**VSOC with MITRE ATT&CK integration with AWS Security Hub**

**Enrichment of native security findings from AWS**

**INDEX**

[1.- Introduction 5](#_bookmark0)

[1.1.- Information 5](#_bookmark1)

[1.2.- Overview 5](#_bookmark2)

[1.3.- Requirements 5](#_bookmark3)

[1.4.- This is how the solution works 6](#_bookmark4)

[1.5.- This is how the result looks like 7](#_bookmark5)

[2.- Project details 8](#_bookmark6)

[2.1.- Source 8](#_bookmark7)

[2.2.- Objectives 8](#_bookmark8)

[2.3.- Status 8](#_bookmark9)

[2.4.- Test and conformity 8](#_bookmark10)

[2.4.1.- Tests 8](#_bookmark11)

[2.4.2.- Conformity, IaC 9](#_bookmark12)

[2.4.3.- Conformity, code 9](#_bookmark13)

[3.- Repository details 10](#_bookmark14)

[3.1.- Database 10](#_bookmark15)

[3.1.1.- Credentials 10](#_bookmark16)

[3.1.2.- Schema 10](#_bookmark17)

[3.1.3.- Content 11](#_bookmark18)

[3.1.4.- Requests and use 11](#_bookmark19)

[4.- Security Hub integration details 13](#_bookmark20)

[4.1.- MITRE ATT&CK Techniques 13](#_bookmark21)

[4.2.- MITRE ATT&CK Tactics 14](#_bookmark22)

[5.- Deployment and configuration 16](#_bookmark23)

[5.1.- Previous 16](#_bookmark24)

[5.2.- Deployment steps 16](#_bookmark25)

[5.3.- Parameters 17](#_bookmark26)

[5.3.1.- Main stack 17](#_bookmark27)

[5.3.2.- RDS stack 18](#_bookmark28)

[5.3.3.- Conformance Pack stack 18](#_bookmark29)

[5.4.- Updates 20](#_bookmark30)

[5.4.1.- Previous steps 20](#_bookmark31)

[5.4.2.- Nested stack updates 20](#_bookmark32)

[5.4.3.- Repository 21](#_bookmark33)

[6.- Self-remediation module 22](#_bookmark34)

[6.1.- Case 1, fix password policy 22](#_bookmark35)

[6.2.- Case 2, enable data recovery 22](#_bookmark36)

[6.3.- Case 3, blocks suspicious user 23](#_bookmark37)

[6.4.- Add-on deployment 23](#_bookmark38)

[6.4.1.- Add-on parameters 24](#_bookmark39)

7.- Next steps 25

[Anexo I. Conformance Pack details 26](#_bookmark40)

[AWS Services 26](#_bookmark41)

[Anexo II. Mapping summary 31](#_bookmark42)

[MITRE ATT&CK v.12 31](#_bookmark43)

[AWS Service & Events 33](#_bookmark44)

[CIS CSC v8 42](#_bookmark45)

[NIST 800-53-rev5 46](#_bookmark46)

[PCI-DSS v3.2.1 50](#_bookmark47)

[C5 (2022) 54](#_bookmark48)

[ENS CNN-STIC (2022) 55](#_bookmark49)

# 1.- Introduction

## 1.1.- Information

Today, we are introducing Virtual Security Operation Center (SOC) with MITRE Attack integration with AWS Security Hub, an example solution targeting small enterprises and Partners. The solution will show how you can retrieve valuable alerts from native AWS services, which have been centralized in Security Hub, to enrich them with information regarding tactics and techniques from [MITRE ATT&CK](https://attack.mitre.org/matrices/enterprise/cloud/), giving you a broad view of attack vectors to which your environment might be exposed. This solution is compatible with multi-account environments and AWS Organizations.

## 1.2.- Overview

This solution will show how valuable alerts from native AWS services can be retrieved, which have been centralised in Security Hub, to enrich them with information regarding tactics and techniques from [MITRE ATT&CK](https://attack.mitre.org/matrices/enterprise/cloud/), providing a broad view of attack vectors to which the environment might be exposed. This solution is compatible with multi-account environments and AWS Organisations.

* [Project details](#_bookmark6)
* [Repository details](#_bookmark10)
* [Conformance Pack details](#_bookmark40)
* [Security Hu](#_bookmark20)b integration details
* [Mapped summary](#_bookmark42)
* [Deployment](#_bookmark23) steps
* [Self-remediation module](#_bookmark34)

## 1.3.- Requirements

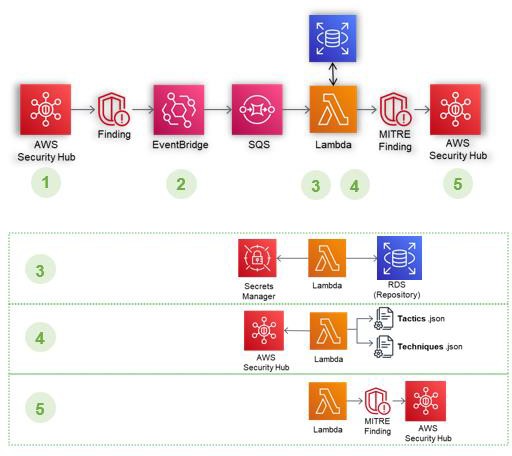
Although this solution can be deployed independently (in isolated accounts) it has been designed to comply with the [AWS security reference architecture](https://docs.aws.amazon.com/wellarchitected/latest/framework/security.html). Its best performance occurs when deployed in centralised security accounts (those designated to centralise the management of AWS Security Hub, AWS Config and Amazon GuardDuty services).

If the following services are not already in use, you can enable them during the deployment process:

* The solution is supported on Security Hub.
* The solution is supported by AWS Config.
* It is highly recommended (but not required) to enable the GuardDuty service. The following network resources must be available to support the deployment:
* At least two sub-networks (we recommend PRIVATE type) in different availability zones, for the deployment of the RDS repository.
* At least two sub-networks (we recommend PRIVATE type) in different availability zones, for the deployment of VPC Lambda, which shall have connectivity to the RDS.

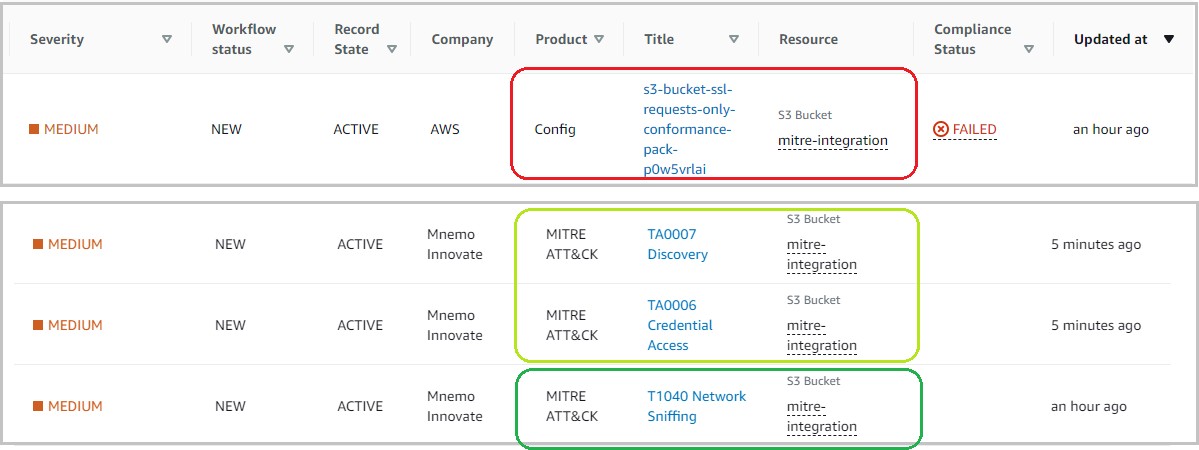
## 1.4.- This is how the solution works

1. The originating service generates a new discovery in Security Hub.
2. A CloudWatch EventBridge rule captures valid findings and sends them to an SQS queue.
3. The Lambda function is invoked. It connects to the repository in RDS and, based on the "rule/event" that triggered the original find, retrieves related information on techniques, tactics, security standards and other details.
4. The Lambda function prepares new enriched findings, corresponding to each technique and tactic retrieved.
5. Finally, the new findings are published in the Security Hub.

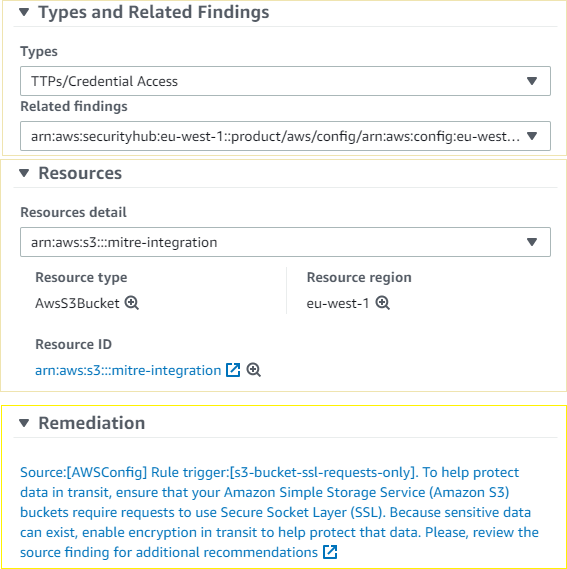


## 1.5.- This is how the result looks like

Depending on the information mapped and recorded in the database, one or more techniques will correspond to each security rule (or event) recorded, and at least one tactic. This generates new MITRE ATT&CK findings in Security Hub.



In addition to maintaining the details of the original finding and referring to it by means of a link, information concerning the technique shall be added.



# 2.- Project details

## 2.1.- Source

As a security operator using **only native tools** from the AWS environment, the information provided in the Security Hub dashboards can be too limited to give a **threat and attacker centric focus**; the findings in Security Hub are more geared towards giving a quick reference to security standards compliance.

Only some findings provide information from the [MITRE ATT&CK](https://attack.mitre.org/matrices/enterprise/cloud/) framework from the originating service (Amazon GuardDuty provides this information for a percentage of its finding types).T

The goal of this project is to extend this capability to a wider range of findings, giving the security operator a quick understanding of how exposed their environment is and *to what kind of attacks*.

## 2.2.- Objectives

1. **Correlation** or mapping of MITRE ATT&CK tactics and techniques applicable to the AWS environment, with rules and events that can be handled natively.
2. Formation of **MITRE ATT&CK Compliance Rules Package** for AWS Config.
3. Finally, creation of a finding’s enrichment process in Security Hub with the above processed information.

## 2.3.- Status

* + **60 Techniques/Sub-Techniques** (TTPs) have been catalogued (out of 97 applicable to cloud environments), spread across 11 different Tactics (TA).
  + These have been linked to **277 rules/events** of AWS native services that can be centralised in Security Hub.
  + Controls have been linked to the main security standards (ENS, NIST, CIS, PCI, C5).
  + A **MITRE ATT&CK Compliance Rules Package** has been formalised with 120 managed rules.
  + The enrichment process currently has the capability to create, update and archive MITRE findings based on the original findings.

