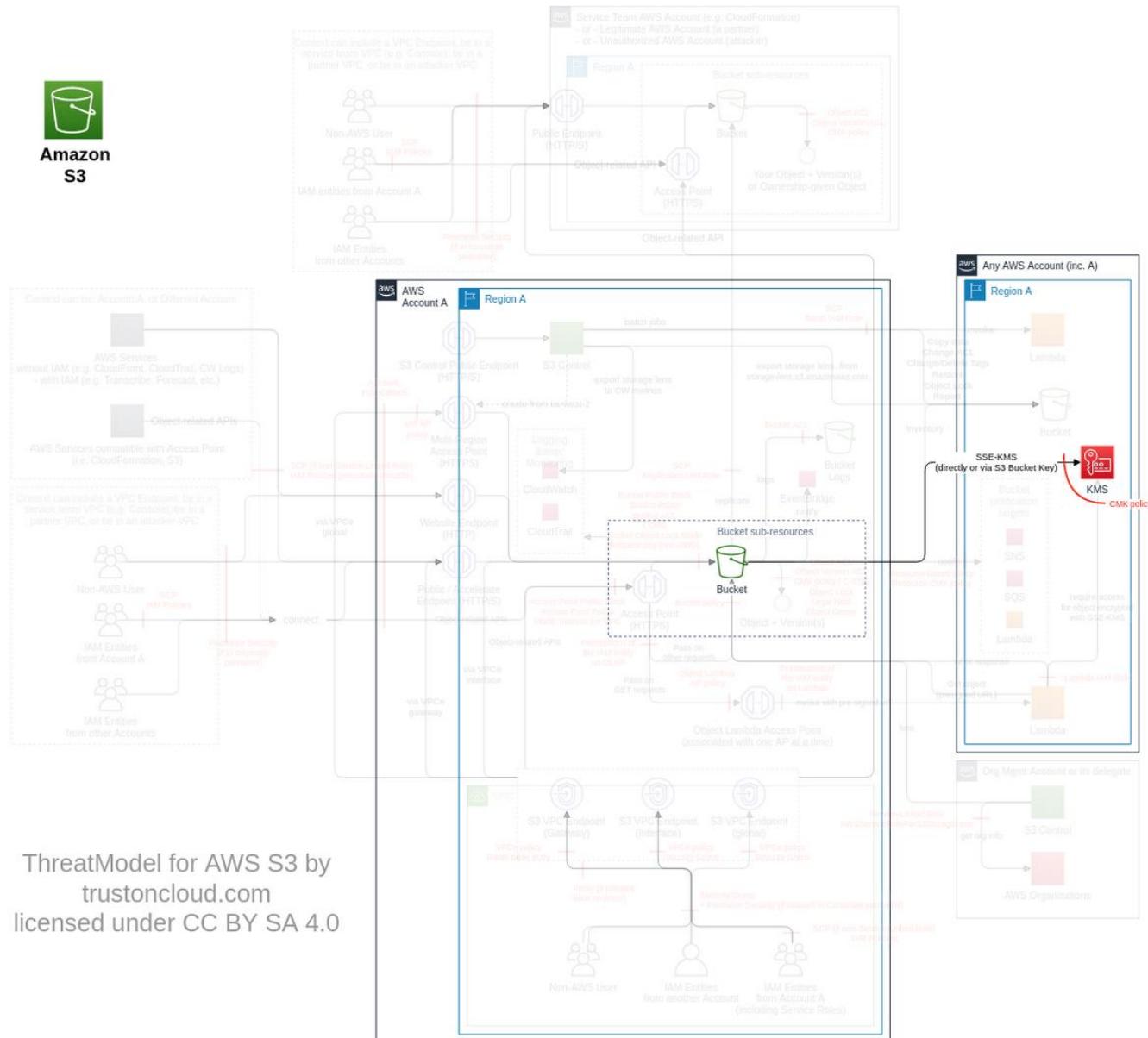
## ***Threat List***

| Name | CVSS |
|------|------|
| None | None |

# Bucket default encryption (*subclass of Bucket, FC23*)

*You can set default encryption on a bucket so that all new objects are encrypted when they are stored in the bucket.*

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

| Action  | IAM Permission                |
|---|-------------------------------|
| Sets the default encryption configuration for the bucket. | s3:PutEncryptionConfiguration |

## ***Threat List***

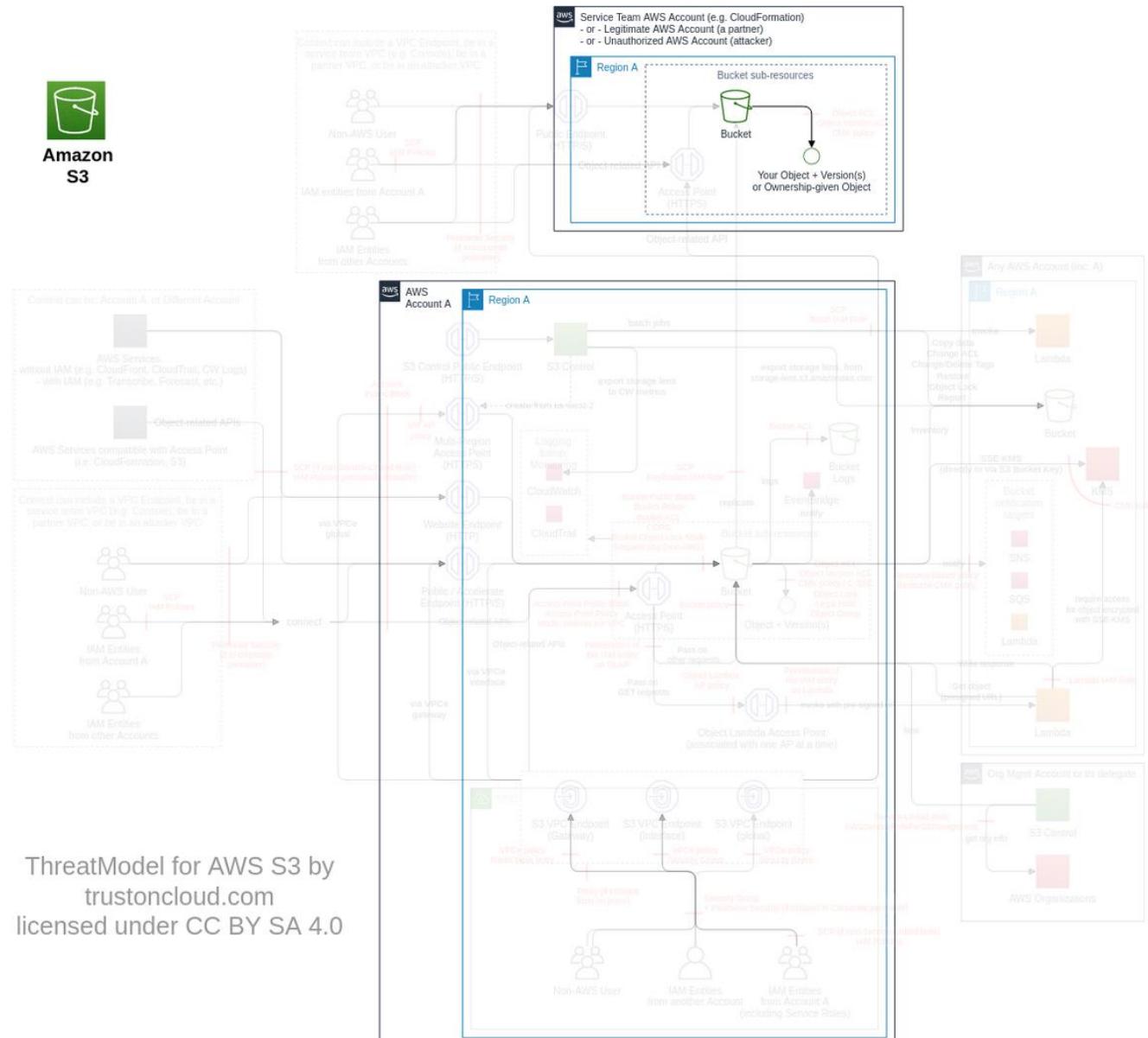
| Name | CVSS |
|------|------|
| None | None |

# S3 Object Ownership *(subclass of Bucket, used by Object)*

*upload/download, FC30)*

*Enables bucket owners to automatically assume ownership of objects that are uploaded to their buckets by other AWS accounts. When the object is Put with an ACL of bucket-owner-full-control, the object will be fully owned by the target bucket owner. If the ACL is added later, the ownership is kept by object owner ([ref](#)).*

## **Data Flow Diagram (DFD)**



#### ***Actions and IAM Permissions to deny the feature***

| Action  | IAM Permission                |
|---|-------------------------------|
| Creates or modifies OwnershipControls for an Amazon S3 bucket | s3:PutBucketOwnershipControls |

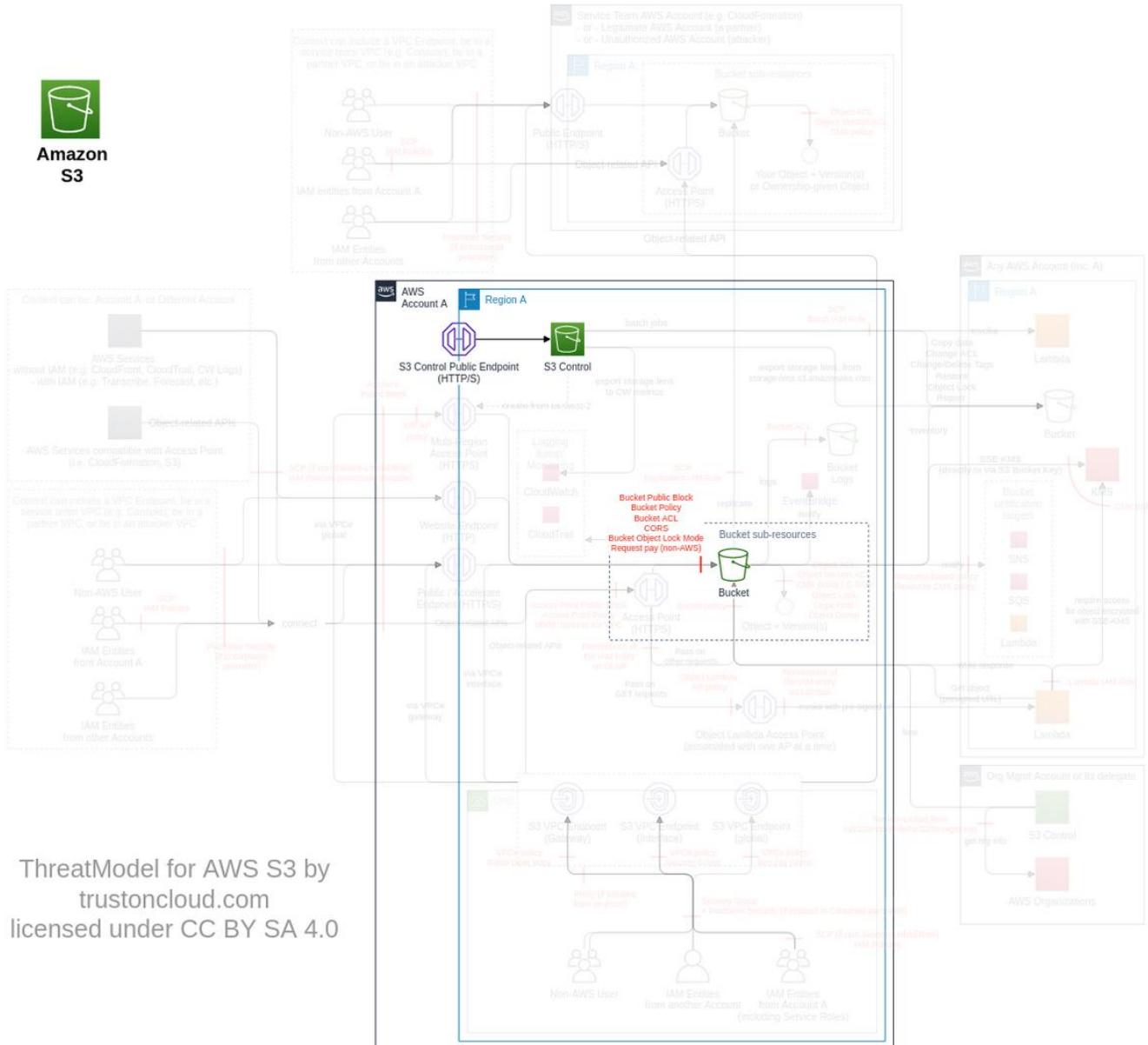
## ***Threat List***

| Name | CVSS |
|------|------|
| None | None |

# Public Access Block (bucket) (subclass of Bucket, FC24)

*S3 Block Public Access (bucket) provides controls across at the individual S3 bucket level to ensure objects never have public access.*

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

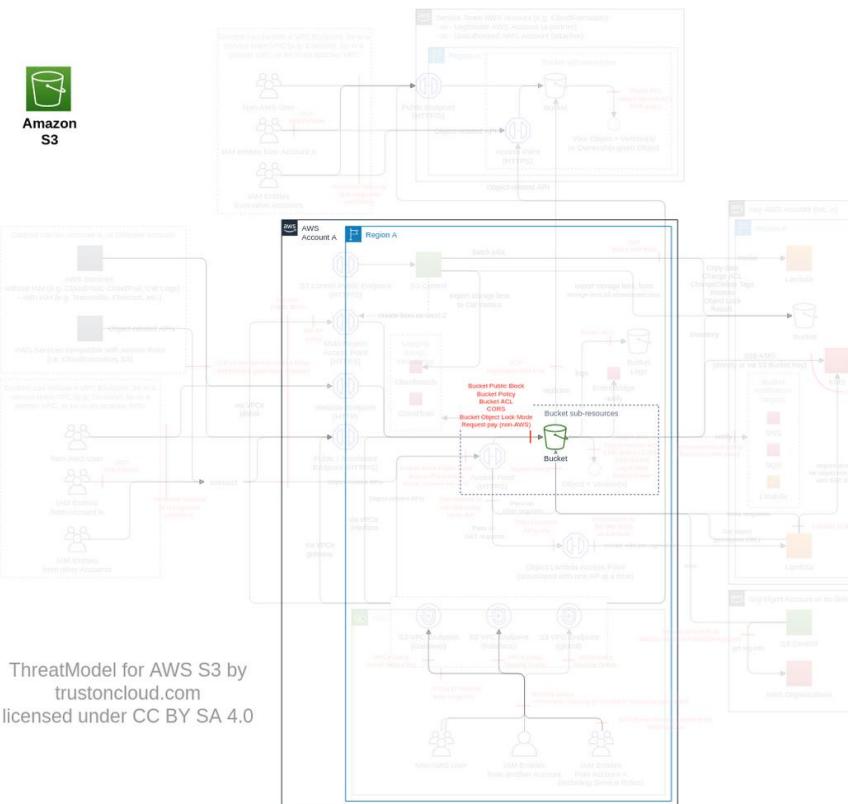
| Action   | IAM Permission                |
|--|-------------------------------|
| Creates or modifies the PublicAccessBlock configuration for an Amazon S3 bucket. | s3:PutBucketPublicAccessBlock |

## ***Threat List***

| Name  | CVSS                         |
|---|------------------------------|
| Reduce bucket security by modify the bucket public access block | <a href="#">Medium (4.9)</a> |

## Reduce bucket security by modify the bucket public access block

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T52  |
| <b>Name</b>             | Reduce bucket security by modify the bucket public access block   |
| <b>Description</b>      | Bucket public access block protect individual buckets from leakage (e.g. object ACL set to public). An attacker can remove this protection by modifying the bucket public access block. |
| <b>Goal</b>             | Launch another attack   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0008</a>  |
| <b>CVSS</b>             | <a href="#">Medium (4.9)</a>  |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutBucketPublicAccessBlock"<br>}   |

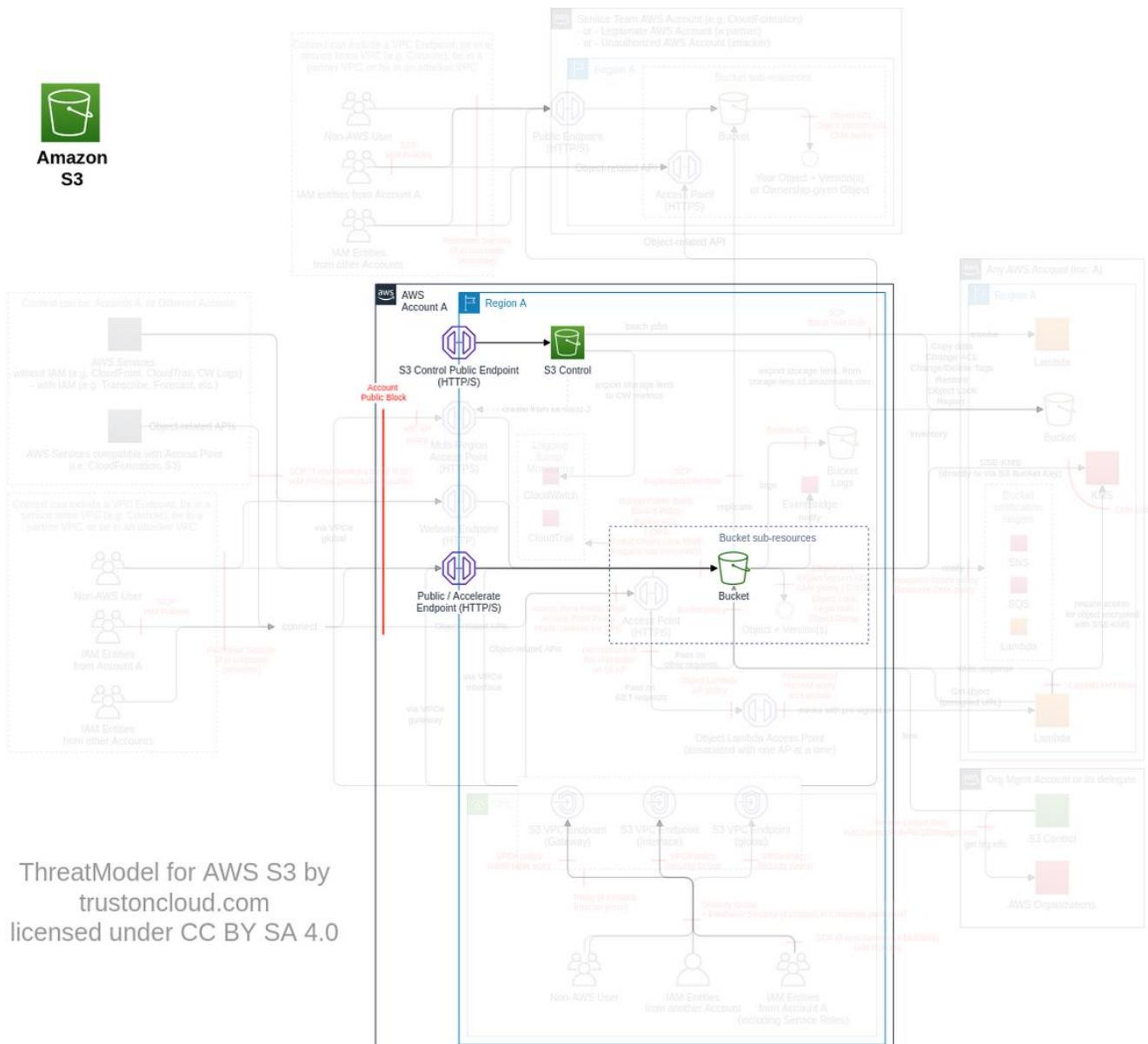


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Disabling ACLs for all buckets</b><br>Ensure bucket ACL and object ACL are disabled on each bucket<br>Prevent the creation of buckets with ACL enabled (e.g. by using a SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note it does not block someone to enable ACL afterwards via PutPutBucketOwnershipControls. | Very High | 1                        | 1            | -         |
| <b>Monitor S3 with Amazon GuardDuty and Macie</b><br>Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using GuardDuty ThreatModel. Ensure findings are investigated (e.g. using Amazon Detective).  | Medium    | 1                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.  | Medium    | 1                        | -            | -         |

# Public Access Block (account) (*subclass of Bucket, FC25*)

*S3 Block Public Access (account) provides controls across an entire AWS account to ensure objects never have public access.*

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

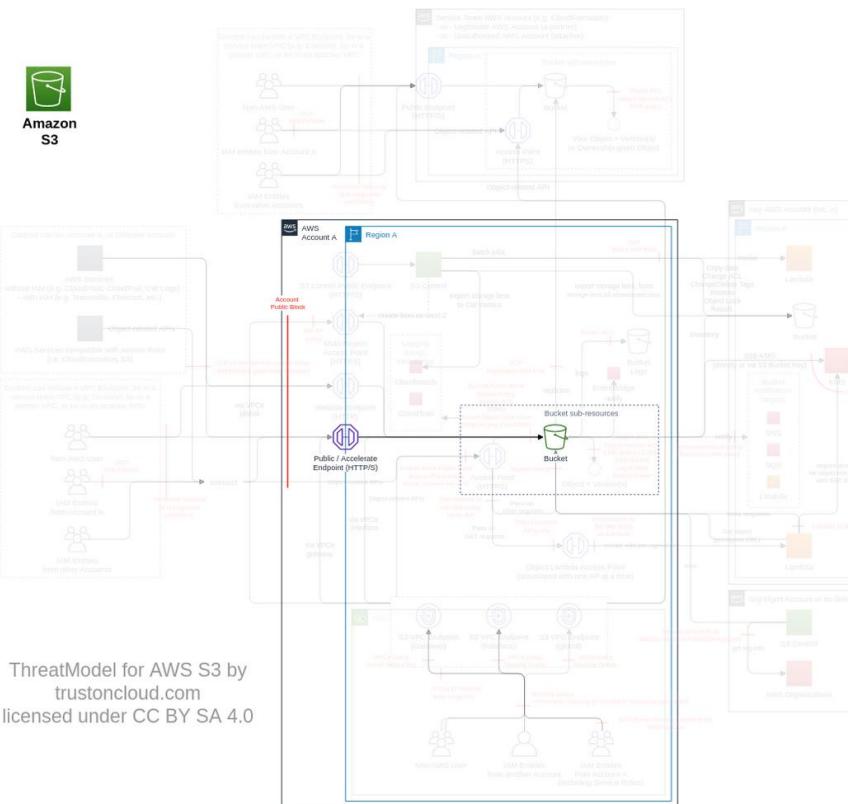
| Action  | IAM Permission                 |
|---|--------------------------------|
| Creates or modifies the PublicAccessBlock configuration for an AWS account. | s3:PutAccountPublicAccessBlock |

## ***Threat List***

| Name   | CVSS                         |
|--|------------------------------|
| Reduce bucket security by modify the account public access block | <a href="#">Medium (4.9)</a> |

## Reduce bucket security by modify the account public access block

|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T53   |
| <b>Name</b>             | Reduce bucket security by modify the account public access block   |
| <b>Description</b>      | Account public access block protect all buckets of an AWS account from leakage (e.g. object ACL set to public). An attacker can remove this protection by modifying the account public access block. |
| <b>Goal</b>             | Launch another attack  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0008</a>   |
| <b>CVSS</b>             | <a href="#">Medium (4.9)</a>   |
| <b>IAM Access</b>       | {<br>"UNIQUE": "s3:PutAccountPublicAccessBlock"<br>}   |

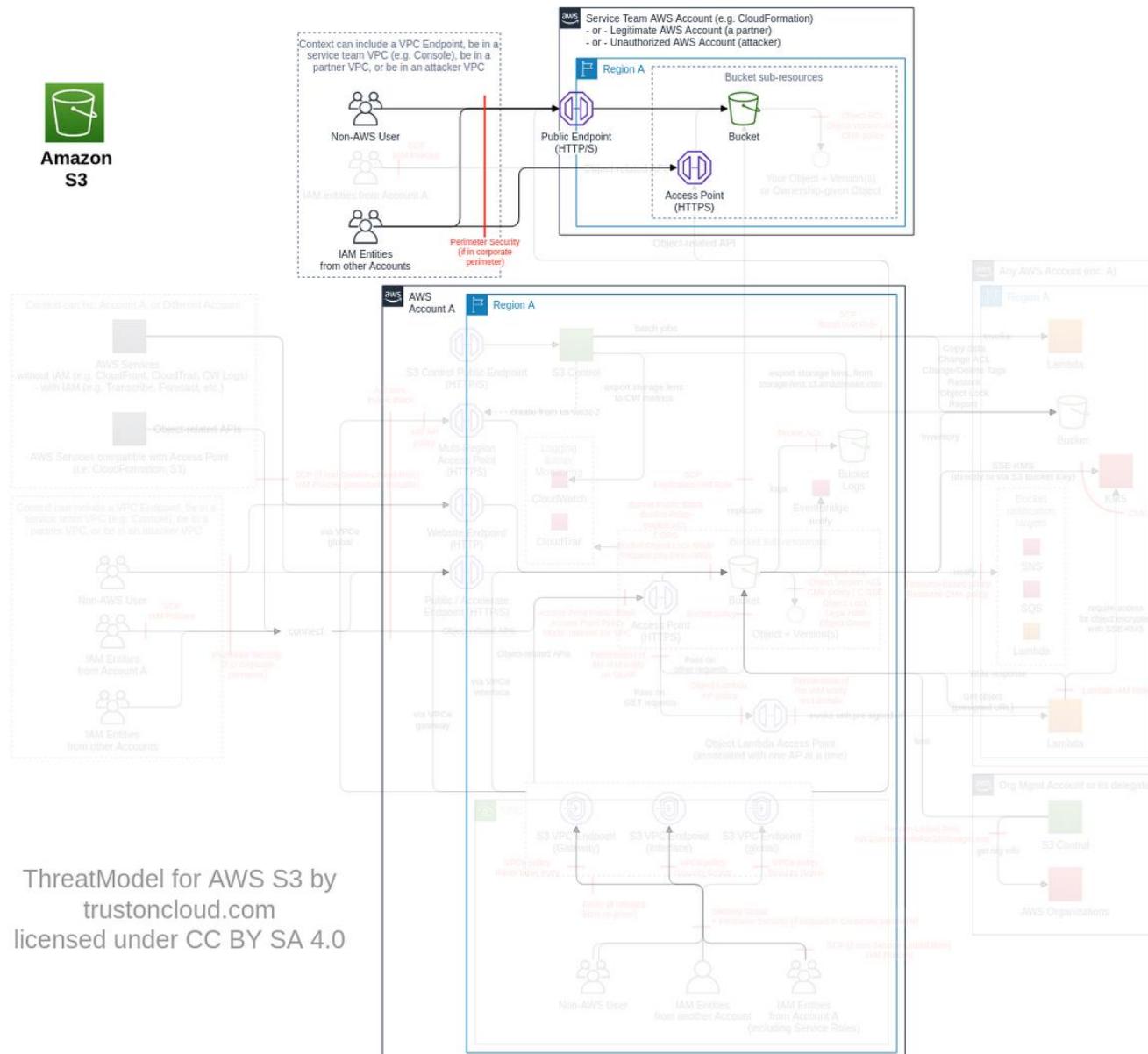


| Control Objectives   | Priority  | # of associated Controls |              |           |
|--|-----------|--------------------------|--------------|-----------|
|  |           | Directive                | Preventative | Detective |
| <b>Disabling ACLs for all buckets</b><br>Ensure bucket ACL and object ACL are disabled on each bucket<br>Prevent the creation of buckets with ACL enabled (e.g. by using a SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note it does not block someone to enable ACL afterwards via PutPutBucketOwnershipControls. | Very High | 1                        | 1            | -         |
| <b>Monitor S3 with Amazon GuardDuty and Macie</b><br>Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using GuardDuty ThreatModel. Ensure findings are investigated (e.g. using Amazon Detective).  | Medium    | 1                        | -            | -         |
| <b>Limit the access to the IAM actions required to execute the threats</b><br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.  | Medium    | 1                        | -            | -         |

## Other uses (*class, FC28*)

*Others can use their own S3 service to impact you in some ways.*

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

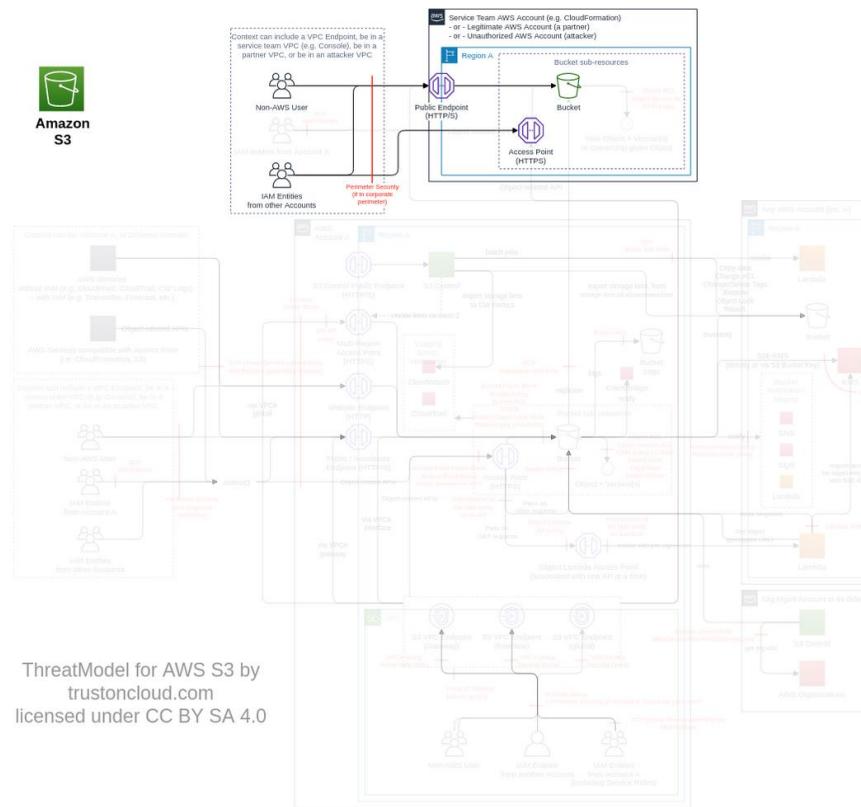
| Action | IAM Permission |
|--------|----------------|
| None   | None           |

## ***Threat List***

| Name  | CVSS                         |
|---|------------------------------|
| Exfiltrate data by using the public endpoint to upload data in an attacker bucket, using external credentials | <a href="#">Medium (6.2)</a> |
| Recon on information about a bucket   | <a href="#">Medium (4.3)</a> |
| Phishing using trademarks   | <a href="#">Low (3.1)</a>    |
| Recon of AWS root account emails using email ACL grantee feature  | <a href="#">Low (2.0)</a>    |
| Recon on valid AWS account or IAM principals  | <a href="#">Low (2.0)</a>    |

