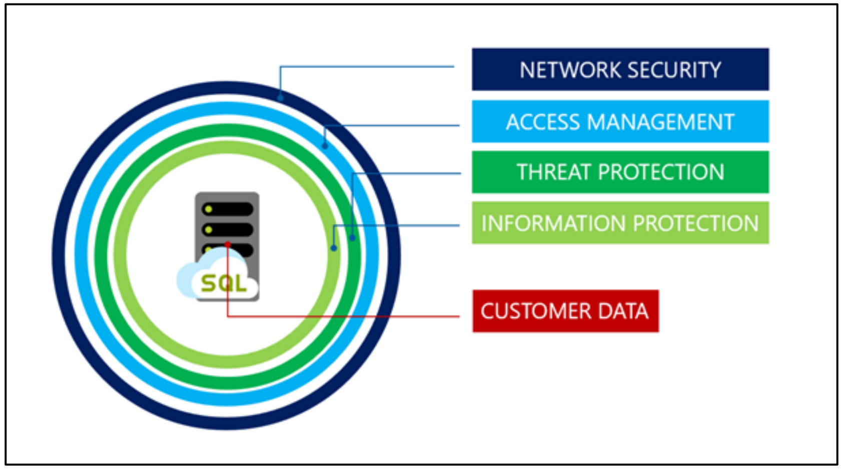
SQL Moderation Hack
Secure Your Data with Azure SQL DB Labs Step-by-step

V5.0

Table of Contents

1. Introduction

This hands-on lab will introduces you to the layered security model available when running databases in Azure. The activities within this hands-on lab will progress from the outer security layers that protect the perimeter of Azure SQL through to the inner layers that protect the information contained within the data.



Because SQL Managed Instance always runs in a private network the Network Security layer has already been implemented at the vNet level. Equally we have already defined and implemented Azure AD and SQL Server logins, roles and permissions so the Access Management tier has also been pre-built.

So this lab will focus on the Threat Protection, Information Protection and Customer Data layers of the security model and how these are implement in Azure SQL Managed Instance through:

- Using Data Discovery & Classification
- Azure Defender for SQL
  - Vulnerability Assessment
  - Advanced Threat Protection

2. Azure SQL Database & Team VM Login Details

All the labs run against the TEAMXX_TenantDataDb that you migrated earlier using either SQL Server Management Studio or the Azure Portal.

Your Win10 VM (vm-TEAMXX) login credentials are also a member of SQL Server sysadmin role.

Username	**localhost\DemoUser**
Password	**Demo@pass1234567**

The Azure Portal credentials are those that your proctor will supply.

3. LAB 1: Data Discovery & Classification

Data Discovery & Classification

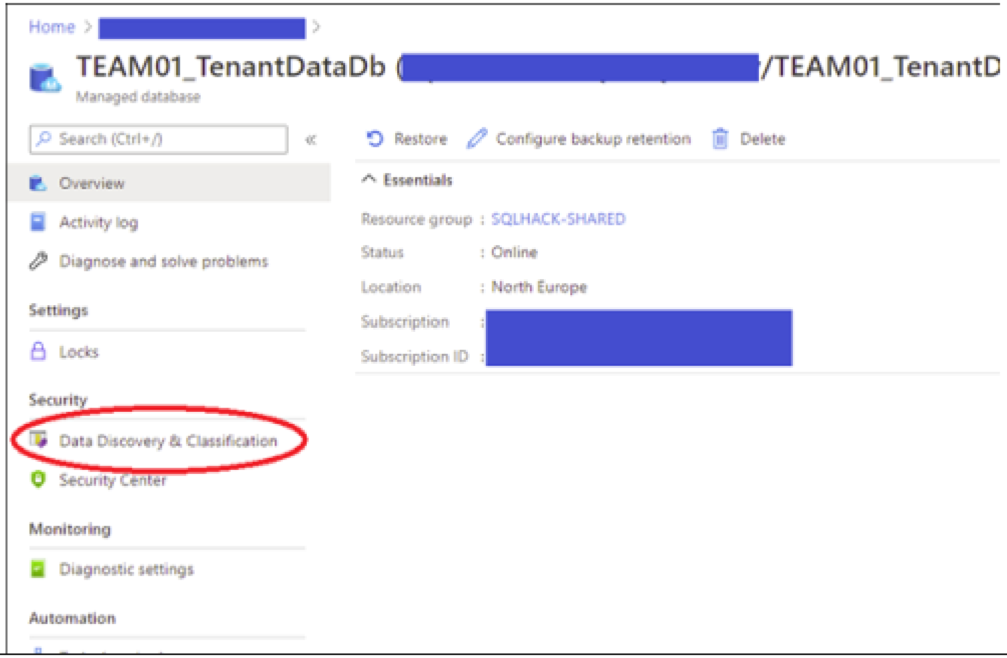
Data Discovery & Classification is a built-in capability for discovering, classifying, labelling and protecting sensitive data in databases. It can be used to support many use cases including financial, healthcare, personally identifiable (PII) data and help meet data privacy standards and regulatory compliance.

More information on Data Discovery & Classification can be found here:

https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview

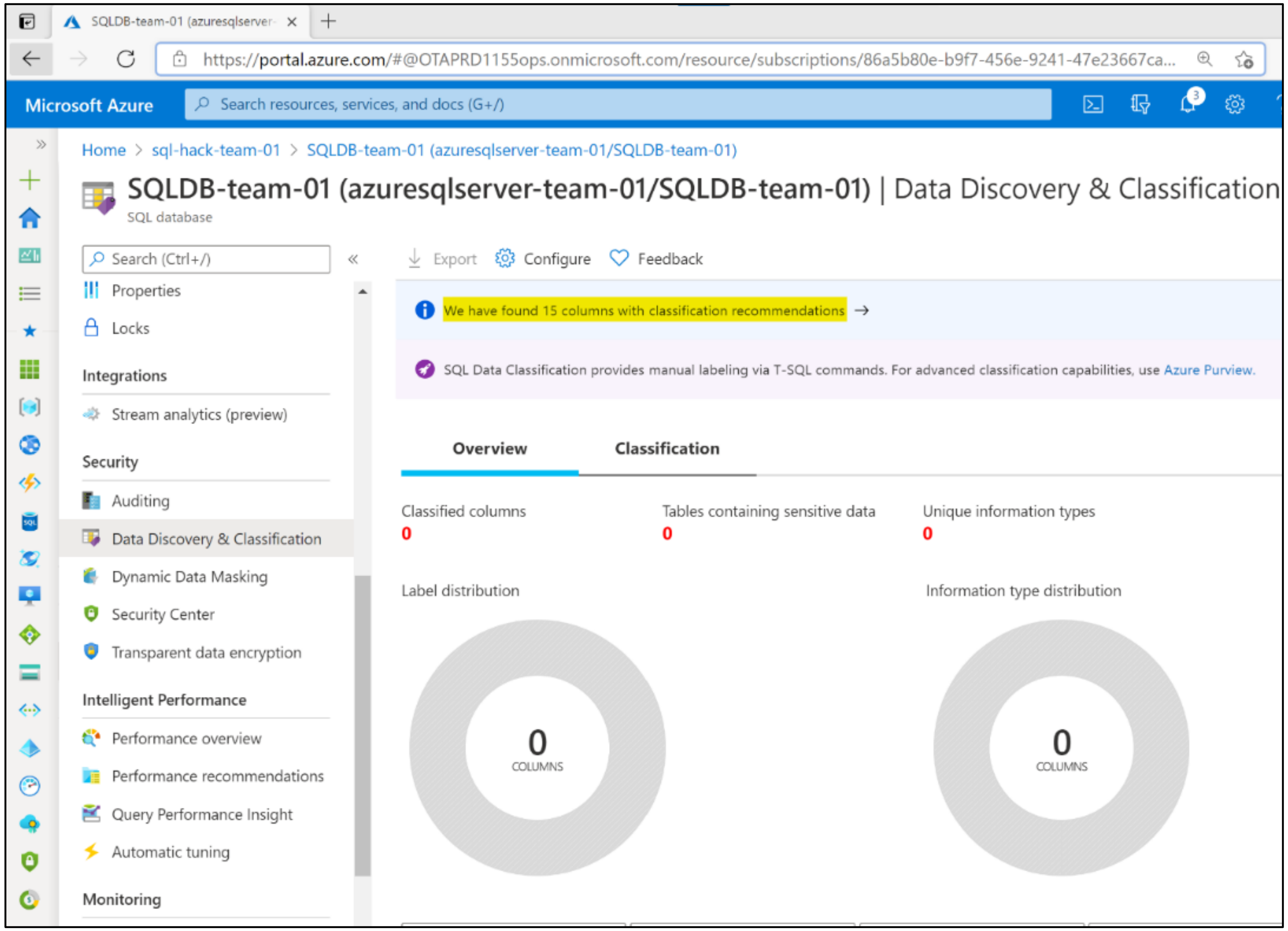
Viewing Data Classification Recommendations

Whenever a database is deployed or schema changes are made to an existing database, the Data Discovery & Classification engine automatically performs a scan to identify columns that may potentially contain sensitive data.