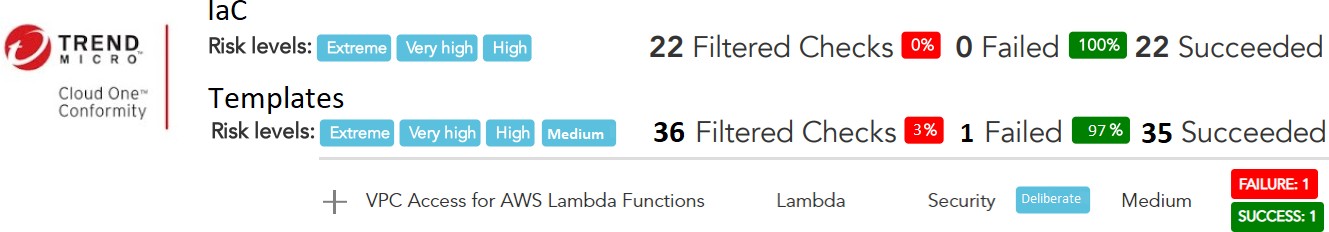
## 2.4.- Test and conformity

### 2.4.1.- Tests

Functional testing has been performed with native tools (AWS GuardDuty findings generator), third-party tools ([AWS CloudSaga](https://github.com/awslabs/aws-cloudsaga)) and manual configuration changes (human activity).

### 2.4.2.- Conformity, IaC

The architecture has undergone scrutiny by TrendMicro's CSPM solution, Cloud One Conformity, with a **successful outcome**:



Medium positives are due non-vpc Lambda necessary for API call to AWS endpoints. Other medium and low failed checks are considered false-positives or suppressed due its low-risk vs need.

### 2.4.3.- Conformity, code

The security analysis carried out, in search of possible vulnerabilities according to the **OWASP TOP 10 classification**, has given **satisfactory results** with the following details:



* + - The **security level** of the application code can be considered **high** since the vulnerabilities detected in the code have a false positive.
    - Since the **security level of the application code is high**, the application code can be considered secure.

# 3.- Repository details

## 3.1.- Database

The solution is designed so that in multi-account or Organisational environments, only **deployment in the account designated for security** (the one that centralises the management of SecurityHub and Config) is necessary. We have chosen to use a *db.t4g.micro* instance of RDS with *PostgreSQL 14.4* engine, in Multi-az. Remaining open to adjustments throughout the life of the project. The amount of data and the number of operations (\*limited) allows the use of machines with low capacity and operating cost.

Since the data contained therein **is not of a sensitive nature**, the use of the public *snapshot* (or backup) is possible for the initial deployment and update:

Latest version:

arn:aws:rds:eu-west-1:794731801658:snapshot:vsoc-mitre-integration-repository-v20230119

### 3.1.1.- Credentials

In the first instance, the repository database maintains default values for the administrator and the lambda user. It is recommended practice that you modify the password for these profiles. See [Deployment steps](#_bookmark23).

Default values:

Database: vsocmitreintegrationdatabase

Administrator user: mirmaster

password: admin12345

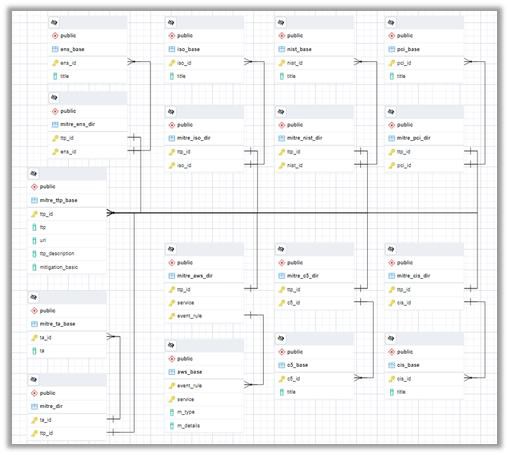
Reader

user: mirlambdareader password: reader12345

### 3.1.2.- Schema

The flow of relationships is as follows:

Each security *event* is related to one or more *techniques*. In turn, each technique will have one or more associated *tactics* and a set of *controls* for each *security standard*.



There is a table of contents for each group (technique, tactic, standard, event...) and an association table for each relationship (event to technique, technique to standard).

### 3.1.3.- Content

There is ongoing work to update data as new versions are released in MITRE ATT&CK and native AWS services are centralised/integrated in Security Hub. These changes will be rolled into updated versions of the public backup.

The following are currently available:

* **60 Techniques** spread across **11 Tactics** from MITRE ATT&CK v12
* **277 AWS Rules and events** (50% AwsConfig, 25% GuardDuty, 10% SecurityHub (CIS, PCI), Others...)

Relations with **security standards** have been developed *autonomously*:

* **NIST 800-53-rev5** : 137 controls
* **CIS CSC v8** : 142 controls
* **PCI-DSS v3.2.1** : 147 controls
* **C5** *(2022)* : 17 controls
* **ENS CNN-STIC** *(2022)* : 17 controls

### 3.1.4.- Requests and use

The deployment of the database is automatic. There will be a public backup in RDS, so you can skip these processes in your environment (unless you amend the content of your database).

* + **Lambda function:** As there are limits on the number of queries (retrieval and import) per second to the Security Hub, the solution does not allow parallel

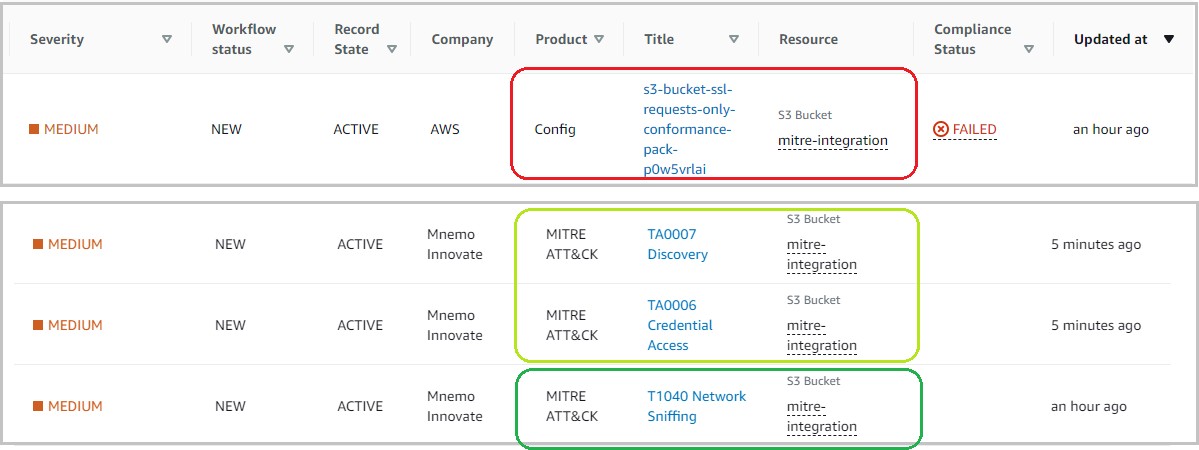
concurrences of the process and, additionally, requires a waiting time between activations for the Security Hub to update. This means that the lambda function *CONSULTOR-SQL* will perform a maximum of **6 read queries** to the database in **30 seconds** windows (\*hence the reduced number of operations).

* + **Administrator:** Access to the database is not required except for administrator profile and lambda reader password change tasks. See [Deployment steps](https://github.com/emgutierrezrubio/integration-mitre-to-aws-security-hub/blob/main/info/deployment.md). However, if upgrade or modification tasks are to be performed, it is advisable to create a new profile for this purpose.

# 4.- Security Hub integration details

Based on the information mapped and registered in the database, one or more techniques correspond to each registered security rule (or event), and at least one tactic. This generates new findings [MITRE ATT&CK](https://attack.mitre.org/matrices/enterprise/cloud/) in Security Hub.

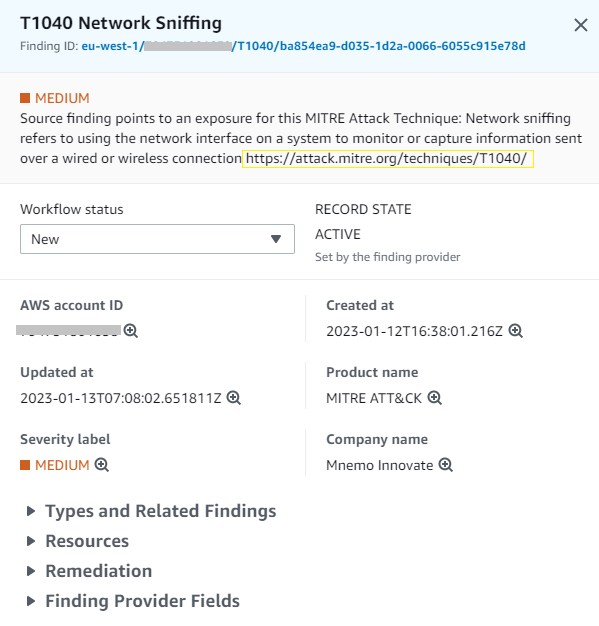
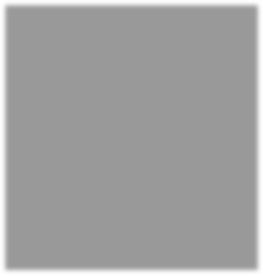
* + **Techniques** findings: contain information about the technique itself, related standards, references to the originating finding and resolution data.
  + **Tactics** findings: are unique per account and region. They contain reference to all underlying active Techniques findings.



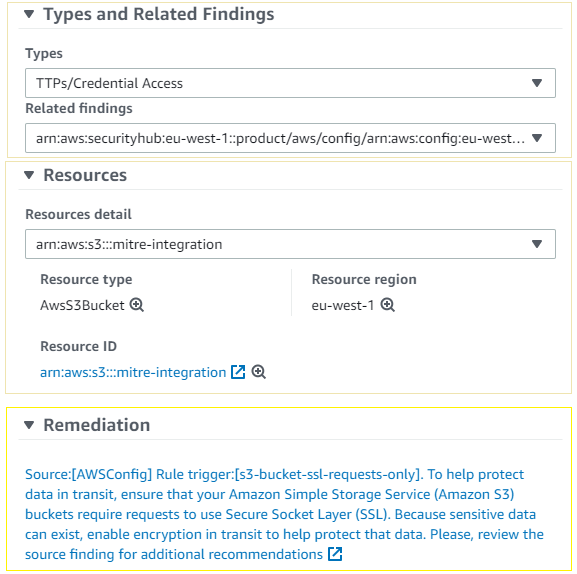
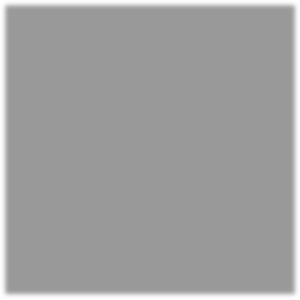
## 4.1.- MITRE ATT&CK Techniques

Information integrated within the type of finding corresponding to a **Technique** of [MITRE ATT&CK](https://attack.mitre.org/matrices/enterprise/cloud/):

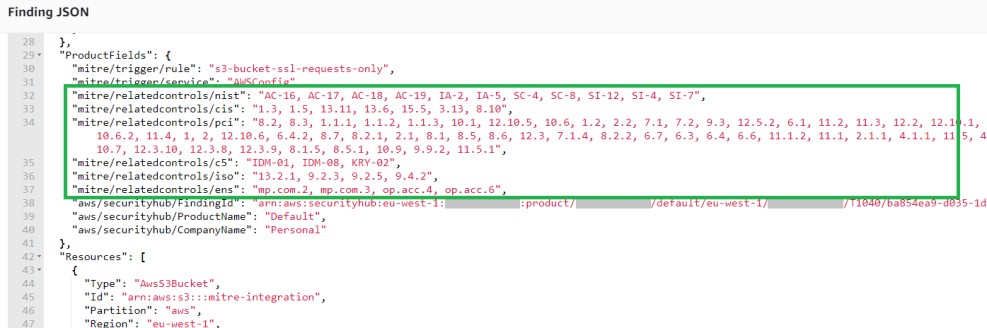
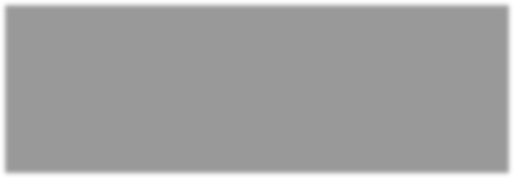
* + **Title**: reflects the identifier of the technique itself.
  + **Severity**: is inherited from the original finding.
  + **Description**: contains general summary information on the technique used. Additionally, an url to access the official site at [**MITRE ATT&CK**](https://attack.mitre.org/matrices/enterprise/cloud/)with extended information is indicated.
  + **Registration** status: will be updated to *ARCHIVED* in case of resolution of the original finding.