## Exfiltrate data by using the public endpoint to upload data in an attacker bucket, using external credentials

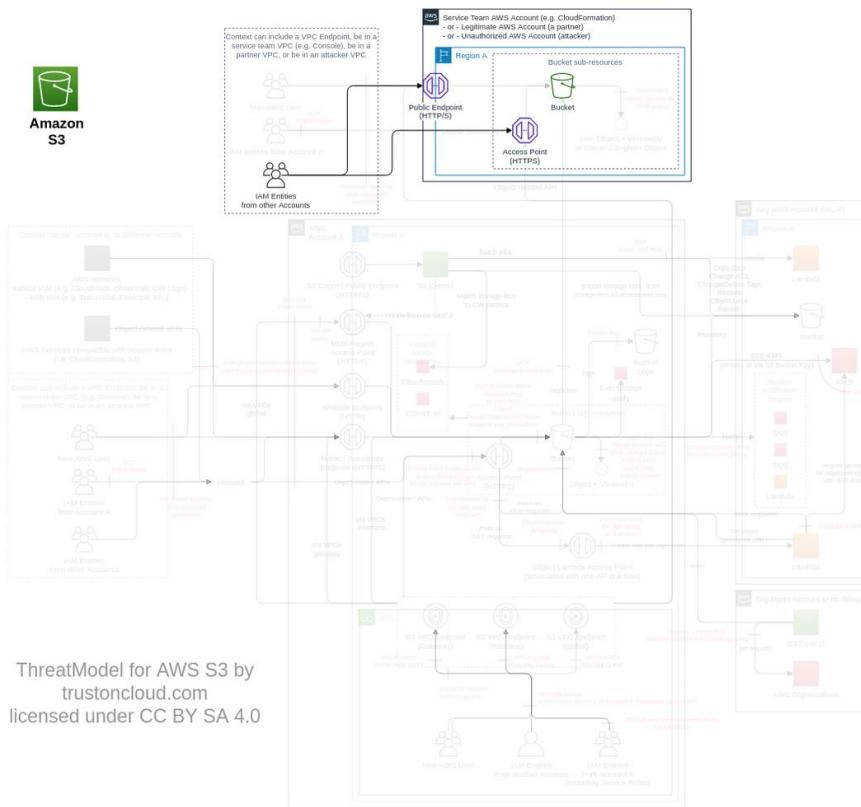
|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T10   |
| <b>Name</b>             | Exfiltrate data by using the public endpoint to upload data in an attacker bucket, using external credentials  |
| <b>Description</b>      | AWS authenticates per AWS account. An attacker can bring its own credentials to exfiltrate data to external S3 buckets through the S3 public endpoint. It can be a non-authenticated user as well. |
| <b>Goal</b>             | Data theft   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>   |
| <b>CVSS</b>             | <a href="#">Medium (6.2)</a>   |
| <b>IAM Access</b>       | 0  |



| Control Objectives  | Priority  | # of associated Controls |              |           |
|---|-----------|--------------------------|--------------|-----------|
|   |           | Directive                | Preventative | Detective |
| <b>Block S3 endpoints in your corporate perimeter security</b><br>Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g. firewalls, or cloud interception proxy like <a href="#">Kivera</a> ) including via Internet Gateway, to force usage of VPC endpoints. It will block data-plane transfer. Note: AWS console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com").   | Very High | 1                        | -            | -         |
| <b>Restrict access point access to VPC when in use</b><br>Maintain a list of authorized access between VPC, S3 access point and S3.<br>Limit access via the S3 access point by using in VPC endpoint and/or bucket policy the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of allowlist bucket name in VPC endpoint/bucket policy.<br>Block all traffic from Internet-configured S3 access point (e.g. on the bucket policy, using a deny statement with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}) | Very High | 1                        | 2            | -         |

## Recon on information about a bucket

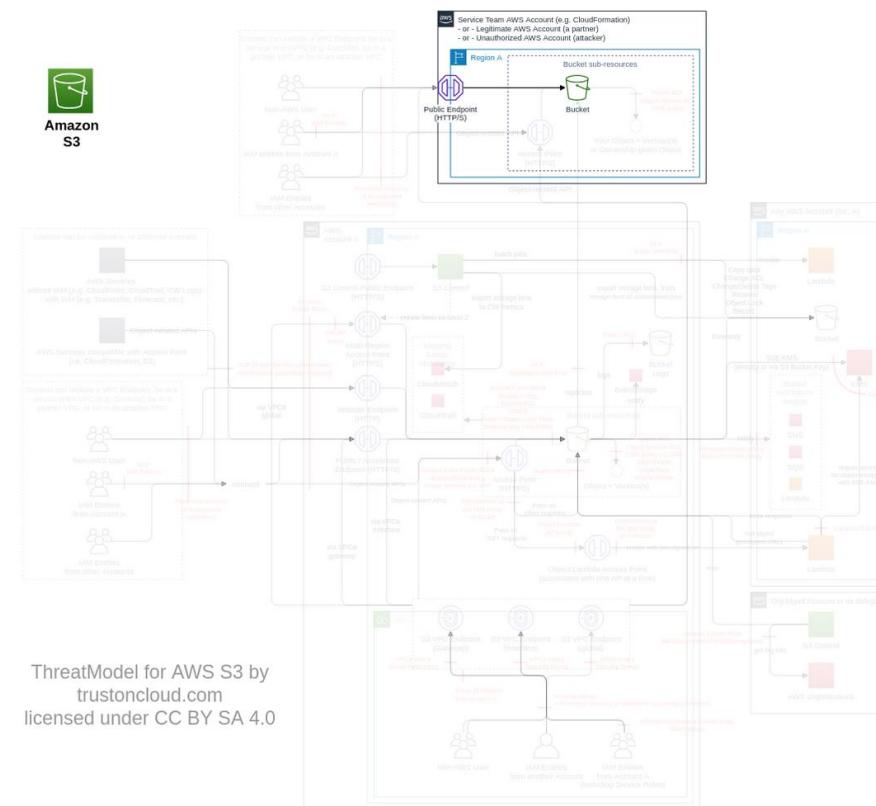
|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T32  |
| <b>Name</b>             | Recon on information about a bucket   |
| <b>Description</b>      | Error messages can give some information about specific buckets. An attacker who knows the bucket name can find its AWS account and AWS Region. To find the AWS Region, use "aws s3 presign bucket-name/whatever" the error message will give you the region if not in the right region. To find the account, look at the call in CloudTrail (with S3 data enabled) under the resource section. |
| <b>Goal</b>             | Launch another attack   |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Medium (4.3)</a>  |
| <b>IAM Access</b>       | 0   |



| Control Objectives | Priority | # of associated Controls |              |           |
|--------------------|----------|--------------------------|--------------|-----------|
|                    |          | Directive                | Preventative | Detective |
| None               |          |                          |              |           |

## Phishing using trademarks

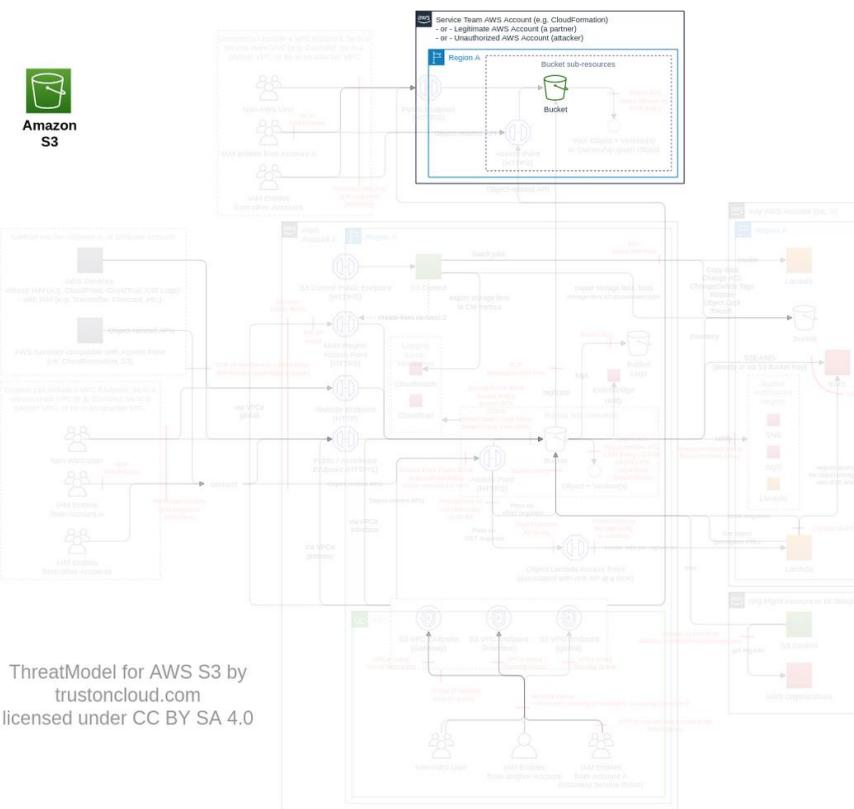
|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T23  |
| <b>Name</b>             | Phishing using trademarks   |
| <b>Description</b>      | S3 provides URLs to buckets using the bucket name (i.e. "mybucket.s3.amazonaws.com"). An attacker can create a bucket with the name of your trademark to phish users. |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Low (3.1)</a>   |
| <b>IAM Access</b>       | 0   |



| Control Objectives  | Priority | # of associated Controls |              |           |
|---|----------|--------------------------|--------------|-----------|
|   |          | Directive                | Preventative | Detective |
| <b>Protect and/or claim your domains and trademarks/copyrights</b><br>Protect and/or claim your domains and trademarks/copyrights (by creating your trademark buckets, and using the <a href="#">copyright infringement process</a> from AWS) | High     | 1                        | -            | -         |

## Recon of AWS root account emails using email ACL grantee feature

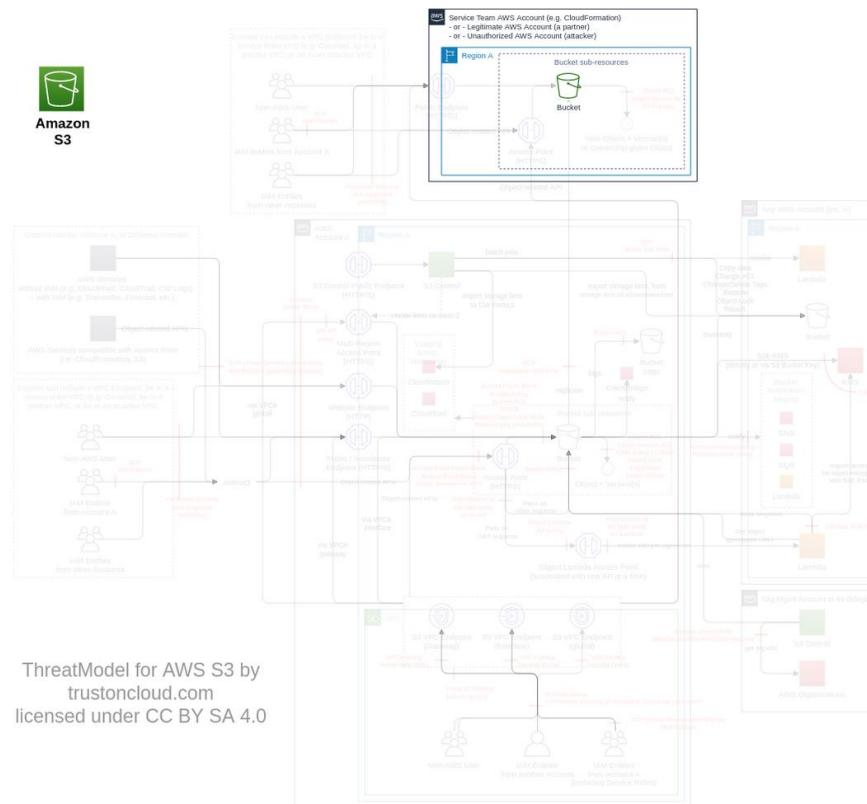
|                         |  |
|-------------------------|--|
| <b>Threat Id</b>        | S3.T19   |
| <b>Name</b>             | Recon of AWS root account emails using email ACL grantee feature   |
| <b>Description</b>      | S3 allows you to add root account emails in ACL ( <a href="#">ref</a> ), and as well resolve the given canonical ID into an AWS account ID (via a bucket policy, which automatically resolves a canonical ID into an ARN). An attacker can do trial-and-error to discover existing AWS root account emails and related AWS account ID (even if you do not use the region where the feature is available); and use this information to launch another attack (e.g. phishing). |
| <b>Goal</b>             | Launch another attack  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0007</a>   |
| <b>CVSS</b>             | <a href="#">Low (2.0)</a>  |
| <b>IAM Access</b>       | 0  |



| Control Objectives   | Priority | # of associated Controls |              |           |
|--|----------|--------------------------|--------------|-----------|
|  |          | Directive                | Preventative | Detective |
| <b>Use unguessable naming convention</b><br>Use unguessable naming convention for the email addresses of your AWS accounts (e.g. add a + sign and a random string to redirect the email in the same mailbox) | High     | 1                        | -            | -         |

## Recon on valid AWS account or IAM principals

|                         |   |
|-------------------------|---|
| <b>Threat Id</b>        | S3.T24  |
| <b>Name</b>             | Recon on valid AWS account or IAM principals  |
| <b>Description</b>      | AWS provides error messages in S3 bucket policy that can be used for basic recon. An attacker can discover whether an AWS account with a specific AWS account ID or AWS IAM principals exists, by modifying the S3 policy to grant some rights to the said AWS account/IAM principal. |
| <b>Goal</b>             | Data theft  |
| <b>Mitre ATT&amp;CK</b> | <a href="#">TA0010</a>  |
| <b>CVSS</b>             | <a href="#">Low (2.0)</a>   |
| <b>IAM Access</b>       | 0   |



| Control Objectives  | Priority | # of associated Controls |              |           |
|---|----------|--------------------------|--------------|-----------|
|   |          | Directive                | Preventative | Detective |
| <b>Use unguessable naming convention</b><br>Use unguessable naming convention for your IAM users and IAM roles (e.g. add a random string) | High     | 1                        | -            | -         |

# Control Implementation

## Enforce encryption-in-transit

| Type                                      | Control   | Testing  | Effort | Feature Class(es) | Threat(s) and Impact                | CVSS-weighted Priority |
|---|---|--|--------|-------------------|-------------------------------------|------------------------|
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C1, depends on S3.C119, assured by S3.C2]<br>Block all unencrypted requests and unauthorized TLS version(s) from IAM entities you control (e.g. by denying all unencrypted request with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != <i>authorized TLS version(s)</i> , using an SCP on your AWS Organization root node) | Make an unencrypted S3 API call, it should be denied.  | Low    | S3.FC1<br>S3.FC5  | S3.T12 (Very High)<br>S3.T34 (High) | High                   |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C2]<br>Verify the control blocking unencrypted requests and unauthorized TLS version(s) from IAM entities you control (e.g. an SCP on your AWS Organizations root node) is properly implemented   | Remove the control blocking unencrypted requests and unauthorized TLS version(s) (e.g. the SCP on your root node), it should be detected.          | High   | S3.FC1<br>S3.FC5  | -                                   | High                   |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C3, depends on S3.C119, assured by S3.C5]<br>Block all unencrypted requests and unauthorized TLS version(s) from VPC endpoints you control (e.g. by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != <i>authorized TLS version(s)</i> , on the VPC endpoint policy)                                | Make an unencrypted AWS API call from one of your VPC with VPC endpoint, it should be denied.  | Low    | S3.FC1<br>S3.FC5  | S3.T12 (Medium)<br>S3.T34 (Medium)  | Medium                 |
| Detective (coso)<br>Detect (NIST CSF)     | [S3.C4]<br>Monitor and investigate that all requests made with HTTP (e.g via CloudTrail S3 data events with the lack of additionalEventData.CipherSuite)  | Make an unencrypted AWS API call from one of your VPC with VPC endpoint, it should be detected.  | Low    | S3.FC1<br>S3.FC5  | S3.T12 (Low)<br>S3.T34 (Low)        | Low                    |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C5]<br>Verify a statement exists on all your VPC endpoint policy denying all requests with the condition "aws:SecureTransport" = False  | Create/remove the statement on a VPC endpoint policy denying 1) all unencrypted requests or 2) unauthorized TLS version(s), it should be detected. | High   | S3.FC1<br>S3.FC5  | -                                   | Medium                 |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C6, depends on S3.C119, assured by S3.C7]<br>Block all unencrypted requests to S3 bucket you control (e.g. by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != <i>authorized TLS version(s)</i> , on the S3 bucket policy)   | Make an unencrypted AWS API call to a bucket you control, it should be denied.   | Low    | S3.FC5            | S3.T34 (Very High)                  | High                   |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C7]<br>Verify all S3 bucket policies block unencrypted traffic (e.g. using the AWS Config rule: <a href="#">S3_BUCKET_SSL_REQUESTS_ONLY</a> ) and unauthorized version(s) of TLS.   | Remove the statement on a S3 bucket policy 1) denying all unencrypted requests and 2) denying unauthorized TLS versions, it should be detected.    | Medium | S3.FC5            | -                                   | High                   |

|   |   |  |     |        |                   |      |
|---|---|--|-----|--------|-------------------|------|
| Directive (coso)<br>Identify (NIST CSF) | [S3.C119]<br>Maintain a list of authorized version(s) of TLS/SSL per bucket (or per account/OU/Org) | Request the list of authorized version(s) of TLS/SSL per bucket (or per account/OU/Org), its review mechanism and associated records | Low | S3.FC1 | S3.T12 (Very Low) | High |
|---|---|--|-----|--------|-------------------|------|

## Block S3 endpoints in your corporate perimeter security

| Type                                   | Control  | Testing   | Effort | Feature Class(es)                     | Threat(s) and Impact   | CVSS-weighted Priority |
|--|--|---|--------|---------------------------------------|--|------------------------|
| Directive (coso)<br>Protect (NIST CSF) | [S3.C8]<br>Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g. firewalls, or cloud interception proxy like <a href="#">Kivera</a> ) including via Internet Gateway, to force usage of VPC endpoints. It will block data-plane transfer. Note: AWS console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com"). | Request the evidence of the implementation of blocking S3 endpoints in your corporate perimeter security (e.g. firewalls) and tests of its effectiveness. | Low    | S3.FC1<br>S3.FC28<br>S3.FC5<br>S3.FC7 | S3.T7 (High)<br>S3.T10 (High)<br>S3.T12 (Low)<br>S3.T18 (Medium)<br>S3.T34 (Very High) | High                   |

## Enable CloudTrail S3 data events

| Type                                  | Control  | Testing   | Effort   | Feature Class(es)          | Threat(s) and Impact  | CVSS-weighted Priority |
|---------------------------------------|--|---|----------|----------------------------|---|------------------------|
| Directive (coso)<br>Detect (NIST CSF) | [S3.C9]<br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel | Request the CloudTrail ThreatModel and the evidence of its application for enabling and protecting S3 data events | Very Low | S3.FC1<br>S3.FC5<br>S3.FC8 | S3.T1 (Low)<br>S3.T4 (Low)<br>S3.T5 (Low)<br>S3.T6 (Low)<br>S3.T7 (Low)<br>S3.T8 (Low)<br>S3.T9 (Low)<br>S3.T11 (Low)<br>S3.T12 (Low)<br>S3.T16 (Low)<br>S3.T21 (Low)<br>S3.T31 (Low)<br>S3.T34 (Low)<br>S3.T35 (Low)<br>S3.T36 (Low)<br>S3.T39 (Low) | Medium                 |

## Monitor S3 with Amazon GuardDuty and Macie

| Type | Control | Testing | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|------|---------|---------|--------|-------------------|----------------------|------------------------|
|------|---------|---------|--------|-------------------|----------------------|------------------------|

|                                       |  |  |          |  |  |        |
|---------------------------------------|--|--|----------|--|--|--------|
| Directive (coso)<br>Detect (NIST CSF) | [S3.C10]<br>Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using GuardDuty ThreatModel. Ensure findings are investigated (e.g. using Amazon Detective). | Request the GuardDuty ThreatModel and the evidence of its application for enabling, monitoring, investigation and protecting S3 protection | Low      | S3.FC1<br>S3.FC24<br>S3.FC25<br>S3.FC5<br>S3.FC8 | S3.T3 (Low)<br>S3.T4 (Low)<br>S3.T16 (Medium)<br>S3.T52 (Medium)<br>S3.T53 (Medium)                          | Medium |
| Directive (coso)<br>Detect (NIST CSF) | [S3.C118]<br>Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect it using Macie ThreatModel  | Request the Macie ThreatModel and the evidence of its application for enabling and protecting S3 policy findings                           | Very Low | S3.FC10<br>S3.FC15<br>S3.FC5<br>S3.FC8           | S3.T2 (Medium)<br>S3.T4 (Medium)<br>S3.T22 (Medium)<br>S3.T36 (Medium)<br>S3.T37 (Medium)<br>S3.T38 (Medium) | High   |

## Identify and ensure the protection all external buckets hosting your objects

| Type                                      | Control   | Testing   | Effort | Feature Class(es)           | Threat(s) and Impact  | CVSS-weighted Priority |
|---|---|---|--------|-----------------------------|---|------------------------|
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C11]<br>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel). | Request the list of all authorized external buckets authorized to host your objects, their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), their data classification and the mechanism used to ensure the security of those buckets | Medium | S3.FC1<br>S3.FC16<br>S3.FC5 | S3.T3 (High)<br>S3.T5 (Very Low)<br>S3.T6 (Low)<br>S3.T7 (Very Low)<br>S3.T8 (Very Low)<br>S3.T9 (Very Low)<br>S3.T11 (Low)<br>S3.T14 (Very Low)<br>S3.T15 (Very Low)<br>S3.T21 (Very Low)<br>S3.T31 (High)<br>S3.T43 (Very High) | High                   |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C12, depends on S3.C11]<br>Allow only authorized ACL on objects for bucket you don't control (e.g. using IAM and VPC endpoint policy with the <a href="#">ACL conditions</a> )  | Put an object with an unauthorized ACL, it should be denied.  | Medium | S3.FC1                      | S3.T5 (Medium)<br>S3.T6 (High)  | Medium                 |
| Detective (coso)<br>Detect (NIST CSF)     | [S3.C13, depends on S3.C11]<br>Monitor that only authorized external buckets are used (e.g. via CloudTrail S3 data events in resources[].accountId and resources[].ARN). Both account ID and bucket name must be verified.  | Make a call to an unauthorized bucket, it should be detected  | Low    | S3.FC1<br>S3.FC5            | S3.T1 (Low)<br>S3.T7 (Low)<br>S3.T11 (Low)<br>S3.T21 (Low)<br>S3.T31 (Medium)   | Medium                 |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C14, depends on S3.C11]<br>Scan all data before uploading to an external bucket to ensure the classification of the data is aligned with the bucket classification (e.g. using Macie).  | Request 1) the mechanism ensuring all data are scanned for proper data classification before upload to an external bucket are configured, 2) its records of execution for all object upload flows, and 3) plan to move any older object upload flows                                      | High   | S3.FC1<br>S3.FC16<br>S3.FC5 | S3.T5 (High)<br>S3.T14 (High)<br>S3.T15 (Medium)  | Medium                 |

|   |  |  |      |        |  |        |
|---|--|--|------|--------|--|--------|
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C15]<br>Request access via S3 access point on bucket you don't own, if compatible with your interaction with the bucket (e.g. not through not-compatible AWS service)  | Request the documented reason access point was not implemented in the use case   | Low  | S3.FC1 | S3.T8 (Medium)<br>S3.T9 (Medium)<br>S3.T31 (Very High) | High   |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C114, depends on S3.C11]<br>For all external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover, block the PutObject with any ACL (e.g. using IAM or SCP and a deny on the condition "StringLike": {"s3:x-amz-acl": "*"}). It should be called via PutObjectAcl. | Make a request to an external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover requirement, it should be denied.   | High | S3.FC1 | S3.T43 (Very High)                                     | Medium |
| Detective (coso)<br>Detect (NIST CSF)     | [S3.C115, depends on S3.C11]<br>For all external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover, monitor that the PutObject do not include the ACL operation   | Make a request to an external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover requirement, it should be detected. | Low  | S3.FC1 | S3.T43 (Low)   | Low    |

## Model the threats on all AWS services accessing S3

| Type                                   | Control   | Testing   | Effort | Feature Class(es) | Threat(s) and Impact                     | CVSS-weighted Priority |
|--|---|---|--------|-------------------|--|------------------------|
| Directive (coso)<br>Protect (NIST CSF) | [S3.C16]<br>Analyse and protect all AWS services accessing S3 (e.g. via ThreatModel). Enforce usage in VPC only, whenever possible. | Request the threat and mitigating controls for all AWS services using S3. | High   | S3.FC1<br>S3.FC5  | S3.T21 (Very High)<br>S3.T30 (Very High) | Medium                 |

## Limit and monitor access via S3 VPC endpoints

| Type                                      | Control   | Testing   | Effort | Feature Class(es) | Threat(s) and Impact                    | CVSS-weighted Priority |
|---|---|---|--------|-------------------|---|------------------------|
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C17]<br>For each VPC, maintain a list of AWS Organizations, OU and/or AWS account(s), where IAM entities are authorized to access S3  | For each VPC, request the list of AWS Organizations, OU and/or AWS account(s), where IAM entities are authorized to access S3, its review process, and its review records | Medium | S3.FC1<br>S3.FC5  | S3.T9 (Very Low)<br>S3.T11 (Very Low)   | High                   |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C18, depends on S3.C17]<br>For each VPC with an IAM entity allowed to use S3, secure them with the VPC ThreatModel (e.g. <a href="#">modification of VPC endpoints</a> , <a href="#">VPC endpoint policy</a> , <a href="#">routing table</a> , <a href="#">Security Groups</a> )  | Request how VPC ThreatModel for S3 is being applied.  | High   | S3.FC1<br>S3.FC5  | S3.T9 (Medium)<br>S3.T11 (Medium)       | Low                    |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C19, depends on S3.C17, assured by S3.C20]<br>Block any IAM entity not belonging to an authorized AWS Organizations, OU and/or AWS account(s) to call S3 from your VPCs by adding a deny statement on S3 VPC endpoint policy of each VPC, with the condition using "aws:PrincipalOrgPaths" ( <a href="#">ref</a> ) including the full Org ID, as those are globally unique. | For each VPC, do an API call with an IAM entity which is not part of its authorized AWS Organizations path(s), it should be denied.                                       | Low    | S3.FC1<br>S3.FC5  | S3.T9 (Very High)<br>S3.T11 (Very High) | High                   |

|  |   |  |        |                  |   |          |
|--|---|--|--------|------------------|---|----------|
| Assurance (coso) Detect (NIST CSF)     | [S3.C20] Verify all S3 VPC endpoint are blocking any IAM entity not belonging to an authorized AWS Organizations, OU and/or AWS account(s)  | Remove the policy statement blocking any IAM entity not belonging to an authorized AWS Organizations, OU and/or AWS account(s) from the VPC endpoint, it should be detected. | High   | S3.FC1<br>S3.FC5 | -   | High     |
| Directive (coso) Detect (NIST CSF)     | [S3.C21] Enable <a href="#">VPC DNS query logging</a> in all VPC  | Request the mechanism to enable VPC DNS query logging in all VPC   | Medium | S3.FC1<br>S3.FC5 | S3.T8 (Very Low)<br>S3.T9 (Very Low)<br>S3.T11 (Very Low) | Very Low |
| Directive (coso) Identify (NIST CSF)   | [S3.C22] Maintain a list of authorized S3 and S3 access point (and their respective AWS accounts) to be access for each VPC   | Request the list of authorized S3 and S3 access point to be access for each VPC, its review process, and its review records  | Medium | S3.FC1<br>S3.FC5 | S3.T8 (Very Low)<br>S3.T9 (Very Low)<br>S3.T11 (Very Low) | Medium   |
| Preventative (coso) Protect (NIST CSF) | [S3.C23, depends on S3.C22, assured by S3.C24] Limit the access to only authorized S3 bucket(s) or their AWS account(s) from each VPC (e.g. using the condition key "s3:ResourceAccount" on the VPC endpoint policy, alternatively use specific resource-level statement for each bucket, or if the VPC endpoint policy size is beyond the limit and more granular control on VPC is required, use access points) | Make a request to an unauthorized bucket from one of your VPC, it should be denied   | Medium | S3.FC1<br>S3.FC5 | S3.T8 (High)<br>S3.T9 (High)<br>S3.T11 (High)             | Medium   |
| Assurance (coso) Detect (NIST CSF)     | [S3.C24] Verify all VPC are limited to limit access to only authorized S3 bucket(s)   | Remove the control limiting access to only authorized S3 bucket(s), it should be detected.   | High   | S3.FC1<br>S3.FC5 | -   | Medium   |
| Detective (coso) Detect (NIST CSF)     | [S3.C25, depends on S3.C21,S3.C22] Monitor VPC DNS query logs that only authorized S3 bucket and S3 access points are being queried in each VPC (e.g. using VPC DNS query logging), and protect it using Route53 ThreatModel  | Make a DNS query to an unauthorized 1) S3 bucket and 2) S3 access points, it should be detected.   | Low    | S3.FC1<br>S3.FC5 | S3.T8 (Low)<br>S3.T9 (Low)<br>S3.T11 (Low)                | Low      |
| Directive (coso) Protect (NIST CSF)    | [S3.C124] Ensure all S3 VPC endpoints (Interface and Gateway) are covered by the VPC endpoints controls   | Request the mechanism ensuring all S3 VPC endpoints (Interface and Gateway) are covered by the VPC endpoints controls, and its records                                       | Low    | S3.FC1           | S3.T45 (Very High)  | Low      |

