



Azure SQL Managed Instance Auditing and Azure Defender

Module 4

Learning Units covered in this Module

- Lesson 1: Introduction to xEvents and SQL Audit
- Lesson 2: Implement Auditing for Azure SQL MI
- Lesson 3: Azure SQL MI Vulnerability Assessment
- Lesson 4: Advanced Threat Protection
- Lesson 5: Data Discovery and Classification

Lesson 1: Introduction to xEvents and SQL Audit

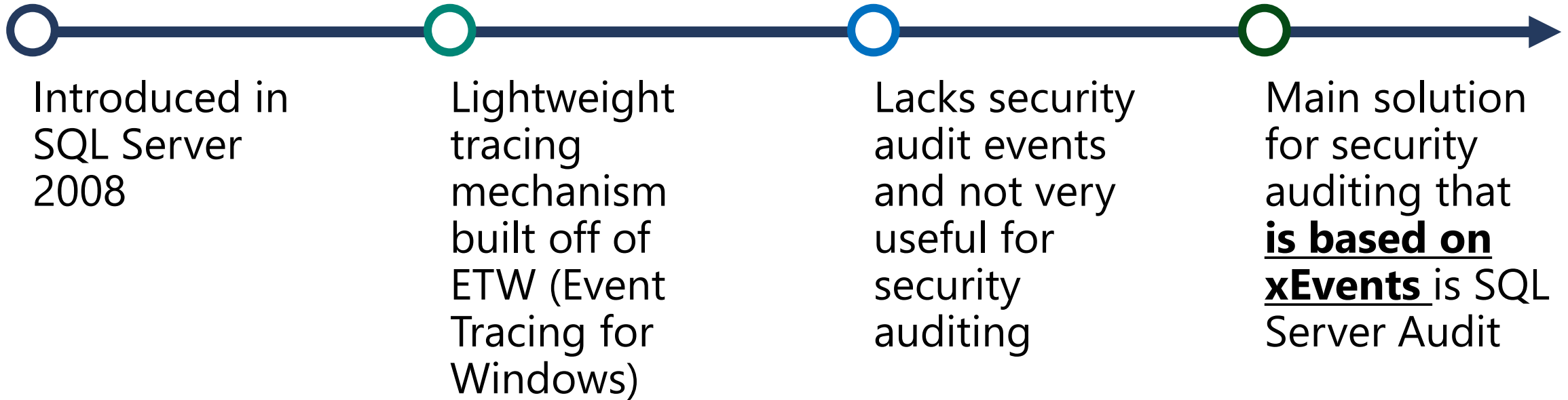
Objectives

After completing this learning, you will be able to:

- Understand xEvents and what they are
- Understand what SQL Server Audit is and how to configure it.



Short introduction to Extended Events (xEvents)



What xEvents are available for security auditing?

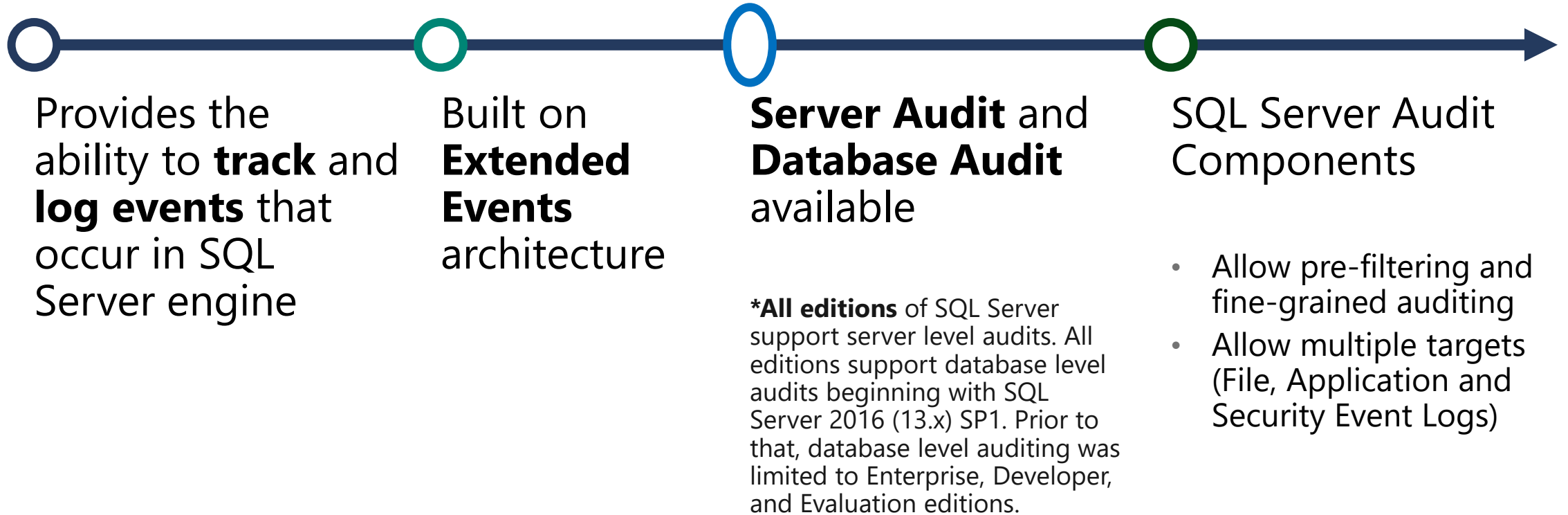
Retrieving all **Security Audit** xEvents

```
select
    txem.xe_event_name
from sys.trace_xe_event_map txem
inner join sys.trace_events te
on txem.trace_event_id = te.trace_event_id
inner join sys.trace_categories tc
on te.category_id = tc.category_id
where tc.name = 'Security Audit';
```

Sample output from SQL Managed Instance

	xe_event_name
1	login
2	logout
3	server_start_stop
4	fulltextlog_written

SQL Server Audit



Key part of security strategy

Who has **accessed** or
attempted to access your
data

Ability to detect
unauthorized access
attempts

Piece together the **actions**
of malicious insiders

Robust **tracking** capability

Primary Goals of SQL Server Audit

Security

- The audit feature must be truly secure.