* + **Related types and results**: refer to the original finding that initiated the process, as well as the types of tactics to which it is related.
  + **Resources**: inherits the resources affected in the original finding, allowing related findings to be filtered in AWS Security Hub.
  + Within **Remediation** the information retrieved from the database will be displayed: general implementation and/or remediation recommendations for the rule or event that triggered the original finding. Additionally, it links to the original finding.



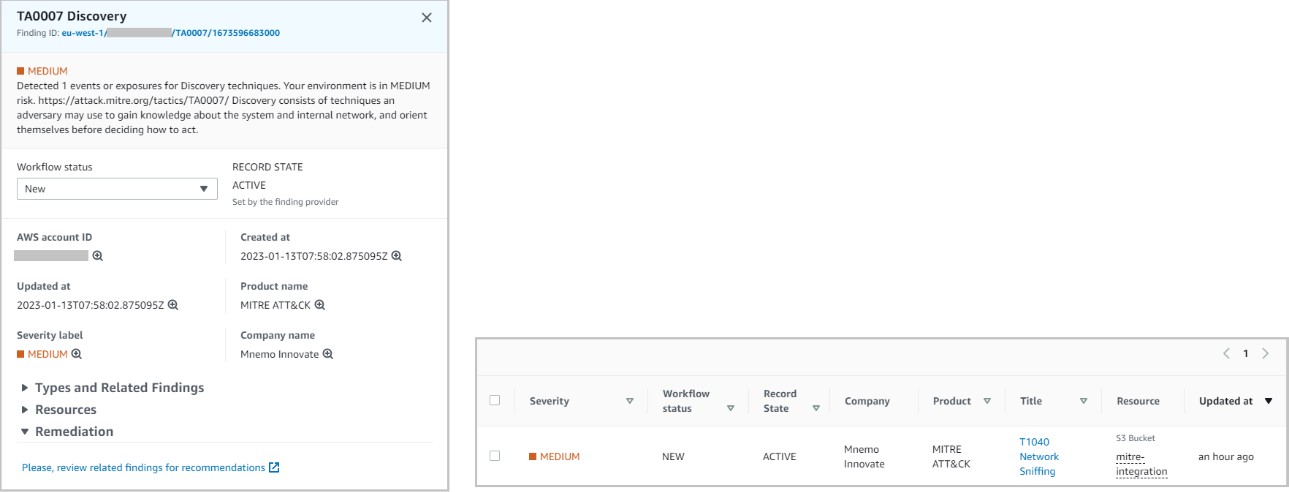
Due to limitations in Security Hub not all information can be displayed in the dashboards. Accessing the JSON document of the enriched finding shows all the information provided by the database, including the **list of controls** by security standard that may be being breached by the identified technique.



## 4.2.- MITRE ATT&CK Tactics

At all times there shall be at most one **Tactic** of each type, encompassing the underlying **Techniques**:

* + **Title**: reflects the identifier of the tactic itself.
  + **Severity**: is derived from *ACTIVE* techniques for this tactic.
  + **Description**: refers to the severity and number of *ACTIVE* techniques. Includes a url to the [**MITRE ATT&CK**](https://attack.mitre.org/matrices/enterprise/cloud/)site and general information on the tactic.
  + The registration status, due to AWS Security Hub limitations, becomes *ARCHIVED* under any update (new, closed, updated techniques), generating a new tactic finding.
  + **Related results and Resources** list the 10 latest *ACTIVE* techniques. However, the link in Correction filters and displays all *ACTIVE* techniques for this tactic.



# 5.- Deployment and configuration

## 5.1.- Previous

For the deployment of the database in RDS, the arn of a valid backup will be required. The latest version of the *public* backup can be found at:

arn:aws:rds:eu-west-1:794731801658:snapshot:vsoc-mitre-integration-repository-v20230119

#### It is recommended to generate an own encrypted backup from this public copy, so that during deployment, encryption is configured on the RDS instance (this step cannot be done later).

1. In your AWS account console, open the **Amazon RDS** service. Access the *Snapshots from* section.
2. Locate the public snapshot listed above. *Mark* it and select the *Copy Snapshot* action.
3. Select the region where you are going to deploy, provide a new flag, *check* the *Copy tags* option.
4. *Check* enable encryption. In the drop-down select one of your CMK keys to perform the encryption of the future RDS.

These steps will generate a new encrypted snapshot from the public snapshot.

Also, you need the **psycopg2** Python Library for AWS Lambda layer deployed in your lambda environment. [You can follow this link to compile and deploy it](https://github.com/jkehler/awslambda-psycopg2).

## 5.2.- Deployment steps

1. Download as Zip the lambda's python code files from the [**python**](https://github.com/emgutierrezrubio/integration-mitre-to-aws-security-hub/tree/main/plantillas)folder for future use in CloudFormation. Download the CloudFormation template set from the [**templates**](https://github.com/emgutierrezrubio/integration-mitre-to-aws-security-hub/tree/main/plantillas)folder and the zip files with code for the Lambda.
2. Copy the files **to an S3 bucket in the target account** and the same region where it will be deployed.
3. In your AWS account console, open the **CloudFormation** service. Click **Create Stack** with new resources.
4. Enter the URL of the S3 object **vsoc-mitreintsh-main.yml** in the Amazon S3 URL field under the Specify template section.
5. Click **Next**. On the next page, enter a name for the stack.
6. On the same page, assign valid values for the **input parameters** (see below).
7. Click on **Next**.
8. Accept all default options on the screens below. Tap **Next**.
9. **Check** I confirm that AWS CloudFormation may create IAM resources with custom names and I confirm that AWS CloudFormation may require the following capability: CAPABILITY\_AUTO\_EXPAND. Click **Submit**.

Deployment may take some time.

## 5.3.- Parameters

The solution consists of a main stack and up to 8 nested stacks. Critical parameters are entered in the deployment of the main stack **vsoc-mitreintsh- main.yml** and are propagated to the secondary stacks during deployment. All other parameters have *default* values in the secondary stacks.

### 5.3.1.- Main stack

* + The values in the **Ownership** parameters correspond to labels that will be propagated to the nested templates. They serve to identify the deployed resources.
  + In **Folders**, you must indicate the URL and the name of the S3 bucket (plus folders, if any) where you have saved the templates and zip files for the deployment.
  + Under **Protection**, you will be given the option to enable AWS Config. If you already have the service, you can skip this step by leaving the value set to **false**. Otherwise, during deployment AWS Config will be enabled with minimum default configuration.
  + Under **Detection**, you will be given the option to enable Security Hub and GuardDuty. If you already have these services, you can skip this step. Otherwise, during deployment they will be enabled with the minimum default configuration. In any case, GuardDuty is an optional (but highly recommended) service.
  + In **Network Configuration**, you must choose a valid VPC for resource deployment. In the RDS and Lambda fields, you must indicate valid subnets:
    - It is recommended that they are subnets without public access.
    - From the designated subnets to VPC Lambda shall allow connectivity up to the RDS.
    - For both cases, the data must be entered in the box as a string of identifiers separated by comma "," without spaces: *subnet- 0ffb6f87xxxxx,subnet-0c023eb98yyyyy*
  + In **RDS Configuration**, you must indicate the arn of the database backup you wish to use either the *public* backup or the *encrypted copy* you have previously generated.
  + In **Language**, you must choose language for the output data: Spanish(**esp**) or english(**eng**).

### 5.3.2.- RDS stack

For modifications only:

* + In **RDS Network Configuration**, the VPC parameters and subnets of the main stack shall have been retrieved.
  + In **Snapshot ARN** it indicates the arn of the *retrieval snapshot*. Data retrieved from the main stack.
  + In **Instance Type** the instance size is defined. We recommend small machines due to their low power consumption. Default *db.t4g.micro* .
  + The **Backup Retention Period** will indicate the backup retention period. Default *7 days*. Since public snapshot is available, if you are not going to make adjustments/additions to your repository, you can disable backups by moving this value to 0.
  + You can adjust the backup periods in the **Preferred Backup Window** and **Preferred Maintenance Window**.
  + You can enable backup on delete in **Snapshot on Delete**, recommended if you make modifications to the repository.
  + In **TCP Port** you can designate a different port for the Postgres protocol. Default *TCP 5432*.

### 5.3.3.- Conformance Pack stack

For adjustments to compliance rules:

* + **AccessKeysRotatedParamMaxAccessKeyAge** indicates the maximum number of days allowed without AccessKey rotation of IAM users. Default *90 days*.
  + **AcmCertificateExpirationCheckParamDaysToExpiration** indicates the minimum number of days of pre-notification before expiry of certificates. Default *90 days*.
  + **CloudwatchAlarmActionCheckParamAlarmActionRequired** checks for the existence of the *AlarmAction* parameter in Cloudwatch alarms. Allowed values TRUE | FALSE . Default *TRUE*.
  + **CloudwatchAlarmActionCheckParamInsufficientDataActionRequired** check s for the existence of the *InsufficientDataAction* parameter in Cloudwatch alarms. Allowed values TRUE | FALSE . Default *TRUE*.
  + **CloudwatchAlarmActionCheckParamOkActionRequired** checks for the existence of the *OkAction* parameter in Cloudwatch alarms. Allowed values TRUE | FALSE . Default *FALSE*.
  + **ElbPredefinedSecurityPolicySslCheckParamPredefinedPolicyName** checks the *default TLS policy* of balancers. Default *ELBSecurityPolicy-TLS-1-2-2017-01*.
  + **IamPasswordPolicyParamMaxPasswordAge** sets the maximum age of IAM passwords. Default *365 days*.
  + **IamPasswordPolicyParamMinimumPasswordLength** sets the minimum length of IAM passwords. Default *14*.
  + **IamPasswordPolicyParamPasswordReusePrevention** sets the minimum number of password changes prior to allowing IAM password reuse. Default *24 days*.
  + **IamPasswordPolicyParamRequireLowercaseCharacters** requires the use of lower case in IAM passwords. Allowed values true | false. Default *true*.
  + **IamPasswordPolicyParamRequireNumbers** requires the use of numbers in IAM passwords. Allowed values true | false. Default *true*.
  + **IamPasswordPolicyParamRequireSymbols** requires the use of symbols in IAM passwords. Allowed values true | false. Default *true*.
  + **IamPasswordPolicyParamRequireUppercaseCharacters** requires the use of upper-case letters in IAM passwords. Allowed values true | false. Default *true*.
  + **IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge** sets the maximum period for unused credentials in IAM. Default *45 days*.
  + **RedshiftClusterConfigurationCheckParamClusterDbEncrypted** checks the encryption on Redshift. Allowed values TRUE | FALSE. Default *TRUE*.
  + **RedshiftClusterConfigurationCheckParamLoggingEnabled** checks the generation of records in Redshift. Allowed values TRUE | FALSE. Default *TRUE*.
  + **RedshiftClusterMaintenancesettingsCheckParamAllowVersionUpgrade** chec ks Redshift version update enablement. Allowed values true | false. Default *true*.
  + **RestrictedIncomingTrafficParamBlockedPort** allows you to define up to 5 TCP ports with restricted access. Default values *20,21,3389,3306,4333*.
  + **S3AccountLevelPublicAccessBlocksPeriodicParamBlockPublicAcls** checks that the *BlockPublicAcls* parameter is enabled. Allowed values True | False. Default *True*.
  + **S3AccountLevelPublicAccessBlocksPeriodicParamBlockPublicPolicy** checks that the *BlockPublicPolicy* parameter is enabled. Allowed values True | False. Default *True*.
  + **S3AccountLevelPublicAccessBlocksPeriodicParamIgnorePublicAcls** checks that the *IgnorePublicAcls* parameter is enabled. Allowed values True | False. Default *True*.
  + **S3AccountLevelPublicAccessBlocksPeriodicParamRestrictPublicBuckets** che cks that the *RestrictPublicBuckets* parameter is enabled. Allowed values True

| False. Default *True*.