## Limit the access to the IAM actions required to execute the threats

| Type                                | Control  | Testing  | Effort | Feature Class(es)   | Threat(s) and Impact  | CVSS-weighted Priority |
|-------------------------------------|--|--|--------|---|---|------------------------|
| Directive (coso) Protect (NIST CSF) | [S3.C26] Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions. | Request the list of authorized IAM principals that have the permissions required to execute the threat actions, its review process, and its review records | High   | S3.FC1<br>S3.FC10<br>S3.FC12<br>S3.FC13<br>S3.FC15<br>S3.FC19<br>S3.FC2<br>S3.FC20<br>S3.FC24 | S3.T1 (High)<br>S3.T2 (High)<br>S3.T5 (Low)<br>S3.T6 (Medium)<br>S3.T7 (High)<br>S3.T8 (High)<br>S3.T11 (High)<br>S3.T14 (Very High)<br>S3.T16 (High) | High                   |

|  |   |  |     |   |  |        |
|--|---|--|-----|---|--|--------|
|  |   |  |     | S3.FC25<br>S3.FC26<br>S3.FC27<br>S3.FC32<br>S3.FC33<br>S3.FC5<br>S3.FC6<br>S3.FC7<br>S3.FC8   | S3.T17 (Very High)<br>S3.T18 (High)<br>S3.T21 (Medium)<br>S3.T25 (High)<br>S3.T26 (High)<br>S3.T28 (High)<br>S3.T30 (High)<br>S3.T33 (Very High)<br>S3.T35 (Very High)<br>S3.T36 (Medium)<br>S3.T37 (Very High)<br>S3.T38 (Very High)<br>S3.T39 (High)<br>S3.T41 (High)<br>S3.T42 (High)<br>S3.T44 (High)<br>S3.T46 (High)<br>S3.T47 (High)<br>S3.T48 (High)<br>S3.T49 (High)<br>S3.T50 (High)<br>S3.T51 (High)<br>S3.T52 (High)<br>S3.T53 (High)<br>S3.T54 (High)<br>S3.T55 (High)<br>S3.T56 (High) |        |
| Directive (COSO)<br>Protect (NIST CSF) | [S3.C27, assured by S3.C28]<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account. | Request all S3 bucket/access point/Object Lambda access point policy statements with "allow", no principal from the same account should be authorized. | Low | S3.FC1<br>S3.FC10<br>S3.FC12<br>S3.FC13<br>S3.FC15<br>S3.FC2<br>S3.FC20<br>S3.FC26<br>S3.FC27<br>S3.FC32<br>S3.FC33<br>S3.FC5<br>S3.FC7 | S3.T1 (Low)<br>S3.T2 (Low)<br>S3.T6 (Low)<br>S3.T7 (Low)<br>S3.T8 (Low)<br>S3.T11 (Low)<br>S3.T14 (Medium)<br>S3.T16 (Low)<br>S3.T17 (Medium)<br>S3.T18 (Low)<br>S3.T21 (Low)<br>S3.T25 (Low)<br>S3.T26 (Medium)<br>S3.T30 (Low)<br>S3.T33 (Medium)<br>S3.T35 (Medium)<br>S3.T36 (Low)<br>S3.T37 (Medium)  | Medium |

|   |   |   |        |   |  |           |
|---|---|---|--------|---|--|-----------|
|   |   |   |        |   | S3.T38 (Medium)<br>S3.T39 (Low)<br>S3.T41 (Low)<br>S3.T42 (Low)<br>S3.T44 (Low)<br>S3.T46 (Medium)<br>S3.T54 (Medium)<br>S3.T55 (Medium) |           |
| Assurance (coso)<br>Detect (NIST CSF)   | [S3.C28]<br>Verify all S3 bucket/access point/Object Lambda access point policies do not allow an IAM principal of the same AWS account (e.g. using the Config rule <a href="#">S3_BUCKET_POLICY_GRANTEE_CHECK</a> for bucket policy) | Add an allow statement for an IAM principal of the same account in 1) a bucket policy, 2) in an access point policy, and 3) in an Object Lambda access point, it should be detected.                        | Medium | S3.FC1<br>S3.FC10<br>S3.FC12<br>S3.FC13<br>S3.FC15<br>S3.FC2<br>S3.FC20<br>S3.FC26<br>S3.FC27<br>S3.FC32<br>S3.FC33<br>S3.FC5<br>S3.FC7 | -  | Medium    |
| Directive (coso)<br>Identify (NIST CSF) | [S3.C149]<br>For each bucket, maintain a list of authorized IAM principals allowed to access via bucket policy  | Request the list of authorized a list of authorized IAM principals allowed to access via bucket policy, its review process, and its review records  | Medium | S3.FC10   | S3.T37 (Very Low)  | Very High |
| Directive (coso)<br>Protect (NIST CSF)  | [S3.C150, depends on S3.C149, assured by S3.C151]<br>Ensure only authorized a list of authorized IAM principals allowed to access via bucket policy are configured (e.g. using IAM Access Analyzer for the reconciliation)            | Request 1) the mechanism ensuring only authorized IAM principals allowed to access via bucket policy are configured, 2) its records of execution for all new buckets, and 3) plan to move any older buckets | Medium | S3.FC10   | S3.T37 (Very High)   | Very High |
| Assurance (coso)<br>Detect (NIST CSF)   | [S3.C151]<br>Verify only authorized IAM principals allowed to access via bucket policy are used (e.g. using the AWS Config rule <a href="#">S3_BUCKET_POLICY_GRANTEE_CHECK</a> )  | Allow an unauthorized IAM principal on a bucket policy, it should be detected.  | Medium | S3.FC10   | -  | Very High |

## Block requests with KMS keys from unauthorized AWS account(s)

| Type                                    | Control  | Testing   | Effort | Feature Class(es)                                | Threat(s) and Impact   | CVSS-weighted Priority |
|---|--|---|--------|--|--|------------------------|
| Directive (coso)<br>Identify (NIST CSF) | [S3.C31]<br>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account | Request the list of authorized AWS accounts to provide KMS keys for S3 for each AWS account, its review process, and its review records | Medium | S3.FC1<br>S3.FC15<br>S3.FC26<br>S3.FC5<br>S3.FC8 | S3.T1 (Very Low)<br>S3.T2 (Very Low)<br>S3.T4 (Very Low)<br>S3.T5 (Very Low)<br>S3.T7 (Very Low)<br>S3.T8 (Very Low) | High                   |

|   |  |  |     |  |  |      |
|---|--|--|-----|--|--|------|
|   |  |  |     |  | S3.T9 (Very Low)<br>S3.T11 (Very Low)<br>S3.T16 (Very Low)<br>S3.T21 (Very Low)<br>S3.T27 (Very Low)<br>S3.T28 (Very Low)<br>S3.T30 (Very Low)<br>S3.T31 (Very Low)  |      |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C32, depends on S3.C31]<br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts) | Make a request encrypted with a KMS key from unauthorized AWS account, it should be denied | Low | S3.FC1<br>S3.FC15<br>S3.FC26<br>S3.FC5<br>S3.FC8 | S3.T1 (High)<br>S3.T2 (Medium)<br>S3.T4 (High)<br>S3.T5 (High)<br>S3.T7 (High)<br>S3.T8 (High)<br>S3.T9 (High)<br>S3.T11 (Medium)<br>S3.T16 (High)<br>S3.T21 (Medium)<br>S3.T27 (Low)<br>S3.T28 (High)<br>S3.T30 (High)<br>S3.T31 (High) | High |
| Detective (coso)<br>Detect (NIST CSF)     | [S3.C33, depends on S3.C31]<br>Monitor that only authorized AWS accounts provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> )  | Make a call to an unauthorized bucket, it should be detected                               | Low | S3.FC1<br>S3.FC15<br>S3.FC26<br>S3.FC5<br>S3.FC8 | S3.T1 (Low)<br>S3.T2 (Low)<br>S3.T4 (Low)<br>S3.T5 (Low)<br>S3.T7 (Low)<br>S3.T8 (Low)<br>S3.T9 (Low)<br>S3.T11 (Low)<br>S3.T16 (Low)<br>S3.T21 (Low)<br>S3.T27 (Very Low)<br>S3.T28 (Low)<br>S3.T30 (Low)<br>S3.T31 (Low)               | Low  |

## Block changes to make an object public via object ACL

| Type                                      | Control  | Testing  | Effort | Feature Class(es) | Threat(s) and Impact                    | CVSS-weighted Priority |
|---|--|--|--------|-------------------|---|------------------------|
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C34, assured by S3.C36]<br>Deny requests to change object ACL to public (e.g. using an SCP, S3 bucket policy and VPC endpoint policy blocking) | Make a call to create a public ObjectACL, it should be denied. | Medium | S3.FC1<br>S3.FC5  | S3.T6 (Very High)<br>S3.T36 (Very High) | High                   |

|                                       |  |  |      |                  |                             |      |
|---------------------------------------|--|--|------|------------------|-----------------------------|------|
|                                       | PutObjectAcl for "s3:x-amz-grant-read", "s3:x-amz-grant-read-acp", "s3:x-amz-grant-write-acp", "s3:x-amz-grant-full-control" on the following predefined groups "http://acs.amazonaws.com/groups/global/AllUsers" and "http://acs.amazonaws.com/groups/global/AuthenticatedUsers") |  |      |                  |                             |      |
| Detective (coso)<br>Detect (NIST CSF) | [S3.C35]<br>Monitor ObjectACL changed (or tentatively changed) to public using CloudTrail S3 data events   | Make a call to create a public ObjectACL, it should be detected.                   | Low  | S3.FC1<br>S3.FC5 | S3.T6 (Low)<br>S3.T36 (Low) | Low  |
| Assurance (coso)<br>Detect (NIST CSF) | [S3.C36]<br>Verify the control blocking change ObjectACL to public (e.g. an SCP and VPC endpoint policy) is properly implemented   | Remove the control blocking changes of ObjectACL to public, it should be detected. | High | S3.FC1<br>S3.FC5 | -                           | High |
| Detective (coso)<br>Detect (NIST CSF) | [S3.C37]<br>Monitor and investigate anonymous requests to objects (e.g. using CloudTrail S3 data events with userIdentity.accountId=ANONYMOUS_PRINCIPAL)   | Make an anonymous call, it should be detected.                                     | Low  | S3.FC5           | S3.T36 (Low)                | Low  |

## Prevent deletion of buckets

| Type                                      | Control  | Testing  | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|---|--|--|--------|-------------------|----------------------|------------------------|
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C38, assured by S3.C39]<br>Block the action "s3:DeleteBucket" (e.g. via SCP, exemption can be managed by authorizing a SuperAdmin to delete buckets with a certain tag, and with bucket owners able to tag bucket) | Do a DeleteBucket, it should be denied   | Low    | S3.FC5            | S3.T1 (Very High)    | High                   |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C39]<br>Verify the control blocking the action "s3:DeleteBucket" (e.g. an SCP on your AWS Organizations root node) is properly implemented   | Remove the control blocking the action "s3:DeleteBucket" (e.g. an SCP on your root node), it should be detected. | High   | S3.FC5            | -                    | High                   |
| Detective (coso)<br>Detect (NIST CSF)     | [S3.C40]<br>Scan your CNAME records (e.g. in Route53) and CloudFront origin for deleted buckets  | Create a CNAME record and CloudFront origin with an invalid bucket, it should be detected.                       | High   | S3.FC5            | S3.T1 (Very Low)     | Very Low               |

## Enforce good coding practice

| Type                                   | Control   | Testing  | Effort   | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|--|---|--|----------|-------------------|----------------------|------------------------|
| Directive (coso)<br>Protect (NIST CSF) | [S3.C41]<br>Parameterize S3 bucket name or S3 access point in your code (no hardcoding) | Request the process on ensuring S3 bucket name or S3 access point are not hard-coded | Medium   | S3.FC5            | S3.T1 (Low)          | Low                    |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C42]  | Request the mechanism ensuring the usage of domain style instead of path style.      | Very Low | S3.FC1            | S3.T35 (High)        | Low                    |

|  |  |  |        |                    |                                  |          |
|--|--|--|--------|--------------------|----------------------------------|----------|
|  | When connecting to S3 endpoints, use virtual-hosted model ("my-bucket-name.s3.amazonaws.com" or "my-bucket-name.my-s3-regional-endpoint.amazonaws.com") instead of path-style model ("s3.amazonaws.com/my-bucket-name" or "my-s3-regional-endpoint.amazonaws.com/my-bucket-name") (see <a href="#">ref</a> ). All the latest SDK make use of domain style, by default. |  |        |                    |                                  |          |
| Detective (COSO)<br>Detect (NIST CSF)  | [S3.C43]<br>Monitor that all S3 connections are made with virtual-hosted model (e.g via CloudTrail S3 requestParameters.Host)  | Make a path-style request to S3, it should be detected.  | Medium | S3.FC1             | S3.T35 (Low)                     | Very Low |
| Directive (COSO)<br>Protect (NIST CSF) | [S3.C44]<br>If etag is used, make sure properly account for its different definitions ( <a href="#">ref</a> )  | Request the process ensuring etag different definitions are properly accounted for   | Low    | S3.FC5             | S3.T27 (High)                    | Low      |
| Directive (COSO)<br>Protect (NIST CSF) | [S3.C45]<br>Do not include sensitive data in bucket names, access point names, object names, object metadata and tags.   | Request the process ensuring no sensitive data is included in bucket names, object names, object metadata and tags.  | Low    | S3.FC12<br>S3.FC20 | S3.T41 (Low)<br>S3.T42 (Medium)  | Very Low |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C46]<br>Ensure all S3 buckets interacted with are in the correct AWS account (e.g. using the condition in all compatible S3 requests: x-amz-expected-bucket-owner and x-amz-source-expected-bucket-owner)  | Request the process on ensuring that all S3 buckets interacted with are in the correct AWS account   | Medium | S3.FC1<br>S3.FC5   | S3.T1 (Medium)<br>S3.T3 (Medium) | Medium   |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C113, depends on S3.C11]<br>When transmitting an object to an external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover, use 2 separate APIs (PutObject and PutObjectAcl), instead of the built-in object ACL operation in PutObject.  | Request the process on ensuring that PutObject requests on external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover use 2 separate APIs | Medium | S3.FC1             | S3.T43 (High)                    | Medium   |

## Block direct public access

| Type                                      | Control   | Testing  | Effort   | Feature Class(es)           | Threat(s) and Impact  | CVSS-weighted Priority |
|---|---|--|----------|-----------------------------|---|------------------------|
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C47, assured by S3.C48]<br>Front buckets required to be public, using authenticated CDN (e.g. CloudFront) or API Gateway, protected with WAF (e.g. for <a href="#">hotlinking</a> )                               | Request the process ensuring that buckets required to be public are front by authenticated CDN or API Gateway  | Medium   | S3.FC16<br>S3.FC5           | S3.T13 (Very High)<br>S3.T14 (Medium)<br>S3.T22 (Very High) | Medium                 |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C48]<br>Verify no bucket is available publicly for write or read (e.g. using the AWS Config rules:<br><a href="#">S3_BUCKET_PUBLIC_READ_PROHIBITED</a> and<br><a href="#">S3_BUCKET_PUBLIC_WRITE_PROHIBITED</a> ) | Create a public S3 bucket, it should be detected.  | Very Low | S3.FC16<br>S3.FC5           | -   | Medium                 |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C49, assured by S3.C50]<br>Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.                     | 1) Create a public bucket and try to access one of its objects without proper authentication, or 2) change the ACL of an existing object to public, it should be denied. | Very Low | S3.FC10<br>S3.FC5<br>S3.FC8 | S3.T4 (High)<br>S3.T14 (High)<br>S3.T36 (Very High)         | Very High              |

|   |  |   |          |   |  |           |
|---|--|---|----------|---|--|-----------|
|   |  |   |          |   | S3.T37 (Very High)<br>S3.T38 (Medium)  |           |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C50]<br>Verify account-level S3 Block Public Access is enabled on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (e.g. using the AWS Config rule: <a href="#">S3 ACCOUNT LEVEL PUBLIC ACCESS BLOCKS</a> ). | Remove the account-level S3 Block Public Access, it should be detected  | Very Low | S3.FC10<br>S3.FC5<br>S3.FC8             | -  | Very High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C51, assured by S3.C52]<br>Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.  | 1) Create a public bucket and try to access one of its objects without proper authentication, and 2) change the ACL of an existing object to public, it should be denied.   | Low      | S3.FC10<br>S3.FC5<br>S3.FC8             | S3.T4 (High)<br>S3.T14 (High)<br>S3.T36 (Very High)<br>S3.T37 (Very High)<br>S3.T38 (Medium)             | Very High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C52]<br>Verify S3 Block Public Access is enabled on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (e.g. using the AWS Config rule: <a href="#">S3 BUCKET LEVEL PUBLIC ACCESS PROHIBITED</a> ).              | Remove a S3 Block Public Access of an S3 bucket, it should be detected  | Very Low | S3.FC10<br>S3.FC5<br>S3.FC8             | -  | Very High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C53, assured by S3.C54]<br>Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.   | 1) Create a public bucket and try to access via access point one of its objects without proper authentication ( <a href="#">ref</a> ), or 2) change the ACL of an existing object to public and try to access via access point one of its objects, it should be denied. | Low      | S3.FC10<br>S3.FC26<br>S3.FC33<br>S3.FC5 | S3.T14 (High)<br>S3.T36 (Medium)<br>S3.T37 (Medium)<br>S3.T38 (Medium)<br>S3.T54 (High)<br>S3.T55 (High) | Very High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C54]<br>Verify S3 Block Public Access is enabled on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.   | Remove S3 Block Public Access of 1) an access point, and 2) a multi-region access point, it should be detected  | Medium   | S3.FC10<br>S3.FC26<br>S3.FC33<br>S3.FC5 | -  | Very High |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C83]<br>Use SDK with SigV4 enabled ( <a href="#">ref</a> )   | Request the mechanism ensuring the use of SDK with SigV4 enabled  | Low      | S3.FC1                                  | S3.T35 (High)  | Low       |

## Block bucket ACL except for server access logging

| Type                                      | Control  | Testing   | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|---|--|---|--------|-------------------|----------------------|------------------------|
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C55, assured by S3.C57]<br>Deny requests to add bucket ACL other than for server access logging (e.g. using an SCP, bucket policy and VPC endpoint policy blocking PutBucketAcl for all but the following predefined group | Make a call to create a bucket ACL other than server access logging, it should be denied. | Medium | S3.FC8            | S3.T4 (Very High)    | High                   |

|                                       |   |   |        |        |             |      |
|---------------------------------------|---|---|--------|--------|-------------|------|
|                                       | "http://acs.amazonaws.com/groups/s3/LogDelivery" using the IAM condition x-amz-acl: "log-delivery-write")   |   |        |        |             |      |
| Detective (coso)<br>Detect (NIST CSF) | [S3.C56]<br>Monitor changes on bucket ACL other than for server access logging (e.g. using CloudTrail, 1) if the CloudTrail PutBucketAcl log indicates requestParameters.AccessControlPolicy.AccessControlList.Grant[].Grantee.xsi:type: "Group", then the URI should be "http://acs.amazonaws.com/groups/s3/LogDelivery", and 2) if the requestParameters.AccessControlPolicy.AccessControlList.Grant[].Grantee.xsi:type: "CanonicalUser" then the ID should be the same than "AccessControlPolicy.Owner.ID", and 3) requestParameters.x-amz-acl should be either "private", "log-delivery-write" or not existing) | Make a call to create a bucket ACL other than server access logging, it should be detected.                 | Medium | S3.FC8 | S3.T4 (Low) | Low  |
| Assurance (coso)<br>Detect (NIST CSF) | [S3.C57]<br>Verify the control blocking bucket ACL changes other than for server access logging (e.g. an SCP, a bucket policy and VPC endpoint policy) is properly implemented  | Remove the control blocking bucket ACL changes other than for server access logging, it should be detected. | High   | S3.FC8 | -           | High |

## Identify and ensure the protection all internal buckets hosting your objects

| Type                                   | Control  | Testing   | Effort    | Feature Class(es) | Threat(s) and Impact                                | CVSS-weighted Priority |
|--|--|---|-----------|-------------------|---|------------------------|
| Directive (coso)<br>Protect (NIST CSF) | [S3.C58]<br>Track all buckets you control, define their authorized data classification, identify whether the hosted data is primary (i.e. source of truth, for example logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g. file-processing, software package, etc.), their WORM requirements (e.g. SEC 17a-4, CTCC, etc.), if they are production/non-production (preferably done at account-level), their storage class. You may use tags, Infra-as-code, AWS Glue Data Catalog or external management tool like <a href="#">FINRA herd</a> ) | Request the list of all buckets you control, define their authorized data classification, identify whether the data is primary and the mechanism and records to ensure the accuracy of those metadata | High      | S3.FC13<br>S3.FC5 | S3.T11 (High)<br>S3.T17 (Very High)<br>S3.T25 (Low) | High                   |
| Detective (coso)<br>Detect (NIST CSF)  | [S3.C59, depends on S3.C58]<br>Use a data discovery tool (e.g. Amazon Macie) to control that no sensitive data are stored in unauthorized bucket   | Upload a higher classification data in a bucket, it should be detected.   | Medium    | S3.FC5            | S3.T11 (Medium)                                     | Medium                 |
| Detective (coso)<br>Detect (NIST CSF)  | [S3.C60]<br>Use a data discovery tool (e.g. Amazon Macie) to ensure the bucket names, object names, tags and metadata do not contain sensitive data  | Create a bucket name, object name, tags, or a metadata of an object with sensitive data, it should be detected.   | Very High | S3.FC5            | S3.T11 (Very Low)                                   | Very Low               |

## Enforce encryption-at-rest

| Type                                      | Control   | Testing  | Effort | Feature Class(es) | Threat(s) and Impact  | CVSS-weighted Priority |
|---|---|--|--------|-------------------|---|------------------------|
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C61]<br>Maintain a list of authorized KMS key(s) for each bucket, and their default encryption key. You might simplify by using only 1 key per bucket, ideally dedicated. Note that S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ).              | Request the list of authorized KMS key(s) for each bucket, its review process, and its review records  | Medium | S3.FC10<br>S3.FC5 | S3.T11 (Very Low)<br>S3.T16 (Very Low)<br>S3.T17 (Very Low)<br>S3.T20 (Very Low)<br>S3.T30 (Very Low)<br>S3.T36 (Very Low)<br>S3.T37 (Very Low) | Very High              |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C140, assured by S3.C62]<br>Ensure all objects on S3 buckets are encrypted with an authorized KMS key   | Request the mechanism (including training, or utility) ensuring only authorized KMS key are used for any objects stored in S3  | Medium | S3.FC10<br>S3.FC5 | S3.T11 (Medium)<br>S3.T16 (Medium)<br>S3.T17 (Medium)<br>S3.T20 (Medium)<br>S3.T30 (Medium)<br>S3.T36 (Medium)<br>S3.T37 (Medium)               | Medium                 |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C62]<br>Verify all objects on S3 buckets are encrypted with an authorized KMS key (e.g. using S3 inventory, see <a href="#">blog</a> , or <a href="#">S3 Storage Lens</a> )   | Upload an encrypted data using an unauthorized KMS key, it should be detected.   | Medium | S3.FC10<br>S3.FC5 | -   | Medium                 |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C63, depends on S3.C61]<br>Use KMS ThreatModel to protect the KMS keys used for S3 (e.g. using encryptionContext on the policy of each KMS key)   | Request the KMS ThreatModel and the evidence of its application to protect S3  | High   | S3.FC10<br>S3.FC5 | S3.T17 (Medium)<br>S3.T36 (Low)<br>S3.T37 (Low)   | Low                    |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C64, depends on S3.C61, assured by S3.C65]<br>Implement an authorized default encryption key on each bucket and enable S3 Bucket Key (note: Amazon S3 evaluates and applies bucket policies before applying bucket default encryption settings)                                       | Request 1) the mechanism implementing an authorized default encryption key on each bucket and enabling S3 Bucket Key, 2) its records of execution for all new buckets, and 3) plan to move any older buckets | Low    | S3.FC10<br>S3.FC5 | S3.T17 (Medium)<br>S3.T20 (High)<br>S3.T36 (High)<br>S3.T37 (High)  | Very High              |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C65]<br>Verify each bucket has an authorized default encryption key and has S3 Bucket Key enabled   | Create/modify a bucket 1) without default encryption, 2) with a wrong default encryption key or 3) without S3 Bucket Key disabled, it should be detected.  | Medium | S3.FC10<br>S3.FC5 | -   | Very High              |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C66, depends on S3.C61, assured by S3.C67]<br>Block PutObject requests with unauthorized KMS key on each bucket (e.g. using an S3 bucket policy deny statement on PutObject if the condition if exists "s3:x-amz-server-side-encryption-aws-kms-key-id" is not an authorized KMS key) | Make a request encrypted with an unauthorized KMS key, it should be denied   | Low    | S3.FC10<br>S3.FC5 | S3.T11 (High)<br>S3.T16 (High)<br>S3.T17 (High)<br>S3.T20 (Very High)<br>S3.T30 (High)<br>S3.T36 (High)<br>S3.T37 (High)                        | Very High              |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C67]<br>Verify all buckets block PutObject requests with an unauthorized KMS key (e.g. using the Config rule: <a href="#">S3 BUCKET POLICY NOT MORE PERMISSIVE</a> , note that a  | Create a bucket not blocking PutObject requests with an unauthorized KMS key, it should be detected.   | Medium | S3.FC10<br>S3.FC5 | -   | Very High              |

|   |   |   |        |                   |  |           |
|---|---|---|--------|-------------------|--|-----------|
|   | <p>new rule needs be deployed for each configuration, then the resource tracked by name or tag; alternatively you might use <a href="#">S3 BUCKET SERVER SIDE ENCRYPTION ENABLED</a> to ensure a limited coverage)</p>  |   |        |                   |  |           |
| Detective (coso)<br>Detect (NIST CSF)     | [S3.C68, depends on S3.C61]<br>Monitor that only authorized KMS key(s) are used on each bucket (using CloudTrail S3 data events in <i>requestParameter.bucketName</i> and <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> )   | Make a request encrypted with an unauthorized KMS key, it should be detected  | Low    | S3.FC5            | S3.T11 (Very Low)<br>S3.T16 (Low)<br>S3.T30 (Very Low)<br>S3.T36 (Low)   | Low       |
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C145]<br>Maintain a list of buckets (or paths) required to be encrypted with server-side encryption with customer-provided keys (SSE-C)   | Request the list of buckets (or paths) required to be encrypted with server-side encryption with customer-provided keys (SSE-C), its review process, and its review records | Medium | S3.FC10<br>S3.FC5 | S3.T11 (Very Low)<br>S3.T16 (Very Low)<br>S3.T20 (Very Low)<br>S3.T30 (Very Low)<br>S3.T36 (Very Low)<br>S3.T37 (Very Low) | Very High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C146, depends on S3.C145, assured by S3.C147]<br>For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g. using an S3 bucket policy deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present) | Make a request to a bucket (or path) requiring SSE-C without the proper encryption, it should be denied   | Low    | S3.FC10<br>S3.FC5 | S3.T11 (High)<br>S3.T16 (High)<br>S3.T20 (Very High)<br>S3.T30 (High)<br>S3.T36 (High)<br>S3.T37 (High)                    | Very High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C147]<br>For buckets (or paths) requiring SSE-C, verify all buckets block PutObject requests with unauthorized encryption   | Create a bucket requiring SSE-C not blocking PutObject requests with unauthorized encryption, it should be detected.  | High   | S3.FC10<br>S3.FC5 | -  | Very High |
| Detective (coso)<br>Detect (NIST CSF)     | [S3.C148, depends on S3.C145]<br>For buckets (or paths) requiring SSE-C, monitor that only authorized encryption is used on each bucket or path (using CloudTrail S3 data events in <i>requestParameter.bucketName</i> and <i>response.x-amz-server-side-encryption-customer-algorithm</i> )                  | Make a request to a bucket (or path) requiring SSE-C without the proper encryption, it should be detected   | Low    | S3.FC5            | S3.T11 (Very Low)<br>S3.T16 (Low)<br>S3.T30 (Very Low)<br>S3.T36 (Low)   | Low       |

## Protect primary data against loss

| Type                                   | Control  | Testing   | Effort   | Feature Class(es) | Threat(s) and Impact                            | CVSS-weighted Priority |
|--|--|---|----------|-------------------|---|------------------------|
| Directive (coso)<br>Protect (NIST CSF) | [S3.C69, depends on S3.C58, assured by S3.C70]<br>Enable versioning on buckets holding primary data                      | Request the mechanism used to ensure versioning on buckets holding primary data, and its records  | Very Low | S3.FC5            | S3.T16 (High)<br>S3.T17 (High)                  | High                   |
| Assurance (coso)<br>Detect (NIST CSF)  | [S3.C70]<br>Verify buckets holding primary data are versioned (e.g. using <a href="#">S3 BUCKET VERSIONING ENABLED</a> ) | Remove versioning from a bucket holding primary data, it should be detected   | Low      | S3.FC5            | -   | High                   |
| Directive (coso)<br>Recover (NIST CSF) | [S3.C71, depends on S3.C58]  | Request the mechanism used to backup primary data in a location which have different security authority, its records of execution, and records of restoration testing | Medium   | S3.FC13<br>S3.FC5 | S3.T16 (High)<br>S3.T17 (High)<br>S3.T25 (High) | Medium                 |

|  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|
|  | Backup primary data in a secure location under a different security authority (e.g. in an <a href="#">AWS data bunker account</a> via replication) |  |  |  |  |  |
|--|--|--|--|--|--|--|

## Encrypt or tokenize critical data

| Type                                   | Control  | Testing  | Effort    | Feature Class(es)                      | Threat(s) and Impact   | CVSS-weighted Priority |
|--|--|--|-----------|--|--|------------------------|
| Directive (coso)<br>Protect (NIST CSF) | [S3.C72]<br>Aligned with your data governance, encrypt on the client side - or tokenize - appropriate data | Request the governance and mechanism(s) used to protect data (e.g. encrypt or tokenize critical data on the client side) | Very High | S3.FC1<br>S3.FC10<br>S3.FC16<br>S3.FC5 | S3.T1 (Medium)<br>S3.T3 (Medium)<br>S3.T5 (High)<br>S3.T7 (High)<br>S3.T11 (Very High)<br>S3.T12 (Very High)<br>S3.T13 (Very High)<br>S3.T17 (High)<br>S3.T20 (High)<br>S3.T30 (High)<br>S3.T31 (High) | Medium                 |

## Have a process to apply legal hold

| Type                                   | Control   | Testing   | Effort | Feature Class(es) | Threat(s) and Impact            | CVSS-weighted Priority |
|--|---|---|--------|-------------------|---------------------------------|------------------------|
| Directive (coso)<br>Protect (NIST CSF) | [S3.C73]<br>Create a process to apply legal hold to any S3 bucket, whenever required. The condition "s3:object-lock-legal-hold" can be used to restrict who can remove such a lock. | Request the process of applying legal hold, and its records | Medium | S3.FC5            | S3.T16 (Low)<br>S3.T17 (Medium) | Medium                 |