Performance

- Performance impact must be minimized

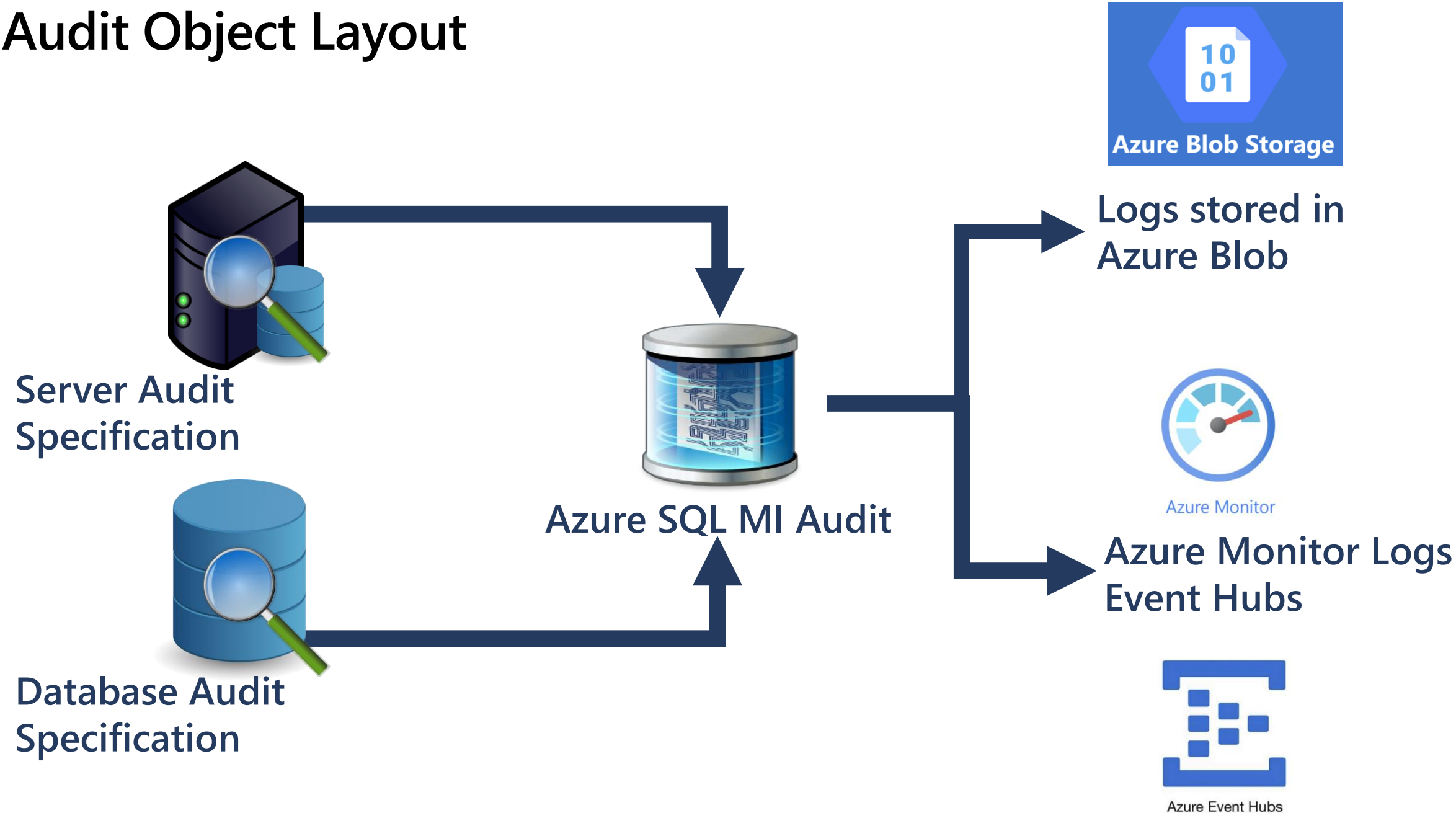
Management

- The audit feature must be easy to manage.

Discoverability

- Audit-centric questions must be easy to answer

Audit Object Layout



Working with SQL Server Audit



Create an audit and define the target



Create either a server audit specification or database audit specification



Enable the audit specification



Enable the audit



Read the audit events

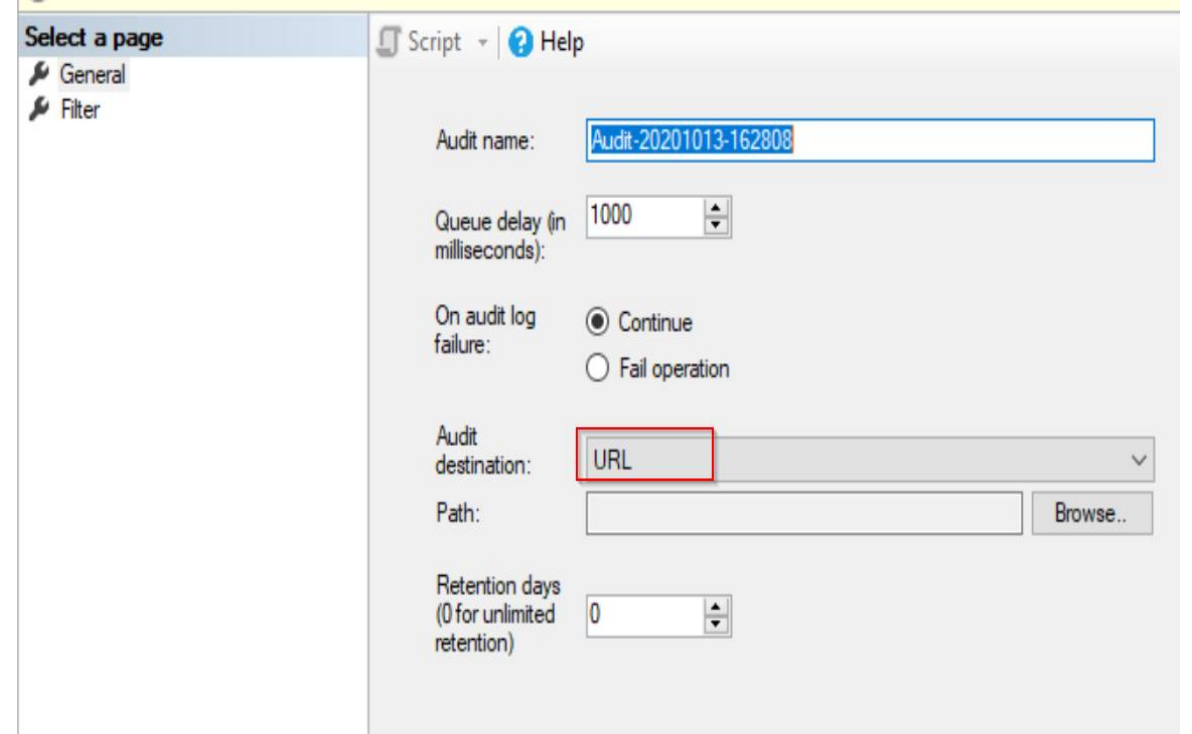
Create Audit

Queue delay (in milliseconds)

On Audit Log Failure - Continue

On Audit Log Failure - Shut down server

On Audit Log Failure - Fail operation



The screenshot shows a configuration window titled 'Create Audit'. On the left, a sidebar labeled 'Select a page' contains two options: 'General' (selected) and 'Filter'. The main area on the right is titled 'Script | ? Help' and contains the following settings:

- Audit name:** A text field containing 'Audit-20201013-162808'.
- Queue delay (in milliseconds):** A numeric spinner field set to '1000'.
- On audit log failure:** Two radio button options: 'Continue' (selected) and 'Fail operation'.
- Audit destination:** A dropdown menu with 'URL' selected and highlighted by a red rectangle.
- Path:** An empty text field with a 'Browse...' button to its right.
- Retention days (0 for unlimited retention):** A numeric spinner field set to '0'.

Create Audit (Continued)

Audit Destination

- URL
 - Azure Blob Storage

URL Settings

- Retention days (0 for unlimited retention)

Audit name:

Queue delay (in milliseconds):

On audit log failure: ☒ Continue ☐ Fail operation

Audit destination:

Path:

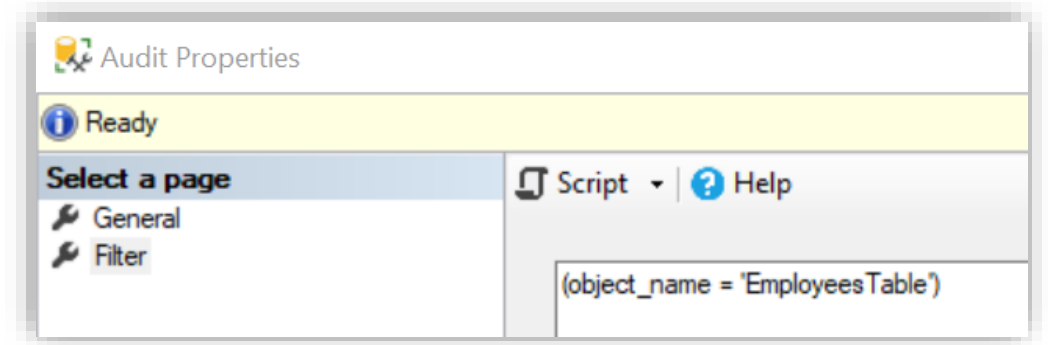
Retention days (0 for unlimited retention)

Create Audit Filter

Enter a predicate, or "WHERE clause"

Audit events are filtered before they are written to the audit log

You can filter on every element of the Audit Records



Server-Level Audit Action Groups

LOGIN_CHANGE_PASSWORD_GROUP

- Whenever a login password is changed

SERVER_OBJECT_CHANGE_GROUP

- CREATE, ALTER, or DROP operations on server objects

SERVER_PRINCIPAL_CHANGE_GROUP

- When server principals are created, altered, or dropped

SERVER_ROLE_MEMBER_CHANGE_GROUP

- Whenever a login is added or removed from a fixed server role.