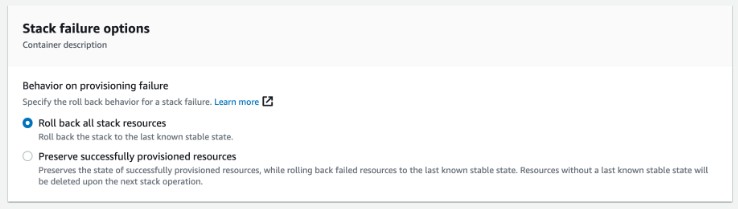
* + **VpcSgOpenOnlyToAuthorizedPortsParamAuthorizedTcpPorts** allows you to define unrestricted port. By default, *TCP 443*.

## 5.4.- Updates

### 5.4.1.- Previous steps

To make important updates to the project or updates in secondary stacks, it will be necessary to previously enable the *rollback mode* in the **main stack**.

1. In your AWS account console, open the **CloudFormation** service. Select the primary stack and click **Update**.
2. Keep the values to *Use Current Stack*. Click **Next**.
3. Do not change parameter values currently. Click **Next**.
4. Under *Stack Failure Options* select **Roll back all stack resources**. Click **Next**.



1. Review the changes. **Check** the required confirmations. Press **Submit**.
2. You can now proceed to make the desired updates to secondary stacks in **CloudFormation**.
3. Once you are done, you'll need to repeat the previous steps on the **main stack** to restore the **Preserve successfully provisioned resources** option.

To perform a repository version upgrade, you will need to manually disable RDS deletion protection.

1. In your AWS account console, open the **Amazon RDS** service. Select the database and click **Modify**.
2. Look for and **uncheck** deletion protection. Click **Next**.
3. Check the option to apply changes immediately. Press **Finish**.

With these modifications applied, you can proceed with the update from the **main stack** in **CloudFormation**.

### 5.4.2.- Nested stack updates

To modify parameters in the secondary stacks:

1. In your AWS account console, open the **CloudFormation** service. Select the stack and click **Upgrade**.
2. In the pop-up window **check** Refresh Nested Stack and click **Upgrade Stack**.
3. Keep the values under Use Current Stack. Press **Next**.
4. In this section you can modify the **parameters** to your needs. Press **Next** when finished.
5. Accept all the default options in the screens below. Click **Next**.
6. Review the changes. **Check** the necessary confirmations. Click **Send**.

### 5.4.3.- Repository

In the first instance the repository database maintains default values for the administrator and the lambda user. It is recommended practice that you change the password for these profiles.

Default values:

Database: vsocmitreintegrationdatabase

Administrator user: mirmaster

password: admin12345

Reader

user: mirlambdareader password: reader12345

To make these changes you will need to access the database through a SQL client with an administrator profile **mirmaster** Remember that the database will be isolated:

* + You will need to connect via a jump instance or allow external connectivity during the process.
  + You will need a PostgreSQL 14.4 compatible client.

Follow the recommended steps of your PostgreSQL client for connection and modifications. An example:

By command line:

Connecting using psql:

$ psql -h <RDS-endpoint> -p <port> -U mirmaster -d vsocmitreintegrationdatabase

User modification:

ALTER USER <user> WITH PASSWORD '<new password>';

Remember to modify the **vsoc-mitreintsh-rds-reader-secret** with the new credentials for the Lambda function.

# 6.- Self-remediation module

This add-on module adds self-remediation mechanisms for three particular **MITRE ATT&CK findings** generated in Security Hub.

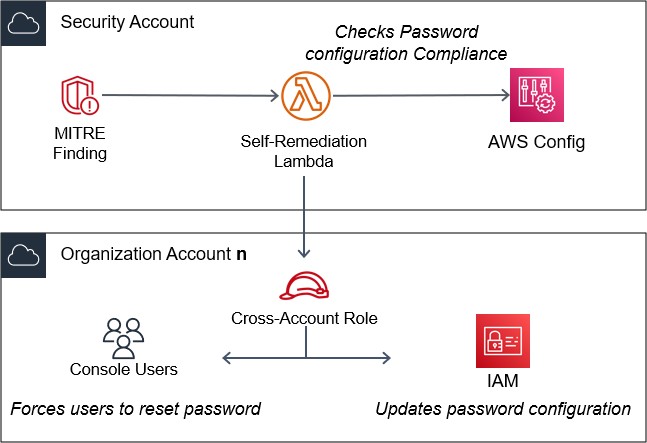
## 6.1.- Case 1, fix password policy

If a finding is generated due tactic *Credential Access (TA0006)* and techniques

*Brute Force (T1110)* or *Unsecured Credentials (T1552)*.

Upon detection of activity related to access attempts or unsecured access, automatically password configuration policies will be reviewed in IAM and the best practices configuration will be applied. By default, standards compliance recommended configuration will be applied unless you modify this policy in the **MITER ATT&CK integration project solution in Security Hub** deployment.

Additionally, *console users* will be forced to reset their password at the next login.

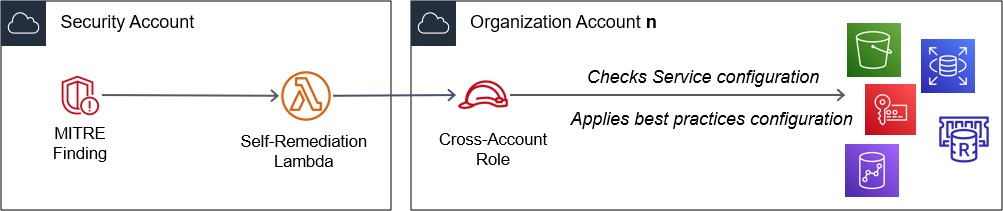


## 6.2.- Case 2, enable data recovery

If a finding is generated due tactic *Impact (TA0040)* and an exposure is detected to technique *Data Destruction (T1485)*.

Automatically, **options to prevent data loss** will be enabled depending on the trigger service:

* CloudTrail logs validation
* AWS KMS key rotation
* ELB and RDS deletion protection
* DynamoDB, Elasticache and Redshift backup enabled
* S3 versioning enabled



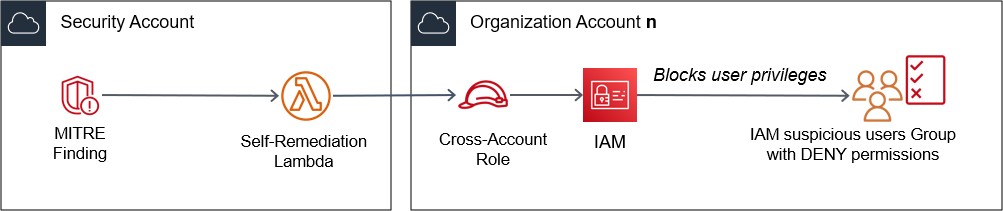
## 6.3.- Case 3, blocks suspicious user

If a finding is generated due tactic *Privilege Escalation (TA0004)* and techniques

#### Domain Policy Modification (T1484) or Valid Accounts (T1078).

Automatically, upon detection of *suspicious activity* or *non-compliance of the principle of least privilege,* the user will be included in a **group of isolated users** or blocked permissions, pending review.

An email will be sent to the Security Team named in the deployment phase.



## 6.4.- Add-on deployment

This template is compatible for single account environments and for multi- account environments or Organizations. It must first be deployed in the account designated for centralized security services. It can then be deployed to each of the accounts you wish to monitor.

1. Dowload as Zip the lambda's python files from [**self-remediation**](https://github.com/emgutierrezrubio/integration-mitre-to-aws-security-hub/tree/main/selfremediation)folder for future use in CloudFormation. Download the CloudFormation template vsoc- mitreintsh-selfremediation.yml.
2. Copy the files **to an S3 bucket accessible from the target account**.
3. In the console of your AWS account, open the **CloudFormation** service. Click **Create Stack** with new resources.
4. Enter the URL of the S3 object **vsoc-mitreintsh-selfremediation.yml** in the Amazon S3 URL field under the Specify template section.
5. Click **Next**. On the next page, enter a name for the stack.
6. On the same page, assign valid values for the **input parameters** (see below).
7. Click on **Next**.
8. Accept all the default options in the screens below. Click on **Next**.
9. **Check** I confirm that AWS CloudFormation might create IAM resources with custom names and/or I confirm that AWS CloudFormation might require the following capability: CAPABILITY\_AUTO\_EXPAND. Click **Submit**.

Deployment may take some time.

### 6.4.1.- Add-on parameters

* + The values in the **Ownership** parameters correspond to labels used to identify the deployed resources.
  + In **Folders**, you must indicate the name of the S3 bucket (plus folders, if any) where you have saved the templates and zip files for the deployment.
  + Under **Organization**, even if it is a single account environment, you must enter the designated account identifier for security services (the one that centralizes the Security Hub findings).
  + Under **Credential Access**, **Impact** and **Privilege Escalation**, you will be given the option to enable each of the modules separately.
  + In **Privilege Escalation** (module for Privilege Escalation tactics), you will need to provide the following data:
    1. E-mail address for receiving notifications by blocked users (ideally a security administrator reception group).
    2. Title so that notifications received by e-mail are easily identifiable.
    3. Name for the user group in IAM with blocked access.
    4. **Especially important**, specify (comma separated) the name of the privileged IAM users. These users, even if marked as *suspicious*, will still have privileges. This measure **is important** to prevent the main administrators or the root user from being blocked, leaving the AWS account without administrators with sufficient privileges to make changes.