## Use S3 Object Lock to protect data integrity

| Type                                      | Control   | Testing  | Effort | Feature Class(es) | Threat(s) and Impact                            | CVSS-weighted Priority |
|---|---|--|--------|-------------------|---|------------------------|
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C74, depends on S3.C58, assured by S3.C75]<br>Implement the authorized default S3 Object Lock on each bucket (note: Amazon S3 evaluates and applies bucket policies before applying bucket default S3 Object Lock settings) | Upload an object without appropriate S3 Object Lock, it should have the S3 Object Lock automatically.            | Low    | S3.FC13<br>S3.FC5 | S3.T16 (High)<br>S3.T17 (High)<br>S3.T25 (High) | High                   |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C75]<br>Verify all buckets have the correct default S3 Object Lock configuration  | Create a bucket 1) without S3 Object Lock or 2) with an incorrect default S3 Object Lock, it should be detected. | Medium | S3.FC13<br>S3.FC5 | -   | High                   |

|   |  |   |        |        |                                |      |
|---|--|---|--------|--------|--------------------------------|------|
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C76, depends on S3.C58, assured by S3.C77]<br>Block PutObject and PutObjectRetention requests with unauthorized S3 Object Lock on each bucket (e.g. using an S3 bucket policy deny statement on PutObject and PutObjectRetention if the condition if exists "s3:object-lock-mode" and "s3:object-lock-remaining-retention-days" is not the defined S3 Object Lock configuration) | Make a request with an incorrect S3 Object Lock configuration, it should be denied  | Low    | S3.FC5 | S3.T16 (High)<br>S3.T17 (High) | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C77]<br>Verify all buckets blocks PutObject and PutObjectRetention requests with unauthorized S3 Object Lock (e.g. using the Config rule: <a href="#">S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE</a> , note that a new rule needs be deployed for each configuration, then the resource tracked by name or tag)  | Create a bucket not blocking PutObject and PutObjectRetention requests with unauthorized S3 Object Lock, it should be detected. | Medium | S3.FC5 | -                              | High |

## Remove incomplete multipart uploads

| Type                                      | Control  | Testing   | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|---|--|---|--------|-------------------|----------------------|------------------------|
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C78, assured by S3.C79]<br>Reduce costs related to incomplete multipart upload by creating a lifecycle policy to remove them after an agreed length of time (e.g. 7 days) ( <a href="#">blog</a> ) | Create an incomplete upload, and wait for the agreed time, it should be deleted automatically.          | Low    | S3.FC5            | S3.T40 (High)        | Low                    |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C79]<br>Verify a lifecycle policy on incomplete multipart uploads is implemented on all buckets  | Create a bucket without a lifecycle policy to remove incomplete multipart upload, it should be detected | Medium | S3.FC5            | -                    | Low                    |

## Block deprecated actions

| Type                                   | Control   | Testing   | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|--|---|---|--------|-------------------|----------------------|------------------------|
| Directive (coso)<br>Protect (NIST CSF) | [S3.C80]<br>Block deprecated S3 actions, using IAM ThreatModel and the S3 actions list. | Request the controls blocking deprecated S3 actions | Low    | S3.FC1            | S3.T35 (Medium)      | Very Low               |

## Block all requests not using SigV4

| Type                                      | Control   | Testing   | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|---|---|---|--------|-------------------|----------------------|------------------------|
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C81]<br>Block all requests not using SigV4 (e.g. using an SCP and S3 policy on all buckets with deny on | Make a non-SigV4 AWS API call, it should be denied. | Low    | S3.FC1            | S3.T35 (High)        | Low                    |

|                                       |  |   |     |        |              |          |
|---------------------------------------|--|---|-----|--------|--------------|----------|
|                                       | "StringNotEquals": {"s3:signatureversion": "AWS4-HMAC-SHA256"}   |   |     |        |              |          |
| Detective (coso)<br>Detect (NIST CSF) | [S3.C82]<br>Monitor and investigate that all requests not using SigV4 (e.g via CloudTrail S3 with the additionalEventData.SignatureVersion different from "SigV4") | Make a non-SigV4 AWS API call, it should be detected. | Low | S3.FC1 | S3.T35 (Low) | Very Low |

## Block all requests not using HTTP authorization header, if not explicitly authorized

| Type                                      | Control  | Testing  | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|---|--|--|--------|-------------------|----------------------|------------------------|
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C84]<br>Block all requests not using HTTP authorization header, i.e. presign via query strings or POST ( <a href="#">ref</a> ) (e.g. using an SCP and S3 policy on all buckets with deny on "StringNotEquals": {"s3:authType": "REST-HEADER"}). Note it blocks uploads via the console, as well. | Make a request with a non-HTTP authorization header, it should be denied       | Low    | S3.FC5            | S3.T39 (Medium)      | Medium                 |
| Detective (coso)<br>Detect (NIST CSF)     | [S3.C85]<br>Monitor and investigate that all requests not using HTTP authorization header (e.g via CloudTrail S3 with the additionalEventData.AuthenticationMethod different from "AuthHeader")  | Make 1) a presigned AWS API call and 2) a POST request, it should be detected. | Low    | S3.FC5            | S3.T39 (Very Low)    | Very Low               |

## Restrict bucket replication

| Type                                    | Control  | Testing  | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|---|--|--|--------|-------------------|----------------------|------------------------|
| Directive (coso)<br>Identify (NIST CSF) | [S3.C86]<br>Maintain a list of authorized buckets to have replication enabled, their target bucket and replication type (i.e. ownership, RTC, etc.) ( <a href="#">ref</a> ). | Request the list of authorized buckets to have replication enabled, their target bucket and replication rights, its review process, and its review records   | Medium | S3.FC15           | S3.T2 (Very Low)     | Medium                 |
| Directive (coso)<br>Protect (NIST CSF)  | [S3.C134, depends on S3.C86, assured by S3.C87,S3.C88,S3.C117]<br>Ensure only authorized buckets have replication enabled and with correct configuration are configured      | Request 1) the mechanism ensuring only authorized buckets have replication enabled and with correct configuration are configured, 2) its records of execution for all new buckets, and 3) plan to move any older buckets | Medium | S3.FC15           | S3.T2 (High)         | Medium                 |
| Assurance (coso)<br>Detect (NIST CSF)   | [S3.C87]<br>Verify only authorized buckets have replication enabled and with correct configuration   | Configure replication on a non-authorized bucket, it should be detected  | Medium | S3.FC15           | -                    | Medium                 |
| Assurance (coso)<br>Detect (NIST CSF)   | [S3.C88]<br>Verify authorized buckets have the correct replication configuration   | Modify the configuration of an authorized replication, it should be detected   | High   | S3.FC15           | -                    | Medium                 |
| Directive (coso)<br>Identify (NIST CSF) | [S3.C89]   | Request the list of all IAM roles configured for replication   | Medium | S3.FC15           | S3.T2 (Very Low)     | Medium                 |

|  |   |  |        |         |                |        |
|--|---|--|--------|---------|----------------|--------|
|  | Maintain a list of IAM roles used for replication, ideally dedicated (e.g. using change management process on infrastructure-as-code)                             |  |        |         |                |        |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C138, depends on S3.C89, assured by S3.C92]<br>Ensure only authorized IAM roles are attached for each replication, ideally dedicated                          | Request the mechanism ensuring authorized IAM roles are attached for each replication, and the evidence of its execution for all replication configuration | Medium | S3.FC15 | S3.T2 (High)   | Medium |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C90, depends on S3.C89]<br>Limit the S3 access to the source/destination bucket and replication rights of each authorized IAM role configured for replication | Request the S3 access of replication role, and how they aligned to the replication requirements  | Medium | S3.FC15 | S3.T2 (Medium) | Medium |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C91, depends on S3.C89]<br>Limit access to authorized IAM roles used for replication, using the IAM ThreatModel (e.g. trust policy, and "iam:PassRole")       | Request the IAM ThreatModel and the evidence of its application to the IAM roles used for replication  | High   | S3.FC15 | S3.T2 (High)   | Medium |
| Assurance (coso)<br>Detect (NIST CSF)  | [S3.C92]<br>Verify only the authorized IAM role is configured for each replication  | Create/modify a replication with an unauthorized IAM role, it should be detected   | High   | S3.FC15 | -              | Medium |
| Detective (coso)<br>Detect (NIST CSF)  | [S3.C116]<br>Monitor abnormal behaviour on replication CloudWatch metrics (i.e. <i>BytesPendingReplication</i> and <i>OperationsPendingReplication</i> )          | Create an abnormal replication, it should be detected  | Low    | S3.FC15 | S3.T2 (Low)    | Low    |
| Assurance (coso)<br>Detect (NIST CSF)  | [S3.C117]<br>Verify all replicated buckets have metrics enabled on each replication rule (included by default in S3 RTC)  | Modify the replication metric of an authorized replication, it should be detected  | Medium | S3.FC15 | -              | Medium |

## Scan input/output objects for malware

| Type                                  | Control  | Testing  | Effort | Feature Class(es) | Threat(s) and Impact            | CVSS-weighted Priority |
|---------------------------------------|--|--|--------|-------------------|---------------------------------|------------------------|
| Detective (coso)<br>Detect (NIST CSF) | [S3.C93, depends on S3.C58]<br>If the bucket is used as an input or the output of a process, scan the objects for malware (e.g. using <a href="#">VirusScan</a> or <a href="#">Trend Micro Cloud One</a> ) | Inject a malware test file, it should be detected. | Medium | S3.FC16<br>S3.FC5 | S3.T14 (Medium)<br>S3.T15 (Low) | Medium                 |

## Control event receivers

| Type                                    | Control  | Testing   | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|---|--|---|--------|-------------------|----------------------|------------------------|
| Directive (coso)<br>Identify (NIST CSF) | [S3.C94]<br>Maintain a list of authorized notification receiver(s) (e.g. SNS Topic, Lambda, etc.) for each bucket. You might use a simpler approach by using authorized account ID(s) to ensure all your receivers are in authorized AWS account(s). | Request the list of authorized notification receiver (e.g. SNS Topic, Lambda, etc.) for each bucket, its review process, and its review records | Low    | S3.FC20           | S3.T41 (Very Low)    | Low                    |

|  |  |  |        |         |               |     |
|--|--|--|--------|---------|---------------|-----|
| Directive (coso)<br>Protect (NIST CSF) | [S3.C135, depends on S3.C94, assured by S3.C95]<br>Ensure only authorized notification receiver(s) (e.g. SNS Topic, Lambda, etc.) for each bucket are configured | Request 1) the mechanism ensuring only authorized notification receiver(s) (e.g. SNS Topic, Lambda, etc.) for each bucket are configured, 2) its records of execution for all new buckets, and 3) plan to move any older buckets | Medium | S3.FC20 | S3.T41 (High) | Low |
| Assurance (coso)<br>Detect (NIST CSF)  | [S3.C95]<br>Verify only authorized notification receiver(s) are configured for buckets.  | Create an unauthorized receiver, it should be detected.  | High   | S3.FC20 | -             | Low |

## Control where the inventory is stored

| Type                                    | Control   | Testing   | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|---|---|---|--------|-------------------|----------------------|------------------------|
| Directive (coso)<br>Identify (NIST CSF) | [S3.C96]<br>Maintain a list of authorized S3 buckets to receive S3 inventory of each bucket   | Request the list of authorized bucket(s) to receive S3 inventory of each bucket, its review process, and its review records   | Low    | S3.FC12           | S3.T42 (Very Low)    | Very Low               |
| Directive (coso)<br>Protect (NIST CSF)  | [S3.C136, depends on S3.C96, assured by S3.C97]<br>Ensure only authorized S3 buckets are configured to receive S3 inventory for each bucket | Request 1) the mechanism ensuring only authorized S3 buckets are configured to receive S3 inventory for each bucket, 2) its records of execution for all new buckets, and 3) plan to move any older buckets | Medium | S3.FC12           | S3.T42 (Medium)      | Very Low               |
| Assurance (coso)<br>Detect (NIST CSF)   | [S3.C97]<br>Verify only authorized buckets are configured to receive inventory.   | Create an unauthorized bucket to receive inventory, it should be detected.  | High   | S3.FC12           | -                    | Very Low               |

## Limit access from only authorized VPCs

| Type                                      | Control  | Testing   | Effort   | Feature Class(es)           | Threat(s) and Impact   | CVSS-weighted Priority |
|---|--|---|----------|-----------------------------|--|------------------------|
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C98]<br>For each S3 bucket, maintain a list of VPC(s), authorized to access it.  | For each S3 bucket, request the list of authorized VPC to access it, its review process, and its review records | Low      | S3.FC10<br>S3.FC2<br>S3.FC5 | S3.T11 (Very Low)<br>S3.T14 (Very Low)<br>S3.T17 (Very Low)<br>S3.T30 (Very Low)<br>S3.T33 (Very Low)<br>S3.T36 (Very Low)<br>S3.T38 (Very Low)<br>S3.T39 (Very Low) | High                   |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C99, depends on S3.C98, assured by S3.C100]<br>Limit the access to only those VPC(s) (e.g. using S3 bucket statement, deny if the condition "aws:SourceVpc", or if the bucket policy size is beyond the limit, use this condition on access point) | Make a request to the bucket outside an authorized VPC, it should be denied                                     | Very Low | S3.FC10<br>S3.FC2<br>S3.FC5 | S3.T11 (Medium)<br>S3.T14 (Medium)<br>S3.T17 (Medium)<br>S3.T30 (High)<br>S3.T33 (High)<br>S3.T36 (High)<br>S3.T38 (High)  | High                   |

|                                       |  |  |        |                             |               |      |
|---------------------------------------|--|--|--------|-----------------------------|---------------|------|
|                                       |  |  |        |                             | S3.T39 (High) |      |
| Assurance (coso)<br>Detect (NIST CSF) | [S3.C100]<br>Verify all buckets include a control to limit access to only authorized VPC(s) (e.g. using the AWS Config rule <a href="#">S3_BUCKET_POLICY_GRANTEE_CHECK</a> ) | Remove the control limiting access to only authorized VPC(s), it should be detected. | Medium | S3.FC10<br>S3.FC2<br>S3.FC5 | -             | High |

## Control CloudFront access

| Type                                    | Control   | Testing   | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|---|---|---|--------|-------------------|----------------------|------------------------|
| Directive (coso)<br>Identify (NIST CSF) | [S3.C101]<br>Maintain a list of authorized CloudFront distribution (via origin access identity) and associated bucket   | Request the list of all authorized CloudFront distribution and associated S3 buckets  | Low    | S3.FC10           | S3.T20 (very Low)    | Medium                 |
| Directive (coso)<br>Protect (NIST CSF)  | [S3.C137, depends on S3.C101, assured by S3.C102]<br>Ensure only authorized CloudFront distributions are associated with their authorized bucket, and vice versa. | Request 1) the mechanism ensuring only authorized only authorized CloudFront distribution are associated with their authorized bucket, and vice versa, 2) its records of execution for all new CloudFront distribution, and 3) plan to move any older CloudFront distribution | Medium | S3.FC10           | S3.T20 (High)        | Medium                 |
| Assurance (coso)<br>Detect (NIST CSF)   | [S3.C102]<br>Verify all associations of CloudFront distributions with buckets are authorized  | Create a non-authorized distribution or association, it should be detected.   | High   | S3.FC10           | -                    | Medium                 |

## Protect and/or claim your domains and trademarks/copyrights

| Type                                   | Control  | Testing  | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|--|--|--|--------|-------------------|----------------------|------------------------|
| Directive (coso)<br>Protect (NIST CSF) | [S3.C103]<br>Protect and/or claim your domains and trademarks/copyrights (by creating your trademark buckets, and using the <a href="#">copyright infringement process</a> from AWS) | Request the process by protecting and/or claiming your domains and trademarks/copyrights | Medium | S3.FC28           | S3.T23 (High)        | Low                    |

## Restrict access point access to VPC when in use

| Type                                    | Control  | Testing  | Effort | Feature Class(es)                      | Threat(s) and Impact  | CVSS-weighted Priority |
|---|--|--|--------|--|---|------------------------|
| Directive (coso)<br>Identify (NIST CSF) | [S3.C104]<br>Maintain a list of authorized access between VPC, S3 access point and S3. | Request the list of authorized access between VPC and S3 access points | Medium | S3.FC1<br>S3.FC26<br>S3.FC28<br>S3.FC5 | S3.T7 (Very Low)<br>S3.T9 (Very Low)<br>S3.T10 (Very Low)<br>S3.T11 (Very Low)<br>S3.T28 (Very Low) | Medium                 |

|   |  |   |        |   |  |      |
|---|--|---|--------|---|--|------|
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C105, depends on S3.C104, assured by S3.C109]<br>Limit access via the S3 access point by using in VPC endpoint and/or bucket policy the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of allowlist bucket name in VPC endpoint/bucket policy. | Do a request on an unauthorized access point or bucket, it should be denied.            | Medium | S3.FC1<br>S3.FC26<br>S3.FC28<br>S3.FC33<br>S3.FC5 | S3.T7 (Medium)<br>S3.T9 (Very High)<br>S3.T10 (Very High)<br>S3.T11 (Medium)<br>S3.T54 (Medium)<br>S3.T55 (Medium) | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C106, assured by S3.C110]<br>In S3 bucket policy, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn"   | Query the bucket outside S3 access point, it should be denied.                          | Medium | S3.FC1<br>S3.FC26<br>S3.FC33                      | S3.T7 (Medium)<br>S3.T28 (High)<br>S3.T55 (Medium)<br>S3.T56 (Very High)   | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C107]<br>Block the creation "s3>CreateAccessPoint" of non-VPC S3 access point (e.g. using the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"})   | Do a request to create an internet-based access point, it should be denied.             | Low    | S3.FC1<br>S3.FC26                                 | S3.T7 (Medium)<br>S3.T28 (Very High)   | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C108, assured by S3.C111]<br>Block all traffic from Internet-configured S3 access point (e.g. on the bucket policy, using a deny statement with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"})   | Create an internet-facing access point and try to access a bucket, it should be denied. | Low    | S3.FC1<br>S3.FC26<br>S3.FC28                      | S3.T7 (Medium)<br>S3.T10 (Medium)<br>S3.T28 (Very High)  | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C109]<br>Verify only access points are used in the resource-level statement in VPC endpoints   | Create a VPC endpoint giving access to an S3 bucket, it should be detected.             | High   | S3.FC1<br>S3.FC26<br>S3.FC28<br>S3.FC33<br>S3.FC5 | -  | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C110]<br>Verify S3 bucket policies deny non-authorized S3 access points  | Remove/modify the deny on the bucket policy, it should be detected.                     | High   | S3.FC1<br>S3.FC26<br>S3.FC33                      | -  | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C111]<br>Verify all S3 access points are VPC attached  | Create an internet-based access point, it should be detected.                           | Low    | S3.FC1<br>S3.FC26<br>S3.FC28                      | -  | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C112, depends on S3.C104]<br>Block any <a href="#">object-related operations</a> access to S3 bucket not through access point (i.e. using a deny IAM policy statement with the condition "ArnNotLike" {"s3:DataAccessPointArn": "arn:aws:s3:Region:AccountId:accesspoint/*"})  | Access any S3 bucket using the S3 public endpoint, it should be denied.                 | Low    | S3.FC1<br>S3.FC5                                  | S3.T7 (Medium)<br>S3.T11 (High)  | High |

## Control IAM roles used for Batch

| Type                                    | Control   | Testing  | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|---|-----------|--|--------|-------------------|----------------------|------------------------|
| Directive (coso)<br>Identify (NIST CSF) | [S3.C120] | Request the list of all IAM roles configured for Batch job | Medium | S3.FC27           | S3.T44 (Very Low)    | High                   |

|  |   |  |        |         |                    |        |
|--|---|--|--------|---------|--------------------|--------|
|  | Maintain a list of IAM roles used for Batch job, ideally dedicated (e.g. using change management process on infrastructure-as-code)   |  |        |         |                    |        |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C139, depends on S3.C120, assured by S3.C123]<br>Ensure only an authorized IAM role is attached on each Batch job   | Request the mechanism ensuring only an authorized IAM role is attached on each Batch job, and the evidence of its execution for all new {resource} | Medium | S3.FC27 | S3.T44 (High)      | Medium |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C121, depends on S3.C120]<br>Limit the access to only required resources/permissions (e.g. source/destination bucket, Lambda functions) of each authorized IAM role configured for Batch jobs | Request the access to only required resources/permissions for each Batch IAM role, and how they aligned to the replication requirements            | Medium | S3.FC27 | S3.T44 (High)      | Medium |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C122, depends on S3.C120]<br>Limit access to authorized IAM roles used for Batch job, using the IAM ThreatModel (e.g. trust policy, and "iam:PassRole")                                       | Request the IAM ThreatModel and the evidence of its application to the IAM roles used for Batch job  | Medium | S3.FC27 | S3.T44 (Very High) | High   |
| Assurance (coso)<br>Detect (NIST CSF)  | [S3.C123]<br>Verify only the authorized IAM role is configured for each Batch job   | Create/modify a Batch job with an unauthorized IAM role, it should be detected   | High   | S3.FC27 | -                  | Medium |

## Enforce only authorized Object Lambda access point and associated access

| Type                                    | Control  | Testing   | Effort   | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|---|--|---|----------|-------------------|----------------------|------------------------|
| Directive (coso)<br>Identify (NIST CSF) | [S3.C125]<br>Maintain a list of authorized Lambda function for each Object Lambda access point, its associated access point, its associated GET request(s), and payload  | Request the list of authorized Lambda function for each Object Lambda access point, its associated access point, its associated GET request(s), and payload, its review process, and its review records   | Low      | S3.FC32           | S3.T46 (very Low)    | High                   |
| Directive (coso)<br>Protect (NIST CSF)  | [S3.C126, depends on S3.C125, assured by S3.C127]<br>Ensure only authorized Lambda function for each Object Lambda access point, its associated access point, its associated GET request(s), and payload are created | Request the mechanism ensuring only authorized Lambda function for each Object Lambda access point, its associated access point, its associated GET request(s), and payload, and the evidence of its execution  | Medium   | S3.FC32           | S3.T46 (Very High)   | High                   |
| Assurance (coso)<br>Detect (NIST CSF)   | [S3.C127]<br>Verify only the authorized Lambda function are configured on each Object Lambda access point, its associated access point, its associated GET request(s), and payload                                   | Attach 1) an unauthorized Lambda function on an Object Lambda access point, 2) an unauthorized Object Lambda access point to an access point, 3) an authorized Lambda function with an unauthorized GET request on an Object Lambda access point, and 4) an authorized Lambda function with an unauthorized payload, it should be detected. | Medium   | S3.FC32           | -                    | High                   |
| Directive (coso)<br>Protect (NIST CSF)  | [S3.C128]<br>Ensure Lambda functions configured on Object Lambda access point are secured using Lambda ThreatModel   | Request the mechanism ensuring Lambda ThreatModel and its application for Lambda functions associated to Object Lambda access point, and its records of execution   | Medium   | S3.FC32           | S3.T46 (High)        | Medium                 |
| Directive (coso)<br>Identify (NIST CSF) | [S3.C129]<br>Maintain a list of cross-account access on each Object Lambda access point  | Request the list of authorized cross-account access for each Object Lambda access point, its review process, and its review records   | Very Low | S3.FC32           | S3.T46 (Very Low)    | Medium                 |

|  |   |  |      |         |                 |        |
|--|---|--|------|---------|-----------------|--------|
| Directive (COSO)<br>Protect (NIST CSF) | [S3.C130, depends on S3.C129, assured by S3.C131]<br>Ensure only authorized cross-account IAM entities are allowed in the Object Lambda access point policy | Request the mechanism ensuring only cross-account IAM entities are allowed in the Object Lambda access point policy, and the evidence of its execution | Low  | S3.FC32 | S3.T46 (Medium) | Medium |
| Assurance (COSO)<br>Detect (NIST CSF)  | [S3.C131]<br>Verify only the authorized cross-account IAM entities are allowed in the Object Lambda access point policy                                     | Add 1) an unauthorized cross-account IAM entity on an Object Lambda access point policy, it should be detected.  | High | S3.FC32 | -               | Medium |
| Directive (COSO)<br>Protect (NIST CSF) | [S3.C132, assured by S3.C133]<br>Ensure CloudWatch is enabled for all Object Lambda access points   | Request the mechanism ensuring CloudWatch is enabled for all Object Lambda access points, and its records of execution                                 | Low  | S3.FC32 | S3.T46 (Low)    | Low    |
| Assurance (COSO)<br>Detect (NIST CSF)  | [S3.C133]<br>Verify CloudWatch is enabled for all Object Lambda access points   | Create an Object Lambda access point without CloudWatch enabled, it should be detected.  | Low  | S3.FC32 | -               | Low    |

## Deploy only authorized S3 website and behind a CDN

| Type                                    | Control   | Testing   | Effort | Feature Class(es) | Threat(s) and Impact                   | CVSS-weighted Priority |
|---|---|---|--------|-------------------|--|------------------------|
| Directive (COSO)<br>Identify (NIST CSF) | [S3.C141]<br>Maintain a list of authorized buckets to be configured as website  | Request the list of authorized buckets to be configured as website, its review process, and its review records  | Low    | S3.FC16           | S3.T13 (Very Low)<br>S3.T29 (Very Low) | Medium                 |
| Directive (COSO)<br>Protect (NIST CSF)  | [S3.C142, depends on S3.C141, assured by S3.C143]<br>Ensure only authorized buckets are configured as website                             | Request 1) the mechanism ensuring only authorized buckets are configured as website, 2) its records of execution for all new website-enabled buckets, and 3) plan to move any older website-enabled buckets | Medium | S3.FC16           | S3.T13 (Medium)<br>S3.T29 (Medium)     | Medium                 |
| Assurance (COSO)<br>Detect (NIST CSF)   | [S3.C143]<br>Verify only authorized buckets are configured as website   | Enable website configuration on an unauthorized bucket, it should be detected.  | Medium | S3.FC16           | -                                      | Medium                 |
| Directive (COSO)<br>Protect (NIST CSF)  | [S3.C144, depends on S3.C141]<br>Ensure S3 websites are protected with HTTP headers ( <a href="#">ref</a> ) using a CDN (e.g. CloudFront) | Request the mechanism ensuring S3 websites are protected with HTTP headers  | Medium | S3.FC16           | S3.T13 (High)<br>S3.T29 (Very High)    | High                   |

## Use unguessable naming convention

| Type                                   | Control  | Testing  | Effort | Feature Class(es) | Threat(s) and Impact | CVSS-weighted Priority |
|--|--|--|--------|-------------------|----------------------|------------------------|
| Directive (COSO)<br>Protect (NIST CSF) | [S3.C29]<br>Use unguessable naming convention for the email addresses of your AWS accounts (e.g. add a + sign and a random string to redirect the email in the same mailbox) | Review naming convention for root account email and their implementation | Medium | S3.FC28           | S3.T19 (High)        | Low                    |
| Directive (COSO)<br>Protect (NIST CSF) | [S3.C30]<br>Use unguessable naming convention for your IAM users and IAM roles (e.g. add a random string)  | Review naming convention for IAM users/role and their implementation     | Medium | S3.FC28           | S3.T24 (High)        | Low                    |

## Disabling ACLs for all buckets

| Type                                      | Control  | Testing   | Effort | Feature Class(es)                                | Threat(s) and Impact   | CVSS-weighted Priority |
|---|--|---|--------|--|--|------------------------|
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C152, assured by S3.C154]<br>Ensure bucket ACL and object ACL are disabled on each bucket  | Request 1) the mechanism ensuring bucket ACL and object ACL are disabled on each bucket, 2) its records of execution for all new buckets, and 3) plan to move any older buckets | Medium | S3.FC1<br>S3.FC24<br>S3.FC25<br>S3.FC5<br>S3.FC8 | S3.T4 (Very High)<br>S3.T6 (Very High)<br>S3.T36 (Very High)<br>S3.T43 (Very High)<br>S3.T52 (Very High)<br>S3.T53 (Very High) | High                   |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C153]<br>Prevent the creation of buckets with ACL enabled (e.g. by using a SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note it does not block someone to enable ACL afterwards via PutPutBucketOwnershipControls. | Create a bucket to enable ACL, it should be denied.   | Low    | S3.FC1<br>S3.FC24<br>S3.FC25<br>S3.FC5<br>S3.FC8 | S3.T4 (High)<br>S3.T6 (High)<br>S3.T36 (High)<br>S3.T43 (High)<br>S3.T52 (High)<br>S3.T53 (High)                               | High                   |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C154]<br>Verify bucket ACL and object ACL are disabled on each bucket  | Create/modify a bucket to enable ACL, it should be detected.  | Medium | S3.FC1<br>S3.FC24<br>S3.FC25<br>S3.FC5<br>S3.FC8 | -  | High                   |