SUCCESSFUL_LOGIN_GROUP

- A principal has successfully logged in to SQL Server

Database-Level Audit Action Groups

BACKUP_RESTORE_GROUP

- Whenever a backup or restore command is issued

DATABASE_CHANGE_GROUP

- When a database is created, altered, or dropped

DATABASE_OBJECT_CHANGE_GROUP

- When a CREATE, ALTER, or DROP statement is executed on database objects

DATABASE_ROLE_MEMBER_CHANGE_GROUP

- Whenever a login is added to or removed from a database role

DBCC_GROUP

- Whenever a principal issues any DBCC command

FAILED_DATABASE_AUTHENTICATION_GROUP

- A principal tried to log on to SQL Server and failed

Database-Level Audit Actions

SELECT

UPDATE

INSERT

DELETE

EXECUTE

RECEIVE

REFERENCES

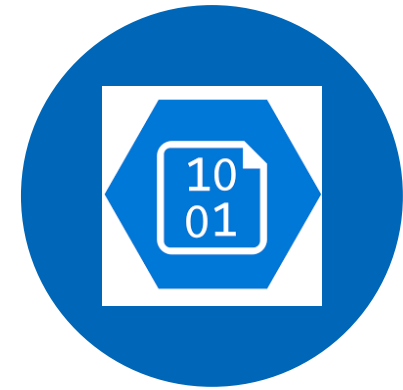
View a SQL Server Audit Log



SQL SERVER
MANAGEMENT STUDIO



SYS.FN_GET_AUDIT_FILE



AZURE DATA STUDIO

sys.fn_get_audit_file

- **file_pattern**

- This argument is used to specify a blob URL (including the storage endpoint and container). While it does not support an asterisk wildcard, you can use a partial file (blob) name prefix (instead of the full blob name) to collect multiple files (blobs) that begin with this prefix. For example:
- **<Storage_endpoint>/<Container>/<ServerName>/<DatabaseName>/** - collects all audit files (blobs) for the specific database.
- **<Storage_endpoint>/<Container>/<ServerName>/<DatabaseName>/<AuditName>/<CreationDate>/<FileName>.&b>xel** - collects a specific audit file (blob).

- **initial_file_name**

- Specifies the path and name of a specific file in the audit file set to start reading audit records from

- **audit_record_offset**

- Specifies a known location with the file specified for the initial_file_name

```
SELECT * FROM sys.fn_get_audit_file (  
'https://mystorage.blob.core.windows.net/sqldbauditlogs/Sh ',default,default);
```

SQL Server Audit Records

Who

Did

What

And

When

On

Which

Object

Considerations



In the case of a failure during audit initiation, the server will not start.



Attaching a Database with an Audit Defined



Always On Availability Groups and SQL Server Audit



Auditing Administrators

Demonstration

Exploring SQL Audit Actions and Action Groups



Questions?

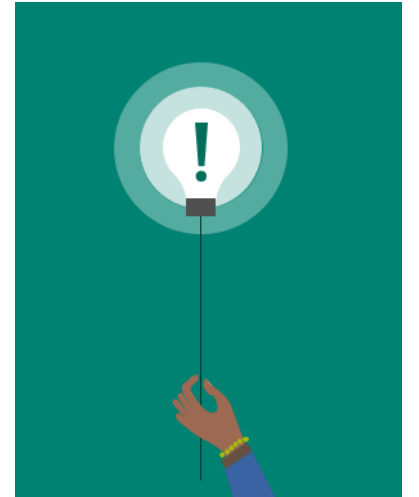


Lesson 2: Implement Auditing for Azure SQL MI

Objectives

After completing this learning, you will be able to:

- Know how you can configure Auditing on Azure SQL MI.



SQL Auditing

SQL Auditing tracks database events and writes them to an audit log in your Azure storage account, Log Analytics workspace or Event Hubs.

Helps you maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.

Enables and facilitates adherence to compliance standards, although it doesn't guarantee compliance.

SQL Auditing (continued)

Gain insight into database events and streamline compliance-related tasks.

Configurable to track and log database activity.

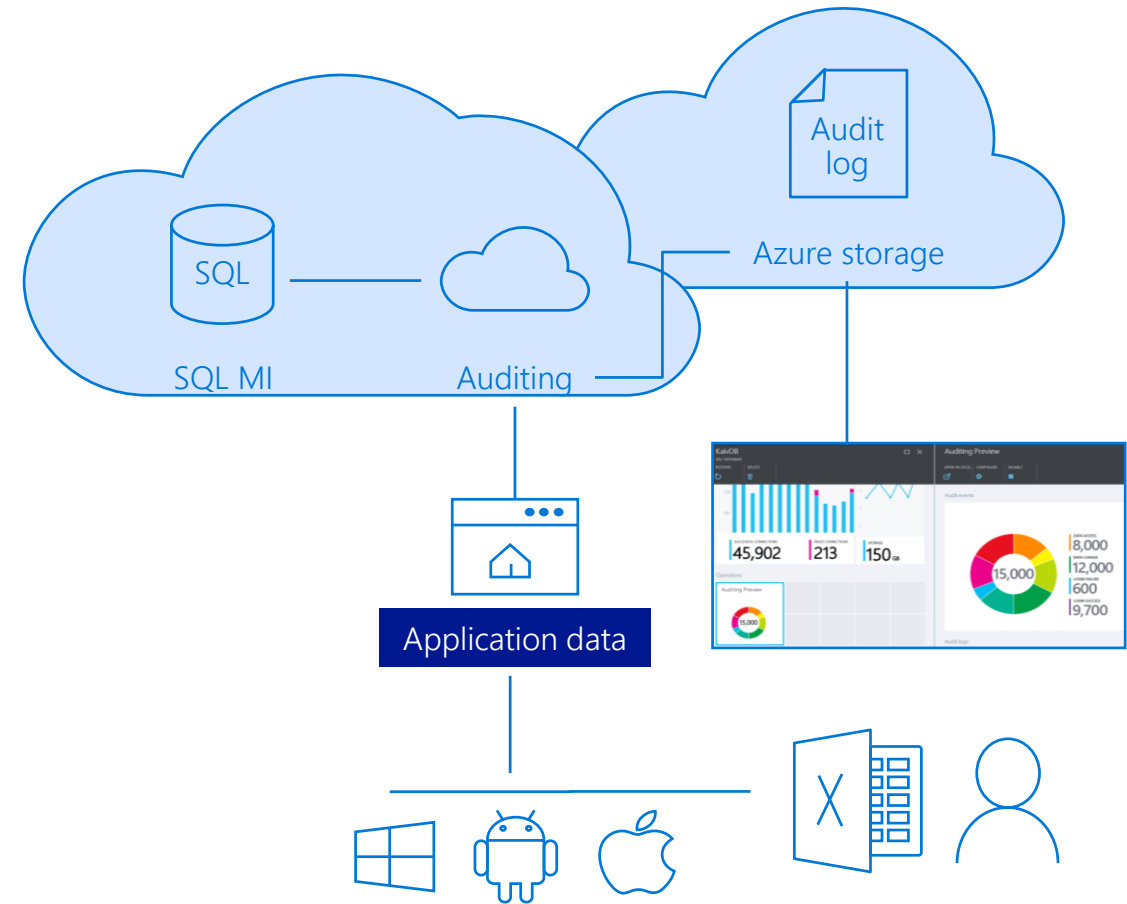
Dashboard views in portal for at-a-glance insights.

Audit logs reside Azure Storage Account, Log Analytics or Event Hub.

Available in Basic, Standard, Premium and Managed Instance.

The default auditing policy includes:

- BATCH_COMPLETED_GROUP
- SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP
- FAILED_DATABASE_AUTHENTICATION_GROUP



Analyze audit logs and reports

Azure Monitor logs

- Azure portal

Event Hub

- Avro Tools or similar tools

Azure storage account

- Azure Storage Explorer
- Azure portal
- Power BI
- SQL Server Management Studio (SSMS)
- PowerShell

Demonstration

Demonstrate how to create an Audit and Audit Specification within Azure SQL Managed Instance



Questions?