Narrative	Screenshot/Code	Notes
1. Within the Azure Portal navigate to the shared Azure SQL Managed Instance screen. Scroll down to the list of databases and click on your teams **TEAMXX_TenantDataDb** database.		
2. On the blade on the left, under the **Security** section click “**Data Discovery & Classification**”	 Home > [redacted] > TEAM01_TenantDataDb ([redacted]/TEAM01_TenantD Managed database Resource group : SQLHACK-SHARED Status : Online Location : North Europe Subscription : [redacted] Subscription ID : Search (Ctrl+/) Restore Configure backup retention Delete Essentials Overview Activity log Diagnose and solve problems Settings Locks Security Data Discovery & Classification Security Center Monitoring Diagnostic settings Automation	

The Data Discovery and Classification **Overview** shows that no data classifications have been made but based on the automatic classification scan there are a number of potential data classification recommendations as shown at the top of the report:

3. Click the blue information bar (highlighted in yellow) to view the data classification recommendations


SQLDB-team-01 (azuresqlserver-
https://portal.azure.com/#@OTAPRD1155ops.onmicrosoft.com/resource/subscriptions/86a5b80e-b9f7-456e-9241-47e23667ca...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > sql-hack-team-01 > SQLDB-team-01 (azuresqlserver-team-01/SQLDB-team-01)
Search (Ctrl+/)
Properties
Locks
Integrations
Stream analytics (preview)
Security
Auditing
Data Discovery & Classification
Dynamic Data Masking
Security Center
Transparent data encryption
Intelligent Performance
Performance overview
Performance recommendations
Query Performance Insight
Automatic tuning
Monitoring
Export
Configure
Feedback
Overview
Classification
Label distribution
Information type distribution
0
COLUMNS
0
COLUMNS

SQLDB-team-01 (azuresqlserver-team-01/SQLDB-team-01) | Data Discovery & Classification

SQL database

We have found 15 columns with classification recommendations →

SQL Data Classification provides manual labeling via T-SQL commands. For advanced classification capabilities, use Azure Purview.

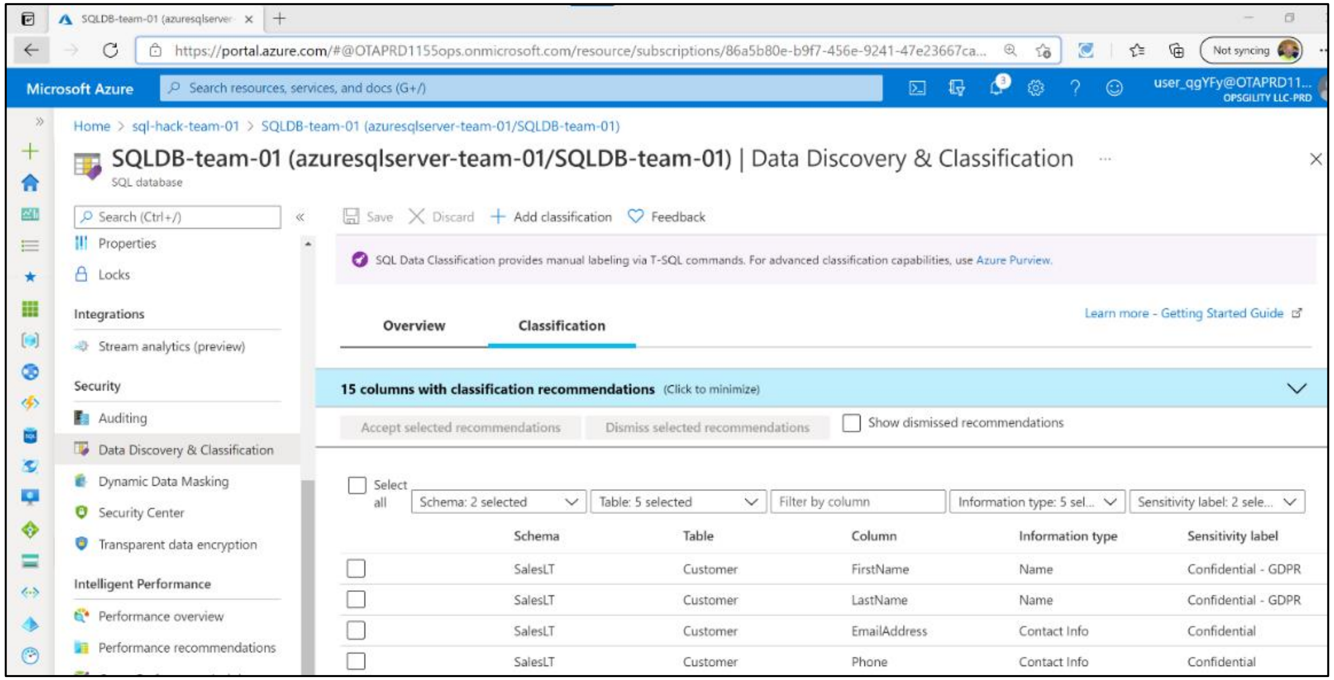
Classified columns 0

Tables containing sensitive data 0

Unique information types 0

The recommendations show the name of the schema, table and column with intelligent information type classification and sensitivity recommendations.

As can be seen the **Customer** table in the **SalesLT** schema contains the columns **FirstName** and **LastName**. The initial data classification scan has identified that the **Information type** of these columns from a data classification perspective is **Name** and the **Sensitivity Label** for these columns is recommended to be **Confidential – GDPR**.


SQLDB-team-01 (azuresqlserver
https://portal.azure.com/#@OTAPRD1155ops.onmicrosoft.com/resource/subscriptions/86a5b80e-b9f7-456e-9241-47e23667ca...
Not syncing
Microsoft Azure
Search resources, services, and docs (G+/)
user_qgYFy@OTAPRD11...
OPSGILITY LLC-PRD
Home > sql-hack-team-01 > SQLDB-team-01 (azuresqlserver-team-01/SQLDB-team-01)
SQLDB-team-01 (azuresqlserver-team-01/SQLDB-team-01) | Data Discovery & Classification
SQL database
Search (Ctrl+/)
Properties
Locks
Integrations
Stream analytics (preview)
Security
Auditing
Data Discovery & Classification
Dynamic Data Masking
Security Center
Transparent data encryption
Intelligent Performance
Performance overview
Performance recommendations
Save
Discard
Add classification
Feedback
Learn more - Getting Started Guide
Overview
Classification
Accept selected recommendations
Dismiss selected recommendations
Schema: 2 selected
Table: 5 selected
Filter by column
Information type: 5 sel...
Sensitivity label: 2 sele...

SQL Data Classification provides manual labeling via T-SQL commands. For advanced classification capabilities, use Azure Purview.

15 columns with classification recommendations (Click to minimize)