# Compliance Mapping

## PCI DSS v3.2

| PCI DSS v3.2  | Control Objectives  | Controls   |                  |   |         |          |
|---|---|--|------------------|---|---------|----------|
|   |   | Very High  | High             | Medium  | Low     | Very Low |
| 1.1<br>1.1.1<br>1.1.2<br>1.1.3<br>1.1.4<br>1.1.5<br>1.1.6<br>1.1.7<br>1.2<br>1.2.1<br>1.2.2<br>1.2.3<br>1.3 | [S3.CO13] Block direct public access<br>[S3.CO30] Control CloudFront access   | S3.C49<br>S3.C50<br>S3.C51<br>S3.C52<br>S3.C53<br>S3.C54 | -                | S3.C47<br>S3.C48<br>S3.C101<br>S3.C102<br>S3.C137 | S3.C83  | -        |
| 1.3.1<br>1.3.2  | [S3.CO13] Block direct public access  | S3.C49<br>S3.C50<br>S3.C51<br>S3.C52<br>S3.C53<br>S3.C54 | -                | S3.C47<br>S3.C48                                  | S3.C83  | -        |
| 1.3.3   | [S3.CO13] Block direct public access<br>[S3.CO30] Control CloudFront access   | S3.C49<br>S3.C50<br>S3.C51<br>S3.C52<br>S3.C53<br>S3.C54 | -                | S3.C47<br>S3.C48<br>S3.C101<br>S3.C102<br>S3.C137 | S3.C83  | -        |
| 1.3.4   | [S3.CO13] Block direct public access  | S3.C49<br>S3.C50<br>S3.C51<br>S3.C52<br>S3.C53<br>S3.C54 | -                | S3.C47<br>S3.C48                                  | S3.C83  | -        |
| 1.3.5<br>1.3.6  | [S3.CO5] Identify and ensure the protection all external buckets hosting your objects<br>[S3.CO15] Identify and ensure the protection all internal buckets hosting your objects | -  | S3.C11<br>S3.C15 | S3.C12<br>S3.C13                                  | S3.C115 | S3.C60   |

|  |   |   |                  |                             |                                       |                             |
|--|---|---|------------------|-----------------------------|---------------------------------------|-----------------------------|
| 1.3.7  |   |   | S3.C58           | S3.C14<br>S3.C114<br>S3.C59 |                                       |                             |
| 2.1<br>2.1.1   | [S3.CO16] Enforce encryption-at-rest<br>[S3.CO18] Encrypt or tokenize critical data   | S3.C61<br>S3.C64<br>S3.C65<br>S3.C66<br>S3.C67<br>S3.C145<br>S3.C146<br>S3.C147 | -                | S3.C62<br>S3.C140<br>S3.C72 | S3.C63<br>S3.C68<br>S3.C148           | -                           |
| 2.2.3  | [S3.CO9] Block requests with KMS keys from unauthorized AWS account(s)<br>[S3.CO16] Enforce encryption-at-rest<br>[S3.CO18] Encrypt or tokenize critical data | S3.C61<br>S3.C64<br>S3.C65<br>S3.C66<br>S3.C67<br>S3.C145<br>S3.C146<br>S3.C147 | S3.C31<br>S3.C32 | S3.C62<br>S3.C140<br>S3.C72 | S3.C33<br>S3.C63<br>S3.C68<br>S3.C148 | -                           |
| 3.5<br>3.5.1<br>3.5.2<br>3.5.3<br>3.5.4<br>3.6<br>3.6.1<br>3.6.2<br>3.6.3<br>3.6.4<br>3.6.5<br>3.6.6<br>3.6.7<br>3.6.8 | [S3.CO16] Enforce encryption-at-rest<br>[S3.CO18] Encrypt or tokenize critical data   | S3.C61<br>S3.C64<br>S3.C65<br>S3.C66<br>S3.C67<br>S3.C145<br>S3.C146<br>S3.C147 | -                | S3.C62<br>S3.C140<br>S3.C72 | S3.C63<br>S3.C68<br>S3.C148           | -                           |
| 4.1  | [S3.CO26] Scan input/output objects for malware   | -   | -                | S3.C93                      | -                                     | -                           |
| 5.1<br>5.1.1<br>5.1.2<br>5.2<br>5.3<br>5.4   | [S3.CO27] Control event receivers<br>[S3.CO28] Control where the inventory is stored  | -   | -                | -                           | S3.C94<br>S3.C95<br>S3.C135           | S3.C96<br>S3.C97<br>S3.C136 |
| 6.4  | [S3.CO12] Enforce good coding practice  | -   | -                | S3.C46                      | S3.C41                                | S3.C43                      |

|   |   |   |   |   |  |        |   |
|---|---|---|---|---|--|--------|---|
| 6.4.1   |   |   |   | S3.C113   | S3.C42   | S3.C45 |   |
| 6.4.2   |   |   |   | S3.C44  |  |        |   |
| 6.4.3   |   |   |   |   |  |        |   |
| 6.4.4   |   |   |   |   |  |        |   |
| 6.4.5   |   |   |   |   |  |        |   |
| 6.4.5.1   |   |   |   |   |  |        |   |
| 6.4.5.2   |   |   |   |   |  |        |   |
| 6.4.5.3   |   |   |   |   |  |        |   |
| 6.4.5.4   |   |   |   |   |  |        |   |
| 6.4.6   |   |   |   |   |  |        |   |
| 6.6   | [S3.CO8] Limit the access to the IAM actions required to execute the threats<br>[S3.CO10] Block changes to make an object public via object ACL<br>[S3.CO13] Block direct public access<br>[S3.CO33] Control IAM roles used for Batch<br>[S3.CO34] Enforce only authorized Object Lambda access point and associated access<br>[S3.CO35] Deploy only authorized S3 website and behind a CDN<br>[S3.CO37] Disabling ACLs for all buckets | S3.C149<br>S3.C150<br>S3.C151<br>S3.C49<br>S3.C50<br>S3.C51<br>S3.C52<br>S3.C53<br>S3.C54 | S3.C26<br>S3.C28<br>S3.C47<br>S3.C48<br>S3.C120<br>S3.C121<br>S3.C122<br>S3.C123<br>S3.C125<br>S3.C126<br>S3.C127<br>S3.C129<br>S3.C144<br>S3.C145<br>S3.C152<br>S3.C153<br>S3.C154 | S3.C27<br>S3.C34<br>S3.C36<br>S3.C48<br>S3.C121<br>S3.C122<br>S3.C123<br>S3.C139<br>S3.C125<br>S3.C126<br>S3.C127<br>S3.C129<br>S3.C130<br>S3.C141<br>S3.C142<br>S3.C143            | S3.C35<br>S3.C37<br>S3.C83<br>S3.C132<br>S3.C133 | -      |   |
| 7.1<br>7.1.1<br>7.1.2<br>7.1.3<br>7.1.4<br>7.2<br>7.2.1 | [S3.CO13] Block direct public access  | S3.C49<br>S3.C50<br>S3.C51<br>S3.C52<br>S3.C53<br>S3.C54                                  | S3.C49<br>S3.C50<br>S3.C51<br>S3.C52<br>S3.C53<br>S3.C54  | -   | S3.C47<br>S3.C48                                 | S3.C83 | - |
| 7.2.2   | [S3.CO8] Limit the access to the IAM actions required to execute the threats<br>[S3.CO10] Block changes to make an object public via object ACL<br>[S3.CO13] Block direct public access<br>[S3.CO33] Control IAM roles used for Batch<br>[S3.CO34] Enforce only authorized Object Lambda access point and associated access<br>[S3.CO35] Deploy only authorized S3 website and behind a CDN<br>[S3.CO37] Disabling ACLs for all buckets | S3.C149<br>S3.C150<br>S3.C151<br>S3.C49<br>S3.C50<br>S3.C51<br>S3.C52<br>S3.C53<br>S3.C54 | S3.C26<br>S3.C28<br>S3.C36<br>S3.C47<br>S3.C120<br>S3.C121<br>S3.C122<br>S3.C123<br>S3.C125<br>S3.C126<br>S3.C127<br>S3.C129<br>S3.C144<br>S3.C145<br>S3.C152<br>S3.C153<br>S3.C154 | S3.C27<br>S3.C34<br>S3.C36<br>S3.C48<br>S3.C120<br>S3.C121<br>S3.C122<br>S3.C123<br>S3.C125<br>S3.C126<br>S3.C127<br>S3.C129<br>S3.C130<br>S3.C131<br>S3.C141<br>S3.C142<br>S3.C143 | S3.C35<br>S3.C37<br>S3.C83<br>S3.C132<br>S3.C133 | -      |   |

|  |  |   |   |  |  |  |
|--|--|---|---|--|--|--|
|  |  |   |   | S3.C142<br>S3.C143   |  |  |
| 7.2.3  | [S3.CO5] Identify and ensure the protection all external buckets hosting your objects<br>[S3.CO15] Identify and ensure the protection all internal buckets hosting your objects  | -   | S3.C11<br>S3.C15<br>S3.C14<br>S3.C58<br>S3.C59  | S3.C12<br>S3.C13<br>S3.C14<br>S3.C114<br>S3.C59  | S3.C115  | S3.C60   |
| 8.1.2  | [S3.CO1] Enforce encryption-in-transit   | -   | S3.C1<br>S3.C2<br>S3.C6<br>S3.C7<br>S3.C119   | S3.C3<br>S3.C5   | S3.C4  | -  |
| 8.1.5  | [S3.CO5] Identify and ensure the protection all external buckets hosting your objects<br>[S3.CO15] Identify and ensure the protection all internal buckets hosting your objects  | -   | S3.C11<br>S3.C15<br>S3.C58  | S3.C12<br>S3.C13<br>S3.C14<br>S3.C114<br>S3.C59  | S3.C115  | S3.C60   |
| 8.2<br>8.2.1<br>8.2.2<br>8.2.3<br>8.2.4<br>8.2.5<br>8.2.6<br>8.3 | [S3.CO8] Limit the access to the IAM actions required to execute the threats<br>[S3.CO10] Block changes to make an object public via object ACL<br>[S3.CO13] Block direct public access<br>[S3.CO33] Control IAM roles used for Batch<br>[S3.CO34] Enforce only authorized Object Lambda access point and associated access<br>[S3.CO35] Deploy only authorized S3 website and behind a CDN<br>[S3.CO37] Disabling ACLs for all buckets  | S3.C149<br>S3.C150<br>S3.C151<br>S3.C49<br>S3.C50<br>S3.C51<br>S3.C52<br>S3.C53<br>S3.C54 | S3.C26<br>S3.C34<br>S3.C36<br>S3.C47<br>S3.C120<br>S3.C122<br>S3.C123<br>S3.C125<br>S3.C126<br>S3.C127<br>S3.C129<br>S3.C144<br>S3.C130<br>S3.C152<br>S3.C153<br>S3.C154                    | S3.C27<br>S3.C28<br>S3.C47<br>S3.C48<br>S3.C121<br>S3.C123<br>S3.C139<br>S3.C137<br>S3.C128<br>S3.C129<br>S3.C127<br>S3.C130<br>S3.C131<br>S3.C141<br>S3.C142<br>S3.C143 | S3.C35<br>S3.C37<br>S3.C83<br>S3.C132<br>S3.C133                                 | -  |
| 8.7  | [S3.CO7] Limit and monitor access via S3 VPC endpoints<br>[S3.CO8] Limit the access to the IAM actions required to execute the threats<br>[S3.CO11] Prevent deletion of buckets<br>[S3.CO14] Block bucket ACL except for server access logging<br>[S3.CO22] Block deprecated actions<br>[S3.CO23] Block all requests not using SigV4<br>[S3.CO24] Block all requests not using HTTP authorization header, if not explicitly authorized<br>[S3.CO25] Restrict bucket replication<br>[S3.CO29] Limit access from only authorized VPCs<br>[S3.CO32] Restrict access point access to VPC when in use<br>[S3.CO33] Control IAM roles used for Batch | S3.C149<br>S3.C150<br>S3.C151   | S3.C17<br>S3.C19<br>S3.C20<br>S3.C24<br>S3.C26<br>S3.C27<br>S3.C38<br>S3.C28<br>S3.C39<br>S3.C84<br>S3.C55<br>S3.C86<br>S3.C57<br>S3.C87<br>S3.C98<br>S3.C88<br>S3.C99<br>S3.C89<br>S3.C100 | S3.C22<br>S3.C23<br>S3.C24<br>S3.C27<br>S3.C28<br>S3.C28<br>S3.C27<br>S3.C28<br>S3.C84<br>S3.C56<br>S3.C81<br>S3.C116<br>S3.C132<br>S3.C133                              | S3.C18<br>S3.C25<br>S3.C124<br>S3.C56<br>S3.C81<br>S3.C116<br>S3.C132<br>S3.C133 | S3.C21<br>S3.C40<br>S3.C80<br>S3.C82<br>S3.C85 |

|        |  |                               |  |  |                               |   |
|--------|--|-------------------------------|--|--|-------------------------------|---|
|        | [S3.CO34] Enforce only authorized Object Lambda access point and associated access<br>[S3.CO35] Deploy only authorized S3 website and behind a CDN<br>[S3.CO37] Disabling ACLs for all buckets   |                               | S3.C105<br>S3.C106<br>S3.C107<br>S3.C108<br>S3.C109<br>S3.C110<br>S3.C111<br>S3.C112<br>S3.C120<br>S3.C122<br>S3.C125<br>S3.C126<br>S3.C127<br>S3.C144<br>S3.C152<br>S3.C153<br>S3.C154                        | S3.C91<br>S3.C92<br>S3.C117<br>S3.C134<br>S3.C138<br>S3.C104<br>S3.C121<br>S3.C123<br>S3.C139<br>S3.C128<br>S3.C129<br>S3.C130<br>S3.C131<br>S3.C141<br>S3.C142<br>S3.C143<br>S3.C143                        |                               |   |
| 8.18.4 | [S3.CO3] Enable CloudTrail S3 data events<br>[S3.CO4] Monitor S3 with Amazon GuardDuty and Macie<br>[S3.CO17] Protect primary data against loss<br>[S3.CO25] Restrict bucket replication   | -                             | S3.C118<br>S3.C69<br>S3.C70  | S3.C9<br>S3.C10<br>S3.C71<br>S3.C86<br>S3.C87<br>S3.C88<br>S3.C89<br>S3.C90<br>S3.C91<br>S3.C92<br>S3.C117<br>S3.C134<br>S3.C138   | S3.C116                       | - |
| 10.1   | [S3.CO3] Enable CloudTrail S3 data events<br>[S3.CO4] Monitor S3 with Amazon GuardDuty and Macie<br>[S3.CO8] Limit the access to the IAM actions required to execute the threats<br>[S3.CO17] Protect primary data against loss<br>[S3.CO25] Restrict bucket replication<br>[S3.CO29] Limit access from only authorized VPCs<br>[S3.CO33] Control IAM roles used for Batch<br>[S3.CO34] Enforce only authorized Object Lambda access point and associated access<br>[S3.CO35] Deploy only authorized S3 website and behind a CDN | S3.C149<br>S3.C150<br>S3.C151 | S3.C118<br>S3.C26<br>S3.C69<br>S3.C70<br>S3.C71<br>S3.C98<br>S3.C86<br>S3.C99<br>S3.C87<br>S3.C100<br>S3.C120<br>S3.C122<br>S3.C128<br>S3.C89<br>S3.C90<br>S3.C125<br>S3.C126<br>S3.C127<br>S3.C144<br>S3.C133 | S3.C9<br>S3.C10<br>S3.C27<br>S3.C28<br>S3.C71<br>S3.C71<br>S3.C98<br>S3.C86<br>S3.C87<br>S3.C87<br>S3.C100<br>S3.C120<br>S3.C122<br>S3.C122<br>S3.C90<br>S3.C125<br>S3.C126<br>S3.C127<br>S3.C144<br>S3.C133 | S3.C116<br>S3.C132<br>S3.C133 | - |

|  |   |  |                               |   |   |                   |   |
|--|---|--|-------------------------------|---|---|-------------------|---|
|  |   |  |                               | S3.C138<br>S3.C121<br>S3.C123<br>S3.C139<br>S3.C128<br>S3.C129<br>S3.C130<br>S3.C131<br>S3.C141<br>S3.C142<br>S3.C143                       |   |                   |   |
| 10.2<br>10.2.1<br>10.2.2<br>10.2.3<br>10.2.4<br>10.2.5<br>10.2.6<br>10.2.7 | [S3.CO3] Enable CloudTrail S3 data events<br>[S3.CO4] Monitor S3 with Amazon GuardDuty and Macie<br>[S3.CO17] Protect primary data against loss<br>[S3.CO25] Restrict bucket replication  |  | -                             | S3.C118<br>S3.C88<br>S3.C69<br>S3.C70   | S3.C9<br>S3.C10<br>S3.C71<br>S3.C86<br>S3.C87<br>S3.C88<br>S3.C89<br>S3.C90<br>S3.C91<br>S3.C92<br>S3.C117<br>S3.C134<br>S3.C138  | S3.C116<br>-      |   |
| 10.3<br>10.3.1<br>10.3.2<br>10.3.3<br>10.3.4<br>10.3.5<br>10.3.6           | [S3.CO3] Enable CloudTrail S3 data events<br>[S3.CO4] Monitor S3 with Amazon GuardDuty and Macie<br>[S3.CO8] Limit the access to the IAM actions required to execute the threats<br>[S3.CO11] Prevent deletion of buckets<br>[S3.CO17] Protect primary data against loss<br>[S3.CO25] Restrict bucket replication<br>[S3.CO33] Control IAM roles used for Batch |  | S3.C149<br>S3.C150<br>S3.C151 | S3.C118<br>S3.C86<br>S3.C26<br>S3.C87<br>S3.C38<br>S3.C88<br>S3.C39<br>S3.C89<br>S3.C69<br>S3.C90<br>S3.C70<br>S3.C91<br>S3.C120<br>S3.C122 | S3.C9<br>S3.C10<br>S3.C27<br>S3.C28<br>S3.C71<br>S3.C86<br>S3.C26<br>S3.C87<br>S3.C38<br>S3.C88<br>S3.C39<br>S3.C89<br>S3.C69<br>S3.C90<br>S3.C70<br>S3.C91<br>S3.C120<br>S3.C122 | S3.C116<br>S3.C40 |   |
| 10.5   | [S3.CO3] Enable CloudTrail S3 data events   |  | -                             | S3.C118   | S3.C9   | S3.C116           | - |

|        |   |  |   |         |        |   |
|--------|---|--|---|---------|--------|---|
| 10.5.1 | [S3.CO4] Monitor S3 with Amazon GuardDuty and Macie         |  |   | S3.C10  |        |   |
| 10.5.2 | [S3.CO25] Restrict bucket replication                       |  |   | S3.C86  |        |   |
| 10.5.3 |   |  |   | S3.C87  |        |   |
| 10.5.4 |   |  |   | S3.C88  |        |   |
| 10.5.5 |   |  |   | S3.C89  |        |   |
|        |   |  |   | S3.C90  |        |   |
|        |   |  |   | S3.C91  |        |   |
|        |   |  |   | S3.C92  |        |   |
|        |   |  |   | S3.C117 |        |   |
|        |   |  |   | S3.C134 |        |   |
|        |   |  |   | S3.C138 |        |   |
| 10.6   |   |  |   |         |        |   |
| 10.6.1 |   |  |   | S3.C1   |        |   |
| 10.6.2 |   |  |   | S3.C2   |        |   |
| 10.6.3 |   |  |   | S3.C6   |        |   |
| 10.8   | [S3.CO1] Enforce encryption-in-transit                      |  |   | S3.C7   |        |   |
| 10.8.1 |   |  |   | S3.C119 |        |   |
| 11.1   |   |  |   |         | S3.C3  |   |
| 11.5   |   |  |   |         | S3.C5  |   |
| 11.5.1 |   |  |   |         | S3.C4  | - |
| 12.3.8 | [S3.CO6] Model the threats on all AWS services accessing S3 |  | - |         | S3.C16 | - |
| 12.3.9 |   |  |   |         |        | - |

The Control Objectives are mapped to the [Secure Controls Framework](#) (SCF), provided under Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0). Compliance mappings are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

You can change the displayed Compliance mappings by contacting [chatbot@trustoncloud.com](mailto:chatbot@trustoncloud.com).

# Appendices

## Appendix 1 - Prioritized list for control implementation

| Type                                      | Control  | Testing   | Effort   | Feature Class(es)                       | Threat(s) and Impact   | CVSS-weighted Priority |
|---|--|---|----------|---|--|------------------------|
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C149]<br>For each bucket, maintain a list of authorized IAM principals allowed to access via bucket policy   | Request the list of authorized IAM principals allowed to access via bucket policy, its review process, and its review records   | Medium   | S3.FC10                                 | S3.T37 (Very Low)  | Very High              |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C150, depends on S3.C149, assured by S3.C151]<br>Ensure only authorized IAM principals allowed to access via bucket policy are configured (e.g. using IAM Access Analyzer for the reconciliation)  | Request 1) the mechanism ensuring only authorized IAM principals allowed to access via bucket policy are configured, 2) its records of execution for all new buckets, and 3) plan to move any older buckets | Medium   | S3.FC10                                 | S3.T37 (Very High)   | Very High              |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C151]<br>Verify only authorized IAM principals allowed to access via bucket policy are used (e.g. using the AWS Config rule <a href="#">S3 BUCKET POLICY GRANTEE CHECK</a> )   | Allow an unauthorized IAM principal on a bucket policy, it should be detected.  | Medium   | S3.FC10                                 | -  | Very High              |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C49, assured by S3.C50]<br>Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.  | 1) Create a public bucket and try to access one of its objects without proper authentication, or 2) change the ACL of an existing object to public, it should be denied.                                    | Very Low | S3.FC10<br>S3.FC5<br>S3.FC8             | S3.T4 (High)<br>S3.T14 (High)<br>S3.T36 (Very High)<br>S3.T37 (Very High)<br>S3.T38 (Medium) | Very High              |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C50]<br>Verify account-level S3 Block Public Access is enabled on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (e.g. using the AWS Config rule: <a href="#">S3 ACCOUNT LEVEL PUBLIC ACCESS BLOCKS</a> ). | Remove the account-level S3 Block Public Access, it should be detected  | Very Low | S3.FC10<br>S3.FC5<br>S3.FC8             | -  | Very High              |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C51, assured by S3.C52]<br>Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.  | 1) Create a public bucket and try to access one of its objects without proper authentication, and 2) change the ACL of an existing object to public, it should be denied.                                   | Low      | S3.FC10<br>S3.FC5<br>S3.FC8             | S3.T4 (High)<br>S3.T14 (High)<br>S3.T36 (Very High)<br>S3.T37 (Very High)<br>S3.T38 (Medium) | Very High              |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C52]<br>Verify S3 Block Public Access is enabled on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (e.g. using the AWS Config rule: <a href="#">S3 BUCKET LEVEL PUBLIC ACCESS PROHIBITED</a> ).              | Remove a S3 Block Public Access of an S3 bucket, it should be detected  | Very Low | S3.FC10<br>S3.FC5<br>S3.FC8             | -  | Very High              |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C53, assured by S3.C54]<br>Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls,   | 1) Create a public bucket and try to access via access point one of its objects without proper authentication ( <a href="#">ref</a> ), or 2) change the ACL of an existing object to public and try to      | Low      | S3.FC10<br>S3.FC26<br>S3.FC33<br>S3.FC5 | S3.T14 (High)<br>S3.T36 (Medium)<br>S3.T37 (Medium)<br>S3.T38 (Medium)                       | Very High              |

|  |  |  |        |   |   |           |
|--|--|--|--------|---|---|-----------|
|  | IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.  | access via access point one of its objects, it should be denied.   |        |   | S3.T54 (High)<br>S3.T55 (High)  |           |
| Assurance (coso) Detect (NIST CSF)     | [S3.C54]<br>Verify S3 Block Public Access is enabled on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.   | Remove S3 Block Public Access of 1) an access point, and 2) a multi-region access point, it should be detected   | Medium | S3.FC10<br>S3.FC26<br>S3.FC33<br>S3.FC5 | -   | Very High |
| Directive (coso) Identify (NIST CSF)   | [S3.C61]<br>Maintain a list of authorized KMS key(s) for each bucket, and their default encryption key. You might simplify by using only 1 key per bucket, ideally dedicated. Note that S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ).   | Request the list of authorized KMS key(s) for each bucket, its review process, and its review records  | Medium | S3.FC10<br>S3.FC5                       | S3.T11 (Very Low)<br>S3.T16 (Very Low)<br>S3.T17 (Very Low)<br>S3.T20 (Very Low)<br>S3.T30 (Very Low)<br>S3.T36 (Very Low)<br>S3.T37 (Very Low) | Very High |
| Directive (coso) Protect (NIST CSF)    | [S3.C64, depends on S3.C61, assured by S3.C65]<br>Implement an authorized default encryption key on each bucket and enable S3 Bucket Key (note: Amazon S3 evaluates and applies bucket policies before applying bucket default encryption settings)  | Request 1) the mechanism implementing an authorized default encryption key on each bucket and enabling S3 Bucket Key, 2) its records of execution for all new buckets, and 3) plan to move any older buckets | Low    | S3.FC10<br>S3.FC5                       | S3.T17 (Medium)<br>S3.T20 (High)<br>S3.T36 (High)<br>S3.T37 (High)  | Very High |
| Assurance (coso) Detect (NIST CSF)     | [S3.C65]<br>Verify each bucket has an authorized default encryption key and has S3 Bucket Key enabled  | Create/modify a bucket 1) without default encryption, 2) with a wrong default encryption key or 3) without S3 Bucket Key disabled, it should be detected.  | Medium | S3.FC10<br>S3.FC5                       | -   | Very High |
| Preventative (coso) Protect (NIST CSF) | [S3.C66, depends on S3.C61, assured by S3.C67]<br>Block PutObject requests with unauthorized KMS key on each bucket (e.g. using an S3 bucket policy deny statement on PutObject if the condition if exists "s3:x-amz-server-side-encryption-aws-kms-key-id" is not an authorized KMS key)  | Make a request encrypted with an unauthorized KMS key, it should be denied   | Low    | S3.FC10<br>S3.FC5                       | S3.T11 (High)<br>S3.T16 (High)<br>S3.T17 (High)<br>S3.T20 (Very High)<br>S3.T30 (High)<br>S3.T36 (High)<br>S3.T37 (High)                        | Very High |
| Assurance (coso) Detect (NIST CSF)     | [S3.C67]<br>Verify all buckets block PutObject requests with an unauthorized KMS key (e.g. using the Config rule: <a href="#">S3 BUCKET POLICY NOT MORE PERMISSIVE</a> , note that a new rule needs be deployed for each configuration, then the resource tracked by name or tag; alternatively you might use <a href="#">S3 BUCKET SERVER SIDE ENCRYPTION ENABLED</a> to ensure a limited coverage) | Create a bucket not blocking PutObject requests with an unauthorized KMS key, it should be detected.   | Medium | S3.FC10<br>S3.FC5                       | -   | Very High |
| Directive (coso) Identify (NIST CSF)   | [S3.C145]<br>Maintain a list of buckets (or paths) required to be encrypted with server-side encryption with customer-provided keys (SSE-C)  | Request the list of buckets (or paths) required to be encrypted with server-side encryption with customer-provided keys (SSE-C), its review process, and its review records                                  | Medium | S3.FC10<br>S3.FC5                       | S3.T11 (Very Low)<br>S3.T16 (Very Low)<br>S3.T20 (Very Low)<br>S3.T30 (Very Low)<br>S3.T36 (Very Low)<br>S3.T37 (Very Low)                      | Very High |

|   |  |   |          |                                       |   |           |
|---|--|---|----------|---------------------------------------|---|-----------|
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C146, depends on S3.C145, assured by S3.C147]<br>For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g. using an S3 bucket policy deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present)  | Make a request to a bucket (or path) requiring SSE-C without the proper encryption, it should be denied   | Low      | S3.FC10<br>S3.FC5                     | S3.T11 (High)<br>S3.T16 (High)<br>S3.T20 (Very High)<br>S3.T30 (High)<br>S3.T36 (High)<br>S3.T37 (High) | Very High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C147]<br>For buckets (or paths) requiring SSE-C, verify all buckets block PutObject requests with unauthorized encryption  | Create a bucket requiring SSE-C not blocking PutObject requests with unauthorized encryption, it should be detected.                                      | High     | S3.FC10<br>S3.FC5                     | -   | Very High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C1, depends on S3.C119, assured by S3.C2]<br>Block all unencrypted requests and unauthorized TLS version(s) from IAM entities you control (e.g. by denying all unencrypted request with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != authorized TLS version(s), using an SCP on your AWS Organization root node)  | Make an unencrypted S3 API call, it should be denied.   | Low      | S3.FC1<br>S3.FC5                      | S3.T12 (Very High)<br>S3.T34 (High)   | High      |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C2]<br>Verify the control blocking unencrypted requests and unauthorized TLS version(s) from IAM entities you control (e.g. an SCP on your AWS Organizations root node) is properly implemented  | Remove the control blocking unencrypted requests and unauthorized TLS version(s) (e.g. the SCP on your root node), it should be detected.                 | High     | S3.FC1<br>S3.FC5                      | -   | High      |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C6, depends on S3.C119, assured by S3.C7]<br>Block all unencrypted requests to S3 bucket you control (e.g. by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != authorized TLS version(s), on the S3 bucket policy)  | Make an unencrypted AWS API call to a bucket you control, it should be denied.  | Low      | S3.FC5                                | S3.T34 (Very High)  | High      |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C7]<br>Verify all S3 bucket policies block unencrypted traffic (e.g. using the AWS Config rule:<br><a href="#">S3_BUCKET_SSL_REQUESTS_ONLY</a> ) and unauthorized version(s) of TLS.   | Remove the statement on a S3 bucket policy 1) denying all unencrypted requests and 2) denying unauthorized TLS versions, it should be detected.           | Medium   | S3.FC5                                | -   | High      |
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C119]<br>Maintain a list of authorized version(s) of TLS/SSL per bucket (or per account/OU/Org)  | Request the list of authorized version(s) of TLS/SSL per bucket (or per account/OU/Org), its review mechanism and associated records                      | Low      | S3.FC1                                | S3.T12 (Very Low)   | High      |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C8]<br>Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g. firewalls, or cloud interception proxy like <a href="#">Kivera</a> ) including via Internet Gateway, to force usage of VPC endpoints. It will block data-plane transfer. Note: AWS console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com"). | Request the evidence of the implementation of blocking S3 endpoints in your corporate perimeter security (e.g. firewalls) and tests of its effectiveness. | Low      | S3.FC1<br>S3.FC28<br>S3.FC5<br>S3.FC7 | S3.T7 (High)<br>S3.T10 (High)<br>S3.T12 (Low)<br>S3.T18 (Medium)<br>S3.T34 (Very High)                  | High      |
| Directive (coso)<br>Detect (NIST CSF)     | [S3.C118]  | Request the Macie ThreatModel and the evidence of its application for enabling and protecting S3 policy findings  | Very Low | S3.FC10<br>S3.FC15<br>S3.FC5          | S3.T2 (Medium)<br>S3.T4 (Medium)<br>S3.T22 (Medium)   | High      |

|   |   |   |        |   |   |      |
|---|---|---|--------|---|---|------|
|   | Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect it using Macie ThreatModel  |   |        | S3.FC8  | S3.T36 (Medium)<br>S3.T37 (Medium)<br>S3.T38 (Medium)   |      |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C11]<br>Track all buckets you don't control hosting your objects, define their authorized data classification, identify their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), and get assured for the protection (e.g. through contractual agreement, verified by assurance programs, or using this ThreatModel).     | Request the list of all authorized external buckets authorized to host your objects, their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), their data classification and the mechanism used to ensure the security of those buckets | Medium | S3.FC1<br>S3.FC16<br>S3.FC5   | S3.T3 (High)<br>S3.T5 (Very Low)<br>S3.T6 (Low)<br>S3.T7 (Very Low)<br>S3.T8 (Very Low)<br>S3.T9 (Very Low)<br>S3.T11 (Low)<br>S3.T14 (Very Low)<br>S3.T15 (Very Low)<br>S3.T21 (Very Low)<br>S3.T31 (High)<br>S3.T43 (Very High) | High |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C15]<br>Request access via S3 access point on bucket you don't own, if compatible with your interaction with the bucket (e.g. not through not-compatible AWS service)   | Request the documented reason access point was not implemented in the use case  | Low    | S3.FC1  | S3.T8 (Medium)<br>S3.T9 (Medium)<br>S3.T31 (Very High)  | High |
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C17]<br>For each VPC, maintain a list of AWS Organizations, OU and/or AWS account(s), where IAM entities are authorized to access S3  | For each VPC, request the list of AWS Organizations, OU and/or AWS account(s), where IAM entities are authorized to access S3, its review process, and its review records   | Medium | S3.FC1<br>S3.FC5  | S3.T9 (Very Low)<br>S3.T11 (very Low)   | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C19, depends on S3.C17, assured by S3.C20]<br>Block any IAM entity not belonging to an authorized AWS Organizations, OU and/or AWS account(s) to call S3 from your VPCs by adding a deny statement on S3 VPC endpoint policy of each VPC, with the condition using "aws:PrincipalOrgPaths" ( <a href="#">ref</a> ) including the full Org ID, as those are globally unique. | For each VPC, do an API call with an IAM entity which is not part of its authorized AWS Organizations path(s), it should be denied.   | Low    | S3.FC1<br>S3.FC5  | S3.T9 (Very High)<br>S3.T11 (Very High)   | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C20]<br>Verify all S3 VPC endpoint are blocking any IAM entity not belonging to an authorized AWS Organizations, OU and/or AWS account(s)   | Remove the policy statement blocking any IAM entity not belonging to an authorized AWS Organizations, OU and/or AWS account(s) from the VPC endpoint, it should be detected.  | High   | S3.FC1<br>S3.FC5  | -   | High |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C26]<br>Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the usage of non-object-related S3 actions.   | Request the list of authorized IAM principals that have the permissions required to execute the threat actions, its review process, and its review records  | High   | S3.FC1<br>S3.FC10<br>S3.FC12<br>S3.FC13<br>S3.FC15<br>S3.FC19<br>S3.FC2<br>S3.FC20<br>S3.FC24<br>S3.FC25<br>S3.FC26 | S3.T1 (High)<br>S3.T2 (High)<br>S3.T5 (Low)<br>S3.T6 (Medium)<br>S3.T7 (High)<br>S3.T8 (High)<br>S3.T11 (High)<br>S3.T14 (Very High)<br>S3.T16 (High)<br>S3.T17 (Very High)<br>S3.T18 (High)                                      | High |