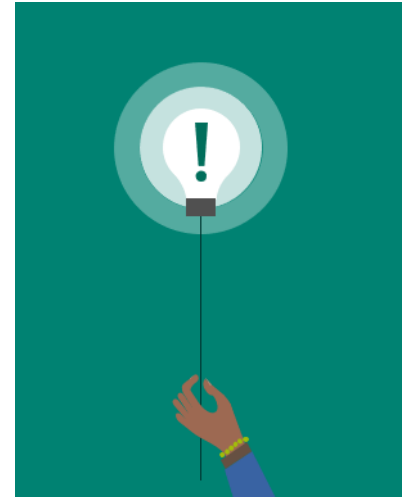


Lesson 3: Azure SQL MI Vulnerability Assessment

Objectives

After completing this learning, you will be able to:

- Understand what is Azure Defender for SQL
- Understand the SQL Server Vulnerability Assessment
 - Azure SQL Managed Instance (PaaS)
 - Available in SQL Server Management Studio (IaaS)



Azure Defender for SQL

- Unified package for advanced SQL security capabilities
- Azure Defender is available for Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics
- Includes functionality:
 - surfacing and mitigating potential database vulnerabilities
 - detecting anomalous activities that could indicate a threat to your database
 - discovering and classifying sensitive data
- Single go-to location for enabling and managing these capabilities

Azure Defender for SQL (continued)

Set of Advanced SQL Security Capabilities

- Includes SQL Vulnerability Assessment and Advanced Threat Protection.
- [Vulnerability Assessment](#) is an easy-to-configure service that can
 - **discover, track**, and help you **remediate** potential database vulnerabilities.
 - provides **visibility** into your **security state**
 - **actionable steps** to resolve security issues and enhance your database fortifications.
- [Advanced Threat Protection](#) detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit your database.
 - **continuously monitors** your database for suspicious activities
 - **immediate security alerts** on potential vulnerabilities, Azure SQL injection attacks, and anomalous database access patterns.
 - **details of the suspicious activity** and **recommend action** on how to investigate and mitigate the threat.

SQL Vulnerability Assessment

SQL Vulnerability Assessment is an easy to configure service that can **discover, track, and help you remediate potential database vulnerabilities**. Use it to **proactively** improve your database security.

SQL Vulnerability Assessment (continued)

Get visibility

Discover sensitive data and potential security holes.

Remediate

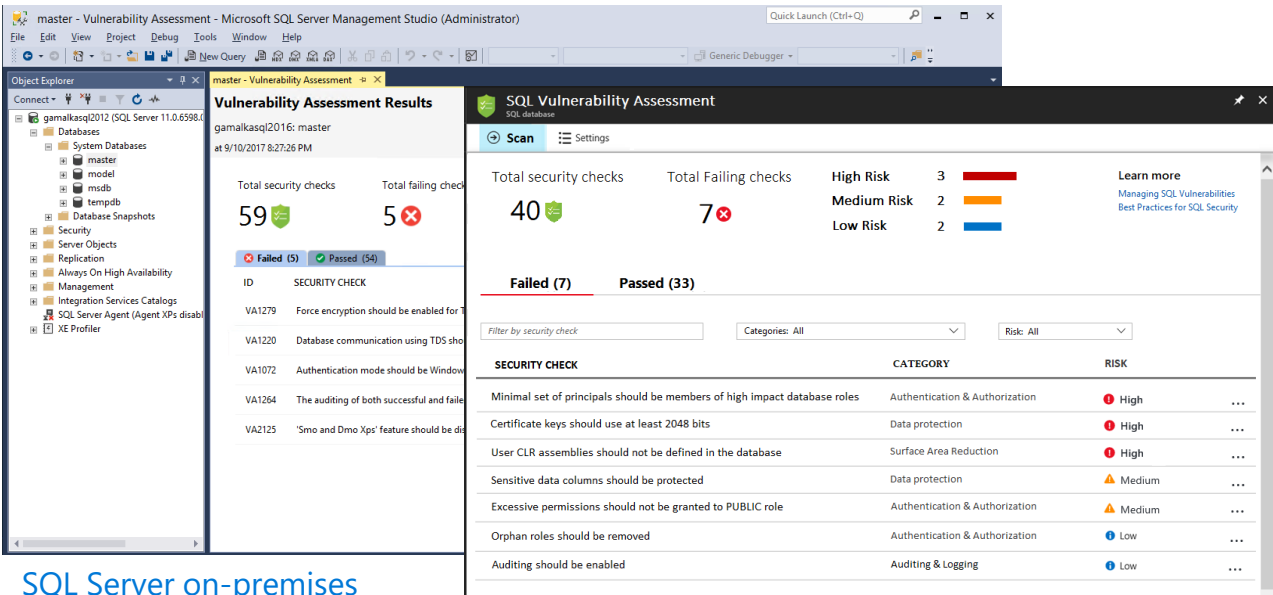
Actionable remediation and security hardening steps

Customize

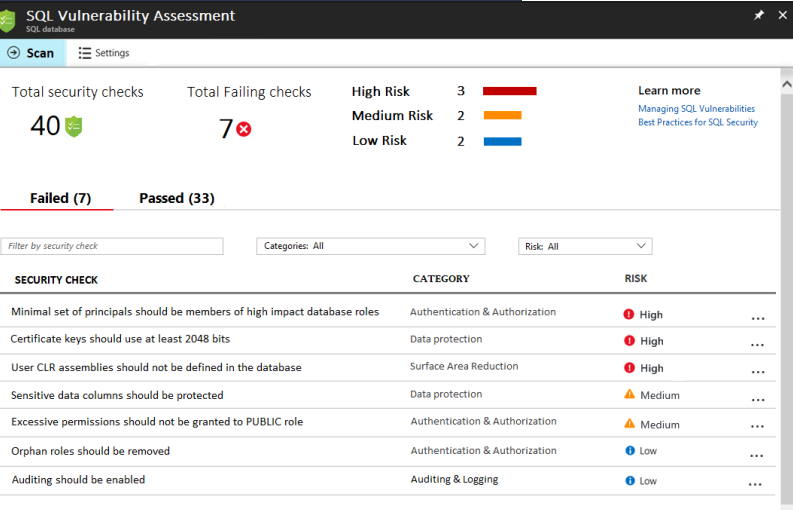
Baseline policy tuned to your environment, allowing you to focus on deviations.

Report

Pass internal or external audits to facilitate compliance.



SQL Server on-premises



Azure SQL MI Database



Vulnerability Assessment

Identifies, tracks, and resolves SQL security vulnerabilities



Developer/DBA

Vulnerability Assessment

Paid Service

- Vulnerability Assessment is part of Azure Defender
- Enable (ON/OFF)
- Vulnerability Assessment Settings
 - Subscription
 - Storage Account
- Period Recurring Scans (ON/OFF)
- Send Scan Reports
- Trial (30 Days Available)

The screenshot displays the Azure Security Center interface for a SQL managed instance. The left sidebar contains a navigation menu with options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Quick start, Settings, Compute + storage, Connection strings, Active Directory admin, Deleted databases, Properties, Locks, Data management, Failover groups, Security, Networking, Security center, Transparent data encryption, and SQL trust groups. The main content area is titled 'sqlmi-... | Security center' and includes a search bar and action buttons (Save, Discard, Feedback). A red box highlights the 'AZURE DEFENDER FOR SQL' toggle, which is currently set to 'ON'. Below this, an information box states: 'Azure Defender for SQL costs 19.2 CAD/managed instance/month. It includes Vulnerability Assessment and Advanced Threat Protection. We invite you to a trial period for the first 30 days, without charge.' The 'VULNERABILITY ASSESSMENT SETTINGS' section shows the 'Subscription' and 'Storage account' fields, both highlighted with red boxes. The 'Periodic recurring scans' section has a toggle set to 'OFF'. The 'Send scan reports to' section has a checkbox for 'Also send email notification to admins and subscription owners' which is checked. The 'ADVANCED THREAT PROTECTION SETTINGS' section shows the 'Send alerts to' field with 'Email addresses' selected and a checkbox for 'Also send email notification to admins and subscription owners' which is checked. The 'Advanced Threat Protection types' section is set to 'All'.

sqlmi-... | Security center

Search (Ctrl+/) Save Discard Feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Quick start

Settings

Compute + storage

Connection strings

Active Directory admin

Deleted databases

Properties

Locks

Data management

Failover groups

Security

Networking

Security center

Transparent data encryption

SQL trust groups

AZURE DEFENDER FOR SQL

ON OFF

Azure Defender for SQL costs 19.2 CAD/managed instance/month. It includes Vulnerability Assessment and Advanced Threat Protection. We invite you to a trial period for the first 30 days, without charge.