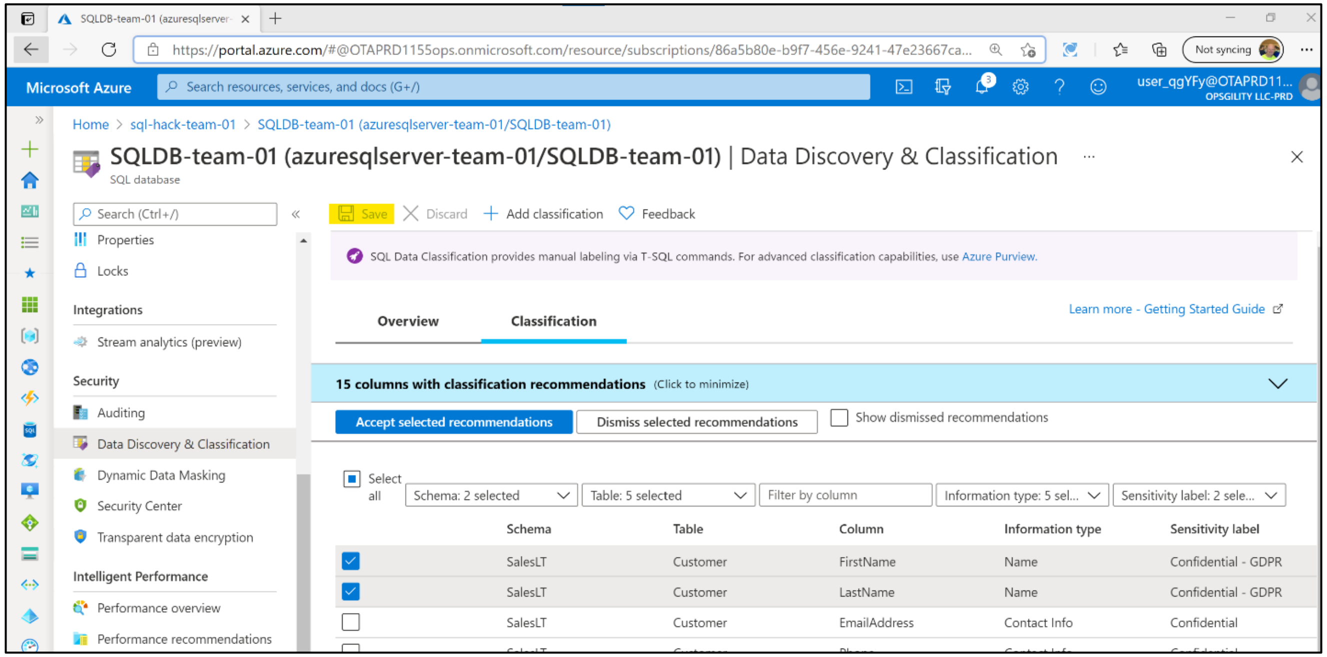
□ Show dismissed recommendations

□ Select all	Schema	Table	Column	Information type	Sensitivity label
□	SalesLT	Customer	FirstName	Name	Confidential - GDPR
□	SalesLT	Customer	LastName	Name	Confidential - GDPR
□	SalesLT	Customer	EmailAddress	Contact Info	Confidential
□	SalesLT	Customer	Phone	Contact Info	Confidential

4. Select the **FirstName** and **LastName** classification recommendations by selecting the recommendation rows, click **Accept selected recommendations** and then click **Save**.

5. Click the **Overview** tab on the Data Discovery & Classification report to look at the saved data classifications.

There are now two columns classified from the Customer table with the information type of **Name** and the sensitivity label **Confidential – GDPR**.



SQLDB-team-01 (azuresqlserver-
https://portal.azure.com/#@OTAPRD1155ops.onmicrosoft.com/resource/subscriptions/86a5b80e-b9f7-456e-9241-47e23667ca...
Not syncing
Microsoft Azure
Search resources, services, and docs (G+/)
user_qgYFy@OTAPRD11...
OPSGILITY LLC-PRD
Home > sql-hack-team-01 > SQLDB-team-01 (azuresqlserver-team-01/SQLDB-team-01)
Search (Ctrl+/)
Properties
Locks
Integrations
Stream analytics (preview)
Security
Auditing
Data Discovery & Classification
Dynamic Data Masking
Security Center
Transparent data encryption
Intelligent Performance
Performance overview
Performance recommendations
Save
Discard
Add classification
Feedback
Learn more - Getting Started Guide
Overview
Classification
Accept selected recommendations
Dismiss selected recommendations
Show dismissed recommendations
Select all
Schema: 2 selected
Table: 5 selected
Filter by column
Information type: 5 sel...
Sensitivity label: 2 sele...

SQLDB-team-01 (azuresqlserver-team-01/SQLDB-team-01) | Data Discovery & Classification

SQL database

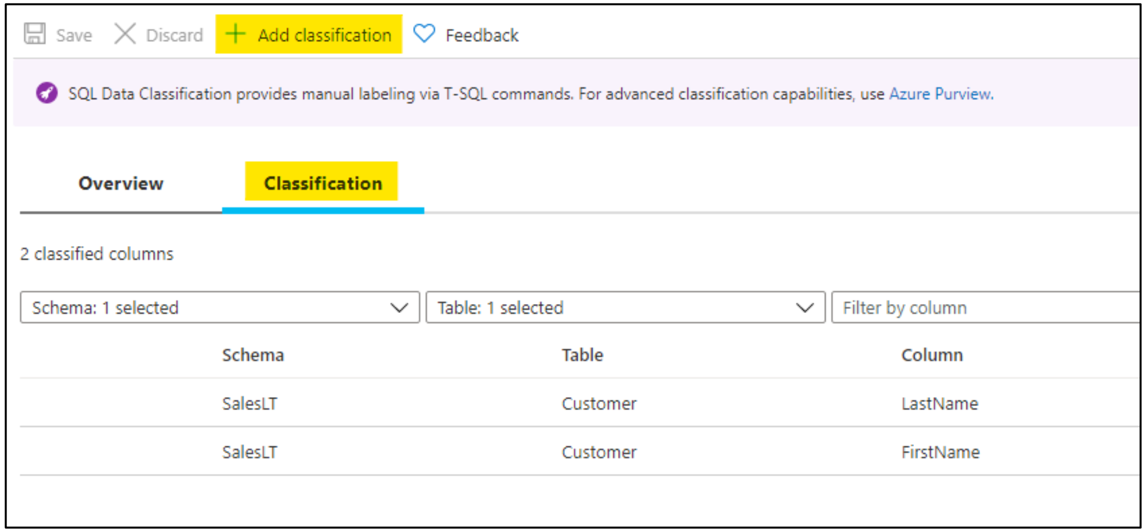
SQL Data Classification provides manual labeling via T-SQL commands. For advanced classification capabilities, use Azure Purview.

15 columns with classification recommendations (Click to minimize)

	Schema	Table	Column	Information type	Sensitivity label
☑	SalesLT	Customer	FirstName	Name	Confidential - GDPR
☑	SalesLT	Customer	LastName	Name	Confidential - GDPR
□	SalesLT	Customer	EmailAddress	Contact Info	Confidential

Now let’s add a custom data classification which is not based on the auto recommendations.

6. Switch back to the **Classification** tab at the top of the report click “**+ Add classification**”.



SQL Data Classification provides manual labeling via T-SQL commands. For advanced classification capabilities, use Azure Purview.

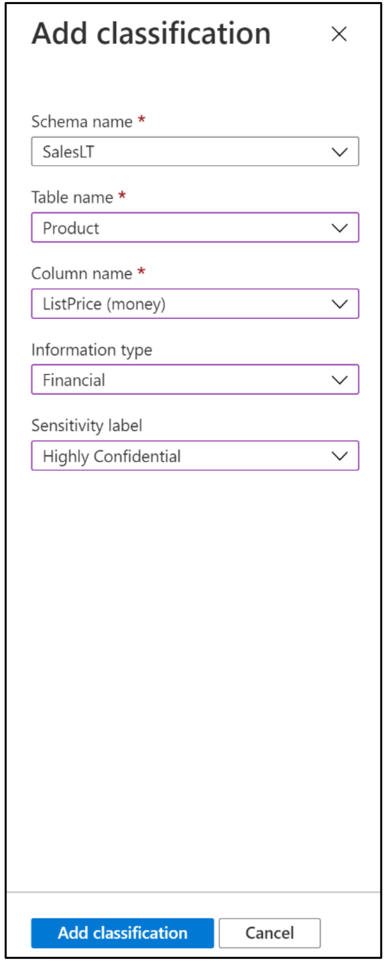
2 classified columns

Schema	Table	Column
SalesLT	Customer	LastName
SalesLT	Customer	FirstName

7. On the **Add Classification** blade on the far right of the screen set the following values and then click **Add Classification** and then **Save** to save your new classification.

8. Click the **Overview** tab to look at the saved data classifications.

Schema name:	**SalesLT**
Table name:	**Product**
Column name:	**ListPrice**
Information type:	**Financial**
Sensitivity Label:	**Highly Confidential**
Click	**Add Classification**
Click	**Save**



Add classification

Schema name * SalesLT

Table name * Product

Column name * ListPrice (money)

Information type Financial

Sensitivity label Highly Confidential

9. Open SQL Server Management Studio, connect to the shared SQL Managed Instance and open a new TSQL query window connected to your **TEAMXX_TenantDataDb** database
10. Run the SELECT statements opposite against your **TEAMXX_TenantDataDb** database.
	`-- 1 Data Discovery & Classification`
	`SELECT`
	`      c.FirstName`
	`     ,c.LastName`
	`     ,c.*`
	`FROM SalesLT.Customer c;`
	
	`SELECT`
	`     p.ListPrice`
	`FROM SalesLT.Product p;`	

Nothing out of the ordinary happens - two simple result sets should be returned containing the FirstName, LastName and ListPrice columns.	***REMEMBER: Data Discovery and Classification is not a security mechanism – it's a data tagging and management tool.***	

4. LAB 2 Part 1: Azure Defender for SQL – Vulnerability Assessment

When provisioning an Azure SQL Managed Instance or an Azure SQL Database logical server there is the option to enable the security feature Azure Defender for SQL.