|   |  |   |        |   |   |      |
|---|--|---|--------|---|---|------|
|   |  |   |        | S3.FC27<br>S3.FC32<br>S3.FC33<br>S3.FC5<br>S3.FC6<br>S3.FC7<br>S3.FC8 | S3.T21 (Medium)<br>S3.T25 (High)<br>S3.T26 (High)<br>S3.T28 (High)<br>S3.T30 (High)<br>S3.T33 (Very High)<br>S3.T35 (Very High)<br>S3.T36 (Medium)<br>S3.T37 (Very High)<br>S3.T38 (Very High)<br>S3.T39 (High)<br>S3.T41 (High)<br>S3.T42 (High)<br>S3.T44 (High)<br>S3.T46 (High)<br>S3.T47 (High)<br>S3.T48 (High)<br>S3.T49 (High)<br>S3.T50 (High)<br>S3.T51 (High)<br>S3.T52 (High)<br>S3.T53 (High)<br>S3.T54 (High)<br>S3.T55 (High)<br>S3.T56 (High) |      |
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C31]<br>Maintain a list of authorized AWS accounts to provide KMS keys for S3 for each AWS account   | Request the list of authorized AWS accounts to provide KMS keys for S3 for each AWS account, its review process, and its review records | Medium | S3.FC1<br>S3.FC15<br>S3.FC26<br>S3.FC5<br>S3.FC8                      | S3.T1 (Very Low)<br>S3.T2 (Very Low)<br>S3.T4 (Very Low)<br>S3.T5 (Very Low)<br>S3.T7 (Very Low)<br>S3.T8 (Very Low)<br>S3.T9 (Very Low)<br>S3.T11 (Very Low)<br>S3.T16 (Very Low)<br>S3.T21 (Very Low)<br>S3.T27 (Very Low)<br>S3.T28 (Very Low)<br>S3.T30 (Very Low)<br>S3.T31 (Very Low)   | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C32, depends on S3.C31]<br>Block requests with unauthorized AWS account providing the KMS key (e.g. using an SCP, bucket policy and VPC endpoint deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS accounts) | Make a request encrypted with a KMS key from unauthorized AWS account, it should be denied  | Low    | S3.FC1<br>S3.FC15<br>S3.FC26<br>S3.FC5<br>S3.FC8                      | S3.T1 (High)<br>S3.T2 (Medium)<br>S3.T4 (High)<br>S3.T5 (High)<br>S3.T7 (High)<br>S3.T8 (High)  | High |

|   |  |   |        |                   |  |      |
|---|--|---|--------|-------------------|--|------|
|   |  |   |        |                   | S3.T9 (High)<br>S3.T11 (Medium)<br>S3.T16 (High)<br>S3.T21 (Medium)<br>S3.T27 (Low)<br>S3.T28 (High)<br>S3.T30 (High)<br>S3.T31 (High) |      |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C34, assured by S3.C36]<br>Deny requests to change object ACL to public (e.g. using an SCP, S3 bucket policy and VPC endpoint policy blocking PutObjectAcl for "s3:x-amz-grant-read", "s3:x-amz-grant-read-acp", "s3:x-amz-grant-write-acp", "s3:x-amz-grant-full-control" on the following predefined groups "http://acs.amazonaws.com/groups/global/AllUsers" and "http://acs.amazonaws.com/groups/global/AuthenticatedUsers") | Make a call to create a public ObjectACL, it should be denied.  | Medium | S3.FC1<br>S3.FC5  | S3.T6 (Very High)<br>S3.T36 (Very High)  | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C36]<br>Verify the control blocking change ObjectACL to public (e.g. an SCP and VPC endpoint policy) is properly implemented   | Remove the control blocking changes of ObjectACL to public, it should be detected.  | High   | S3.FC1<br>S3.FC5  | -  | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C38, assured by S3.C39]<br>Block the action "s3:DeleteBucket" (e.g. via SCP, exemption can be managed by authorizing a SuperAdmin to delete buckets with a certain tag, and with bucket owners able to tag bucket)   | Do a DeleteBucket, it should be denied  | Low    | S3.FC5            | S3.T1 (Very High)  | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C39]<br>Verify the control blocking the action "s3:DeleteBucket" (e.g. an SCP on your AWS Organizations root node) is properly implemented   | Remove the control blocking the action "s3:DeleteBucket" (e.g. an SCP on your root node), it should be detected.  | High   | S3.FC5            | -  | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C55, assured by S3.C57]<br>Deny requests to add bucket ACL other than for server access logging (e.g. using an SCP, bucket policy and VPC endpoint policy blocking PutBucketAcl for all but the following predefined group "http://acs.amazonaws.com/groups/s3/LogDelivery" using the IAM condition x-amz-acl: "log-delivery-write")   | Make a call to create a bucket ACL other than server access logging, it should be denied.   | Medium | S3.FC8            | S3.T4 (Very High)  | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C57]<br>Verify the control blocking bucket ACL changes other than for server access logging (e.g. an SCP, a bucket policy and VPC endpoint policy) is properly implemented   | Remove the control blocking bucket ACL changes other than for server access logging, it should be detected.   | High   | S3.FC8            | -  | High |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C58]<br>Track all buckets you control, define their authorized data classification, identify whether the hosted data is primary (i.e. source of truth, for example logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g. file-processing, software package, etc.), their WORM  | Request the list of all buckets you control, define their authorized data classification, identify whether the data is primary and the mechanism and records to ensure the accuracy of those metadata | High   | S3.FC13<br>S3.FC5 | S3.T11 (High)<br>S3.T17 (Very High)<br>S3.T25 (Low)  | High |

|   |  |   |          |                             |  |      |
|---|--|---|----------|-----------------------------|--|------|
|   | requirements (e.g. SEC 17a-4, CTCC, etc.), if they are production/non-production (preferably done at account-level), their storage class. You may use tags, Infra-as-code, AWS Glue Data Catalog or external management tool like <a href="#">FINRA herd</a> )   |   |          |                             |  |      |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C69, depends on S3.C58, assured by S3.C70]<br>Enable versioning on buckets holding primary data  | Request the mechanism used to ensure versioning on buckets holding primary data, and its records                                | Very Low | S3.FC5                      | S3.T16 (High)<br>S3.T17 (High)   | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C70]<br>Verify buckets holding primary data are versioned (e.g. using <a href="#">S3_BUCKET_VERSIONING_ENABLED</a> )   | Remove versioning from a bucket holding primary data, it should be detected   | Low      | S3.FC5                      | -  | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C74, depends on S3.C58, assured by S3.C75]<br>Implement the authorized default S3 Object Lock on each bucket (note: Amazon S3 evaluates and applies bucket policies before applying bucket default S3 Object Lock settings)  | Upload an object without appropriate S3 Object Lock, it should have the S3 Object Lock automatically.                           | Low      | S3.FC13<br>S3.FC5           | S3.T16 (High)<br>S3.T17 (High)<br>S3.T25 (High)  | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C75]<br>Verify all buckets have the correct default S3 Object Lock configuration   | Create a bucket 1) without S3 Object Lock or 2) with an incorrect default S3 Object Lock, it should be detected.                | Medium   | S3.FC13<br>S3.FC5           | -  | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C76, depends on S3.C58, assured by S3.C77]<br>Block PutObject and PutObjectRetention requests with unauthorized S3 Object Lock on each bucket (e.g. using an S3 bucket policy deny statement on PutObject and PutObjectRetention if the condition if exists "s3:object-lock-mode" and "s3:object-lock-remaining-retention-days" is not the defined S3 Object Lock configuration) | Make a request with an incorrect S3 Object Lock configuration, it should be denied  | Low      | S3.FC5                      | S3.T16 (High)<br>S3.T17 (High)   | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C77]<br>Verify all buckets blocks PutObject and PutObjectRetention requests with unauthorized S3 Object Lock (e.g. using the Config rule: <a href="#">S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE</a> , note that a new rule needs be deployed for each configuration, then the resource tracked by name or tag)  | Create a bucket not blocking PutObject and PutObjectRetention requests with unauthorized S3 Object Lock, it should be detected. | Medium   | S3.FC5                      | -  | High |
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C98]<br>For each S3 bucket, maintain a list of VPC(s), authorized to access it.  | For each S3 bucket, request the list of authorized VPC to access it, its review process, and its review records                 | Low      | S3.FC10<br>S3.FC2<br>S3.FC5 | S3.T11 (Very Low)<br>S3.T14 (Very Low)<br>S3.T17 (Very Low)<br>S3.T30 (Very Low)<br>S3.T33 (Very Low)<br>S3.T36 (Very Low)<br>S3.T38 (Very Low)<br>S3.T39 (Very Low) | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C99, depends on S3.C98, assured by S3.C100]<br>Limit the access to only those VPC(s) (e.g. using S3 bucket statement, deny if the condition "aws:SourceVpce", or if the bucket policy size is beyond the limit, use this condition on access point)  | Make a request to the bucket outside an authorized VPC, it should be denied   | Very Low | S3.FC10<br>S3.FC2<br>S3.FC5 | S3.T11 (Medium)<br>S3.T14 (Medium)<br>S3.T17 (Medium)<br>S3.T30 (High)<br>S3.T33 (High)<br>S3.T36 (High)   | High |

|   |  |   |        |   | S3.T38 (High)<br>S3.T39 (High)   |      |
|---|--|---|--------|---|--|------|
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C100]<br>Verify all buckets include a control to limit access to only authorized VPC(s) (e.g. using the AWS Config rule <a href="#">S3 BUCKET POLICY GRANTEE CHECK</a> )   | Remove the control limiting access to only authorized VPC(s), it should be detected.    | Medium | S3.FC10<br>S3.FC2<br>S3.FC5                       | -  | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C105, depends on S3.C104, assured by S3.C109]<br>Limit access via the S3 access point by using in VPC endpoint and/or bucket policy the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of allowlist bucket name in VPC endpoint/bucket policy. | Do a request on an unauthorized access point or bucket, it should be denied.            | Medium | S3.FC1<br>S3.FC26<br>S3.FC28<br>S3.FC33<br>S3.FC5 | S3.T7 (Medium)<br>S3.T9 (Very High)<br>S3.T10 (Very High)<br>S3.T11 (Medium)<br>S3.T54 (Medium)<br>S3.T55 (Medium) | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C106, assured by S3.C110]<br>In S3 bucket policy, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn"   | Query the bucket outside S3 access point, it should be denied.                          | Medium | S3.FC1<br>S3.FC26<br>S3.FC33                      | S3.T7 (Medium)<br>S3.T28 (High)<br>S3.T55 (Medium)<br>S3.T56 (Very High)   | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C107]<br>Block the creation "s3>CreateAccessPoint" of non-VPC S3 access point (e.g. using the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"})   | Do a request to create an internet-based access point, it should be denied.             | Low    | S3.FC1<br>S3.FC26                                 | S3.T7 (Medium)<br>S3.T28 (Very High)   | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C108, assured by S3.C111]<br>Block all traffic from Internet-configured S3 access point (e.g. on the bucket policy, using a deny statement with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"})   | Create an internet-facing access point and try to access a bucket, it should be denied. | Low    | S3.FC1<br>S3.FC26<br>S3.FC28                      | S3.T7 (Medium)<br>S3.T10 (Medium)<br>S3.T28 (Very High)  | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C109]<br>Verify only access points are used in the resource-level statement in VPC endpoints   | Create a VPC endpoint giving access to an S3 bucket, it should be detected.             | High   | S3.FC1<br>S3.FC26<br>S3.FC28<br>S3.FC33<br>S3.FC5 | -  | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C110]<br>Verify S3 bucket policies deny non-authorized S3 access points  | Remove/modify the deny on the bucket policy, it should be detected.                     | High   | S3.FC1<br>S3.FC26<br>S3.FC33                      | -  | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C111]<br>Verify all S3 access points are VPC attached  | Create an internet-based access point, it should be detected.                           | Low    | S3.FC1<br>S3.FC26<br>S3.FC28                      | -  | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C112, depends on S3.C104]<br>Block any <a href="#">object-related operations</a> access to S3 bucket not through access point (i.e. using a deny IAM policy statement with the condition "ArnNotLike" {"s3:DataAccessPointArn": "arn:aws:s3:Region:AccountId:accesspoint/*"})  | Access any S3 bucket using the S3 public endpoint, it should be denied.                 | Low    | S3.FC1<br>S3.FC5                                  | S3.T7 (Medium)<br>S3.T11 (High)  | High |
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C120]  | Request the list of all IAM roles configured for Batch job                              | Medium | S3.FC27   | S3.T44 (Very Low)  | High |

|   |  |   |        |  |  |      |
|---|--|---|--------|--|--|------|
|   | Maintain a list of IAM roles used for Batch job, ideally dedicated (e.g. using change management process on infrastructure-as-code)  |   |        |  |  |      |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C122, depends on S3.C120]<br>Limit access to authorized IAM roles used for Batch job, using the IAM ThreatModel (e.g. trust policy, and "iam:PassRole")  | Request the IAM ThreatModel and the evidence of its application to the IAM roles used for Batch job   | Medium | S3.FC27  | S3.T44 (Very High)   | High |
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C125]<br>Maintain a list of authorized Lambda function for each Object Lambda access point, its associated access point, its associated GET request(s), and payload  | Request the list of authorized Lambda function for each Object Lambda access point, its associated access point, its associated GET request(s), and payload, its review process, and its review records   | Low    | S3.FC32  | S3.T46 (Very Low)  | High |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C126, depends on S3.C125, assured by S3.C127]<br>Ensure only authorized Lambda function for each Object Lambda access point, its associated access point, its associated GET request(s), and payload are created   | Request the mechanism ensuring only authorized Lambda function for each Object Lambda access point, its associated access point, its associated GET request(s), and payload, and the evidence of its execution  | Medium | S3.FC32  | S3.T46 (Very High)   | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C127]<br>Verify only the authorized Lambda function are configured on each Object Lambda access point, its associated access point, its associated GET request(s), and payload   | Attach 1) an unauthorized Lambda function on an Object Lambda access point, 2) an unauthorized Object Lambda access point to an access point, 3) an authorized Lambda function with an unauthorized GET request on an Object Lambda access point, and 4) an authorized Lambda function with an unauthorized payload, it should be detected. | Medium | S3.FC32  | -  | High |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C144, depends on S3.C141]<br>Ensure S3 websites are protected with HTTP headers ( <a href="#">ref</a> ) using a CDN (e.g. CloudFront)  | Request the mechanism ensuring S3 websites are protected with HTTP headers  | Medium | S3.FC16  | S3.T13 (High)<br>S3.T29 (Very High)  | High |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C152, assured by S3.C154]<br>Ensure bucket ACL and object ACL are disabled on each bucket  | Request 1) the mechanism ensuring bucket ACL and object ACL are disabled on each bucket, 2) its records of execution for all new buckets, and 3) plan to move any older buckets   | Medium | S3.FC1<br>S3.FC24<br>S3.FC25<br>S3.FC5<br>S3.FC8 | S3.T4 (Very High)<br>S3.T6 (Very High)<br>S3.T36 (Very High)<br>S3.T43 (Very High)<br>S3.T52 (Very High)<br>S3.T53 (Very High) | High |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C153]<br>Prevent the creation of buckets with ACL enabled (e.g. by using a SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note it does not block someone to enable ACL afterwards via PutPutBucketOwnershipControls. | Create a bucket to enable ACL, it should be denied.   | Low    | S3.FC1<br>S3.FC24<br>S3.FC25<br>S3.FC5<br>S3.FC8 | S3.T4 (High)<br>S3.T6 (High)<br>S3.T36 (High)<br>S3.T43 (High)<br>S3.T52 (High)<br>S3.T53 (High)                               | High |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C154]<br>Verify bucket ACL and object ACL are disabled on each bucket  | Create/modify a bucket to enable ACL, it should be detected.  | Medium | S3.FC1<br>S3.FC24<br>S3.FC25<br>S3.FC5<br>S3.FC8 | -  | High |

|   |  |  |          |  |   |        |
|---|--|--|----------|--|---|--------|
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C3, depends on S3.C119, assured by S3.C5]<br>Block all unencrypted requests and unauthorized TLS version(s) from VPC endpoints you control (e.g. by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != <i>authorized TLS version(s)</i> , on the VPC endpoint policy) | Make an unencrypted AWS API call from one of your VPC with VPC endpoint, it should be denied.  | Low      | S3.FC1<br>S3.FC5                                 | S3.T12 (Medium)<br>S3.T34 (Medium)  | Medium |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C5]<br>Verify a statement exists on all your VPC endpoint policy denying all requests with the condition "aws:SecureTransport" = False   | Create/remove the statement on a VPC endpoint policy denying 1) all unencrypted requests or 2) unauthorized TLS version(s), it should be detected.   | High     | S3.FC1<br>S3.FC5                                 | -   | Medium |
| Directive (coso)<br>Detect (NIST CSF)     | [S3.C9]<br>Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions and buckets (e.g. production, with sensitive data, etc.). Make it available for security analysis, and protect it using CloudTrail ThreatModel   | Request the CloudTrail ThreatModel and the evidence of its application for enabling and protecting S3 data events  | Very Low | S3.FC1<br>S3.FC5<br>S3.FC8                       | S3.T1 (Low)<br>S3.T4 (Low)<br>S3.T5 (Low)<br>S3.T6 (Low)<br>S3.T7 (Low)<br>S3.T8 (Low)<br>S3.T9 (Low)<br>S3.T11 (Low)<br>S3.T12 (Low)<br>S3.T16 (Low)<br>S3.T21 (Low)<br>S3.T31 (Low)<br>S3.T34 (Low)<br>S3.T35 (Low)<br>S3.T36 (Low)<br>S3.T39 (Low) | Medium |
| Directive (coso)<br>Detect (NIST CSF)     | [S3.C10]<br>Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using GuardDuty ThreatModel. Ensure findings are investigated (e.g. using Amazon Detective).   | Request the GuardDuty ThreatModel and the evidence of its application for enabling, monitoring, investigation and protecting S3 protection   | Low      | S3.FC1<br>S3.FC24<br>S3.FC25<br>S3.FC5<br>S3.FC8 | S3.T3 (Low)<br>S3.T4 (Low)<br>S3.T16 (Medium)<br>S3.T52 (Medium)<br>S3.T53 (Medium)   | Medium |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C12, depends on S3.C11]<br>Allow only authorized ACL on objects for bucket you don't control (e.g. using IAM and VPC endpoint policy with the <a href="#">ACL conditions</a> )   | Put an object with an unauthorized ACL, it should be denied.   | Medium   | S3.FC1   | S3.T5 (Medium)<br>S3.T6 (High)  | Medium |
| Detective (coso)<br>Detect (NIST CSF)     | [S3.C13, depends on S3.C11]<br>Monitor that only authorized external buckets are used (e.g. via CloudTrail S3 data events in resources[].accountId and resources[].ARN). Both account ID and bucket name must be verified.   | Make a call to an unauthorized bucket, it should be detected   | Low      | S3.FC1<br>S3.FC5                                 | S3.T1 (Low)<br>S3.T7 (Low)<br>S3.T11 (Low)<br>S3.T21 (Low)<br>S3.T31 (Medium)   | Medium |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C14, depends on S3.C11]<br>Scan all data before uploading to an external bucket to ensure the classification of the data is aligned with the bucket classification (e.g. using Macie).   | Request 1) the mechanism ensuring all data are scanned for proper data classification before upload to an external bucket are configured, 2) its records of execution for all object upload flows, and 3) plan to move any older object upload flows | High     | S3.FC1<br>S3.FC16<br>S3.FC5                      | S3.T5 (High)<br>S3.T14 (High)<br>S3.T15 (Medium)  | Medium |

|   |  |  |        |   |  |        |
|---|--|--|--------|---|--|--------|
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C114, depends on S3.C11]<br>For all external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover, block the PutObject with any ACL (e.g. using IAM or SCP and a deny on the condition "StringLike": {"s3:x-amz-acl": "*"}). It should be called via PutObjectAcl.   | Make a request to an external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover requirement, it should be denied. | High   | S3.FC1  | S3.T43 (Very High)   | Medium |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C16]<br>Analyse and protect all AWS services accessing S3 (e.g. via ThreatModel). Enforce usage in VPC only, whenever possible.  | Request the threat and mitigating controls for all AWS services using S3.  | High   | S3.FC1<br>S3.FC5  | S3.T21 (Very High)<br>S3.T30 (Very High)   | Medium |
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C22]<br>Maintain a list of authorized S3 and S3 access point (and their respective AWS accounts) to be access for each VPC   | Request the list of authorized S3 and S3 access point to be access for each VPC, its review process, and its review records                                    | Medium | S3.FC1<br>S3.FC5  | S3.T8 (Very Low)<br>S3.T9 (Very Low)<br>S3.T11 (Very Low)  | Medium |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C23, depends on S3.C22, assured by S3.C24]<br>Limit the access to only authorized S3 bucket(s) or their AWS account(s) from each VPC (e.g. using the condition key "s3:ResourceAccount" on the VPC endpoint policy, alternatively use specific resource-level statement for each bucket, or if the VPC endpoint policy size is beyond the limit and more granular control on VPC is required, use access points) | Make a request to an unauthorized bucket from one of your VPC, it should be denied   | Medium | S3.FC1<br>S3.FC5  | S3.T8 (High)<br>S3.T9 (High)<br>S3.T11 (High)  | Medium |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C24]<br>Verify all VPC are limited to limit access to only authorized S3 bucket(s)   | Remove the control limiting access to only authorized S3 bucket(s), it should be detected.   | High   | S3.FC1<br>S3.FC5  | -  | Medium |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C27, assured by S3.C28]<br>In S3 bucket/access point/Object Lambda access point policy, do not allow IAM principals of the same AWS account. Only AWS IAM should be used to provide permissions to a principal of the same AWS account.  | Request all S3 bucket/access point/Object Lambda access point policy statements with "allow", no principal from the same account should be authorized.         | Low    | S3.FC1<br>S3.FC10<br>S3.FC12<br>S3.FC13<br>S3.FC15<br>S3.FC2<br>S3.FC20<br>S3.FC26<br>S3.FC27<br>S3.FC32<br>S3.FC33<br>S3.FC5<br>S3.FC7 | S3.T1 (Low)<br>S3.T2 (Low)<br>S3.T6 (Low)<br>S3.T7 (Low)<br>S3.T8 (Low)<br>S3.T11 (Low)<br>S3.T14 (Medium)<br>S3.T16 (Low)<br>S3.T17 (Medium)<br>S3.T18 (Low)<br>S3.T21 (Low)<br>S3.T25 (Low)<br>S3.T26 (Medium)<br>S3.T30 (Low)<br>S3.T33 (Medium)<br>S3.T35 (Medium)<br>S3.T36 (Low)<br>S3.T37 (Medium)<br>S3.T38 (Medium)<br>S3.T39 (Low)<br>S3.T41 (Low) | Medium |

|  |   |  |          |   |   |        |
|--|---|--|----------|---|---|--------|
|  |   |  |          |   | S3.T42 (Low)<br>S3.T44 (Low)<br>S3.T46 (Medium)<br>S3.T54 (Medium)<br>S3.T55 (Medium) |        |
| Assurance (coso)<br>Detect (NIST CSF)  | [S3.C28]<br>Verify all S3 bucket/access point/Object Lambda access point policies do not allow an IAM principal of the same AWS account (e.g. using the Config rule S3_BUCKET_POLICY_GRANTEE_CHECK for bucket policy)   | Add an allow statement for an IAM principal of the same account in 1) a bucket policy, 2) in an access point policy, and 3) in an Object Lambda access point, it should be detected.   | Medium   | S3.FC1<br>S3.FC10<br>S3.FC12<br>S3.FC13<br>S3.FC15<br>S3.FC2<br>S3.FC20<br>S3.FC26<br>S3.FC27<br>S3.FC32<br>S3.FC33<br>S3.FC5<br>S3.FC7 | -   | Medium |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C46]<br>Ensure all S3 buckets interacted with are in the correct AWS account (e.g. using the condition in all compatible S3 requests: x-amz-expected-bucket-owner and x-amz-source-expected-bucket-owner)   | Request the process on ensuring that all S3 buckets interacted with are in the correct AWS account   | Medium   | S3.FC1<br>S3.FC5  | S3.T1 (Medium)<br>S3.T3 (Medium)  | Medium |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C113, depends on S3.C11]<br>When transmitting an object to an external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover, use 2 separate APIs (PutObject and PutObjectAcl), instead of the built-in object ACL operation in PutObject. | Request the process on ensuring that PutObject requests on external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover use 2 separate APIs | Medium   | S3.FC1  | S3.T43 (High)   | Medium |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C47, assured by S3.C48]<br>Front buckets required to be public, using authenticated CDN (e.g. CloudFront) or API Gateway, protected with WAF (e.g. for <a href="#">hotlinking</a> )   | Request the process ensuring that buckets required to be public are front by authenticated CDN or API Gateway  | Medium   | S3.FC16<br>S3.FC5   | S3.T13 (Very High)<br>S3.T14 (Medium)<br>S3.T22 (Very High)                           | Medium |
| Assurance (coso)<br>Detect (NIST CSF)  | [S3.C48]<br>Verify no bucket is available publicly for write or read (e.g. using the AWS Config rules:<br><a href="#">S3_BUCKET_PUBLIC_READ_PROHIBITED</a> and<br><a href="#">S3_BUCKET_PUBLIC_WRITE_PROHIBITED</a> )   | Create a public S3 bucket, it should be detected.  | Very Low | S3.FC16<br>S3.FC5   | -   | Medium |
| Detective (coso)<br>Detect (NIST CSF)  | [S3.C59, depends on S3.C58]<br>Use a data discovery tool (e.g. Amazon Macie) to control that no sensitive data are stored in unauthorized bucket  | Upload a higher classification data in a bucket, it should be detected.  | Medium   | S3.FC5  | S3.T11 (Medium)   | Medium |
| Assurance (coso)<br>Detect (NIST CSF)  | [S3.C62]<br>Verify all objects on S3 buckets are encrypted with an authorized KMS key (e.g. using S3 inventory, see <a href="#">blog</a> , or <a href="#">S3 Storage Lens</a> )   | Upload an encrypted data using an unauthorized KMS key, it should be detected.   | Medium   | S3.FC10<br>S3.FC5   | -   | Medium |

|   |   |   |           |  |  |        |
|---|---|---|-----------|--|--|--------|
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C140, assured by S3.C62]<br>Ensure all objects on S3 buckets are encrypted with an authorized KMS key   | Request the mechanism (including training, or utility) ensuring only authorized KMS key are used for any objects stored in S3   | Medium    | S3.FC10<br>S3.FC5                      | S3.T11 (Medium)<br>S3.T16 (Medium)<br>S3.T17 (Medium)<br>S3.T20 (Medium)<br>S3.T30 (Medium)<br>S3.T36 (Medium)<br>S3.T37 (Medium)  | Medium |
| Directive (coso)<br>Recover (NIST CSF)    | [S3.C71, depends on S3.C58]<br>Backup primary data in a secure location under a different security authority (e.g. in an <a href="#">AWS data bunker account</a> via replication)   | Request the mechanism used to backup primary data in a location which have different security authority, its records of execution, and records of restoration testing | Medium    | S3.FC13<br>S3.FC5                      | S3.T16 (High)<br>S3.T17 (High)<br>S3.T25 (High)  | Medium |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C72]<br>Aligned with your data governance, encrypt on the client side - or tokenize - appropriate data  | Request the governance and mechanism(s) used to protect data (e.g. encrypt or tokenize critical data on the client side)  | Very High | S3.FC1<br>S3.FC10<br>S3.FC16<br>S3.FC5 | S3.T1 (Medium)<br>S3.T3 (Medium)<br>S3.T5 (High)<br>S3.T7 (High)<br>S3.T11 (Very High)<br>S3.T12 (Very High)<br>S3.T13 (Very High)<br>S3.T17 (High)<br>S3.T20 (High)<br>S3.T30 (High)<br>S3.T31 (High) | Medium |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C73]<br>Create a process to apply legal hold to any S3 bucket, whenever required. The condition "s3:object-lock-legal-hold" can be used to restrict who can remove such a lock.   | Request the process of applying legal hold, and its records   | Medium    | S3.FC5                                 | S3.T16 (Low)<br>S3.T17 (Medium)  | Medium |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C84]<br>Block all requests not using HTTP authorization header, i.e. presign via query strings or POST ( <a href="#">ref</a> ) (e.g. using an SCP and S3 policy on all buckets with deny on "StringNotEquals":{"s3:authType": "REST-HEADER"}). Note it blocks uploads via the console, as well. | Make a request with a non-HTTP authorization header, it should be denied  | Low       | S3.FC5                                 | S3.T39 (Medium)  | Medium |
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C86]<br>Maintain a list of authorized buckets to have replication enabled, their target bucket and replication type (i.e. ownership, RTC, etc.) ( <a href="#">ref</a> ).  | Request the list of authorized buckets to have replication enabled, their target bucket and replication rights, its review process, and its review records            | Medium    | S3.FC15                                | S3.T2 (Very Low)   | Medium |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C87]<br>Verify only authorized buckets have replication enabled and with correct configuration  | Configure replication on a non-authorized bucket, it should be detected   | Medium    | S3.FC15                                | -  | Medium |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C88]<br>Verify authorized buckets have the correct replication configuration  | Modify the configuration of an authorized replication, it should be detected  | High      | S3.FC15                                | -  | Medium |
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C89]<br>Maintain a list of IAM roles used for replication, ideally dedicated (e.g. using change management process on infrastructure-as-code)   | Request the list of all IAM roles configured for replication  | Medium    | S3.FC15                                | S3.T2 (Very Low)   | Medium |