VULNERABILITY ASSESSMENT SETTINGS

Subscription

Storage account

Periodic recurring scans

ON OFF

Send scan reports to

Also send email notification to admins and subscription owners

ADVANCED THREAT PROTECTION SETTINGS

Send alerts to

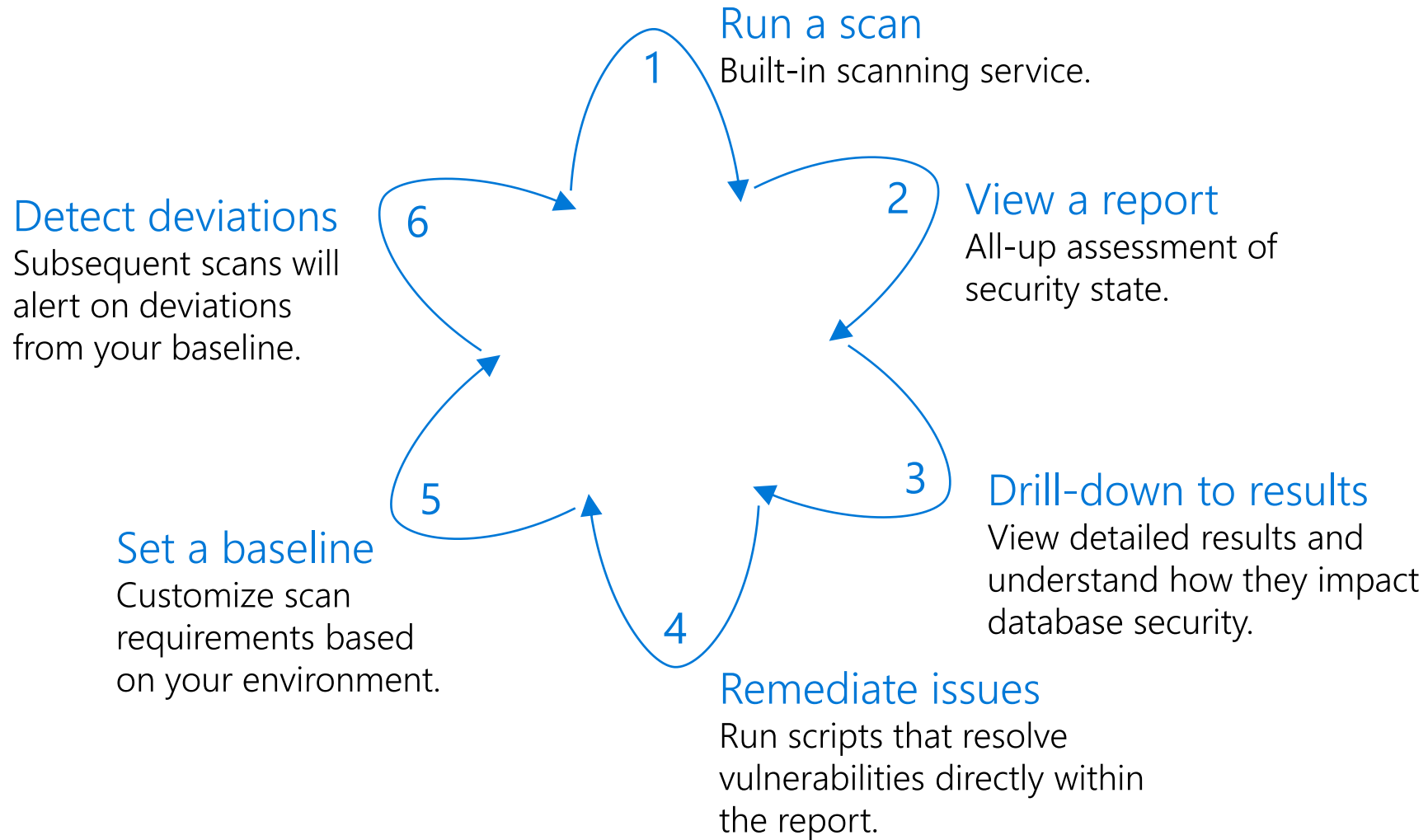
Email addresses

Also send email notification to admins and subscription owners

Advanced Threat Protection types

All

Using Vulnerability Assessment



Vulnerability Assessment in SSMS

To Be Updated:

<https://docs.microsoft.com/en-us/sql/relational-databases/security/sql-vulnerability-assessment?view=sql-server-ver15#tutorial>

Run a customized tracking report

Subsequent scans will alert on deviations from your baseline.

Set a baseline

Customize scan requirements and set a Rules Baseline.

Run a scan

Built-in scanning service.

View a report

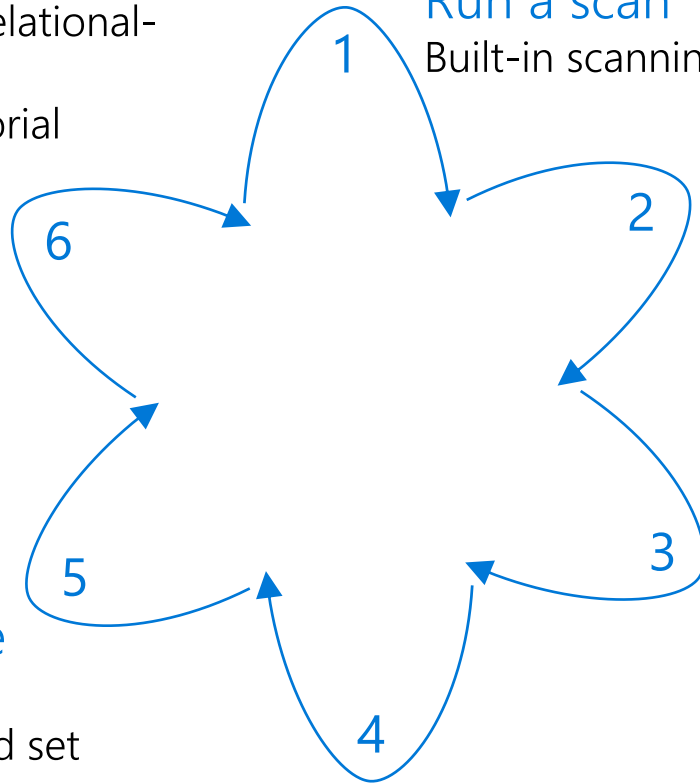
All-up assessment of security state

Analyze the results

View detailed results and understand how they impact database security.

Resolve issues


Run scripts that resolve vulnerabilities directly within the report.



View the Report

Vulnerability Assessment Results

Server: sqlmi-~~idb~~ga.24e3006c6684.database.windows.net Database: testmi Scan time: 2020-10-13T17:00:48.4357052-04:00

 Export to Excel

Total failing checks

2 

Total passing checks

31 

High Risk 0


Medium Risk 1 



Low Risk 1 

Learn more

[SQL Security Center](#)
[Best Practices for SQL Security](#)

 Failed (2)

 Passed (31)

ID	Security Check	Category	Risk	Additional Information
VA1143	'dbo' user should not be used for normal service operation	Surface Area Reduction	 Medium	
VA1069	Permissions to select from system tables and views should be revoked from non-sysadmins	Authentication and Authorization	 Low	No baseline set