This security feature offers two security components:

- Vulnerability Assessments
- Advanced Threat Protection

This first part of the lab will focus on Vulnerability Assessments, Part 2 will deal with Advanced Threat Protection.

Vulnerability Assessment

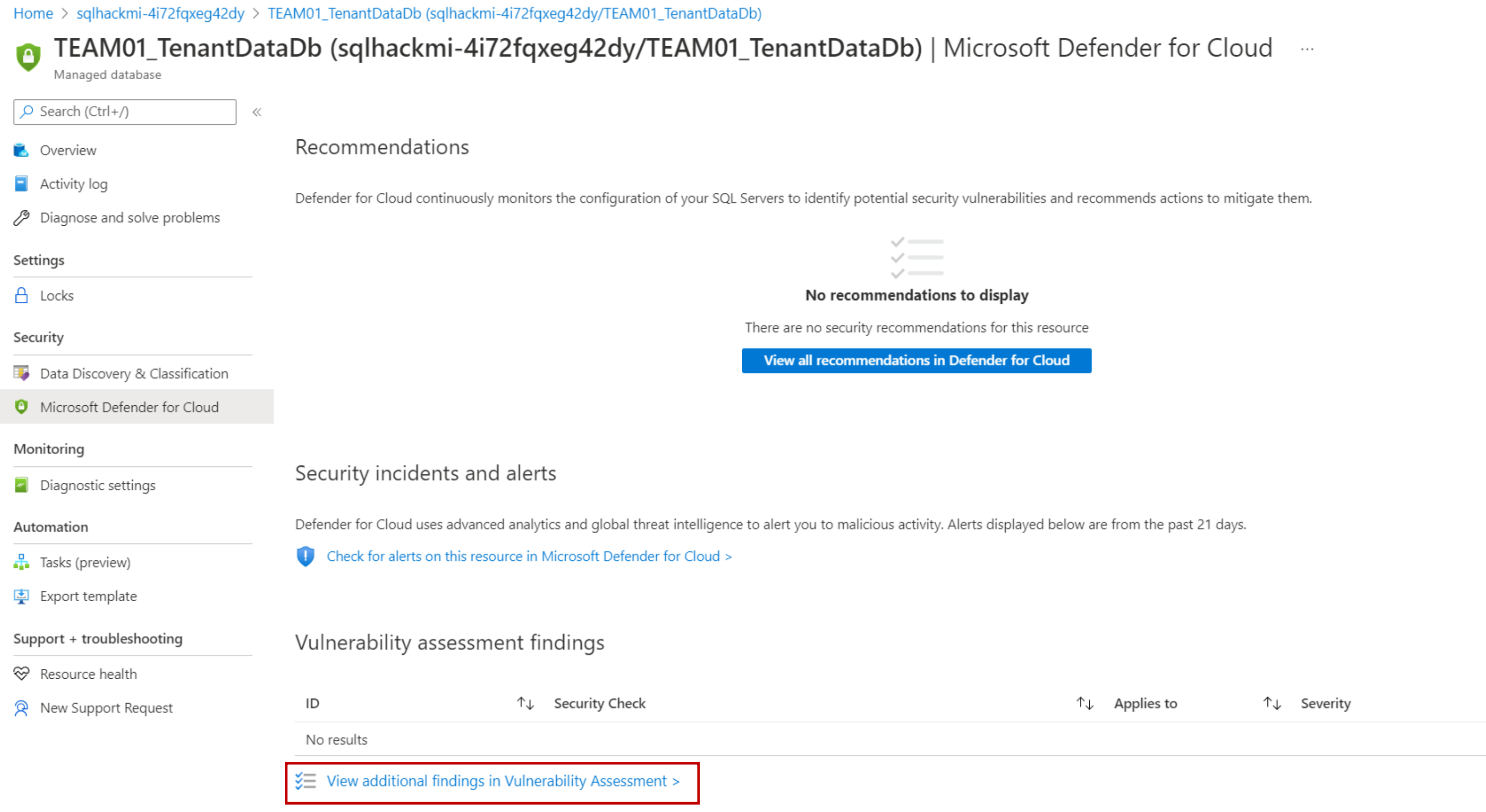
A Vulnerability Assessment is an output position (or report) from a vulnerability scan.

A Vulnerability Assessment scan is the application of SQL Server best practices based on a rules engine, the goal being to improve the security posture of your Azure SQL Managed Instance or Azure SQL Database. The first scan will produce the initial vulnerability scan baseline. The first scan happens automatically once a database is deployed.

More details on Azure SQL vulnerability assessments can be found here:

https://docs.microsoft.com/en-us/azure/azure-sql/database/sql-vulnerability-assessment

Narrative	Screenshot/Code	Notes
1. In the Azure portal navigate to the shared SQL Managed Instance.		
2. Scroll down the Overview screen until you see the list of databases and click on your **TEAMXX_TenantDataDB** database.		

3. In the **TEAMXX_TenantDataDB** database screen. On the left hand blade click **Microsoft Defender for Cloud** in the Security section 4. Scroll down the screen to the bottom and click the “**View additional findings in Vulnerability Assessment >**” link	

Home > sqlhackmi-4i72fqxeg42dy > TEAM01_TenantDataDb (sqlhackmi-4i72fqxeg42dy/TEAM01_TenantDataDb)

TEAM01_TenantDataDb (sqlhackmi-4i72fqxeg42dy/TEAM01_TenantDataDb) | Microsoft Defender for Cloud

Managed database

Recommendations

Defender for Cloud continuously monitors the configuration of your SQL Servers to identify potential security vulnerabilities and recommends actions to mitigate them.

No recommendations to display

There are no security recommendations for this resource

Security incidents and alerts

Defender for Cloud uses advanced analytics and global threat intelligence to alert you to malicious activity. Alerts displayed below are from the past 21 days.

Check for alerts on this resource in Microsoft Defender for Cloud >

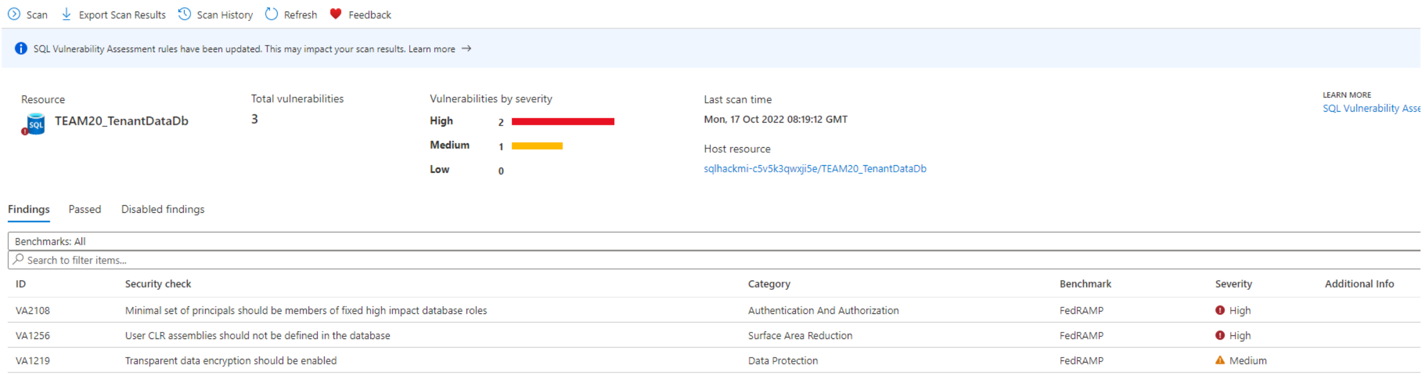
Vulnerability assessment findings

ID	Security Check	Applies to	Severity
No results			

View additional findings in Vulnerability Assessment >

The “Vulnerability Assessment” page can be used to run a scan, view scan history and will show the number of checks that have been passed and failed for the last scan with failed checks listed in the table below.