|   |  |   |        |  |   |        |
|---|--|---|--------|--|---|--------|
| Directive (coso)<br>Protect (NIST CSF)  | [S3.C90, depends on S3.C89]<br>Limit the S3 access to the source/destination bucket and replication rights of each authorized IAM role configured for replication  | Request the S3 access of replication role, and how they aligned to the replication requirements   | Medium | S3.FC15                                | S3.T2 (Medium)  | Medium |
| Directive (coso)<br>Protect (NIST CSF)  | [S3.C91, depends on S3.C89]<br>Limit access to authorized IAM roles used for replication, using the IAM ThreatModel (e.g. trust policy, and "iam:PassRole")  | Request the IAM ThreatModel and the evidence of its application to the IAM roles used for replication   | High   | S3.FC15                                | S3.T2 (High)  | Medium |
| Assurance (coso)<br>Detect (NIST CSF)   | [S3.C92]<br>Verify only the authorized IAM role is configured for each replication   | Create/modify a replication with an unauthorized IAM role, it should be detected  | High   | S3.FC15                                | -   | Medium |
| Assurance (coso)<br>Detect (NIST CSF)   | [S3.C117]<br>Verify all replicated buckets have metrics enabled on each replication rule (included by default in S3 RTC)   | Modify the replication metric of an authorized replication, it should be detected   | Medium | S3.FC15                                | -   | Medium |
| Directive (coso)<br>Protect (NIST CSF)  | [S3.C134, depends on S3.C86, assured by S3.C87,S3.C88,S3.C117]<br>Ensure only authorized buckets have replication enabled and with correct configuration are configured                                    | Request 1) the mechanism ensuring only authorized buckets have replication enabled and with correct configuration are configured, 2) its records of execution for all new buckets, and 3) plan to move any older buckets  | Medium | S3.FC15                                | S3.T2 (High)  | Medium |
| Directive (coso)<br>Protect (NIST CSF)  | [S3.C138, depends on S3.C89, assured by S3.C92]<br>Ensure only authorized IAM roles are attached for each replication, ideally dedicated   | Request the mechanism ensuring authorized IAM roles are attached for each replication, and the evidence of its execution for all replication configuration  | Medium | S3.FC15                                | S3.T2 (High)  | Medium |
| Detective (coso)<br>Detect (NIST CSF)   | [S3.C93, depends on S3.C58]<br>If the bucket is used as an input or the output of a process, scan the objects for malware (e.g. using <a href="#">VirusScan</a> or <a href="#">Trend Micro Cloud One</a> ) | Inject a malware test file, it should be detected.  | Medium | S3.FC16<br>S3.FC5                      | S3.T14 (Medium)<br>S3.T15 (Low)   | Medium |
| Directive (coso)<br>Identify (NIST CSF) | [S3.C101]<br>Maintain a list of authorized CloudFront distribution (via origin access identity) and associated bucket  | Request the list of all authorized CloudFront distribution and associated S3 buckets  | Low    | S3.FC10                                | S3.T20 (Very Low)   | Medium |
| Assurance (coso)<br>Detect (NIST CSF)   | [S3.C102]<br>Verify all associations of CloudFront distributions with buckets are authorized   | Create a non-authorized distribution or association, it should be detected.   | High   | S3.FC10                                | -   | Medium |
| Directive (coso)<br>Protect (NIST CSF)  | [S3.C137, depends on S3.C101, assured by S3.C102]<br>Ensure only authorized CloudFront distributions are associated with their authorized bucket, and vice versa.  | Request 1) the mechanism ensuring only authorized only authorized CloudFront distribution are associated with their authorized bucket, and vice versa, 2) its records of execution for all new CloudFront distribution, and 3) plan to move any older CloudFront distribution | Medium | S3.FC10                                | S3.T20 (High)   | Medium |
| Directive (coso)<br>Identify (NIST CSF) | [S3.C104]<br>Maintain a list of authorized access between VPC, S3 access point and S3.   | Request the list of authorized access between VPC and S3 access points  | Medium | S3.FC1<br>S3.FC26<br>S3.FC28<br>S3.FC5 | S3.T7 (Very Low)<br>S3.T9 (Very Low)<br>S3.T10 (Very Low)<br>S3.T11 (Very Low)<br>S3.T28 (Very Low) | Medium |
| Directive (coso)<br>Protect (NIST CSF)  | [S3.C121, depends on S3.C120]<br>Limit the access to only required resources/permissions (e.g. source/destination bucket, Lambda functions) of each authorized IAM role configured for Batch jobs          | Request the access to only required resources/permissions for each Batch IAM role, and how they aligned to the replication requirements   | Medium | S3.FC27                                | S3.T44 (High)   | Medium |

|                                      |   |   |          |                  |  |        |
|--------------------------------------|---|---|----------|------------------|--|--------|
| Assurance (coso) Detect (NIST CSF)   | [S3.C123] Verify only the authorized IAM role is configured for each Batch job  | Create/modify a Batch job with an unauthorized IAM role, it should be detected  | High     | S3.FC27          | -  | Medium |
| Directive (coso) Protect (NIST CSF)  | [S3.C139, depends on S3.C120, assured by S3.C123] Ensure only an authorized IAM role is attached on each Batch job  | Request the mechanism ensuring only an authorized IAM role is attached on each Batch job, and the evidence of its execution for all new {resource}  | Medium   | S3.FC27          | S3.T44 (High)                              | Medium |
| Directive (coso) Protect (NIST CSF)  | [S3.C128] Ensure Lambda functions configured on Object Lambda access point are secured using Lambda ThreatModel   | Request the mechanism ensuring Lambda ThreatModel and its application for Lambda functions associated to Object Lambda access point, and its records of execution   | Medium   | S3.FC32          | S3.T46 (High)                              | Medium |
| Directive (coso) Identify (NIST CSF) | [S3.C129] Maintain a list of cross-account access on each Object Lambda access point  | Request the list of authorized cross-account access for each Object Lambda access point, its review process, and its review records   | Very Low | S3.FC32          | S3.T46 (Very Low)                          | Medium |
| Directive (coso) Protect (NIST CSF)  | [S3.C130, depends on S3.C129, assured by S3.C131] Ensure only authorized cross-account IAM entities are allowed in the Object Lambda access point policy  | Request the mechanism ensuring only cross-account IAM entities are allowed in the Object Lambda access point policy, and the evidence of its execution  | Low      | S3.FC32          | S3.T46 (Medium)                            | Medium |
| Assurance (coso) Detect (NIST CSF)   | [S3.C131] Verify only the authorized cross-account IAM entities are allowed in the Object Lambda access point policy  | Add 1) an unauthorized cross-account IAM entity on an Object Lambda access point policy, it should be detected.   | High     | S3.FC32          | -  | Medium |
| Directive (coso) Identify (NIST CSF) | [S3.C141] Maintain a list of authorized buckets to be configured as website   | Request the list of authorized buckets to be configured as website, its review process, and its review records  | Low      | S3.FC16          | S3.T13 (Very Low)<br>S3.T29 (Very Low)     | Medium |
| Directive (coso) Protect (NIST CSF)  | [S3.C142, depends on S3.C141, assured by S3.C143] Ensure only authorized buckets are configured as website  | Request 1) the mechanism ensuring only authorized buckets are configured as website, 2) its records of execution for all new website-enabled buckets, and 3) plan to move any older website-enabled buckets | Medium   | S3.FC16          | S3.T13 (Medium)<br>S3.T29 (Medium)         | Medium |
| Assurance (coso) Detect (NIST CSF)   | [S3.C143] Verify only authorized buckets are configured as website  | Enable website configuration on an unauthorized bucket, it should be detected.  | Medium   | S3.FC16          | -  | Medium |
| Detective (coso) Detect (NIST CSF)   | [S3.C4] Monitor and investigate that all requests made with HTTP (e.g via CloudTrail S3 data events with the lack of additionalEventData.CipherSuite)   | Make an unencrypted AWS API call from one of your VPC with VPC endpoint, it should be detected.   | Low      | S3.FC1<br>S3.FC5 | S3.T12 (Low)<br>S3.T34 (Low)               | Low    |
| Detective (coso) Detect (NIST CSF)   | [S3.C115, depends on S3.C11] For all external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover, monitor that the PutObject do not include the ACL operation   | Make a request to an external bucket with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover requirement, it should be detected.  | Low      | S3.FC1           | S3.T43 (Low)                               | Low    |
| Directive (coso) Protect (NIST CSF)  | [S3.C18, depends on S3.C17] For each VPC with an IAM entity allowed to use S3, secure them with the VPC ThreatModel (e.g. <a href="#">modification of VPC endpoints</a> , <a href="#">VPC endpoint policy</a> , <a href="#">routing table</a> , <a href="#">Security Groups</a> ) | Request how VPC ThreatModel for S3 is being applied.  | High     | S3.FC1<br>S3.FC5 | S3.T9 (Medium)<br>S3.T11 (Medium)          | Low    |
| Detective (coso) Detect (NIST CSF)   | [S3.C25, depends on S3.C21,S3.C22] Monitor VPC DNS query logs that only authorized S3 bucket and S3 access points are being queried in each VPC (e.g.   | Make a DNS query to an unauthorized 1) S3 bucket and 2) S3 access points, it should be detected.  | Low      | S3.FC1<br>S3.FC5 | S3.T8 (Low)<br>S3.T9 (Low)<br>S3.T11 (Low) | Low    |

|  |  |  |          |  |  |     |
|--|--|--|----------|--|--|-----|
|  | using VPC DNS query logging), and protect it using Route53 ThreatModel   |  |          |  |  |     |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C124]<br>Ensure all S3 VPC endpoints (Interface and Gateway) are covered by the VPC endpoints controls   | Request the mechanism ensuring all S3 VPC endpoints (Interface and Gateway) are covered by the VPC endpoints controls, and its records | Low      | S3.FC1   | S3.T45 (Very High)   | Low |
| Detective (coso)<br>Detect (NIST CSF)  | [S3.C33, depends on S3.C31]<br>Monitor that only authorized AWS accounts to provide KMS keys are used for each AWS account (using CloudTrail S3 data events in <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> )   | Make a call to an unauthorized bucket, it should be detected   | Low      | S3.FC1<br>S3.FC15<br>S3.FC26<br>S3.FC5<br>S3.FC8 | S3.T1 (Low)<br>S3.T2 (Low)<br>S3.T4 (Low)<br>S3.T5 (Low)<br>S3.T7 (Low)<br>S3.T8 (Low)<br>S3.T9 (Low)<br>S3.T11 (Low)<br>S3.T16 (Low)<br>S3.T21 (Low)<br>S3.T27 (Very Low)<br>S3.T28 (Low)<br>S3.T30 (Low)<br>S3.T31 (Low) | Low |
| Detective (coso)<br>Detect (NIST CSF)  | [S3.C35]<br>Monitor ObjectACL changed (or tentatively changed) to public using CloudTrail S3 data events   | Make a call to create a public ObjectACL, it should be detected.   | Low      | S3.FC1<br>S3.FC5                                 | S3.T6 (Low)<br>S3.T36 (Low)  | Low |
| Detective (coso)<br>Detect (NIST CSF)  | [S3.C37]<br>Monitor and investigate anonymous requests to objects (e.g. using CloudTrail S3 data events with <i>userIdentity.accountId=ANONYMOUS_PRINCIPAL</i> )   | Make an anonymous call, it should be detected.   | Low      | S3.FC5   | S3.T36 (Low)   | Low |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C41]<br>Parameterize S3 bucket name or S3 access point in your code (no hardcoding)  | Request the process on ensuring S3 bucket name or S3 access point are not hard-coded   | Medium   | S3.FC5   | S3.T1 (Low)  | Low |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C42]<br>When connecting to S3 endpoints, use virtual-hosted model ("my-bucket-name.s3.amazonaws.com" or "my-bucket-name.my-s3-regional-endpoint.amazonaws.com") instead of path-style model ("s3.amazonaws.com/my-bucket-name" or "my-s3-regional-endpoint.amazonaws.com/my-bucket-name") (see <a href="#">ref</a> ). All the latest SDK make use of domain style, by default. | Request the mechanism ensuring the usage of domain style instead of path style.  | Very Low | S3.FC1   | S3.T35 (High)  | Low |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C44]<br>If etag is used, make sure properly account for its different definitions ( <a href="#">ref</a> )  | Request the process ensuring etag different definitions are properly accounted for   | Low      | S3.FC5   | S3.T27 (High)  | Low |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C83]<br>Use SDK with SigV4 enabled ( <a href="#">ref</a> )   | Request the mechanism ensuring the use of SDK with SigV4 enabled   | Low      | S3.FC1   | S3.T35 (High)  | Low |
| Detective (coso)<br>Detect (NIST CSF)  | [S3.C56]<br>Monitor changes on bucket ACL other than for server access logging (e.g. using CloudTrail, 1) if the CloudTrail  | Make a call to create a bucket ACL other than server access logging, it should be detected.  | Medium   | S3.FC8   | S3.T4 (Low)  | Low |

|   |   |   |        |                   |  |
|---|---|---|--------|-------------------|--|
|   | PutBucketAcl log indicates requestParameters.AccessControlPolicy.AccessControlList.Grant[].Grantee.xsi:type: "Group", then the URI should be "http://acs.amazonaws.com/groups/s3/LogDelivery", and 2) if the requestParameters.AccessControlPolicy.AccessControlList.Grant[].Grantee.xsi:type: "CanonicalUser" then the ID should be the same than "AccessControlPolicy.Owner.ID", and 3) requestParameters.x-amz-acl should be either "private", "log-delivery-write" or not existing) |   |        |                   |  |
| Directive (coso)<br>Protect (NIST CSF)    | [S3.C63, depends on S3.C61]<br>Use KMS ThreatModel to protect the KMS keys used for S3 (e.g. using encryptionContext on the policy of each KMS key)   | Request the KMS ThreatModel and the evidence of its application to protect S3   | High   | S3.FC10<br>S3.FC5 | S3.T17 (Medium)<br>S3.T36 (Low)<br>S3.T37 (Low)                        |
| Detective (coso)<br>Detect (NIST CSF)     | [S3.C68, depends on S3.C61]<br>Monitor that only authorized KMS key(s) are used on each bucket (using CloudTrail S3 data events in <i>requestParameter.bucketName</i> and <i>response.x-amz-server-side-encryption-aws-kms-key-id</i> )   | Make a request encrypted with an unauthorized KMS key, it should be detected  | Low    | S3.FC5            | S3.T11 (Very Low)<br>S3.T16 (Low)<br>S3.T30 (Very Low)<br>S3.T36 (Low) |
| Detective (coso)<br>Detect (NIST CSF)     | [S3.C148, depends on S3.C145]<br>For buckets (or paths) requiring SSE-C, monitor that only authorized encryption is used on each bucket or path (using CloudTrail S3 data events in <i>requestParameter.bucketName</i> and <i>response.x-amz-server-side-encryption-customer-algorithm</i> )  | Make a request to a bucket (or path) requiring SSE-C without the proper encryption, it should be detected                                       | Low    | S3.FC5            | S3.T11 (Very Low)<br>S3.T16 (Low)<br>S3.T30 (very Low)<br>S3.T36 (Low) |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C78, assured by S3.C79]<br>Reduce costs related to incomplete multipart upload by creating a lifecycle policy to remove them after an agreed length of time (e.g. 7 days) ( <a href="#">blog</a> )  | Create an incomplete upload, and wait for the agreed time, it should be deleted automatically.  | Low    | S3.FC5            | S3.T40 (High)  |
| Assurance (coso)<br>Detect (NIST CSF)     | [S3.C79]  | Create a bucket without a lifecycle policy to remove incomplete multipart upload, it should be detected   | Medium | S3.FC5            | -  |
| Preventative (coso)<br>Protect (NIST CSF) | [S3.C81]<br>Block all requests not using SigV4 (e.g. using an SCP and S3 policy on all buckets with deny on "StringNotEquals": {"s3:signatureversion": "AWS4-HMAC-SHA256"})   | Make a non-SigV4 AWS API call, it should be denied.   | Low    | S3.FC1            | S3.T35 (High)  |
| Detective (coso)<br>Detect (NIST CSF)     | [S3.C116]<br>Monitor abnormal behaviour on replication CloudWatch metrics (i.e. <i>BytesPendingReplication</i> and <i>OperationsPendingReplication</i> )  | Create an abnormal replication, it should be detected   | Low    | S3.FC15           | S3.T2 (Low)  |
| Directive (coso)<br>Identify (NIST CSF)   | [S3.C94]<br>Maintain a list of authorized notification receiver(s) (e.g. SNS Topic, Lambda, etc.) for each bucket. You might use a simpler approach by using authorized account ID(s) to ensure all your receivers are in authorized AWS account(s).  | Request the list of authorized notification receiver (e.g. SNS Topic, Lambda, etc.) for each bucket, its review process, and its review records | Low    | S3.FC20           | S3.T41 (Very Low)  |

|  |  |  |           |                    |   |          |
|--|--|--|-----------|--------------------|---|----------|
| Assurance (coso)<br>Detect (NIST CSF)  | [S3.C95]<br>Verify only authorized notification receiver(s) are configured for buckets.  | Create an unauthorized receiver, it should be detected.  | High      | S3.FC20            | -   | Low      |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C135, depends on S3.C94, assured by S3.C95]<br>Ensure only authorized notification receiver(s) (e.g. SNS Topic, Lambda, etc.) for each bucket are configured                     | Request 1) the mechanism ensuring only authorized notification receiver(s) (e.g. SNS Topic, Lambda, etc.) for each bucket are configured, 2) its records of execution for all new buckets, and 3) plan to move any older buckets | Medium    | S3.FC20            | S3.T41 (High)   | Low      |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C103]<br>Protect and/or claim your domains and trademarks/copyrights (by creating your trademark buckets, and using the <a href="#">copyright infringement process</a> from AWS) | Request the process by protecting and/or claiming your domains and trademarks/copyrights   | Medium    | S3.FC28            | S3.T23 (High)   | Low      |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C132, assured by S3.C133]<br>Ensure CloudWatch is enabled for all Object Lambda access points  | Request the mechanism ensuring CloudWatch is enabled for all Object Lambda access points, and its records of execution   | Low       | S3.FC32            | S3.T46 (Low)  | Low      |
| Assurance (coso)<br>Detect (NIST CSF)  | [S3.C133]<br>Verify CloudWatch is enabled for all Object Lambda access points  | Create an Object Lambda access point without CloudWatch enabled, it should be detected.  | Low       | S3.FC32            | -   | Low      |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C29]<br>Use unguessable naming convention for the email addresses of your AWS accounts (e.g. add a + sign and a random string to redirect the email in the same mailbox)         | Review naming convention for root account email and their implementation   | Medium    | S3.FC28            | S3.T19 (High)   | Low      |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C30]<br>Use unguessable naming convention for your IAM users and IAM roles (e.g. add a random string)  | Review naming convention for IAM users/role and their implementation   | Medium    | S3.FC28            | S3.T24 (High)   | Low      |
| Directive (coso)<br>Detect (NIST CSF)  | [S3.C21]<br>Enable <a href="#">VPC DNS query logging</a> in all VPC  | Request the mechanism to enable VPC DNS query logging in all VPC   | Medium    | S3.FC1<br>S3.FC5   | S3.T8 (Very Low)<br>S3.T9 (Very Low)<br>S3.T11 (Very Low) | Very Low |
| Detective (coso)<br>Detect (NIST CSF)  | [S3.C40]<br>Scan your CNAME records (e.g. in Route53) and CloudFront origin for deleted buckets  | Create a CNAME record and CloudFront origin with an invalid bucket, it should be detected.   | High      | S3.FC5             | S3.T1 (Very Low)  | Very Low |
| Detective (coso)<br>Detect (NIST CSF)  | [S3.C43]<br>Monitor that all S3 connections are made with virtual-hosted model (e.g via CloudTrail S3 requestParameters.Host)  | Make a path-style request to S3, it should be detected.  | Medium    | S3.FC1             | S3.T35 (Low)  | Very Low |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C45]<br>Do not include sensitive data in bucket names, access point names, object names, object metadata and tags.   | Request the process ensuring no sensitive data is included in bucket names, object names, object metadata and tags.  | Low       | S3.FC12<br>S3.FC20 | S3.T41 (Low)<br>S3.T42 (Medium)                           | Very Low |
| Detective (coso)<br>Detect (NIST CSF)  | [S3.C60]<br>Use a data discovery tool (e.g. Amazon Macie) to ensure the bucket names, object names, tags and metadata do not contain sensitive data                                  | Create a bucket name, object name, tags, or a metadata of an object with sensitive data, it should be detected.  | Very High | S3.FC5             | S3.T11 (Very Low)   | Very Low |
| Directive (coso)<br>Protect (NIST CSF) | [S3.C80]<br>Block deprecated S3 actions, using IAM ThreatModel and the S3 actions list.  | Request the controls blocking deprecated S3 actions  | Low       | S3.FC1             | S3.T35 (Medium)   | Very Low |
| Detective (coso)                       | [S3.C82]   | Make a non-SigV4 AWS API call, it should be detected.  | Low       | S3.FC1             | S3.T35 (Low)  | Very Low |

|   |   |   |        |         |                   |          |
|---|---|---|--------|---------|-------------------|----------|
| Detect (NIST CSF)                       | Monitor and investigate that all requests not using SigV4 (e.g via CloudTrail S3 with the additionalEventData.SignatureVersion different from "SigV4")  |   |        |         |                   |          |
| Detective (coso)<br>Detect (NIST CSF)   | [S3.C85]<br>Monitor and investigate that all requests not using HTTP authorization header (e.g via CloudTrail S3 with the additionalEventData.AuthenticationMethod different from "AuthHeader") | Make 1) a presigned AWS API call and 2) a POST request, it should be detected.  | Low    | S3.FC5  | S3.T39 (Very Low) | Very Low |
| Directive (coso)<br>Identify (NIST CSF) | [S3.C96]<br>Maintain a list of authorized S3 buckets to receive S3 inventory of each bucket   | Request the list of authorized bucket(s) to receive S3 inventory of each bucket, its review process, and its review records   | Low    | S3.FC12 | S3.T42 (Very Low) | Very Low |
| Assurance (coso)<br>Detect (NIST CSF)   | [S3.C97]<br>Verify only authorized buckets are configured to receive inventory.   | Create an unauthorized bucket to receive inventory, it should be detected.  | High   | S3.FC12 | -                 | Very Low |
| Directive (coso)<br>Protect (NIST CSF)  | [S3.C136, depends on S3.C96, assured by S3.C97]<br>Ensure only authorized S3 buckets are configured to receive S3 inventory for each bucket   | Request 1) the mechanism ensuring only authorized S3 buckets are configured to receive S3 inventory for each bucket, 2) its records of execution for all new buckets, and 3) plan to move any older buckets | Medium | S3.FC12 | S3.T42 (Medium)   | Very Low |

## Appendix 2 - List of all Actions and their details

| <b>Id</b> | <b>Description</b>   | <b>Feature Class ID</b> | <b>IAM Permission</b>          | <b>Event</b>                       | <b>API</b>                         |
|-----------|--|-------------------------|--------------------------------|------------------------------------|------------------------------------|
| S3.A1     | Aborts a multipart upload  | S3.FC1                  | s3:AbortMultipartUpload        | AbortMultipartUpload               | AbortMultipartUpload               |
| S3.A2     | Grants permission to allow circumvention of governance-mode object retention settings (for DeleteObject, DeleteObjects and PutObjectRetention)   | S3.FC17                 | s3:BypassGovernanceRetention   | -                                  | -                                  |
| S3.A3     | Completes a multipart upload by assembling previously uploaded parts   | S3.FC1                  | s3:PutObject                   | CompleteMultipartUpload            | CompleteMultipartUpload            |
| S3.A4     | Creates a copy of an object that is already stored in Amazon S3  | S3.FC1                  | s3:GetObject<br>s3:PutObject   | CopyObject                         | CopyObject                         |
| S3.A5     | Creates a new bucket   | S3.FC5                  | s3:CreateBucket                | CreateBucket                       | CreateBucket                       |
| S3.A6     | Initiates a multipart upload and returns an upload ID  | S3.FC1                  | s3:GetObject<br>s3:PutObject   | CreateMultipartUpload              | CreateMultipartUpload              |
| S3.A7     | Deletes the bucket. All objects (including all object versions and delete markers) in the bucket must be deleted before the bucket itself can be deleted   | S3.FC5                  | s3:DeleteBucket                | DeleteBucket                       | DeleteBucket                       |
| S3.A8     | Deletes an analytics configuration for the bucket  | S3.FC11                 | s3:PutAnalyticsConfiguration   | DeleteBucketAnalyticsConfiguration | DeleteBucketAnalyticsConfiguration |
| S3.A9     | Deletes the CORS configuration information set for the bucket  | S3.FC22                 | s3:PutBucketCORS               | DeleteBucketCors                   | DeleteBucketCors                   |
| S3.A10    | Removes default encryption from the bucket   | S3.FC23                 | s3:PutEncryptionConfiguration  | DeleteBucketEncryption             | DeleteBucketEncryption             |
| S3.A11    | Deletes an inventory configuration from the bucket   | S3.FC12                 | s3:PutInventoryConfiguration   | DeleteBucketInventoryConfiguration | DeleteBucketInventoryConfiguration |
| S3.A12    | Deletes the lifecycle configuration from the bucket  | S3.FC13                 | s3:PutLifecycleConfiguration   | DeleteBucketLifecycle              | DeleteBucketLifecycle              |
| S3.A13    | Deletes a metrics configuration for the Amazon CloudWatch request metrics (specified by the metrics configuration ID) from the bucket. Note that this doesn't include the daily storage metrics. | S3.FC14                 | s3:PutMetricsConfiguration     | DeleteBucketMetricsConfiguration   | DeleteBucketMetricsConfiguration   |
| S3.A14    | Deletes the policy on a specified bucket   | S3.FC10                 | s3:DeleteBucketPolicy          | DeleteBucketPolicy                 | DeleteBucketPolicy                 |
| S3.A15    | Deletes the replication configuration from the bucket  | S3.FC15                 | s3:PutReplicationConfiguration | DeleteBucketReplication            | DeleteBucketReplication            |
| S3.A16    | Deletes the tags from the bucket.  | S3.FC7                  | s3:PutBucketTagging            | DeleteBucketTagging                | DeleteBucketTagging                |
| S3.A17    | Removes the website configuration for a bucket   | S3.FC16                 | s3:DeleteBucketWebsite         | DeleteBucketWebsite                | DeleteBucketWebsite                |
| S3.A18    | Deletes an object permanently (non-versioned bucket) or inserts a delete marker (versioned bucket)   | S3.FC1                  | s3:DeleteObject                | DeleteObject                       | DeleteObject                       |
| S3.A19    | Permanently deletes an object or a delete marker from a bucket   | S3.FC3                  | s3:DeleteObjectVersion         | DeleteObject                       | DeleteObject(VersionId=)           |
| S3.A20    | Deletes multiple objects permanently (non-versioned bucket) or inserts delete markers (versioned bucket)   | S3.FC1                  | s3:DeleteObject                | DeleteObjects                      | DeleteObjects                      |
| S3.A21    | Permanently deletes multiple objects or delete markers from a bucket   | S3.FC3                  | s3:DeleteObjectVersion         | DeleteObjects                      | DeleteObjects(VersionId=)          |
| S3.A22    | Removes the entire tag set from the specified object.  | S3.FC2                  | s3:DeleteObjectTagging         | DeleteObjectTagging                | DeleteObjectTagging                |

|        |   |         |                                     |                                    |                                    |
|--------|---|---------|-------------------------------------|------------------------------------|------------------------------------|
| S3.A23 | Removes the entire tag set from the specified object version.   | S3.FC4  | s3:DeleteObjectVersionTagging       | DeleteObjectTagging                | DeleteObjectTagging(VersionId=)    |
| S3.A24 | Removes the PublicAccessBlock configuration for an Amazon S3 bucket.                                  | S3.FC24 | s3:PutBucketPublicAccessBlock       | DeletePublicAccessBlock            | DeletePublicAccessBlock            |
| S3.A25 | Returns the Transfer Acceleration state of a bucket, which is either "Enabled" or "Suspended".        | S3.FC18 | s3:GetAccelerateConfiguration       | GetBucketAccelerateConfiguration   | GetBucketAccelerateConfiguration   |
| S3.A26 | Returns the access control list (ACL) of a bucket   | S3.FC8  | s3:GetBucketAcl                     | GetBucketAcl                       | GetBucketAcl                       |
| S3.A27 | Returns an analytics configuration from the bucket.   | S3.FC11 | s3:GetAnalyticsConfiguration        | GetBucketAnalyticsConfiguration    | GetBucketAnalyticsConfiguration    |
| S3.A28 | Returns the CORS configuration information set for the bucket.  | S3.FC22 | s3:GetBucketCORS                    | GetBucketCors                      | GetBucketCors                      |
| S3.A29 | Returns the default encryption configuration for an Amazon S3 bucket.                                 | S3.FC23 | s3:GetEncryptionConfiguration       | GetBucketEncryption                | GetBucketEncryption                |
| S3.A30 | Returns an inventory configuration from the bucket.   | S3.FC12 | s3:GetInventoryConfiguration        | GetBucketInventoryConfiguration    | GetBucketInventoryConfiguration    |
| S3.A31 | (Deprecated) Returns the lifecycle configuration information set on the bucket.                       | S3.FC13 | s3:GetLifecycleConfiguration        | GetBucketLifecycle                 | GetBucketLifecycle                 |
| S3.A32 | Returns the lifecycle configuration information set on the bucket.                                    | S3.FC13 | s3:GetLifecycleConfiguration        | GetBucketLifecycleConfiguration    | GetBucketLifecycleConfiguration    |
| S3.A33 | Returns a bucket's region.  | S3.FC5  | s3:GetBucketLocation                | GetBucketLocation                  | GetBucketLocation                  |
| S3.A34 | Returns the logging status of a bucket and the permissions users have to view and modify that status. | S3.FC19 | s3:GetBucketLogging                 | GetBucketLogging                   | GetBucketLogging                   |
| S3.A35 | Gets a metrics configuration from the bucket.   | S3.FC14 | s3:GetMetricsConfiguration          | GetBucketMetricsConfiguration      | GetBucketMetricsConfiguration      |
| S3.A36 | (Deprecated) Returns the notification configuration of a bucket.                                      | S3.FC20 | s3:GetBucketNotification            | GetBucketNotification              | GetBucketNotification              |
| S3.A37 | Returns the notification configuration of a bucket.   | S3.FC20 | s3:GetBucketNotification            | GetBucketNotificationConfiguration | GetBucketNotificationConfiguration |
| S3.A38 | Returns the policy of a specified bucket.   | S3.FC10 | s3:GetBucketPolicy                  | GetBucketPolicy                    | GetBucketPolicy                    |
| S3.A39 | Retrieves the policy status for an Amazon S3 bucket, indicating whether the bucket is public.         | S3.FC10 | s3:GetBucketPolicyStatus            | GetBucketPolicyStatus              | GetBucketPolicyStatus              |
| S3.A40 | Returns the replication configuration of a bucket.  | S3.FC15 | s3:GetReplicationConfiguration      | GetBucketReplication               | GetBucketReplication               |
| S3.A41 | Returns the request payment configuration of a bucket.  | S3.FC5  | s3:GetBucketRequestPayment          | GetBucketRequestPayment            | GetBucketRequestPayment            |
| S3.A42 | Returns the tag set associated with the bucket.   | S3.FC7  | s3:GetBucketTagging                 | GetBucketTagging                   | GetBucketTagging                   |
| S3.A43 | Returns the versioning state of a bucket.   | S3.FC6  | s3:GetBucketVersioning              | GetBucketVersioning                | GetBucketVersioning                |
| S3.A44 | Returns the website configuration for a bucket.   | S3.FC16 | s3:GetBucketWebsite                 | GetBucketWebsite                   | GetBucketWebsite                   |
| S3.A45 | Retrieves an object from Amazon S3.   | S3.FC1  | s3:GetObject                        | GetObject                          | GetObject                          |
| S3.A46 | Retrieves an object version from Amazon S3.   | S3.FC3  | s3:GetObjectVersion                 | GetObject                          | GetObject(VersionId=)              |
| S3.A47 | Returns ACL information about an object   | S3.FC1  | s3:GetObjectAcl                     | GetObjectAcl                       | GetObjectAcl                       |
| S3.A48 | Returns ACL information about an object version, use the versionId subresource.                       | S3.FC9  | s3:GetObjectVersionAcl              | GetObjectAcl                       | GetObjectAcl(VersionId=)           |
| S3.A49 | Gets Object Lock legal hold for a specific object   | S3.FC29 | s3:GetObjectLegalHold               | GetObjectLegalHold                 | GetObjectLegalHold                 |
| S3.A50 | Gets the default S3 Object Lock configuration for a bucket.   | S3.FC17 | s3:GetBucketObjectLockConfiguration | GetObjectLockConfiguration         | GetObjectLockConfiguration         |

