OpenSecOps SOAR AWS DynamoDB

Standard Operating Procedure

Table of Contents

1 Introduction

The purpose of this document is to specify baseline settings for AWS DynamoDB tables so that teams can provision them in a safe, conformant way.

2 Scope of SOP

This document covers AWS DynamoDB tables and their configuration options.

Document Versions

Version	Date	Changes	Author
1.0	2022-09-12	First version	Peter Bengtson
1.1	2025-04-07	Replaced “Delegat” with “OpenSecOps” throughout	Peter Bengtson
1.2	2025-04-27	Removed obsolete info	Peter Bengtson

3 Security Hub Controls for DynamoDB Tables

Below are the enabled controls in AWS Security Hub pertaining to DynamoDB tables.

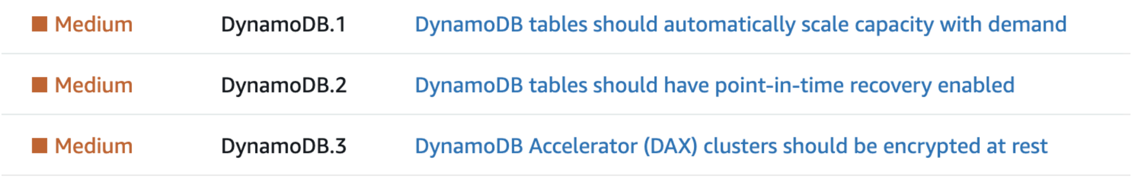
3.1 CRITICAL

None

3.2 HIGH

None

3.3 MEDIUM



🟧 Medium	DynamoDB.1	DynamoDB tables should automatically scale capacity with demand
🟧 Medium	DynamoDB.2	DynamoDB tables should have point-in-time recovery enabled
🟧 Medium	DynamoDB.3	DynamoDB Accelerator (DAX) clusters should be encrypted at rest

3.4 LOW

None

4 Disabling Point-In-Time Recovery

If you need a DynamoDB table *not* to have PITR enabled, tag your DynamoDB table at creation time with the following tag:

```
soar:dynamodb:no-pit-recovery
```

The tag is case-sensitive.

When the above tag is present, the auto-remediation which enables PITR for a DynamoDB table will not be performed. Use cases include caches and other short-lived data such as session data. PITR is required, however, for tables as part of Disaster Recovery.

If the DynamoDB table already has PITR enabled, adding the tag after the fact will *not* disable PITR. You must add the tag, then turn off PITR either manually in the console, using the CLI, the API, or in code.