5. Run a scan if prompted to do so which should only take a few minutes.



SQL Vulnerability Assessment rules have been updated. This may impact your scan results. Learn more →

Resource: TEAM20_TenantDataDb

Total vulnerabilities: 3

Vulnerabilities by severity: High 2, Medium 1, Low 0

Last scan time: Mon, 17 Oct 2022 08:19:12 GMT

Host resource: sqlhackmi-c5v5k3qwxji5e/TEAM20_TenantDataDb

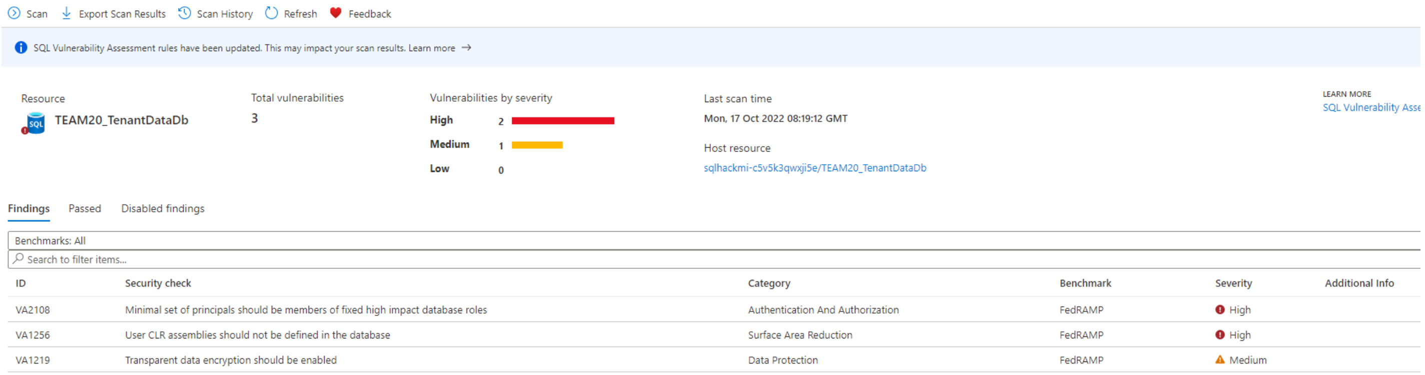
Findings | Passed | Disabled findings

Benchmarks: All

Search to filter items...

ID	Security check	Category	Benchmark	Severity	Additional Info
VA2108	Minimal set of principals should be members of fixed high impact database roles	Authentication And Authorization	FedRAMP	● High	
VA1256	User CLR assemblies should not be defined in the database	Surface Area Reduction	FedRAMP	● High	
VA1219	Transparent data encryption should be enabled	Data Protection	FedRAMP	⚠ Medium	

6. Review the lists of passed and failed checks. Notice that the report is specific to database you ran the scan for but does also include events against the system database and therefore flag server configuration issues.



SQL Vulnerability Assessment rules have been updated. This may impact your scan results. Learn more →

Resource: TEAM20_TenantDataDb

Total vulnerabilities: 3

Vulnerabilities by severity: High 2, Medium 1, Low 0

Last scan time: Mon, 17 Oct 2022 08:19:12 GMT

Host resource: sqlhackmi-c5v5k3qwxji5e/TEAM20_TenantDataDb

Findings | Passed | Disabled findings

Benchmarks: All

Search to filter items...

ID	Security check	Category	Benchmark	Severity	Additional Info
VA2108	Minimal set of principals should be members of fixed high impact database roles	Authentication And Authorization	FedRAMP	● High	
VA1256	User CLR assemblies should not be defined in the database	Surface Area Reduction	FedRAMP	● High	
VA1219	Transparent data encryption should be enabled	Data Protection	FedRAMP	⚠ Medium	

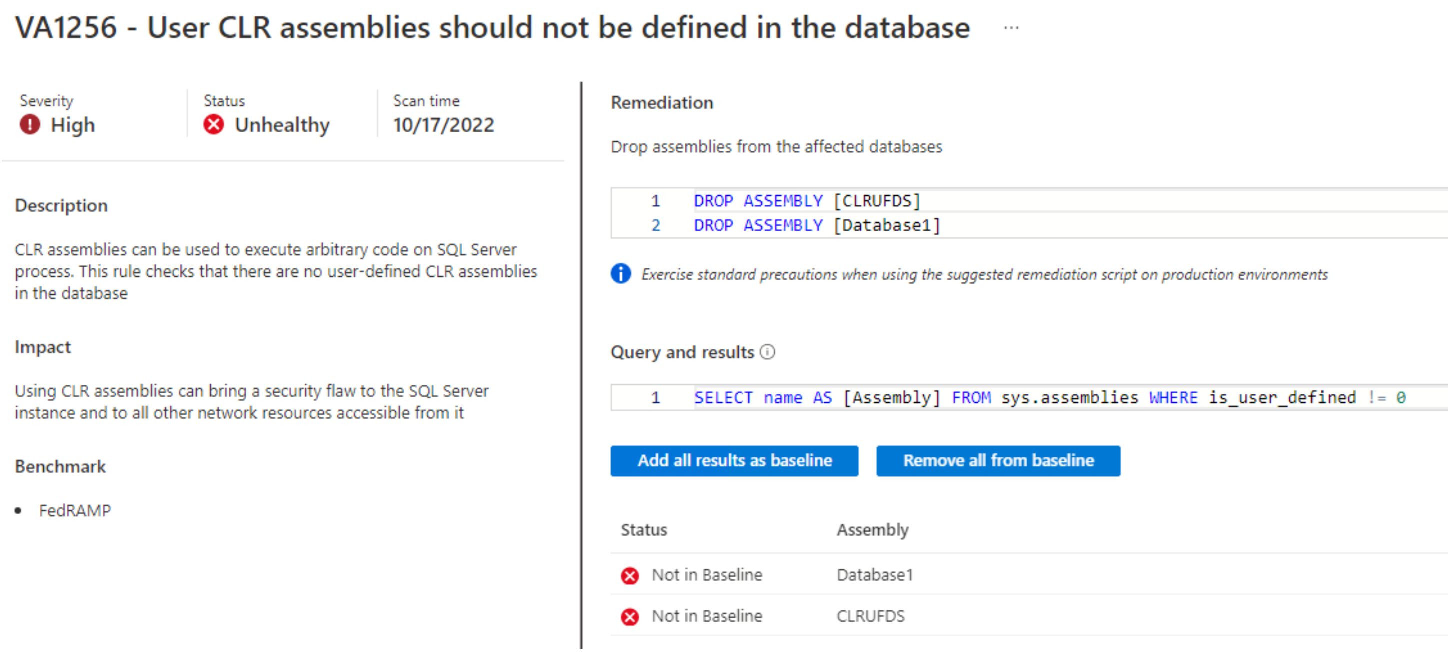
7. In the **Findings** tab, which lists the failed checks, click on finding:

ID	Security Check
VA1256	User CLR assemblies should not be defined in the database

8. Note the detailed report lists the rule's details, the offending CLRs and a remediation script to remove them.

However, because these 2 CLRs are an integral part of our migrated legacy application we need to keep them.

But equally we don't want them to be continuously flagged as an issue in the Vulnerability Assessment reports. To do this we can add exceptions to the Vulnerability Assessment's "baseline" position.



VA1256 - User CLR assemblies should not be defined in the database

Severity: High

Status: Unhealthy

Scan time: 10/17/2022

Description

CLR assemblies can be used to execute arbitrary code on SQL Server process. This rule checks that there are no user-defined CLR assemblies in the database

Impact

Using CLR assemblies can bring a security flaw to the SQL Server instance and to all other network resources accessible from it

Benchmark

- FedRAMP

Remediation

Drop assemblies from the affected databases

```
DROP ASSEMBLY [CLRUFDS]
DROP ASSEMBLY [Database1]
```

Exercise standard precautions when using the suggested remediation script on production environments