Analyze Results and Resolve Issues

✓ Approve as Baseline ✗ Clear Baseline >

Name	VA1020 - Server principal GUEST should not be a member of any role				
Risk	High				
Status	✗ Fail				
Description	The guest user permits access to a database for any logins that are not mapped to a specific database user. This rule checks that no database roles are assigned to the Guest user.				
Impact	Database Roles are the basic building block at the heart of separation of duties and the principle of least permission. Granting the Guest user membership to specific roles defeats this purpose.				
Rule Query	<pre>SELECT name as [Role] FROM sys.database_role_members AS drms JOIN sys.database_principals AS dps</pre> <div>Open in Query Editor Window</div>				
Microsoft Recommendation	Empty set				
Actual Result	<table><thead><tr><th>In Baseline</th><th>Role</th></tr></thead><tbody><tr><td>✗</td><td>app_role</td></tr></tbody></table>	In Baseline	Role	✗	app_role
In Baseline	Role				
✗	app_role				
Remediation	Remove the special principal GUEST from all roles.				
Remediation Script	<pre>ALTER ROLE [app_role] DROP MEMBER GUEST</pre> <div>Open in Query Editor Window</div>				

Set Baseline

WideWorldImporter...ability Assessment

Vulnerability Assessment Results

sql2016: WideWorldImporters

at 11/22/2017 1:39:00 PM

Total security checks

54

Total failing checks

6

High Risk

2

Medium Risk

3

Low Risk

1

Learn more

[SQL Security Center](#)

[Best Practices for SQL Security](#)

Failed (6)

Passed (48)

ID	Security Check	Category	Risk	Additional Information
VA1281	All memberships for user-defined roles should be intended	Auditing and Logging	Medium	No baseline set
VA1285	Sensitive data columns should be identified	Data Protection	Medium	No baseline set

Approve as Baseline

Clear Baseline

Name

VA1281 - All memberships for user-defined roles should be intended

Risk

Medium

Status

Fail (no baseline set)

Demonstration

Vulnerability Assessment

- Run a scan, review the report and set a baseline.



Questions?



Lesson 4: Advanced Threat Protection

Objectives

After completing this learning, you will be able to:

- Know how to proactively identify security threats like SQL Injection or anomalous SQL login by enabling threat detection
- Know how to discover, classify, label & protect the sensitive data in your databases
- Know how to discover, track, and help you remediate potential database vulnerabilities



Advanced Threat Protection



Advanced Threat Protection monitors the connections and queries which are being executed against your Azure SQL DB Database and Managed Instance



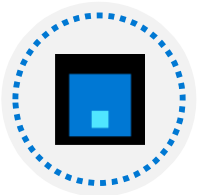
Advanced Threat Protections watches for:

Suspicious database activities

Potential database vulnerabilities

SQL Injection Attacks

Anomalous database access and query patterns

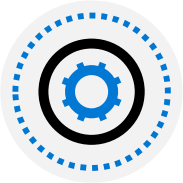


You should enable auditing in conjunction with Azure SQL MI

How to check for vulnerabilities in azure sql database



Issues that Advanced Threat Protection identifies can be found in the "Advanced data security"



Click on the Vulnerability Assessment in order to see the current vulnerability assessment for the database



If there is no current assessment, click "Scan" on the Vulnerability Assessment page to scan the server

What is SQL Injection?

- SQL Injection is an attack in which malicious code is inserted into strings that are later passed to a database engine
- An example is shown here

C#:

```
var Shipcity;  
ShipCity = Request.form ("ShipCity");  
var sql = "select * from OrdersTable where ShipCity =  
'" + ShipCity + "'";
```

User Input:

```
Redmond'; drop table OrdersTable--
```

Executed SQL:

```
SELECT * FROM OrdersTable WHERE ShipCity =  
'Redmond';drop table OrdersTable--'
```

Advanced Data Security (ADS)

Advanced Data Security (ADS) offering part of Azure Defender, which is a unified package for advanced SQL security capabilities, including:

- Advanced Threat Protection
- Vulnerability

All these capabilities can be accessed and managed via the central SQL ADS portal.

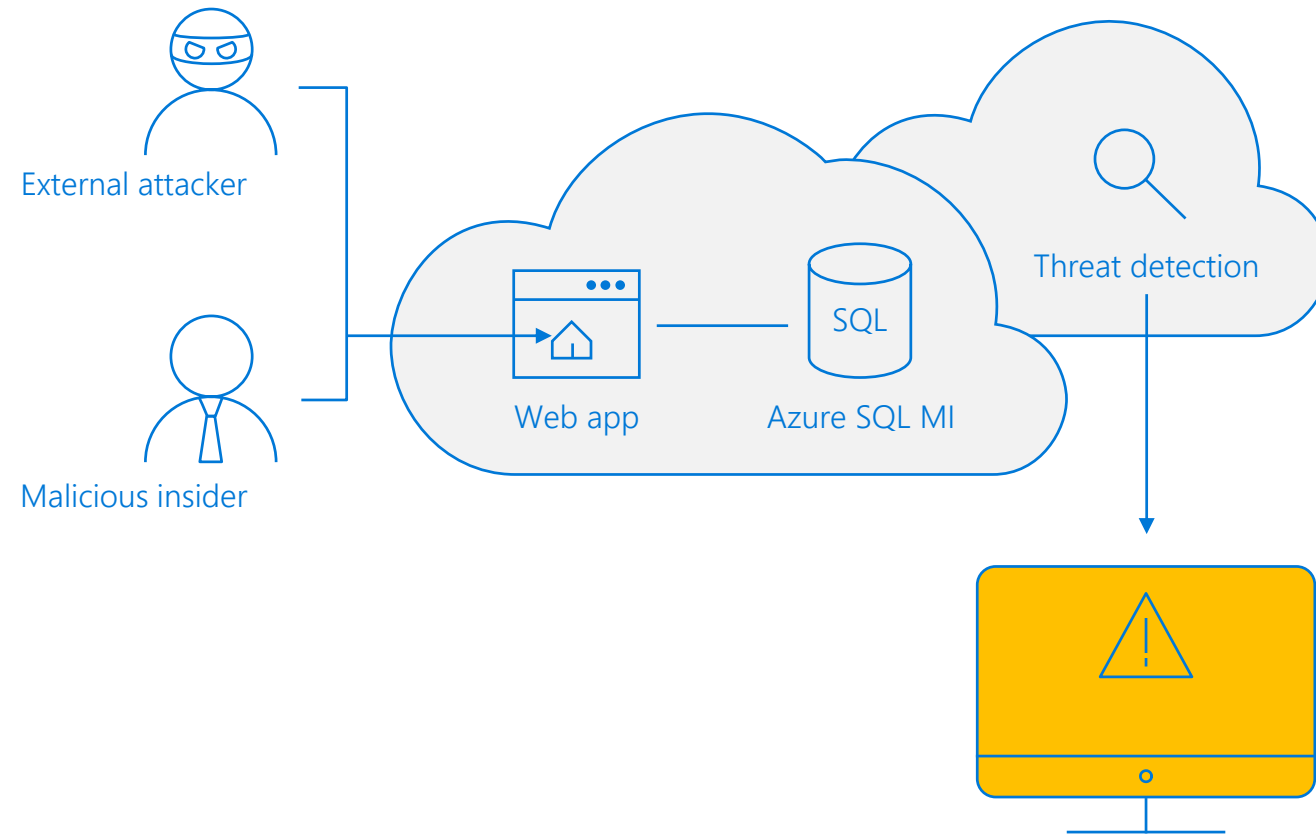
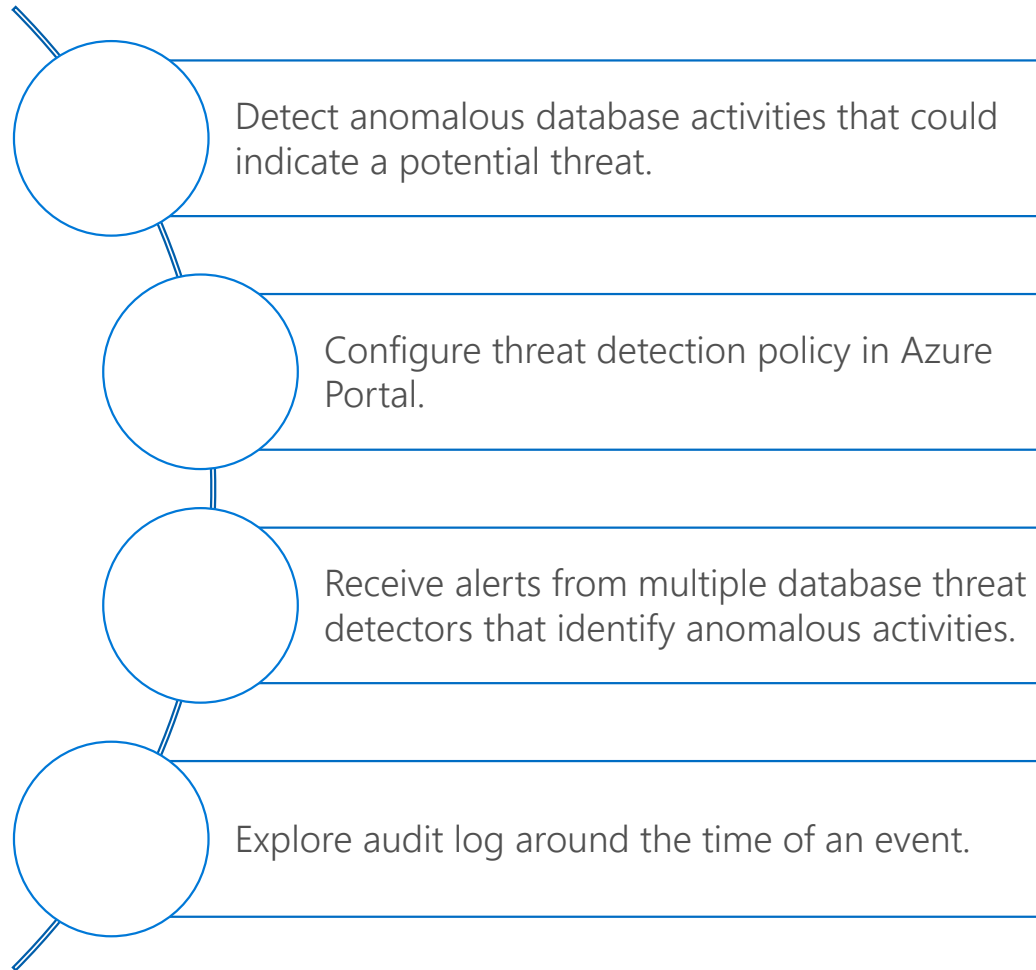
Advanced Threat Detection