|        |  |         |                                     |                                   |                                   |
|--------|--|---------|-------------------------------------|-----------------------------------|-----------------------------------|
| S3.A51 | Retrieves an object's retention settings.  | S3.FC17 | s3:GetObjectRetention               | GetObjectRetention                | GetObjectRetention                |
| S3.A52 | Returns the tag-set of an object.  | S3.FC2  | s3:GetObjectTagging                 | GetObjectTagging                  | GetObjectTagging                  |
| S3.A53 | Returns the tag-set of a specific version of an object.  | S3.FC4  | s3:GetObjectVersionTagging          | GetObjectTagging                  | GetObjectTagging(VersionId=)      |
| S3.A54 | Returns torrent files from an object.  | S3.FC21 | s3:GetObjectTorrent                 | GetObjectTorrent                  | GetObjectTorrent                  |
| S3.A55 | (Deprecated) No documented usage of this action.   | S3.FC21 | s3:GetObjectVersionTorrent          | -                                 | -                                 |
| S3.A56 | Grants Amazon S3 the permission to replicate both unencrypted objects and objects encrypted with SSE-S3 or SSE-KMS | S3.FC15 | s3:GetObjectVersionForReplication   | -                                 | -                                 |
| S3.A57 | Retrieves the PublicAccessBlock configuration for an Amazon S3 bucket.   | S3.FC24 | s3:GetBucketPublicAccessBlock       | GetPublicAccessBlock              | GetPublicAccessBlock              |
| S3.A58 | Determines if a bucket exists and you have permission to access it.  | S3.FC1  | s3:HeadBucket                       | HeadBucket                        | HeadBucket                        |
| S3.A59 | Retrieves metadata from an object without returning the object itself.   | S3.FC1  | s3:GetObject                        | HeadObject                        | HeadObject                        |
| S3.A60 | Retrieves metadata from an object version without returning the object itself.                                     | S3.FC3  | s3:GetObjectVersion                 | HeadObject                        | HeadObject(VersionId=)            |
| S3.A61 | Lists the analytics configurations for the bucket.   | S3.FC11 | s3:GetAnalyticsConfiguration        | ListBucketAnalyticsConfigurations | ListBucketAnalyticsConfigurations |
| S3.A62 | Returns a list of inventory configurations for the bucket.   | S3.FC12 | s3:GetInventoryConfiguration        | ListBucketInventoryConfigurations | ListBucketInventoryConfigurations |
| S3.A63 | Lists the metrics configurations for the bucket.   | S3.FC14 | s3:GetMetricsConfiguration          | ListBucketMetricsConfigurations   | ListBucketMetricsConfigurations   |
| S3.A64 | Returns a list of all buckets owned by the authenticated sender of the request.                                    | S3.FC5  | s3>ListAllMyBuckets                 | ListBuckets                       | ListBuckets                       |
| S3.A65 | Lists in-progress multipart uploads.   | S3.FC1  | s3>ListBucketMultipartUploads       | ListMultipartUploads              | ListMultipartUploads              |
| S3.A66 | (Deprecated) Returns some or all (up to 1000) of the objects in a bucket.  | S3.FC1  | s3>ListBucket                       | ListObjects                       | ListObjects                       |
| S3.A67 | Returns some or all (up to 1000) of the objects in a bucket.   | S3.FC1  | s3>ListBucket                       | ListObjectsV2                     | ListObjectsV2                     |
| S3.A68 | Lists metadata about all of the versions of objects in a bucket.   | S3.FC3  | s3>ListBucketVersions               | ListObjectVersions                | ListObjectVersions                |
| S3.A69 | Lists the parts that have been uploaded for a specific multipart upload.   | S3.FC1  | s3>ListMultipartUploadParts         | ListParts                         | ListParts                         |
| S3.A70 | Allows Amazon S3 to change the ownership of a replicated object  | S3.FC15 | s3:ObjectOwnerOverrideToBucketOwner | -                                 | -                                 |
| S3.A71 | Sets the Transfer Acceleration state of an existing bucket.  | S3.FC18 | s3:PutAccelerateConfiguration       | PutBucketAccelerateConfiguration  | PutBucketAccelerateConfiguration  |
| S3.A72 | Sets the permissions on an existing bucket using access control lists (ACL).                                       | S3.FC8  | s3:PutBucketAcl                     | PutBucketAcl                      | PutBucketAcl                      |
| S3.A73 | Adds an analytics configuration (identified by the analytics ID) to the bucket.                                    | S3.FC11 | s3:PutAnalyticsConfiguration        | PutBucketAnalyticsConfiguration   | PutBucketAnalyticsConfiguration   |
| S3.A74 | Sets the CORS configuration for your bucket.   | S3.FC22 | s3:PutBucketCORS                    | PutBucketCors                     | PutBucketCors                     |
| S3.A75 | Sets the default encryption configuration for the bucket.  | S3.FC23 | s3:PutEncryptionConfiguration       | PutBucketEncryption               | PutBucketEncryption               |
| S3.A76 | Adds an inventory configuration (identified by the inventory ID) to the bucket                                     | S3.FC12 | s3:PutInventoryConfiguration        | PutBucketInventoryConfiguration   | PutBucketInventoryConfiguration   |
| S3.A77 | (Deprecated) Creates a new lifecycle configuration for the bucket or replaces an existing lifecycle configuration. | S3.FC13 | s3:PutLifecycleConfiguration        | PutBucketLifecycle                | PutBucketLifecycle                |

|         |   |         |                                |                                    |                                     |
|---------|---|---------|--------------------------------|------------------------------------|-------------------------------------|
| S3.A78  | Creates a new lifecycle configuration for the bucket or replaces an existing lifecycle configuration.   | S3.FC13 | s3:PutLifecycleConfiguration   | PutBucketLifecycleConfiguration    | PutBucketLifecycleConfiguration     |
| S3.A79  | Sets the logging parameters for a bucket.   | S3.FC19 | s3:PutBucketLogging            | PutBucketLogging                   | PutBucketLogging                    |
| S3.A80  | Sets or updates a metrics configuration for the CloudWatch request metrics (specified by the metrics configuration ID) from the bucket.   | S3.FC14 | s3:PutMetricsConfiguration     | PutBucketMetricsConfiguration      | PutBucketMetricsConfiguration       |
| S3.A81  | (Deprecated) Enables you to receive notifications when certain events happen in your bucket.  | S3.FC20 | s3:PutBucketNotification       | PutBucketNotification              | PutBucketNotification               |
| S3.A82  | Enables you to receive notifications when certain events happen in your bucket.   | S3.FC20 | s3:PutBucketNotification       | PutBucketNotificationConfiguration | PutBucketNotificationConfiguration  |
| S3.A83  | Adds to or replaces a policy on a bucket.   | S3.FC10 | s3:PutBucketPolicy             | PutBucketPolicy                    | PutBucketPolicy                     |
| S3.A84  | Creates a new replication configuration (or replaces an existing one, if present).  | S3.FC15 | s3:PutReplicationConfiguration | PutBucketReplication               | PutBucketReplication                |
| S3.A85  | Sets the request payment configuration of a bucket.   | S3.FC5  | s3:PutBucketRequestPayment     | PutBucketRequestPayment            | PutBucketRequestPayment             |
| S3.A86  | Adds a set of tags to an existing bucket.   | S3.FC7  | s3:PutBucketTagging            | PutBucketTagging                   | PutBucketTagging                    |
| S3.A87  | Sets the versioning state of an existing bucket.  | S3.FC6  | s3:PutBucketVersioning         | PutBucketVersioning                | PutBucketVersioning                 |
| S3.A88  | Sets the configuration of the website that is specified in the website subresource.   | S3.FC16 | s3:PutBucketWebsite            | PutBucketWebsite                   | PutBucketWebsite                    |
| S3.A89  | Adds an object to a bucket.   | S3.FC1  | s3:PutObject                   | PutObject, PostObject              | PutObject                           |
| S3.A90  | Sets the access control list (ACL) permissions for an object. You must have WRITE_ACP permission to set the ACL of an object.   | S3.FC1  | s3:PutObjectAcl                | PutObjectAcl                       | PutObjectAcl                        |
| S3.A91  | Sets the access control list (ACL) permissions for an object version. You must have WRITE_ACP permission to set the ACL of an object version.   | S3.FC9  | s3:PutObjectVersionAcl         | PutObjectAcl                       | PutObjectAcl(VersionId=)            |
| S3.A92  | Puts Object Lock legal hold on a specific object  | S3.FC29 | s3:PutObjectLegalHold          | PutObjectLegalHold                 | PutObjectLegalHold                  |
| S3.A93  | Allows to place a default S3 Object Lock configuration at bucket creation (AWS Support needs to be contacted for existing buckets). It automatically enables versioning, even without the permission. | S3.FC17 | s3:PutObjectLockConfiguration  | PutObjectLockConfiguration         | PutObjectLockConfiguration          |
| S3.A94  | Puts object retention on a specific object  | S3.FC17 | s3:PutObjectRetention          | PutObjectRetention                 | PutObjectRetention                  |
| S3.A95  | Adds a set of tags to an existing object.   | S3.FC2  | s3:PutObjectTagging            | PutObjectTagging                   | PutObjectTagging                    |
| S3.A96  | Adds a set of tags to an existing object version  | S3.FC4  | s3:PutObjectVersionTagging     | PutObjectVersionTagging            | PutObjectVersionTagging(VersionId=) |
| S3.A97  | Creates or modifies the PublicAccessBlock configuration for an Amazon S3 bucket.  | S3.FC24 | s3:PutBucketPublicAccessBlock  | PutPublicAccessBlock               | PutPublicAccessBlock                |
| S3.A98  | Allows Amazon S3 to replicate delete markers to the destination bucket  | S3.FC15 | s3:ReplicateDelete             | -                                  | -                                   |
| S3.A99  | Allows Amazon S3 to replicate objects to the destination bucket, including tags   | S3.FC15 | s3:ReplicateObject             | -                                  | -                                   |
| S3.A100 | Allows Amazon S3 to replicate object tags to the destination bucket   | S3.FC15 | s3:ReplicateTags               | -                                  | -                                   |
| S3.A101 | Restores a temporary copy of an archived object.  | S3.FC1  | s3:RestoreObject               | RestoreObject                      | RestoreObject                       |
| S3.A102 | Filters the contents of an Amazon S3 object based on a simple structured query language (SQL) statement.  | S3.FC1  | s3:GetObject                   | SelectObjectContent                | SelectObjectContent                 |

|         |   |         |  |   |   |
|---------|---|---------|--|---|---|
| S3.A103 | Uploads a part in a multipart upload.   | S3.FC1  | s3:PutObject                             | UploadPart                                  | UploadPart                                  |
| S3.A104 | Uploads a part by copying data from an existing object as a data source.            | S3.FC1  | s3:PutObject<br>s3:GetObject             | UploadPartCopy                              | UploadPartCopy                              |
| S3.A105 | Creates a new access point.   | S3.FC26 | s3>CreateAccessPoint                     | CreateAccessPoint                           | CreateAccessPoint                           |
| S3.A106 | Creates a new Amazon S3 Batch Operations job.                                       | S3.FC27 | s3:CreateJob                             | JobCreated                                  | CreateJob                                   |
| S3.A107 | Deletes the specified access point.   | S3.FC26 | s3>DeleteAccessPoint                     | DeleteAccessPoint                           | DeleteAccessPoint                           |
| S3.A108 | Deletes the policy on a specified access point                                      | S3.FC26 | s3>DeleteAccessPointPolicy               | DeleteAccessPointPolicy                     | DeleteAccessPointPolicy                     |
| S3.A109 | Removes the PublicAccessBlock configuration for an AWS account.                     | S3.FC25 | s3:PutAccountPublicAccessBlock           | DeletePublicAccessBlock                     | DeletePublicAccessBlock                     |
| S3.A110 | Retrieves the configuration parameters and status for a Batch Operations job.       | S3.FC27 | s3:DescribeJob                           | DescribeJob                                 | DescribeJob                                 |
| S3.A111 | Retrieves access point metadata   | S3.FC26 | s3:GetAccessPoint                        | GetAccessPoint                              | GetAccessPoint                              |
| S3.A112 | Returns the policy of a specified access point.                                     | S3.FC26 | s3:GetAccessPointPolicy                  | GetAccessPointPolicy                        | GetAccessPointPolicy                        |
| S3.A113 | Retrieves the policy status for a specific access point's policy                    | S3.FC26 | s3:GetAccessPointPolicyStatus            | GetAccessPointPolicyStatus                  | GetAccessPointPolicyStatus                  |
| S3.A114 | Retrieves the PublicAccessBlock configuration for an AWS account                    | S3.FC25 | s3:GetAccountPublicAccessBlock           | GetPublicAccessBlock                        | GetPublicAccessBlock                        |
| S3.A115 | Returns a list of the access points currently associated with the specified bucket. | S3.FC26 | s3>ListAccessPoints                      | ListAccessPoints                            | ListAccessPoints                            |
| S3.A116 | Lists current jobs and jobs that have ended recently.                               | S3.FC27 | s3>ListJobs                              | ListJobs                                    | ListJobs                                    |
| S3.A117 | Adds to or replaces a data policy on an access point.                               | S3.FC26 | s3:PutAccessPointPolicy                  | PutAccessPointPolicy                        | PutAccessPointPolicy                        |
| S3.A118 | Creates or modifies the PublicAccessBlock configuration for an AWS account.         | S3.FC25 | s3:PutAccountPublicAccessBlock           | PutPublicAccessBlock                        | PutPublicAccessBlock                        |
| S3.A119 | Updates an existing job's priority.   | S3.FC27 | s3:UpdateJobPriority                     | -   | UpdateJobPriority                           |
| S3.A120 | Updates the status for the specified job.   | S3.FC27 | s3:UpdateJobStatus                       | JobStatusChanged                            | UpdateJobStatus                             |
| S3.A121 | Removes OwnershipControls for an Amazon S3 bucket.                                  | S3.FC30 | s3:PutBucketOwnershipControls            | DeleteBucketOwnershipControls               | DeleteBucketOwnershipControls               |
| S3.A122 | Retrieves OwnershipControls for an Amazon S3 bucket.                                | S3.FC30 | s3:GetBucketOwnershipControls            | GetBucketOwnershipControls                  | GetBucketOwnershipControls                  |
| S3.A123 | Creates or modifies OwnershipControls for an Amazon S3 bucket                       | S3.FC30 | s3:PutBucketOwnershipControls            | PutBucketOwnershipControls                  | PutBucketOwnershipControls                  |
| S3.A124 | Deletes the S3 Intelligent-Tiering configuration from the specified bucket          | S3.FC13 | s3>DeleteIntelligentTieringConfiguration | DeleteBucketIntelligentTieringConfiguration | DeleteBucketIntelligentTieringConfiguration |
| S3.A125 | Gets the S3 Intelligent-Tiering configuration from the specified bucket             | S3.FC13 | s3:GetIntelligentTieringConfiguration    | GetBucketIntelligentTieringConfiguration    | GetBucketIntelligentTieringConfiguration    |
| S3.A126 | Lists the S3 Intelligent-Tiering configuration from the specified bucket            | S3.FC13 | s3>ListIntelligentTieringConfigurations  | ListBucketIntelligentTieringConfigurations  | ListBucketIntelligentTieringConfigurations  |
| S3.A127 | Puts a S3 Intelligent-Tiering configuration to the specified bucket                 | S3.FC13 | s3:PutIntelligentTieringConfiguration    | PutBucketIntelligentTieringConfiguration    | PutBucketIntelligentTieringConfiguration    |
| S3.A128 | Deletes the Amazon S3 Storage Lens configuration                                    | S3.FC31 | s3>DeleteStorageLensConfiguration        | DeleteStorageLensConfiguration              | DeleteStorageLensConfiguration              |
| S3.A129 | Deletes the Amazon S3 Storage Lens configuration tags                               | S3.FC31 | s3>DeleteStorageLensConfigurationTagging | DeleteStorageLensConfigurationTagging       | DeleteStorageLensConfigurationTagging       |

|         |   |         |   |  |  |
|---------|---|---------|---|--|--|
| S3.A130 | Gets the Amazon S3 Storage Lens configuration   | S3.FC31 | s3:GetStorageLensConfiguration                | GetStorageLensConfiguration                | GetStorageLensConfiguration                |
| S3.A131 | Gets the tags of Amazon S3 Storage Lens configuration   | S3.FC31 | s3:GetStorageLensConfigurationTagging         | GetStorageLensConfigurationTagging         | GetStorageLensConfigurationTagging         |
| S3.A132 | Gets a list of Amazon S3 Storage Lens configurations  | S3.FC31 | s3>ListStorageLensConfigurations              | ListStorageLensConfigurations              | ListStorageLensConfigurations              |
| S3.A133 | Puts an Amazon S3 Storage Lens configuration  | S3.FC31 | s3:PutStorageLensConfiguration                | PutStorageLensConfiguration                | PutStorageLensConfiguration                |
| S3.A134 | Puts or replaces tags on an existing Amazon S3 Storage Lens configuration   | S3.FC31 | s3:PutStorageLensConfigurationTagging         | PutStorageLensConfigurationTagging         | PutStorageLensConfigurationTagging         |
| S3.A135 | Creates an Object Lambda access point   | S3.FC32 | s3>CreateAccessPointForObjectLambda           | CreateAccessPointForObjectLambda           | CreateAccessPointForObjectLambda           |
| S3.A136 | Deletes the specified Object Lambda access point  | S3.FC32 | s3>DeleteAccessPointForObjectLambda           | DeleteAccessPointForObjectLambda           | DeleteAccessPointForObjectLambda           |
| S3.A137 | Removes the resource policy for an Object Lambda access point   | S3.FC32 | s3>DeleteAccessPointPolicyForObjectLambda     | DeleteAccessPointPolicyForObjectLambda     | DeleteAccessPointPolicyForObjectLambda     |
| S3.A138 | Returns configuration for an Object Lambda access point   | S3.FC32 | s3:GetAccessPointConfigurationForObjectLambda | GetAccessPointConfigurationForObjectLambda | GetAccessPointConfigurationForObjectLambda |
| S3.A139 | Returns configuration information about the specified Object Lambda access point  | S3.FC32 | s3:GetAccessPointForObjectLambda              | GetAccessPointForObjectLambda              | GetAccessPointForObjectLambda              |
| S3.A140 | Returns the resource policy for an Object Lambda access point   | S3.FC32 | s3:GetAccessPointPolicyForObjectLambda        | GetAccessPointPolicyForObjectLambda        | GetAccessPointPolicyForObjectLambda        |
| S3.A141 | Returns the status of the resource policy associated with an Object Lambda access point   | S3.FC32 | s3:GetAccessPointPolicyStatusForObjectLambda  | GetAccessPointPolicyStatusForObjectLambda  | GetAccessPointPolicyStatusForObjectLambda  |
| S3.A142 | Returns a list of the access points associated with the Object Lambda access point  | S3.FC32 | s3>ListAccessPointsForObjectLambda            | ListAccessPointsForObjectLambda            | ListAccessPointsForObjectLambda            |
| S3.A143 | Replaces configuration for an Object Lambda access point  | S3.FC32 | s3:PutAccessPointConfigurationForObjectLambda | PutAccessPointConfigurationForObjectLambda | PutAccessPointConfigurationForObjectLambda |
| S3.A144 | Creates or replaces resource policy for an Object Lambda access point   | S3.FC32 | s3:PutAccessPointPolicyForObjectLambda        | PutAccessPointPolicyForObjectLambda        | PutAccessPointPolicyForObjectLambda        |
| S3.A145 | Grants permission to abort a multipart upload   | S3.FC32 | s3-object-lambda:AbortMultipartUpload         | -  | -  |
| S3.A146 | Grants permission to remove the null version of an object and insert a delete marker, which becomes the current version of the object | S3.FC32 | s3-object-lambda:DeleteObject                 | -  | -  |
| S3.A147 | Grants permission to use the tagging subresource to remove the entire tag set from the specified object                               | S3.FC32 | s3-object-lambda:DeleteObjectTagging          | -  | -  |
| S3.A148 | Grants permission to retrieve objects from Amazon S3  | S3.FC32 | s3-object-lambda:GetObject                    | -  | -  |
| S3.A149 | Grants permission to return the access control list (ACL) of an object  | S3.FC32 | s3-object-lambda:GetObjectAcl                 | -  | -  |
| S3.A150 | Grants permission to get an object's current legal hold status  | S3.FC32 | s3-object-lambda:GetObjectLegalHold           | -  | -  |

|         |   |         |   |                        |                        |
|---------|---|---------|---|------------------------|------------------------|
| S3.A151 | Grants permission to retrieve the retention settings for an object  | S3.FC32 | s3-object-lambda:GetObjectRetention         | -                      | -                      |
| S3.A152 | Grants permission to return the tag set of an object  | S3.FC32 | s3-object-lambda:GetObjectTagging           | -                      | -                      |
| S3.A153 | Grants permission to retrieve a specific version of an object   | S3.FC32 | s3-object-lambda:GetObjectVersion           | -                      | -                      |
| S3.A154 | Grants permission to list some or all of the objects in an Amazon S3 bucket (up to 1000)                        | S3.FC32 | s3-object-lambda>ListBucket                 | -                      | -                      |
| S3.A155 | Grants permission to list the parts that have been uploaded for a specific multipart upload                     | S3.FC32 | s3-object-lambda>ListMultipartUploadParts   | -                      | -                      |
| S3.A156 | Grants permission to add an object to a bucket  | S3.FC32 | s3-object-lambda:PutObject                  | -                      | -                      |
| S3.A157 | Grants permission to set the access control list (ACL) permissions for new or existing objects in an S3 bucket. | S3.FC32 | s3-object-lambda:PutObjectAcl               | -                      | -                      |
| S3.A158 | Grants permission to apply a legal hold configuration to the specified object                                   | S3.FC32 | s3-object-lambda:PutObjectLegalHold         | -                      | -                      |
| S3.A159 | Grants permission to place an object retention configuration on an object                                       | S3.FC32 | s3-object-lambda:PutObjectRetention         | -                      | -                      |
| S3.A160 | Grants permission to set the supplied tag-set to an object that already exists in a bucket                      | S3.FC32 | s3-object-lambda:PutObjectTagging           | -                      | -                      |
| S3.A161 | Grants permission to restore an archived copy of an object back into Amazon S3                                  | S3.FC32 | s3-object-lambda:RestoreObject              | -                      | -                      |
| S3.A162 | Passes transformed objects to a GetObject operation when using Object Lambda access points                      | S3.FC32 | s3-object-lambda:WriteGetObjectResponse     | WriteGetObjectResponse | WriteGetObjectResponse |
| S3.A163 | Grants permission to remove a specific version of an object   | S3.FC32 | s3-object-lambda>DeleteObjectVersion        | -                      | -                      |
| S3.A164 | Grants permission to remove the entire tag set for a specific version of the object                             | S3.FC32 | s3-object-lambda>DeleteObjectVersionTagging | -                      | -                      |
| S3.A165 | Grants permission to return the access control list (ACL) of a specific object version                          | S3.FC32 | s3-object-lambda:GetObjectVersionAcl        | -                      | -                      |
| S3.A166 | Grants permission to return the tag set for a specific version of the object                                    | S3.FC32 | s3-object-lambda:GetObjectVersionTagging    | -                      | -                      |
| S3.A167 | Grants permission to list in-progress multipart uploads   | S3.FC32 | s3-object-lambda>ListBucketMultipartUploads | -                      | -                      |
| S3.A168 | Grants permission to list metadata about all the versions of objects in an Amazon S3 bucket                     | S3.FC32 | s3-object-lambda>ListBucketVersions         | -                      | -                      |

|         |  |         |  |   |   |
|---------|--|---------|--|---|---|
| S3.A169 | Grants permission to use the ACL subresource to set the access control list (ACL) permissions for an object that already exists in a bucket                            | S3.FC32 | s3-object-lambda:PutObjectVersionAcl       | -                                       | -                                       |
| S3.A170 | Grants permission to set the supplied tag-set for a specific version of an object  | S3.FC32 | s3-object-lambda:PutObjectVersionTagging   | -                                       | -                                       |
| S3.A171 | Returns configuration information about the specified Multi-Region Access Point.   | S3.FC33 | s3:GetMultiRegionAccessPoint               | GetMultiRegionAccessPoint               | GetMultiRegionAccessPoint               |
| S3.A172 | Indicates whether the specified Multi-Region Access Point has an access control policy that allows public access.  | S3.FC33 | s3:GetMultiRegionAccessPointPolicyStatus   | GetMultiRegionAccessPointPolicyStatus   | GetMultiRegionAccessPointPolicyStatus   |
| S3.A173 | Creates a Multi-Region Access Point and associates it with the specified buckets.  | S3.FC33 | s3>CreateMultiRegionAccessPoint            | CreateMultiRegionAccessPoint            | CreateMultiRegionAccessPoint            |
| S3.A174 | Retrieves the status of an asynchronous request to manage a Multi-Region Access Point.   | S3.FC33 | s3:DescribeMultiRegionAccessPointOperation | DescribeMultiRegionAccessPointOperation | DescribeMultiRegionAccessPointOperation |
| S3.A175 | Deletes a Multi-Region Access Point. This action does not delete the buckets associated with the Multi-Region Access Point, only the Multi-Region Access Point itself. | S3.FC33 | s3>DeleteMultiRegionAccessPoint            | DeleteMultiRegionAccessPoint            | DeleteMultiRegionAccessPoint            |
| S3.A176 | Returns a list of the Multi-Region Access Points currently associated with the specified AWS account.  | S3.FC33 | s3>ListMultiRegionAccessPoints             | ListMultiRegionAccessPoints             | ListMultiRegionAccessPoints             |
| S3.A177 | Returns the access control policy of the specified Multi-Region Access Point.  | S3.FC33 | s3:GetMultiRegionAccessPointPolicy         | GetMultiRegionAccessPointPolicy         | GetMultiRegionAccessPointPolicy         |
| S3.A178 | Associates an access control policy with the specified Multi-Region Access Point.  | S3.FC33 | s3:PutMultiRegionAccessPointPolicy         | PutMultiRegionAccessPointPolicy         | PutMultiRegionAccessPointPolicy         |
| S3.A179 | Remove tags from an existing Amazon S3 Batch operations job  | S3.FC27 | s3>DeleteJobTagging                        | DeleteJobTagging                        | DeleteJobTagging                        |
| S3.A180 | Return the tag set of an existing Amazon S3 Batch operations job   | S3.FC27 | s3:GetJobTagging                           | GetJobTagging                           | GetJobTagging                           |
| S3.A181 | Get an Amazon S3 storage lens dashboard  | S3.FC31 | s3:GetStorageLensDashboard                 | GetStorageLensDashboardDataInternal     | GetStorageLensDashboard                 |
| S3.A182 | Replace tags on an existing Amazon S3 Batch operations job   | S3.FC27 | s3:PutJobTagging                           | PutJobTagging                           | PutJobTagging                           |

## Appendix 3 - List of the Service availability in AWS Regions

| Region Name               | Region Id      | Amazon Simple Storage Service (S3) (s3) | AWS S3 Control (s3-control) |
|---------------------------|----------------|---|-----------------------------|
| Africa (Cape Town)        | af-south-1     | Yes                                     | No                          |
| Asia Pacific (Hong Kong)  | ap-east-1      | Yes                                     | No                          |
| Asia Pacific (Tokyo)      | ap-northeast-1 | Yes                                     | Yes                         |
| Asia Pacific (Seoul)      | ap-northeast-2 | Yes                                     | Yes                         |
| Asia Pacific (Osaka)      | ap-northeast-3 | Yes                                     | Yes                         |
| Asia Pacific (Mumbai)     | ap-south-1     | Yes                                     | Yes                         |
| Asia Pacific (Singapore)  | ap-southeast-1 | Yes                                     | Yes                         |
| Asia Pacific (Sydney)     | ap-southeast-2 | Yes                                     | Yes                         |
| Canada (Central)          | ca-central-1   | Yes                                     | Yes                         |
| China (Beijing)           | cn-north-1     | Yes                                     | Yes                         |
| China (Ningxia)           | cn-northwest-1 | Yes                                     | Yes                         |
| Europe (Frankfurt)        | eu-central-1   | Yes                                     | Yes                         |
| Europe (Stockholm)        | eu-north-1     | Yes                                     | Yes                         |
| Europe (Milan)            | eu-south-1     | Yes                                     | No                          |
| Europe (Ireland)          | eu-west-1      | Yes                                     | Yes                         |
| Europe (London)           | eu-west-2      | Yes                                     | Yes                         |
| Europe (Paris)            | eu-west-3      | Yes                                     | Yes                         |
| Middle East (Bahrain)     | me-south-1     | Yes                                     | No                          |
| South America (São Paulo) | sa-east-1      | Yes                                     | Yes                         |
| US East (N. Virginia)     | us-east-1      | Yes                                     | Yes                         |
| US East (Ohio)            | us-east-2      | Yes                                     | Yes                         |
| AWS GovCloud (US-East)    | us-gov-east-1  | Yes                                     | Yes                         |
| AWS GovCloud (US-West)    | us-gov-west-1  | Yes                                     | Yes                         |
| US ISO East               | us-iso-east-1  | Yes                                     | No                          |
| US ISO WEST               | us-iso-west-1  | Yes                                     | No                          |
| US ISOB East (Ohio)       | us-isob-east-1 | Yes                                     | No                          |
| US West (N. California)   | us-west-1      | Yes                                     | Yes                         |
| US West (Oregon)          | us-west-2      | Yes                                     | Yes                         |