Query and results

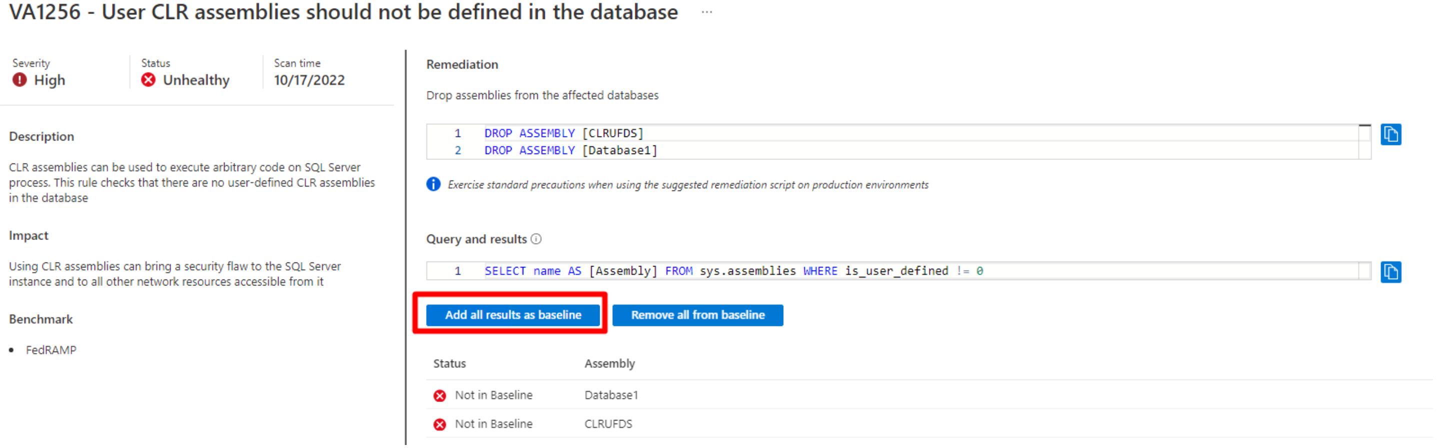
```
SELECT name AS [Assembly] FROM sys.assemblies WHERE is_user_defined != 0
```

Status	Assembly
☒ Not in Baseline	Database1
☒ Not in Baseline	CLRUFDS

9. On the details page for V1256 click **Add all results as baseline** and select **Yes** in the Set base line message.

Adding the results as the baseline will update the Vulnerability Assessment rules engine to accept the current CLR Assemblies as allowable and set a new baseline position for the rule.

Notice, in the upper side of the details page for 1256, a warning saying There are pending baseline changes. Run a new scan to see updated results.



VA1256 - User CLR assemblies should not be defined in the database ···

Severity	Status	Scan time
! High	✖ Unhealthy	10/17/2022

Description

CLR assemblies can be used to execute arbitrary code on SQL Server process. This rule checks that there are no user-defined CLR assemblies in the database

Impact

Using CLR assemblies can bring a security flaw to the SQL Server instance and to all other network resources accessible from it

Benchmark

- FedRAMP

Remediation

Drop assemblies from the affected databases

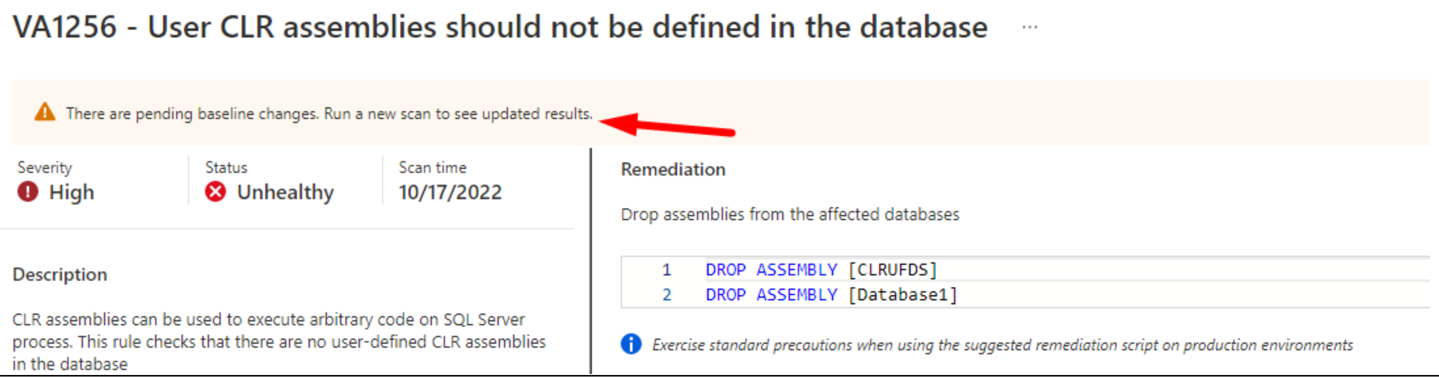
```
DROP ASSEMBLY [CLRUFDS]
DROP ASSEMBLY [Database1]
```

Exercise standard precautions when using the suggested remediation script on production environments

Query and results

```
SELECT name AS [Assembly] FROM sys.assemblies WHERE is_user_defined != 0
```

Status	Assembly
✖ Not in Baseline	Database1
✖ Not in Baseline	CLRUFDS



VA1256 - User CLR assemblies should not be defined in the database ···

⚠ There are pending baseline changes. Run a new scan to see updated results.

Severity	Status	Scan time
! High	✖ Unhealthy	10/17/2022

Description

CLR assemblies can be used to execute arbitrary code on SQL Server process. This rule checks that there are no user-defined CLR assemblies in the database

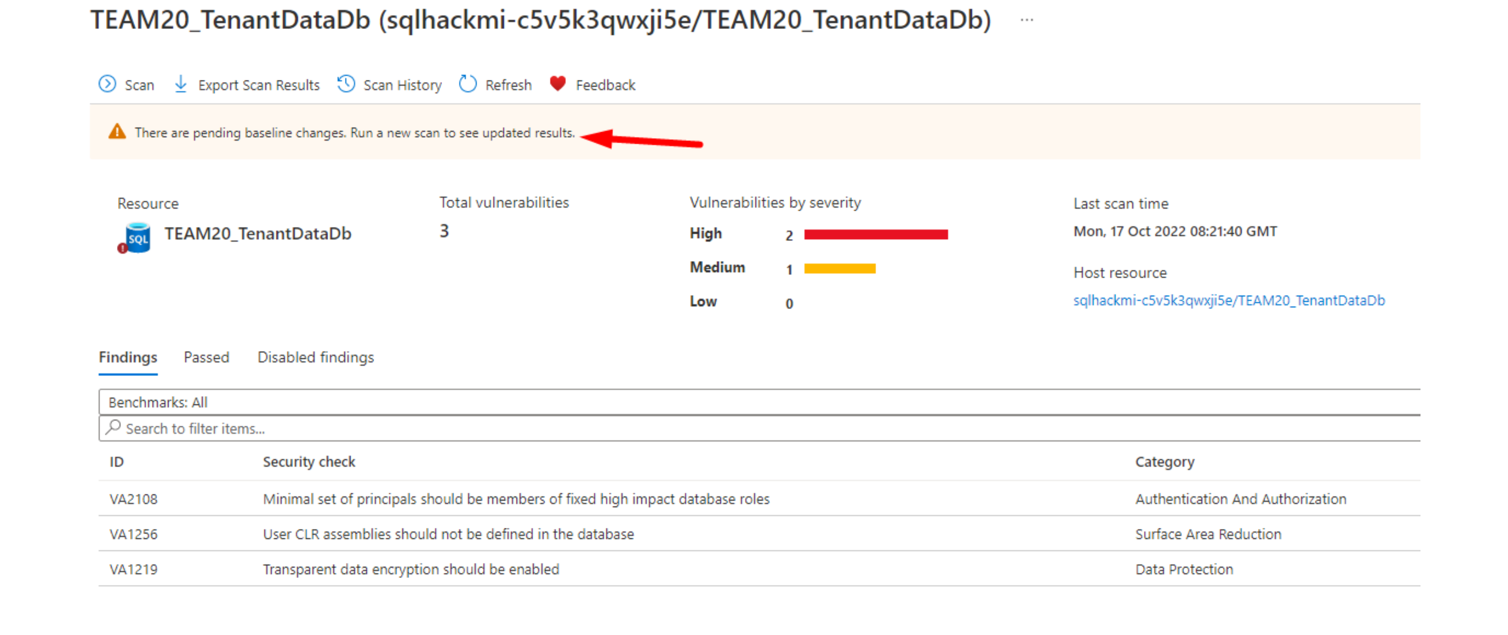
Remediation

Drop assemblies from the affected databases

```
DROP ASSEMBLY [CLRUFDS]
DROP ASSEMBLY [Database1]
```

Exercise standard precautions when using the suggested remediation script on production environments

10. Close the details page for 1256 to get back to the Assessment summary page and notice the same warning



TEAM20_TenantDataDb (sqlhackmi-c5v5k3qwxji5e/TEAM20_TenantDataDb) ...

There are pending baseline changes. Run a new scan to see updated results.