# Annex I. Conformance Pack details

## AWS Services

* Auto Scaling AUTOSCALING\_GROUP\_ELB\_HEALTHCHECK\_REQUIRED AUTOSCALING\_LAUNCH\_CONFIG\_PUBLIC\_IP\_DISABLED
* Amazon API Gateway API\_GW\_CACHE\_ENABLED\_AND\_ENCRYPTED API\_GW\_SSL\_ENABLED API\_GW\_EXECUTION\_LOGGING\_ENABLED API\_GW\_ASSOCIATED\_WITH\_WAF
* Amazon CloudWatch CLOUDWATCH\_ALARM\_ACTION\_CHECK CLOUDWATCH\_LOG\_GROUP\_ENCRYPTED
* Amazon DynamoDB DYNAMODB\_PITR\_ENABLED DYNAMODB\_IN\_BACKUP\_PLAN DYNAMODB\_THROUGHPUT\_LIMIT\_CHECK DMS\_REPLICATION\_NOT\_PUBLIC
* Amazon EC2 INSTANCES\_IN\_VPC

EC2\_SECURITY\_GROUP\_ATTACHED\_TO\_ENI\_PERIODIC EC2\_INSTANCE\_PROFILE\_ATTACHED EC2\_INSTANCE\_NO\_PUBLIC\_IP

EC2\_IMDSV2\_CHECK EC2\_EBS\_ENCRYPTION\_BY\_DEFAULT EBS\_IN\_BACKUP\_PLAN EBS\_SNAPSHOT\_PUBLIC\_RESTORABLE\_CHECK ENCRYPTED\_VOLUMES

* Amazon ECS ECS\_CONTAINERS\_READONLY\_ACCESS ECS\_CONTAINERS\_NONPRIVILEGED

ECS\_TASK\_DEFINITION\_USER\_FOR\_HOST\_MODE\_CHECK

* Amazon EFS EFS\_ACCESS\_POINT\_ENFORCE\_USER\_IDENTITY

EFS\_ACCESS\_POINT\_ENFORCE\_ROOT\_DIRECTORY EFS\_IN\_BACKUP\_PLAN

EFS\_ENCRYPTED\_CHECK

* Amazon ElastiCache ELASTICACHE\_REDIS\_CLUSTER\_AUTOMATIC\_BACKUP\_CHECK
* Amazon EMR EMR\_KERBEROS\_ENABLED EMR\_MASTER\_NO\_PUBLIC\_IP
* Amazon GuardDuty GUARDDUTY\_ENABLED\_CENTRALIZED
* Amazon OpenSearch Service OPENSEARCH\_ACCESS\_CONTROL\_ENABLED ELASTICSEARCH\_NODE\_TO\_NODE\_ENCRYPTION\_CHECK ELASTICSEARCH\_LOGS\_TO\_CLOUDWATCH ELASTICSEARCH\_IN\_VPC\_ONLY ELASTICSEARCH\_ENCRYPTED\_AT\_REST
* Amazon RDS RDS\_MULTI\_AZ\_SUPPORT RDS\_LOGGING\_ENABLED RDS\_STORAGE\_ENCRYPTED

RDS\_SNAPSHOTS\_PUBLIC\_PROHIBITED RDS\_INSTANCE\_PUBLIC\_ACCESS\_CHECK RDS\_INSTANCE\_DELETION\_PROTECTION\_ENABLED RDS\_IN\_BACKUP\_PLAN RDS\_ENHANCED\_MONITORING\_ENABLED RDS\_AUTOMATIC\_MINOR\_VERSION\_UPGRADE\_ENABLED DB\_INSTANCE\_BACKUP\_ENABLED

* Amazon Redshift REDSHIFT\_REQUIRE\_TLS\_SSL

REDSHIFT\_ENHANCED\_VPC\_ROUTING\_ENABLED REDSHIFT\_CLUSTER\_PUBLIC\_ACCESS\_CHECK REDSHIFT\_CLUSTER\_MAINTENANCESETTINGS\_CHECK REDSHIFT\_CLUSTER\_KMS\_ENABLED REDSHIFT\_CLUSTER\_CONFIGURATION\_CHECK REDSHIFT\_BACKUP\_ENABLED

* Amazon S3 S3\_BUCKET\_ACL\_PROHIBITED S3\_BUCKET\_VERSIONING\_ENABLED S3\_BUCKET\_SSL\_REQUESTS\_ONLY

S3\_BUCKET\_SERVER\_SIDE\_ENCRYPTION\_ENABLED S3\_BUCKET\_REPLICATION\_ENABLED S3\_BUCKET\_PUBLIC\_WRITE\_PROHIBITED S3\_BUCKET\_PUBLIC\_READ\_PROHIBITED S3\_BUCKET\_LOGGING\_ENABLED S3\_BUCKET\_LEVEL\_PUBLIC\_ACCESS\_PROHIBITED S3\_BUCKET\_DEFAULT\_LOCK\_ENABLED S3\_ACCOUNT\_LEVEL\_PUBLIC\_ACCESS\_BLOCKS\_PERIODIC

* Amazon SageMaker SAGEMAKER\_NOTEBOOK\_NO\_DIRECT\_INTERNET\_ACCESS SAGEMAKER\_NOTEBOOK\_INSTANCE\_KMS\_KEY\_CONFIGURED SAGEMAKER\_ENDPOINT\_CONFIGURATION\_KMS\_KEY\_CONFIGURED
* Amazon SNS SNS\_ENCRYPTED\_KMS
* Amazon VPC Managed rules:

VPC\_FLOW\_LOGS\_ENABLED VPC\_SG\_OPEN\_ONLY\_TO\_AUTHORIZED\_PORTS VPC\_DEFAULT\_SECURITY\_GROUP\_CLOSED SUBNET\_AUTO\_ASSIGN\_PUBLIC\_IP\_DISABLED INCOMING\_SSH\_DISABLED INTERNET\_GATEWAY\_AUTHORIZED\_VPC\_ONLY NO\_UNRESTRICTED\_ROUTE\_TO\_IGW RESTRICTED\_INCOMING\_TRAFFIC

* AWS Certificate Manager ACM\_CERTIFICATE\_EXPIRATION\_CHECK
* AWS CloudTrail CLOUD\_TRAIL\_ENCRYPTION\_ENABLED CLOUD\_TRAIL\_LOG\_FILE\_VALIDATION\_ENABLED CLOUD\_TRAIL\_CLOUD\_WATCH\_LOGS\_ENABLED CLOUD\_TRAIL\_ENABLED

MULTI\_REGION\_CLOUD\_TRAIL\_ENABLED CLOUDTRAIL\_SECURITY\_TRAIL\_ENABLED CLOUDTRAIL\_S3\_DATAEVENTS\_ENABLED

* AWS Codebuild CODEBUILD\_PROJECT\_SOURCE\_REPO\_URL\_CHECK CODEBUILD\_PROJECT\_ENVVAR\_AWSCRED\_CHECK
* AWS Elastic Beanstalk BEANSTALK\_ENHANCED\_HEALTH\_REPORTING\_ENABLED ELASTIC\_BEANSTALK\_MANAGED\_UPDATES\_ENABLED
* AWS Identity and Access Management (IAM) IAM\_USER\_GROUP\_MEMBERSHIP\_CHECK IAM\_ROOT\_ACCESS\_KEY\_CHECK IAM\_POLICY\_NO\_STATEMENTS\_WITH\_FULL\_ACCESS IAM\_POLICY\_NO\_STATEMENTS\_WITH\_ADMIN\_ACCESS IAM\_PASSWORD\_POLICY IAM\_USER\_UNUSED\_CREDENTIALS\_CHECK IAM\_USER\_MFA\_ENABLED MFA\_ENABLED\_FOR\_IAM\_CONSOLE\_ACCESS ROOT\_ACCOUNT\_MFA\_ENABLED ROOT\_ACCOUNT\_HARDWARE\_MFA\_ENABLED ACCESS\_KEYS\_ROTATED
* AWS Key Management Service (AWS KMS) CMK\_BACKING\_KEY\_ROTATION\_ENABLED
* AWS Lambda LAMBDA\_CONCURRENCY\_CHECK

LAMBDA\_FUNCTION\_PUBLIC\_ACCESS\_PROHIBITED

* AWS Secrets Manager SECRETSMANAGER\_SECRET\_UNUSED
* AWS Systems Manager Managed rules: SSM\_DOCUMENT\_NOT\_PUBLIC

EC2\_MANAGEDINSTANCE\_PATCH\_COMPLIANCE\_STATUS\_CHECK EC2\_INSTANCE\_MANAGED\_BY\_SSM

* AWS WAF WAFV2\_LOGGING\_ENABLED

- Elastic Load Balancing ALB\_WAF\_ENABLED

ALB\_HTTP\_DROP\_INVALID\_HEADER\_ENABLED ALB\_HTTP\_TO\_HTTPS\_REDIRECTION\_CHECK ELB\_TLS\_HTTPS\_LISTENERS\_ONLY ELB\_PREDEFINED\_SECURITY\_POLICY\_SSL\_CHECK ELB\_LOGGING\_ENABLED ELB\_DELETION\_PROTECTION\_ENABLED ELB\_CROSS\_ZONE\_LOAD\_BALANCING\_ENABLED ELB\_ACM\_CERTIFICATE\_REQUIRED

ELBV2\_ACM\_CERTIFICATE\_REQUIRED

# Annex II. Mapping summary

**MITRE ATT&CK *v.12***

* *Tactics: 11*

TA0001 Initial Access TA0002 Execution TA0003 Persistence

TA0004 Privilege Escalation TA0005 Defense Evasion TA0006 Credential Access TA0007 Discovery

TA0008 Lateral Movement TA0009 Collection

TA0010 Exfiltration

TA0040 Impact

* *Techniques: 61*

T1040 Network Sniffing

T1046 Network Service Discovery T1078 Valid Accounts

T1078.001 Valid Accounts: Default Accounts T1078.004 Valid Accounts: Cloud Accounts T1087.004 Account Discovery: Cloud Account T1098 Account Manipulation

T1098.001 Account Manipulation: Additional Cloud Credentials T1098.004 Account Manipulation: SSH Authorized Keys

T1110 Brute Force

T1110.001 Brute Force: Password Guessing T1110.002 Brute Force: Password Cracking T1110.003 Brute Force: Password Spraying T1110.004 Brute Force: Credential Stuffing T1119 Automated Collection

T1136 Create Account

T1136.003 Create Account: Cloud Account T1189 Drive-by Compromise

T1190 Exploit Public-Facing Application

T1199 Trusted Relationship

T1201 Password Policy Discovery T1204 User Execution

T1204.003 User Execution: Malicious Image T1485 Data Destruction

T1486 Data Encrypted for Impact T1491 Defacement

T1491.002 Defacement: External Defacement T1496 Resource Hijacking

T1498 Network Denial of Service

T1498.001 Network Denial of Service: Direct Network Flood T1498.002 Network Denial of Service: Reflection Amplification T1499.002 Endpoint Denial of Service: Service Exhaustion Flood T1499.003 Endpoint Denial of Service: Application Exhaustion Flood

T1499.004 Endpoint Denial of Service: Application or System Exploitation T1525 Implant Internal Image

T1526 Cloud Service Discovery

T1528 Steal Application Access Token T1530 Data from Cloud Storage Object T1531 Account Access Removal

T1535 Unused/Unsupported Cloud Regions T1537 Transfer Data to Cloud Account T1538 Cloud Service Dashboard

T1550 Use Alternate Authentication Material

T1550.001 Use Alternate Authentication Material: Application Access Token T1552 Unsecured Credentials

T1552.001 Unsecured Credentials: Credentials In Files

T1552.005 Unsecured Credentials: Cloud Instance Metadata API T1562 Impair Defenses

T1562.001 Impair Defenses: Disable or Modify Tools T1562.007 Impair Defenses: Disable or Modify Cloud Firewall T1562.008 Impair Defenses: Disable Cloud Logs

T1566 Phishing

T1578 Modify Cloud Compute Infrastructure

T1578.001 Modify Cloud Compute Infrastructure: Create Snapshot

T1578.002 Modify Cloud Compute Infrastructure: Create Cloud Instance T1578.003 Modify Cloud Compute Infrastructure: Delete Cloud Instance T1578.004 Modify Cloud Compute Infrastructure: Revert Cloud Instance T1580 Cloud Infrastructure Discovery