Advanced Threat Protection for single and pooled databases detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases.

Advanced Threat Protection can identify:

- Potential SQL injection, Access from unusual location or data center.
- Access from unfamiliar principal or potentially harmful application.
- Brute force SQL credentials.

Advanced Threat Detection (continued)



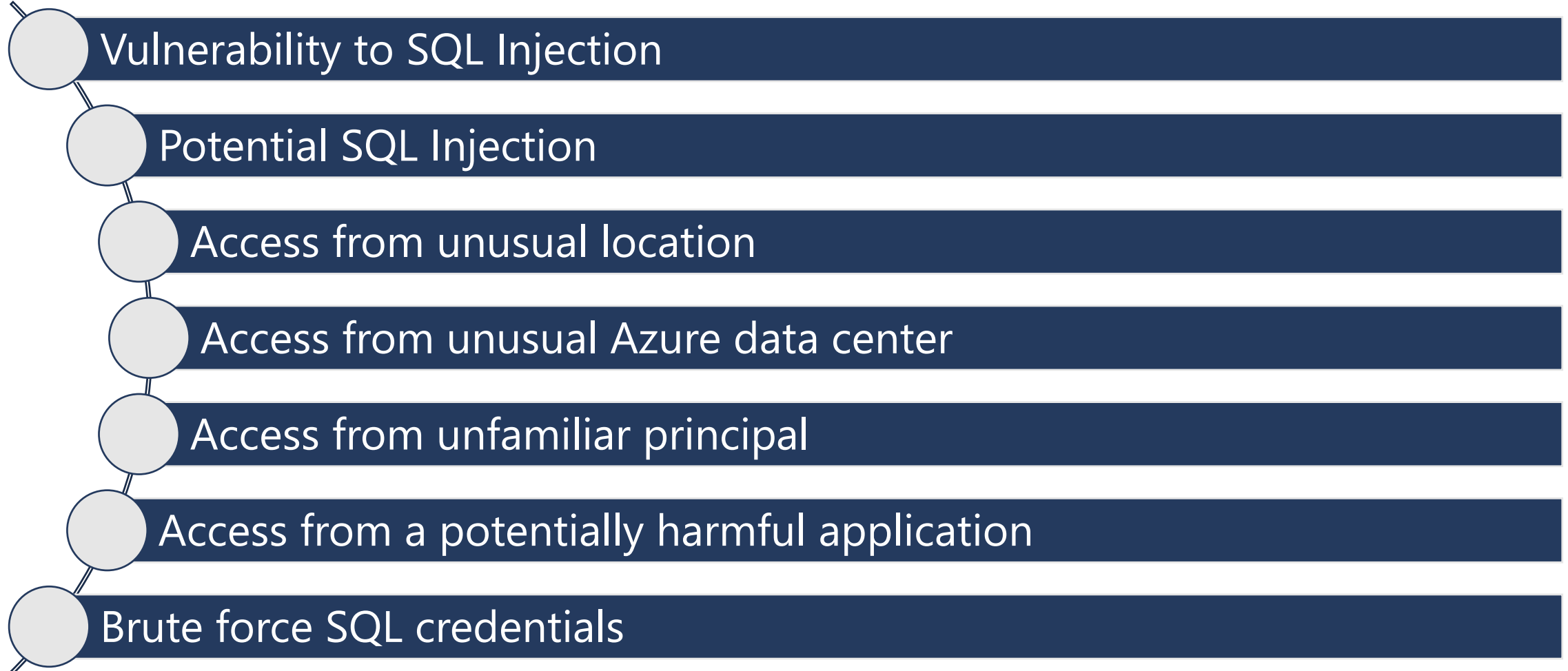
Set up

Alert

Explore

[illegible]

Azure SQL MI Threat Detection Alerts



Demonstration

Advanced Threat Protection for Azure SQL MI

- Enable Threat Detection for Azure SQL MI.



Questions?



Lesson 6: Data Discovery and Classification

Objectives

After completing this learning, you will be able to:

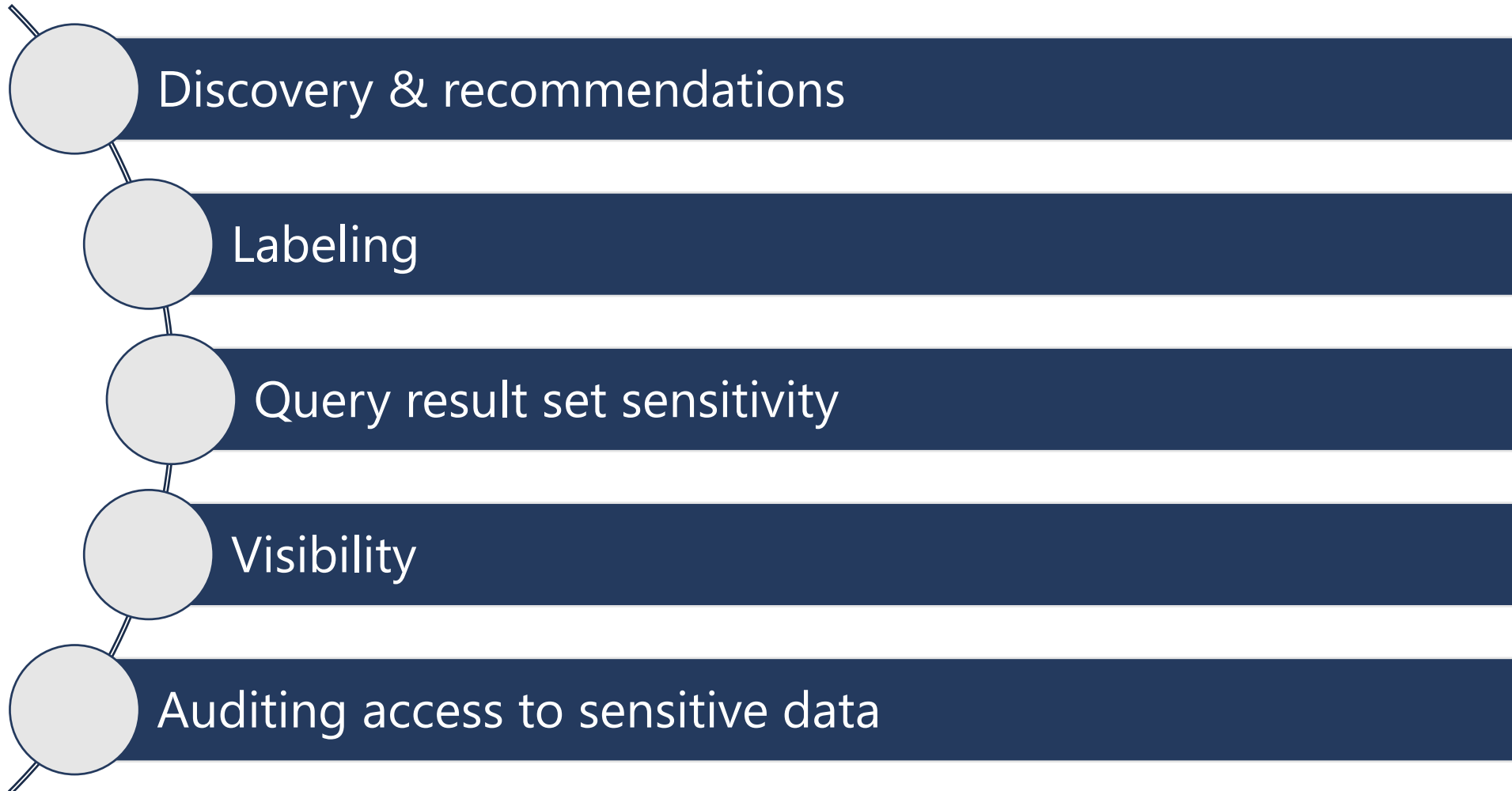
- Know how to enable data discovery and classification