Resource: TEAM20_TenantDataDb

Total vulnerabilities: 3

Vulnerabilities by severity

High	2
Medium	1
Low	0

Last scan time: Mon, 17 Oct 2022 08:21:40 GMT

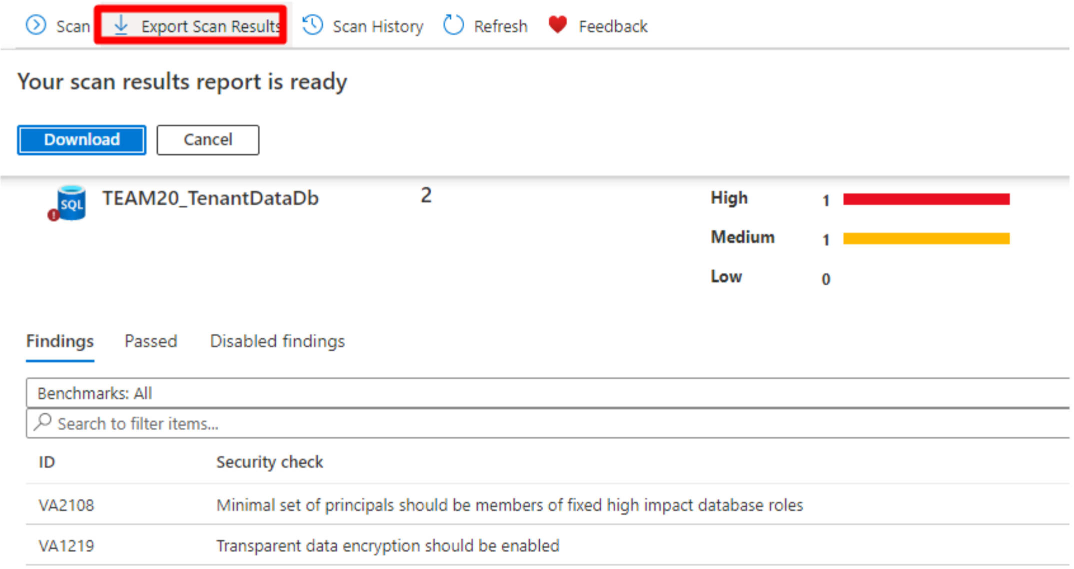
Host resource: sqlhackmi-c5v5k3qwxji5e/TEAM20_TenantDataDb

ID	Security check	Category
VA2108	Minimal set of principals should be members of fixed high impact database roles	Authentication And Authorization
VA1256	User CLR assemblies should not be defined in the database	Surface Area Reduction
VA1219	Transparent data encryption should be enabled	Data Protection

11. Click the **Scan** button to run a manual scan which will take about a minute. Once the scan completes the finding VA1256 will be removed from the Findings list.

When making changes to a Vulnerability Assessment baseline it may be necessary for compliance reasons to export a Scan Findings report to show the security posture of the Azure SQL Database in relation to the amended baseline.

To export the results of a scan to reflect the current baseline click "**Export Scan Results**" at the top of the portal screen:



Your scan results report is ready

TEAM20_TenantDataDb	2		
		High	1
		Medium	1
		Low	0

ID	Security check
VA2108	Minimal set of principals should be members of fixed high impact database roles
VA1219	Transparent data encryption should be enabled

NOTE: Excel is *not* installed on your lab VMs *so you will have to copy the report to your own desktop to have a look at it.*

5. LAB 2 Part 2: Azure Defender for SQL – Advanced Threat Protection

The other security component of Azure Defender for SQL is Advanced Threat Protection.

Advanced Threat Protection provides a layer of security that can detect and respond to potential threats as they occur by providing security alerts on anomalous activities. Alerts can be generated based on suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access and queries patterns.

More information in Azure Defender for SQL – Advanced Threat Protection can be found here:

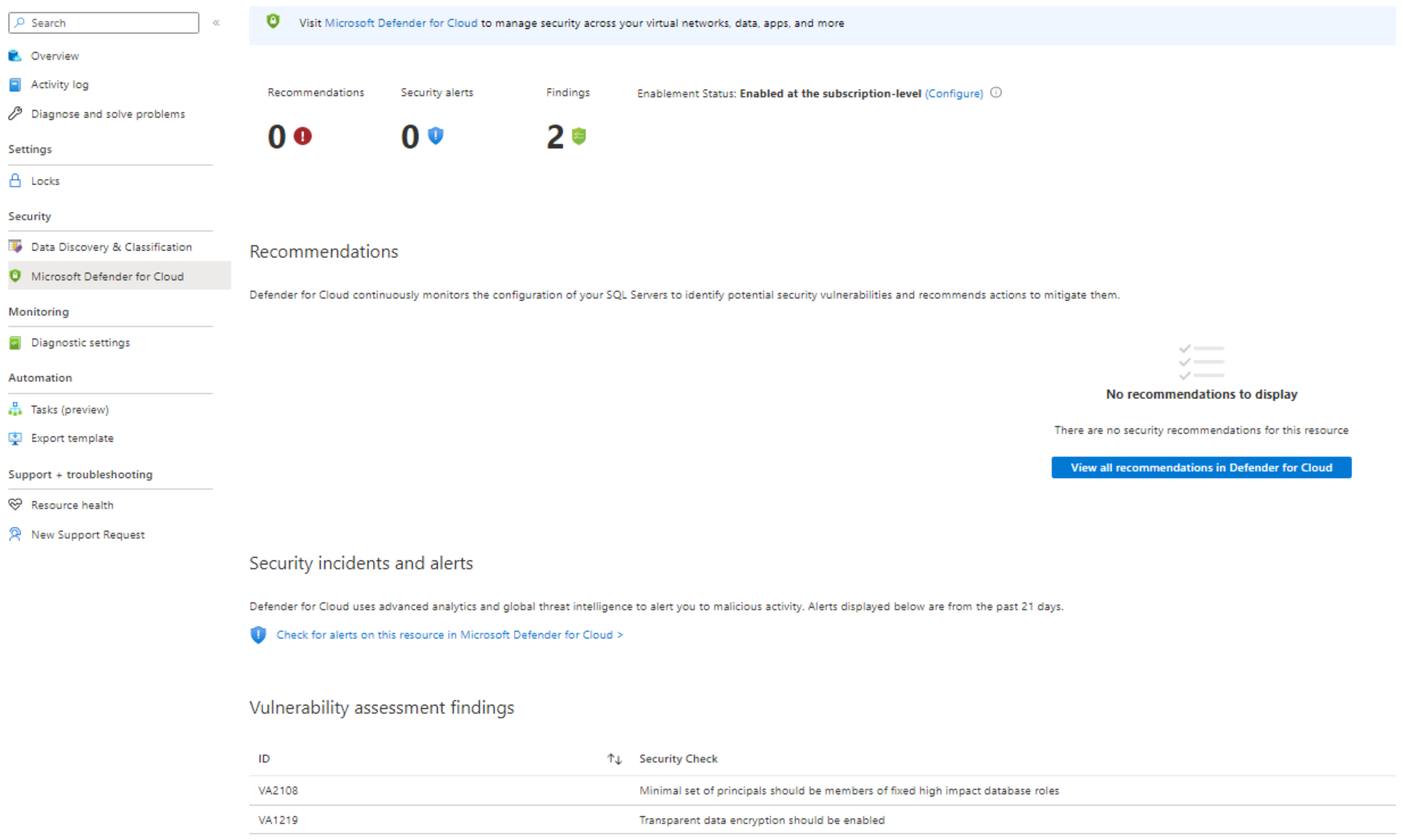
https://docs.microsoft.com/en-us/azure/azure-sql/database/threat-detection-overview

Advanced Threat Protection

Narrative	Screenshot/Code	Notes
1. In the Azure portal navigate to the shared SQL Managed Instance.		
2. Scroll down the Overview screen until you see the list of databases and click on your **TEAMXX_TenantDataDB** database.		

3. In the **TEAMXX_TenantDataDB** database screen, on the left-hand blade click **Microsoft Defender for Cloud** in the Security section

4. Scroll down to the **Security incidents and alters heading** – note no incidents or alerts are listed:



Visit Microsoft Defender for Cloud to manage security across your virtual networks, data, apps, and more

Recommendations	Security alerts	Findings
0	0	2

Enablement Status: **Enabled at the subscription-level** (Configure)

Recommendations

Defender for Cloud continuously monitors the configuration of your SQL Servers to identify potential security vulnerabilities and recommends actions to mitigate them.

No recommendations to display

There are no security recommendations for this resource

View all recommendations in Defender for Cloud

Security incidents and alerts

Defender for Cloud uses advanced analytics and global threat intelligence to alert you to malicious activity. Alerts displayed below are from the past 21 days.