T1619 Cloud Storage Object Discovery

T1621 Multi-Factor Authentication Request Generation T1648 Serverless Execution

## AWS Service & Events

* AmazonCognito: 4
* AmazonGuardDuty: 55
* AmazonInspector: 5
* AmazonMacie: 10
* AmazonVirtualPrivatecloud: 3
* AWSCloudHSM: 1
* AWSCloudWatch: 3
* AWSConfig: 114
* AWSIAM: 5
* AWSIOTDeviceDefender: 31
* AWSKeyManagementService: 1
* AWSNetworkFirewall: 4
* AWSOrganizations: 3
* AWSRDS: 4
* AWSS3: 1
* AWSSecretsManager: 1
* AWSSecurityHub: 34
* AWSSSO: 3
* AWSWebApplicationFirewall: 4

AmazonCognito CredentialAccess:IAMUser/AnomalousBehavior iam-password-policy

iam-user-mfa-enabled Impact:EC2/WinRMBruteForce

AmazonGuardDuty

Backdoor:EC2/DenialOfService.Dns Backdoor:EC2/DenialOfService.Tcp Backdoor:EC2/DenialOfService.Udp Backdoor:EC2/DenialOfService.UdpOnTcpPorts Backdoor:EC2/DenialOfService.UnusualProtocol CredentialAccess:IAMUser/AnomalousBehavior CryptoCurrency:EC2/BitcoinTool.B CryptoCurrency:EC2/BitcoinTool.B!DNS DefenseEvasion:IAMUser/AnomalousBehavior Discovery:IAMUser/AnomalousBehavior Discovery:S3/MaliciousIPCaller Discovery:S3/MaliciousIPCaller.Custom Discovery:S3/TorIPCaller Exfiltration:IAMUser/AnomalousBehavior Exfiltration:S3/MaliciousIPCaller Impact:EC2/BitcoinDomainRequest.Reputation Impact:EC2/PortSweep Impact:EC2/WinRMBruteForce Impact:IAMUser/AnomalousBehavior Impact:S3/MaliciousIPCaller PenTest:IAMUser/KaliLinux PenTest:IAMUser/ParrotLinux PenTest:IAMUser/PentooLinux PenTest:S3/KaliLinux

PenTest:S3/ParrotLinux PenTest:S3/PentooLinux Persistence:IAMUser/AnomalousBehavior Policy:IAMUser/RootCredentialUsage Policy:S3/AccountBlockPublicAccessDisabled Policy:S3/BucketAnonymousAccessGranted Policy:S3/BucketBlockPublicAccessDisabled Policy:S3/BucketPublicAccessGranted Recon:EC2/PortProbeEMRUnprotectedPort Recon:EC2/PortProbeUnprotectedPort Recon:EC2/Portscan

Recon:IAMUser/MaliciousIPCaller Recon:IAMUser/MaliciousIPCaller.Custom Recon:IAMUser/TorIPCaller Stealth:IAMUser/CloudTrailLoggingDisabled Stealth:IAMUser/PasswordPolicyChange Stealth:S3/ServerAccessLoggingDisabled Trojan:EC2/DriveBySourceTraffic!DNS Trojan:EC2/PhishingDomainRequest!DNS UnauthorizedAccess:EC2/MetadataDNSRebind UnauthorizedAccess:EC2/RDPBruteForce UnauthorizedAccess:EC2/SSHBruteForce UnauthorizedAccess:EC2/TorRelay UnauthorizedAccess:IAMUser/ConsoleLogin UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration UnauthorizedAccess:IAMUser/MaliciousIPCaller UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom UnauthorizedAccess:IAMUser/TorIPCaller UnauthorizedAccess:S3/MaliciousIPCaller.Custom UnauthorizedAccess:S3/TorIPCaller

AmazonInspector

iam-password-policy Recon:EC2/Portscan Trojan:EC2/DriveBySourceTraffic!DNS

UnauthorizedAccess:EC2/MetadataDNSRebind UnauthorizedAccess:EC2/SSHBruteForce

AmazonMacie Policy:IAMUser/S3BlockPublicAccessDisabled Policy:IAMUser/S3BucketEncryptionDisabled Policy:IAMUser/S3BucketPublic Policy:IAMUser/S3BucketReplicatedExternally Policy:IAMUser/S3BucketSharedExternally SensitiveData:S3Object/Credentials SensitiveData:S3Object/CustomIdentifier SensitiveData:S3Object/Financial

SensitiveData:S3Object/Multiple SensitiveData:S3Object/Personal

AmazonVirtualPrivatecloud Backdoor:EC2/DenialOfService.Dns elb-tls-https-listeners-only Recon:EC2/Portscan

AWSCloudHSM encrypted-volumes

AWSCloudWatch CryptoCurrency:EC2/BitcoinTool.B elb-tls-https-listeners-only

access-keys-rotated AWSConfig

acm-certificate-expiration-check

alb-http-drop-invalid-header-enabled alb-http-to-https-redirection-check alb-waf-enabled

api-gw-associated-with-waf

api-gw-cache-enabled-and-encrypted api-gw-execution-logging-enabled

api-gw-ssl-enabled

autoscaling-group-elb-healthcheck-required autoscaling-launch-config-public-ip-disabled beanstalk-enhanced-health-reporting-enabled cloud-trail-cloud-watch-logs-enabled cloudtrail-enabled

cloud-trail-encryption-enabled

cloud-trail-log-file-validation-enabled cloudtrail-s3-dataevents-enabled cloudtrail-security-trail-enabled cloudwatch-alarm-action-check cloudwatch-log-group-encrypted cmk-backing-key-rotation-enabled

codebuild-project-envvar-awscred-check codebuild-project-source-repo-url-check

db-instance-backup-enabled dms-replication-not-public dynamodb-in-backup-plan dynamodb-pitr-enabled

dynamodb-throughput-limit-check ebs-in-backup-plan

ebs-snapshot-public-restorable-check ec2-ebs-encryption-by-default

ec2-imdsv2-check

ec2-instance-managed-by-systems-manager ec2-instance-no-public-ip

ec2-instance-profile-attached ec2-instances-in-vpc

ec2-managedinstance-patch-compliance-status-check ec2-security-group-attached-to-eni

ecs-containers-nonprivileged ecs-containers-readonly-access

efs-access-point-enforce-root-directory efs-access-point-enforce-user-identity efs-encrypted-check

efs-in-backup-plan

elasticache-redis-cluster-automatic-backup-check elastic-beanstalk-managed-updates-enabled elasticsearch-encrypted-at-rest

elasticsearch-in-vpc-only elasticsearch-logs-to-cloudwatch

elasticsearch-node-to-node-encryption-check elb-acm-certificate-required

elb-cross-zone-load-balancing-enabled elb-deletion-protection-enabled

elb-logging-enabled

elb-predefined-security-policy-ssl-check elb-tls-https-listeners-only

elbv2-acm-certificate-required emr-kerberos-enabled

emr-master-no-public-ip encrypted-volumes

iam-password-policy

iam-policy-no-statements-with-admin-access iam-policy-no-statements-with-full-access iam-root-access-key-check

iam-user-group-membership-check iam-user-mfa-enabled

iam-user-unused-credentials-check internet-gateway-authorized-vpc-only lambda-concurrency-check

lambda-function-public-access-prohibited mfa-enabled-for-iam-console-access multi-region-cloudtrail-enabled opensearch-access-control-enabled

rds-automatic-minor-version-upgrade-enabled rds-enhanced-monitoring-enabled

rds-in-backup-plan

rds-instance-deletion-protection-enabled rds-instance-public-access-check

rds-logging-enabled rds-multi-az-support

rds-snapshot-encrypted

rds-snapshots-public-prohibited rds-storage-encrypted

redshift-backup-enabled

redshift-cluster-configuration-check redshift-cluster-kms-enabled

redshift-cluster-maintenancesettings-check redshift-cluster-public-access-check redshift-enhanced-vpc-routing-enabled redshift-require-tls-ssl

restricted-common-ports restricted-ssh

root-account-hardware-mfa-enabled

root-account-mfa-enabled

s3-account-level-public-access-blocks-periodic s3-bucket-acl-prohibited

s3-bucket-default-lock-enabled

s3-bucket-level-public-access-prohibited s3-bucket-logging-enabled

s3-bucket-public-read-prohibited s3-bucket-public-write-prohibited s3-bucket-replication-enabled

s3-bucket-server-side-encryption-enabled s3-bucket-ssl-requests-only

s3-bucket-versioning-enabled

sagemaker-endpoint-configuration-kms-key-configured sagemaker-notebook-instance-kms-key-configured sagemaker-notebook-no-direct-internet-access securityhub-enabled

sns-encrypted-kms

ssm-document-not-public

subnet-auto-assign-public-ip-disabled vpc-flow-logs-enabled

vpc-sg-open-only-to-authorized-ports wafv2-logging-enabled

AWSIAM

Discovery:IAMUser/AnomalousBehavior iam-user-mfa-enabled Impact:IAMUser/AnomalousBehavior multi-region-cloudtrail-enabled Persistence:IAMUser/AnomalousBehavior

AWSIOTDeviceDefender AUTHENTICATED\_COGNITO\_ROLE\_OVERLY\_PERMISSIVE\_CHECK

aws:all-bytes-in aws:all-bytes-out aws:all-packets-in aws:all-packets-out

aws:destination-ip-addresses

aws:listening-tcp-ports aws:listening-udp-ports aws:message-byte-size aws:num-authorization-failures aws:num-connection-attempts aws:num-disconnects

aws:num-established-tcp-connections aws:num-listening-tcp-ports

aws:num-listening-udp-ports aws:num-messages-received aws:num-messages-sent aws:source-ip-address CA\_CERTIFICATE\_EXPIRING\_CHECK

CA\_CERTIFICATE\_KEY\_QUALITY\_CHECK CONFLICTING\_CLIENT\_IDS\_CHECK DEVICE\_CERTIFICATE\_EXPIRING\_CHECK DEVICE\_CERTIFICATE\_KEY\_QUALITY\_CHECK DEVICE\_CERTIFICATE\_SHARED\_CHECK IOT\_POLICY\_OVERLY\_PERMISSIVE\_CHECK IOT\_ROLE\_ALIAS\_ALLOWS\_ACCESS\_TO\_UNUSED\_SERVICES\_CHECK IOT\_ROLE\_ALIAS\_OVERLY\_PERMISSIVE\_CHECK LOGGING\_DISABLED\_CHECK REVOKED\_CA\_CERTIFICATE\_STILL\_ACTIVE\_CHECK REVOKED\_DEVICE\_CERTIFICATE\_STILL\_ACTIVE\_CHECK UNAUTHENTICATED\_COGNITO\_ROLE\_OVERLY\_PERMISSIVE\_CHECK

AWSKeyManagementService encrypted-volumes

AWSNetworkFirewall Backdoor:EC2/DenialOfService.Dns

elb-cross-zone-load-balancing-enabled Exfiltration:S3/MaliciousIPCaller Recon:EC2/Portscan

AWSOrganizations Discovery:IAMUser/AnomalousBehavior Exfiltration:IAMUser/AnomalousBehavior

mfa-enabled-for-iam-console-access AWSRDS

elb-tls-https-listeners-only

rds-automatic-minor-version-upgrade-enabled rds-instance-deletion-protection-enabled

rds-storage-encrypted AWSS3

s3-bucket-versioning-enabled AWSSecretsManager

Impact:IAMUser/AnomalousBehavior AWSSecurityHub

* 1. Ensure a log metric filter and alarm exist for security group changes
  2. Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)
  3. Ensure a log metric filter and alarm exist for changes to network gateways
  4. Ensure a log metric filter and alarm exist for route table changes
  5. Ensure a log metric filter and alarm exist for VPC changes
  6. Ensure a log metric filter and alarm exist for unauthorized API calls
  7. Ensure a log metric filter and alarm exist for Management Console sign-in without MFA
  8. Ensure a log metric filter and alarm exist for usage of root account
  9. Ensure a log metric filter and alarm exist for IAM policy changes
  10. Ensure a log metric filter and alarm exist for IAM policy changes
  11. Ensure a log metric filter and alarm exist for CloudTrail configuration changes
  12. Ensure a log metric filter and alarm exist for AWS Management Console authentication failures
  13. Ensure a log metric filter and alarm exist for S3 bucket policy changes
  14. Ensure a log metric filter and alarm exist for AWS Config configuration changes