Data Discovery and Classification

Data discovery & classification provides advanced capabilities built into Azure SQL MI for **discovering, classifying, labeling & protecting** the sensitive data in your databases.

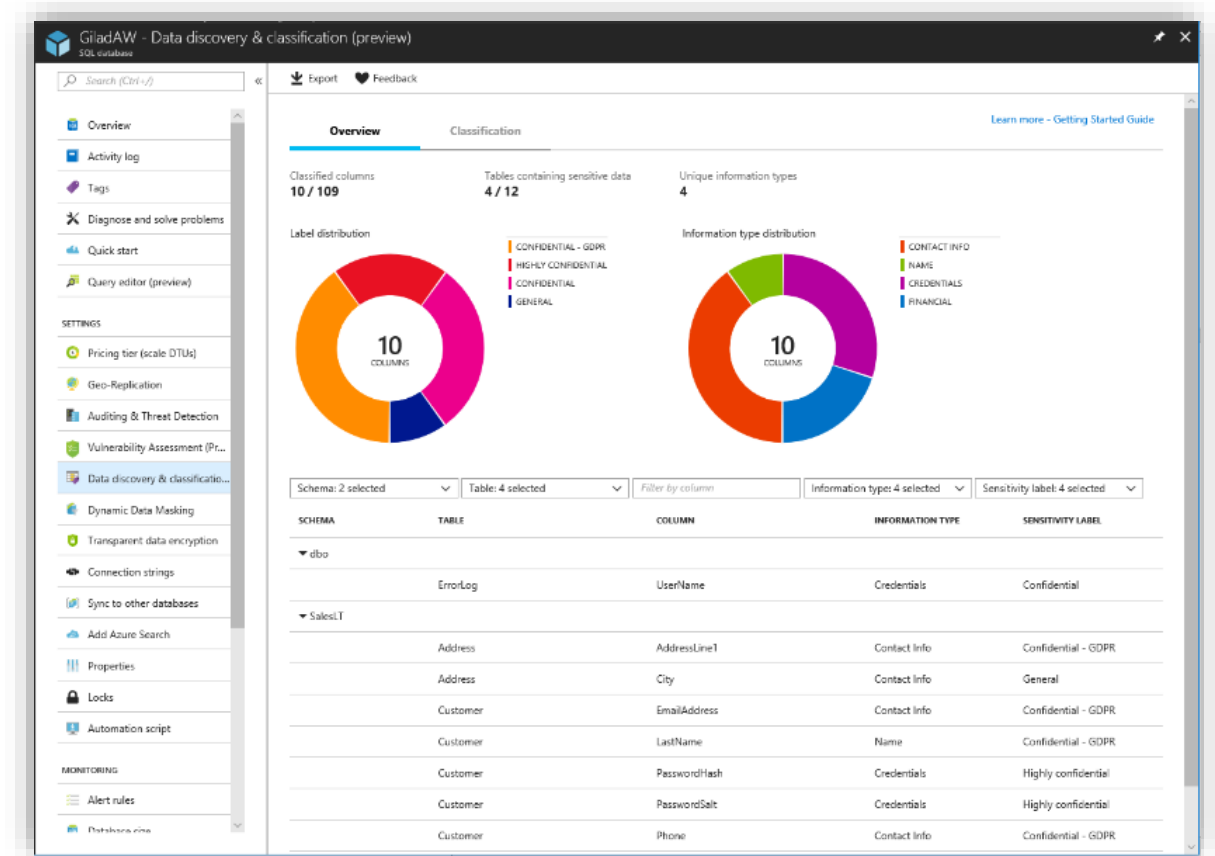
Data Discovery and Classification (continued)



SQL Data Classification

Discover, classify and track access to sensitive data

- Automatic **discovery** of columns with sensitive data
- **Classify** columns with labels
 - Part of Metadata and TDS protocol stream
- **Audit** and **detect** access to the sensitive data
- **Manage labels** for your entire Azure tenant using Azure Security Center

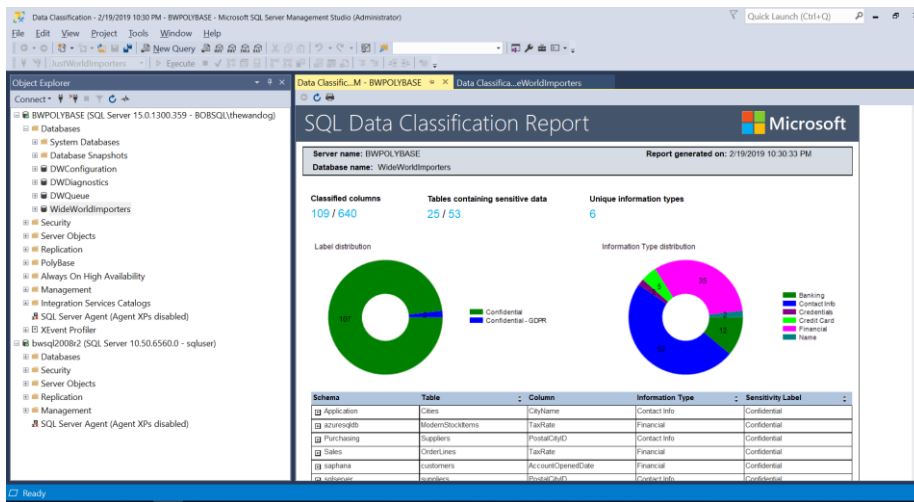


Data Classification and Auditing

The problem

I need to classify my data in SQL Server and audit access to the classified data

SQL Server 2017



SQL Server 2019 and Azure SQL Database

Planned →

ADD SENSITIVITY CLASSIFICATION TO
dbo.sales.price, dbo.sales.discount
WITH (LABEL='Highly Confidential',
INFORMATION_TYPE='Financial')

SQL Server Auditing

data_sensitivity_information

Who, what, and when accessed my
classified data?

Data Classification Permissions

- These built-in roles can **read** the **data classification** of a database:
 - Owner
 - Reader
 - Contributor
 - SQL Security Manager
 - User Access Administrator
- These built-in roles can **modify** the **data classification** of a database:
 - Owner
 - Contributor
 - SQL Security Manager

Demonstration

Data Discovery and Classification

- Classify your SQL Database.



Questions?



Module Summary

SQL MI Audit and Logging

SQL Vulnerability Assessment

Advanced Threat Protection

Data Discovery and Classification