Check for alerts on this resource in Microsoft Defender for Cloud >

Vulnerability assessment findings

ID	Security Check
VA2108	Minimal set of principals should be members of fixed high impact database roles
VA1219	Transparent data encryption should be enabled

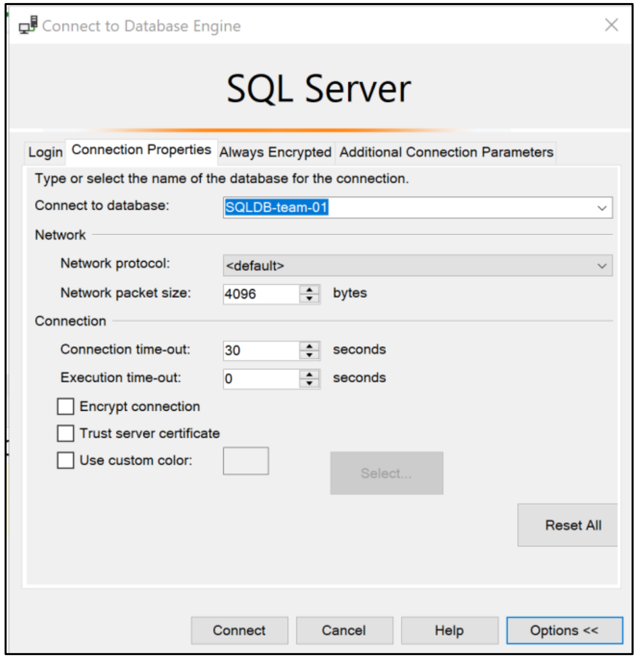
5. On the team VM, open a new query window in SQL Server Management Studio connected to your **TEAMXX_TenantDataDB** database.

6. To simulate a potential SQL injection query copy the following SELECT into the new query window ***BUT DON'T RUN IT YET***:	`--Advanced Threat Protection`
	`SELECT *`
	`FROM sys.databases`
	`WHERE database_id like '' or 1 = 1 -- ' and family = 'test1';`
		Notice that the logic in the WHERE clause will always equate to true and the positioning of single-quotes including in the comment represents a potential SQL injection vulnerability

7. Before running the query change the connection properties as show opposite using the **Query\Connection\Change Connection**… menu in SSMS.

8. Click **Connect**

Specify the name of the team Azure SQL Database: **TEAMXX_TenantDataDB**



Type or select the name of the database for the connection.

Connect to database: SQLDB-team-01

Network

Network protocol: <default>

Network packet size: 4096 bytes

Connection

Connection time-out: 30 seconds

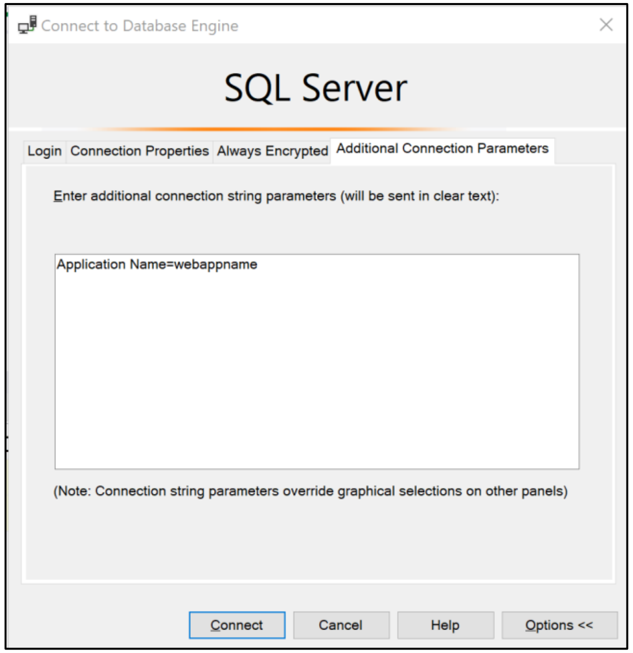
Execution time-out: 0 seconds

□ Encrypt connection

□ Trust server certificate

□ Use custom color:

On “Additional Connection Parameters add a connection string option to specify the application name:
Application Name=webappname

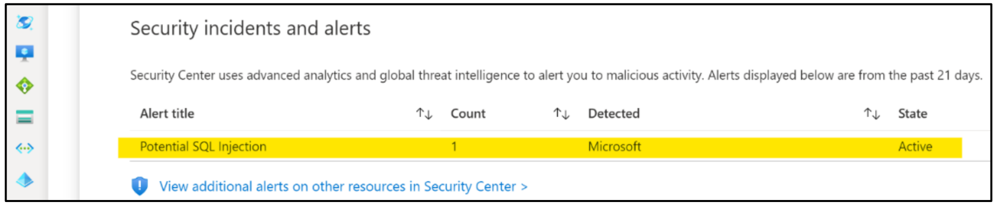


Enter additional connection string parameters (will be sent in clear text):

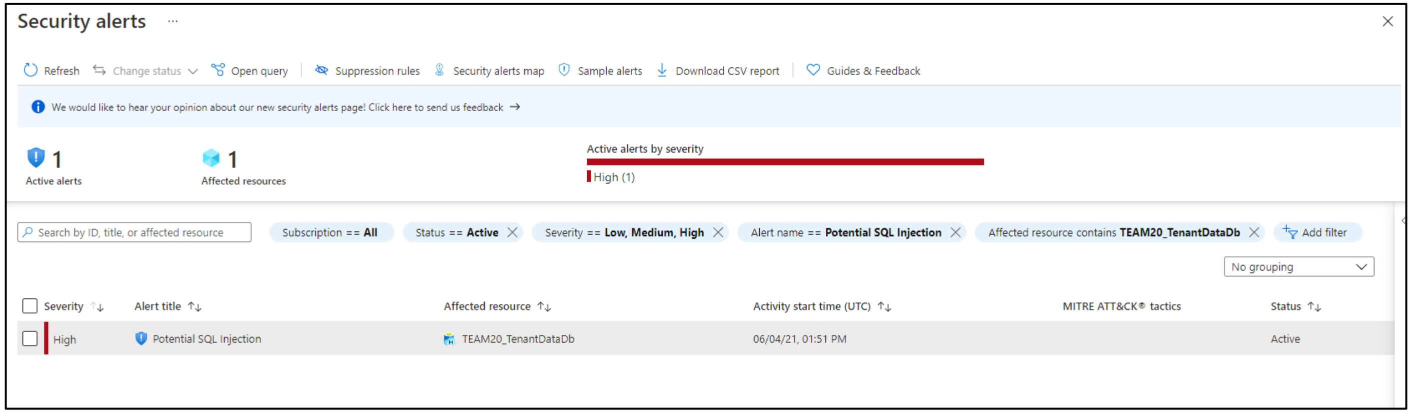
Application Name=webappname

(Note: Connection string parameters override graphical selections on other panels)

<table>
<tr>
<td>9. Run the query.

It will return a list of databases on the server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Back in the Azure Portal <b>Microsoft Defender for Cloud</b> screen, after a few minutes an Alert should be generated:</td>
<td>
Security incidents and alerts

Security Center uses advanced analytics and global threat intelligence to alert you to malicious activity. Alerts displayed below are from the past 21 days.
<table>
<tr><th>Alert title</th><th>Count</th><th>Detected</th><th>State</th></tr>
<tr><td>Potential SQL Injection</td><td>1</td><td>Microsoft</td><td>Active</td></tr>
</table>
View additional alerts on other resources in Security Center &gt;</td>
<td><b>NOTE:</b> It might take up to 10mins for the alert to appear in the portal</td>
</tr>
<tr>
<td>11. Once the Later appears click on it to see the details.

Depending on the progress of other teams you may see multiple entries in the details table.</td>
<td colspan="2">

We would like to hear your opinion about our new security alerts page! Click here to send us feedback →

1 Active alerts
1 Affected resources
Active alerts by severity
High (1)

Search by ID, title, or affected resource
Subscription == <b>All</b>
Status == <b>Active</b>
Severity == <b>Low, Medium, High</b>
Alert name == <b>Potential SQL Injection</b>
Affected resource contains <b>TEAM20_TenantDataDb</b>
Add filter
No grouping
<table>
<tr><th>☐ Severity</th><th>Alert title</th><th>Affected resource</th><th>Activity start time (UTC)</th><th>MITRE ATT&amp;CK® tactics</th><th>Status</th></tr>
<tr><td>☐ High</td><td>Potential SQL Injection</td><td>TEAM20_TenantDataDb</td><td>06/04/21, 01:51 PM</td><td></td><td>Active</td></tr>
</table></td>
</tr>
</table>

12. Try clicking on the Alert. Note that you can drill further into the alert to see more details, get explanations and links to documentation on the alert and even advice on how negate and remediate the problem.		