4.7 Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs

AWS principals with suspicious access key activity AWS resources with unauthorized access attempts Credentials that may have leaked

EC2 instances that are open to the Internet

EC2 instances that have missing security patches for important vulnerabilities EC2 instances that have ports accessible from the Internet

IAM users with suspicious activity

[PCI.CW.1] A log metric filter and alarm should exist for usage of the root user S3 buckets with public write or read permissions

AWSSSO

Exfiltration:IAMUser/AnomalousBehavior iam-user-mfa-enabled Impact:EC2/WinRMBruteForce

AWSWebApplicationFirewall Recon:EC2/PortProbeUnprotectedPort Recon:EC2/Portscan Trojan:EC2/DriveBySourceTraffic!DNS

UnauthorizedAccess:EC2/MetadataDNSRebind

## CIS CSC *v8*

- Controls: 142

* 1. Deploy and Maintain Anti-Malware Software
  2. Configure Automatic Anti-Malware Signature Updates
  3. Disable Autorun and Autoplay for Removable Media
  4. Configure Automatic Anti-Malware Scanning of Removable Media
  5. Enable Anti-Exploitation Features
  6. Centrally Manage Anti-Malware Software
  7. Use Behavior-Based Anti-Malware Software
  8. Establish and Maintain Detailed Enterprise Asset Inventory
  9. Establish and Maintain a Data Recovery Process
  10. Perform Automated Backups
  11. Protect Recovery Data
  12. Establish and Maintain an Isolated Instance of Recovery Data
  13. Test Data Recovery

1.2 Address Unauthorized Assets

* 1. Ensure Network Infrastructure is Up-to-Date
  2. Establish and Maintain a Secure Network Architecture
  3. Securely Manage Network Infrastructure
  4. Establish and Maintain Architecture Diagram(s)
  5. Centralize Network Authentication, Authorization, and Auditing (AAA)
  6. Use of Secure Network Management and Communication Protocols
  7. Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise Infrastructure
  8. Establish and Maintain Dedicated Computing Resources for All Administrative Work

1.3 Utilize an Active Discovery Tool

13.1 Centralize Security Event Alerting

* 1. Perform Application Layer Filtering
  2. Tune Security Event Alerting Thresholds
  3. Deploy a Host-Based Intrusion Detection Solution
  4. Deploy a Network Intrusion Detection Solution
  5. Perform Traffic Filtering Between Network Segments
  6. Manage Access Control for Remote Assets
  7. Collect Network Traffic Flow Logs
  8. Deploy a Host-Based Intrusion Prevention Solution
  9. Deploy a Network Intrusion Prevention Solution
  10. Deploy Port-Level Access Control

1.4 Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory

* 1. Establish and Maintain a Security Awareness Program
  2. Train Workforce Members to Recognize Social Engineering Attacks
  3. Train Workforce Members on Authentication Best Practices
  4. Train Workforce on Data Handling Best Practices
  5. Train Workforce Members on Causes of Unintentional Data Exposure
  6. Train Workforce Members on Recognizing and Reporting Security Incidents
  7. Train Workforce
  8. Train Workforce
  9. Conduct Role-Specific Security Awareness and Skills Training

1.5 Use a Passive Asset Discovery Tool

* 1. Establish and Maintain a Service Provider Management Policy
  2. Classify Service Providers
  3. Ensure Service Provider Contracts Include Security Requirements
  4. Assess Service Providers
  5. Monitor Service Providers
  6. Securely Decommission Service Providers
  7. Establish and Maintain a Secure Application DevelopmentProcess
  8. Apply Secure Design Principles in Application Architectures
  9. Leverage Vetted Modules or Services for Application Security Components
  10. Implement Code-Level Security Checks
  11. Conduct Application Penetration Testing
  12. Establish and Maintain a Process to Accept and Address Software Vulnerabilities
  13. Perform Root Cause Analysis on Security Vulnerabilities
  14. Establish and Manage an Inventory of Third-Party Software Components
  15. Use Up-to-Date and Trusted Third-Party Software Components
  16. Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities
  17. Use Standard Hardening Configuration Templates for Application Infrastructure
  18. Separate Production and Non-Production Systems
  19. Train Developers in Application Security Concepts and Secure Coding

17.8 Conduct Post-Incident Reviews

* 1. Establish and Maintain a Penetration Testing Program
  2. Perform Periodic External Penetration Tests
  3. Remediate Penetration Test Findings

18.5 Perform Periodic Internal Penetration Tests

* 1. Establish and Maintain a Software Inventory
  2. Ensure Authorized Software is Currently Supported
  3. Address Unauthorized Software
  4. Utilize Automated Software Inventory Tools
  5. Allowlist Authorized Software
  6. Allowlist Authorized Libraries
  7. Allowlist Authorized Scripts
  8. Establish and Maintain a Data Management Process
  9. Encrypt Sensitive Data in Transit
  10. Encrypt Sensitive Data at Rest
  11. Segment Data Processing and Storage Based on Sensitivity
  12. Deploy a Data Loss Prevention Solution
  13. Log Sensitive Data Access
  14. Establish and Maintain a Data Inventory
  15. Configure Data Access Control Lists
  16. Enforce Data Retention
  17. Securely Dispose of Data
  18. Encrypt Data on End-User Devices
  19. Establish and Maintain a Data Classification Scheme
  20. Document Data Flows
  21. Encrypt Data on Removable Media
  22. Establish and Maintain a Secure Configuration Process
  23. Enforce Automatic Device Lockout on Portable End-User Devices
  24. Enforce Remote Wipe Capability on Portable End-User Devices
  25. Separate Enterprise Workspaces on Mobile End-User Devices
  26. Establish and Maintain a Secure Configuration Process for Network Infrastructure
  27. Configure Automatic Session Locking on Enterprise Assets
  28. Implement and Manage a Firewall on Servers
  29. Implement and Manage a Firewall on End-User Devices
  30. Securely Manage Enterprise Assets and Software
  31. Manage Default Accounts on Enterprise Assets and Software
  32. Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
  33. Configure Trusted DNS Servers on Enterprise Assets
  34. Establish and Maintain an Inventory of Accounts
  35. Use Unique Passwords
  36. Disable Dormant Accounts
  37. Restrict Administrator Privileges to Dedicated Administrator Accounts
  38. Establish and Maintain an Inventory of Service Accounts
  39. Centralize Account Management
  40. Establish an Access Granting Process
  41. Establish an Access Revoking Process
  42. Require MFA for Externally-Exposed Applications
  43. Require MFA for Remote Network Access
  44. Require MFA for Administrative Access
  45. Establish and Maintain an Inventory of Authentication and Authorization Systems
  46. Centralize Access Contro
  47. Define and Maintain Role-Based Access Control
  48. Establish and Maintain a Vulnerability Management Process
  49. Establish and Maintain a Remediation Process
  50. Perform Automated Operating System Patch Management
  51. Perform Automated Application Patch Management
  52. Perform Automated Vulnerability Scans of Internal Enterprise Assets
  53. Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
  54. Remediate Detected Vulnerabilities
  55. Establish and maintain an audit log management process that defines the enterpriseâ€™s logging requirements.
  56. Retain Audit Logs
  57. Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat.
  58. Collect Service Provider Logs
  59. Collect Audit Logs
  60. Ensure Adequate Audit Log Storage
  61. Standardize Time Synchronization
  62. Collect Detailed Audit Logs
  63. Collect DNS Query Audit Logs
  64. Collect URL Request Audit Logs
  65. Collect Command-Line Audit Logs
  66. Centralize Audit Logs
  67. Ensure Use of Only Fully Supported Browsers and Email Clients
  68. Use DNS Filtering Services
  69. Maintain and Enforce Network-Based URL Filters
  70. Restrict Unnecessary or Unauthorized Browser and Email Client Extensions
  71. Implement DMARC
  72. Block Unnecessary File Types
  73. Deploy and Maintain Email Server Anti-Malware Protections

## NIST 800-53-rev5

- Controls: 135

AC-1 POLICY AND PROCEDURES

AC-10 CONCURRENT SESSION CONTROL AC-11 SESSION LOCK

AC-12 SESSION TERMINATION

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION AC-16 SECURITY ATTRIBUTES

AC-17 REMOTE ACCESS AC-18 WIRELESS ACCESS

AC-19 ACCESS CONTROL FOR MOBILE DEVICES AC-2 ACCOUNT MANAGEMENT

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS AC-21 INFORMATION SHARING

AC-22 PUBLICLY ACCESSIBLE CONTENT AC-23 DATA MINING PROTECTION

AC-3 ACCESS ENFORCEMENT

AC-4 INFORMATION FLOW ENFORCEMENT AC-5 SEPARATION OF DUTIES

AC-6 LEAST PRIVILEGE

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

AC-8 SYSTEM USE NOTIFICATION AT-1 POLICY AND PROCEDURES

AT-2 LITERACY TRAINING AND AWARENESS AT-3 ROLE-BASED TRAINING

AU-1 POLICY AND PROCEDURES AU-11 AUDIT RECORD RETENTION AU-12 AUDIT RECORD GENERATION AU-2 EVENT LOGGING

AU-3 CONTENT OF AUDIT RECORDS AU-4 AUDIT LOG STORAGE CAPACITY

AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION AU-9 PROTECTION OF AUDIT INFORMATION

CA-2 SECURITY ASSESSMENTS

CA-3 SYSTEM INTERCONNECTIONS

CA-5 PLAN OF ACTION AND MILESTONES CA-7 CONTINUOUS MONITORING

CA-8 PENETRATION TESTING

CA-9 INTERNAL SYSTEM CONNECTION CM-1 POLICY AND PROCEDURES

CM-10 SOFTWARE USAGE RESTRICTIONS CM-11 USER-INSTALLED SOFTWARE

CM-12 INFORMATION LOCATION CM-2 BASELINE CONFIGURATION

CM-3 CONFIGURATION CHANGE CONTROL CM-5 ACCESS RESTRICTIONS FOR CHANGE CM-6 CONFIGURATION SETTINGS

CM-7 LEAST FUNCTIONALITY

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY CM-9 CONFIGURATION MANAGEMENT PLAN

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION CP-2 CONTINGENCY PLAN

CP-4 CONTINGENCY PLAN TESTING CP-6 ALTERNATE STORAGE SITE

CP-7 ALTERNATE PROCESSING SITE

CP-9 INFORMATION SYSTEM BACKUP IA-11 RE-AUTHENTICATION

IA-12 IDENTITY PROOFING

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

IA-4 IDENTIFIER MANAGEMENT

IA-5 AUTHENTICATOR MANAGEMENT IA-6 AUTHENTICATOR FEEDBACK

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

IR-4 INCIDENT HANDLING MA-3 MAINTENANCE TOOLS

MA-4 NONLOCAL MAINTENANCE MP-2 MEDIA ACCESS

MP-7 MEDIA USE

PL-8 SECURITY AND PRIVACY ARCHITECTURES PM-13 SECURITY AND PRIVACY WORKFORCE PM-5 SYSTEM INVENTORY

PM-7 ENTERPRISE ARCHITECTURE RA-1 POLICY AND PROCEDURES RA-10 THREAT HUNTING

RA-2 SECURITY CATEGORIZATION RA-5 VULNERABILITY SCANNING RA-7 RISK RESPONSE

RA-9 CRITICALITY ANALYSIS

SA-10 DEVELOPER CONFIGURATION MANAGEMENT SA-11 DEVELOPER SECURITY TESTING AND EVALUATION

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS SA-16 DEVELOPER-PROVIDED TRAINING

SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN SA-22 UNSUPPORTED SYSTEM COMPONENTS

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE SA-4 ACQUISITION PROCESS

SA-8 SECURITY ENGINEERING PRINCIPLES

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES SC-10 NETWORK DISCONNECT

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT SC-13 CRYPTOGRAPHIC PROTECTION

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES SC-18 MOBILE CODE

SC-2 APPLICATION PARTITIONING

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

SC-23 SESSION AUTHENTICITY SC-26 HONEYPOTS

SC-28 PROTECTION OF INFORMATION AT REST SC-29 HETEROGENEITY

SC-3 SECURITY FUNCTION ISOLATION

SC-30 CONCEALMENT AND MISDIRECTION SC-31 COVERT CHANNEL ANALYSIS

SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS SC-35 HONEYCLIENTS

SC-36 DISTRIBUTED PROCESSING AND STORAGE SC-37 OUT-OF-BAND CHANNELS

SC-38 OPERATIONS SECURITY SC-39 PROCESS ISOLATION

SC-4 INFORMATION IN SHARED RESOURCES SC-41 PORT AND I/O DEVICE ACCESS

SC-43 USAGE RESTRICTIONS

SC-44 DETONATION CHAMBERS

SC-46 CROSS DOMAIN POLICY ENFORCEMENT SC-7 BOUNDARY PROTECTION

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY SI-10 INFORMATION INPUT VALIDATION

SI-12 INFORMATION HANDLING AND RETENTION SI-15 INFORMATION OUTPUT FILTERING

SI-16 MEMORY PROTECTION SI-2 FLAW REMEDIATION

SI-23 INFORMATION FRAGMENTATIO SI-3 MALICIOUS CODE PROTECTION

SI-4 INFORMATION SYSTEM MONITORING

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY SI-8 SPAM PROTECTION

SR-11 COMPONENT AUTHENTICITY SR-12 COMPONENT DISPOSAL

SR-4 PROVENANCE

SR-5 ACQUISITION STRATEGIES, TOOLS, AND METHODS SR-6 SUPPLIER ASSESSMENTS AND REVIEWS

**PCI-DSS *v3.2.1***

- Controls: 147

1 Install and maintain a firewall configuration to protect cardholder data

* 1. Track and monitor all access to network resources and cardholder data
  2. Track and monitor all access to network resources and cardholder data
     1. Track and monitor all access to network resources and cardholder data
     2. Track and monitor all access to network resources and cardholder data
     3. Track and monitor all access to network resources and cardholder data
     4. Track and monitor all access to network resources and cardholder data
  3. Track and monitor all access to network resources and cardholder data
  4. Track and monitor all access to network resources and cardholder data

10.5.3 Track and monitor all access to network resources and cardholder data

10.5.4 Track and monitor all access to network resources and cardholder data

* 1. Track and monitor all access to network resources and cardholder data
     1. Track and monitor all access to network resources and cardholder data
     2. Track and monitor all access to network resources and cardholder data
     3. Track and monitor all access to network resources and cardholder data
  2. Track and monitor all access to network resources and cardholder data
  3. Track and monitor all access to network resources and cardholder data
  4. Track and monitor all access to network resources and cardholder data
  5. Install and maintain a firewall configuration to protect cardholder data
     1. Install and maintain a firewall configuration to protect cardholder data
  6. Regularly test security systems and processes
     1. Regularly test security systems and processes
     2. Regularly test security systems and processes
     3. Install and maintain a firewall configuration to protect cardholder data
  7. Regularly test security systems and processes
     1. Regularly test security systems and processes
     2. Install and maintain a firewall configuration to protect cardholder data
  8. Regularly test security systems and processes
     1. Regularly test security systems and processes
     2. Regularly test security systems and processes
     3. Install and maintain a firewall configuration to protect cardholder data
  9. Regularly test security systems and processes
     1. Install and maintain a firewall configuration to protect cardholder data
  10. Regularly test security systems and processes
      1. Regularly test security systems and processes
      2. Install and maintain a firewall configuration to protect cardholder data
  11. Install and maintain a firewall configuration to protect cardholder data
      1. Install and maintain a firewall configuration to protect cardholder data
  12. Maintain a policy that addresses information security for all personnel
      1. Maintain a policy that addresses information security for all personnel
      2. Maintain a policy that addresses information security for all personnel
      3. Maintain a policy that addresses information security for all personnel
      4. Maintain a policy that addresses information security for all personnel
      5. Maintain a policy that addresses information security for all personnel
      6. Maintain a policy that addresses information security for all personnel
      7. Maintain a policy that addresses information security for all personnel

12.11 Maintain a policy that addresses information security for all personnel

* + 1. Install and maintain a firewall configuration to protect cardholder data
  1. Maintain a policy that addresses information security for all personnel
     1. Install and maintain a firewall configuration to protect cardholder data
  2. Maintain a policy that addresses information security for all personnel

12.3.10 Maintain a policy that addresses information security for all personnel

12.3.8 Maintain a policy that addresses information security for all personnel

12.3.9 Maintain a policy that addresses information security for all personnel

* 1. Maintain a policy that addresses information security for all personnel
  2. Maintain a policy that addresses information security for all personnel
     1. Maintain a policy that addresses information security for all personnel
     2. Maintain a policy that addresses information security for all personnel
  3. Maintain a policy that addresses information security for all personnel
     1. Maintain a policy that addresses information security for all personnel
     2. Maintain a policy that addresses information security for all personnel
  4. Maintain a policy that addresses information security for all personnel
  5. Maintain a policy that addresses information security for all personnel
     1. Maintain a policy that addresses information security for all personnel
  6. Maintain a policy that addresses information security for all personnel
  7. Install and maintain a firewall configuration to protect cardholder data
     1. Install and maintain a firewall configuration to protect cardholder data
     2. Install and maintain a firewall configuration to protect cardholder data
     3. Install and maintain a firewall configuration to protect cardholder data
     4. Install and maintain a firewall configuration to protect cardholder data
     5. Install and maintain a firewall configuration to protect cardholder data
  8. Install and maintain a firewall configuration to protect cardholder data

1. Do not use vendor-supplied defaults for system passwords and other security parameters
   1. Do not use vendor-supplied defaults for system passwords and other security parameters
      1. Do not use vendor-supplied defaults for system passwords and other security parameters
   2. Do not use vendor-supplied defaults for system passwords and other security parameters
      1. Do not use vendor-supplied defaults for system passwords and other security parameters
      2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.2.5 Do not use vendor-supplied defaults for system passwords and other security parameters

* 1. Do not use vendor-supplied defaults for system passwords and other security parameters
  2. Do not use vendor-supplied defaults for system passwords and other security parameters 3,1 Protect stored cardholder data
  3. Protect stored cardholder data
  4. Protect stored cardholder data
     1. Protect stored cardholder data
  5. Encrypt transmission of cardholder data across open, public networks
     1. Encrypt transmission of cardholder data across open, public networks 5 Use and regularly update anti-virus software or programs
  6. Use and regularly update anti-virus software or programs
     1. Use and regularly update anti-virus software or programs
  7. Use and regularly update anti-virus software or programs
  8. Develop and maintain secure systems and applications
  9. Develop and maintain secure systems and applications
  10. Develop and maintain secure systems and applications

6.3.2 Develop and maintain secure systems and applications

* 1. Develop and maintain secure systems and applications
     1. Develop and maintain secure systems and applications
     2. Develop and maintain secure systems and applications
  2. Develop and maintain secure systems and applications
     1. Develop and maintain secure systems and applications

6.5.10 Develop and maintain secure systems and applications

* + 1. Develop and maintain secure systems and applications
    2. Develop and maintain secure systems and applications
    3. Develop and maintain secure systems and applications
    4. Develop and maintain secure systems and applications
    5. Develop and maintain secure systems and applications
    6. Develop and maintain secure systems and applications
    7. Develop and maintain secure systems and applications
    8. Develop and maintain secure systems and applications
  1. Develop and maintain secure systems and applications
  2. Develop and maintain secure systems and applications
  3. Restrict access to cardholder data by business need to know
     1. Restrict access to cardholder data by business need to know
     2. Restrict access to cardholder data by business need to know
     3. Restrict access to cardholder data by business need to know
     4. Restrict access to cardholder data by business need to know
  4. Restrict access to cardholder data by business need to know
  5. Restrict access to cardholder data by business need to know
  6. Assign a unique ID to each person with computer access
     1. Assign a unique ID to each person with computer access
     2. Assign a unique ID to each person with computer access
     3. Assign a unique ID to each person with computer access
     4. Assign a unique ID to each person with computer access

8.1.8 Assign a unique ID to each person with computer access

* 1. Assign a unique ID to each person with computer access
     1. Assign a unique ID to each person with computer access
     2. Assign a unique ID to each person with computer access
  2. Assign a unique ID to each person with computer access
     1. Assign a unique ID to each person with computer access
     2. Assign a unique ID to each person with computer access
  3. Assign a unique ID to each person with computer access
  4. Assign a unique ID to each person with computer access
     1. Assign a unique ID to each person with computer access
  5. Assign a unique ID to each person with computer access
  6. Assign a unique ID to each person with computer access
     1. Restrict access to cardholder data by business need to know

9.3 Restrict access to cardholder data by business need to know

* 1. Restrict physical access to cardholder data
     1. Restrict access to cardholder data by business need to know
  2. Restrict physical access to cardholder data
     1. Restrict access to cardholder data by business need to know
  3. Restrict physical access to cardholder data
  4. Restrict physical access to cardholder data
  5. Restrict access to cardholder data by business need to know
     1. Restrict access to cardholder data by business need to know
     2. Restrict access to cardholder data by business need to know
     3. Restrict access to cardholder data by business need to know

## C5 (2022)

* + - * Controls: 17

HR-03 Security training and awareness-raising programme IDM-01 Policy for system and data access authorisations IDM-02 User registration

IDM-06 Administrator authorisations IDM-08 Secure login methods

IDM-11 Password requirements and validation parameters IDM-12 Restriction and control of administrative software KOS-01 Technical safeguards

KOS-02 Monitoring of connections KOS-03 Cross-network access

KRY-02 Encryption of data for transmission (transport encryption) KRY-03 Encryption of sensitive data for storage

RB-05 Protection against malware

RB-06 Data backup and restoration (concept)

RB-21 Handling of vulnerabilities, malfunctions and errors (check of open vulnerabilities) RB-22 Handling of vulnerabilities, malfunctions and errors (system hardening)

RB-23 Segregation of stored and processed data of the cloud customers in jointly used resources

**ENS CNN-STIC *(2022)***

* + - * Controls: 17

mp.com.2 Confidentiality protection mp.com.3 Integrity and authenticity protection

mp.com.4 Separation of information flows in the network mp.info.6 Backups

mp.per.3 Training

mp.s.2 Services and Web Applications protection mp.s.3 Web browsing protection

mp.s.4 DoS protection

mp.sw.1 Applications development op.acc.2 Access requirements op.acc.3 Tasks and duties segregation

op.acc.4 Access rights management process

op.acc.6 Authentication mechanism (users of the organization) op.exp.2 Security settings

op.exp.8 Activity log

op.mon.1 Intrusion detection op.mon.3 Monitoring