# Troubleshoot for Azure SQL Threat Detection Alerts

Last updated by | Charlene Wang | Oct 14, 2020 at 8:37 PM PDT

Contents

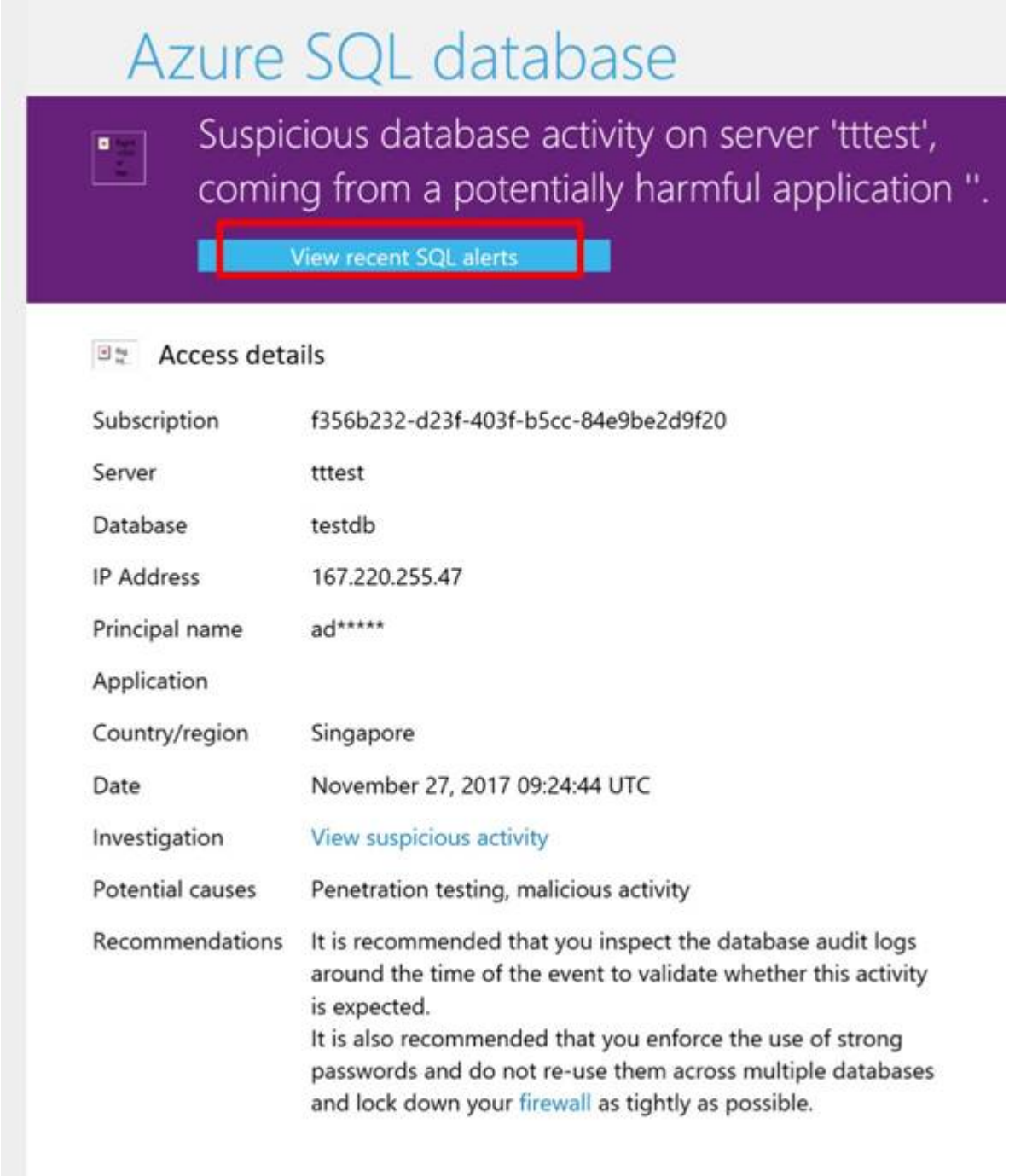


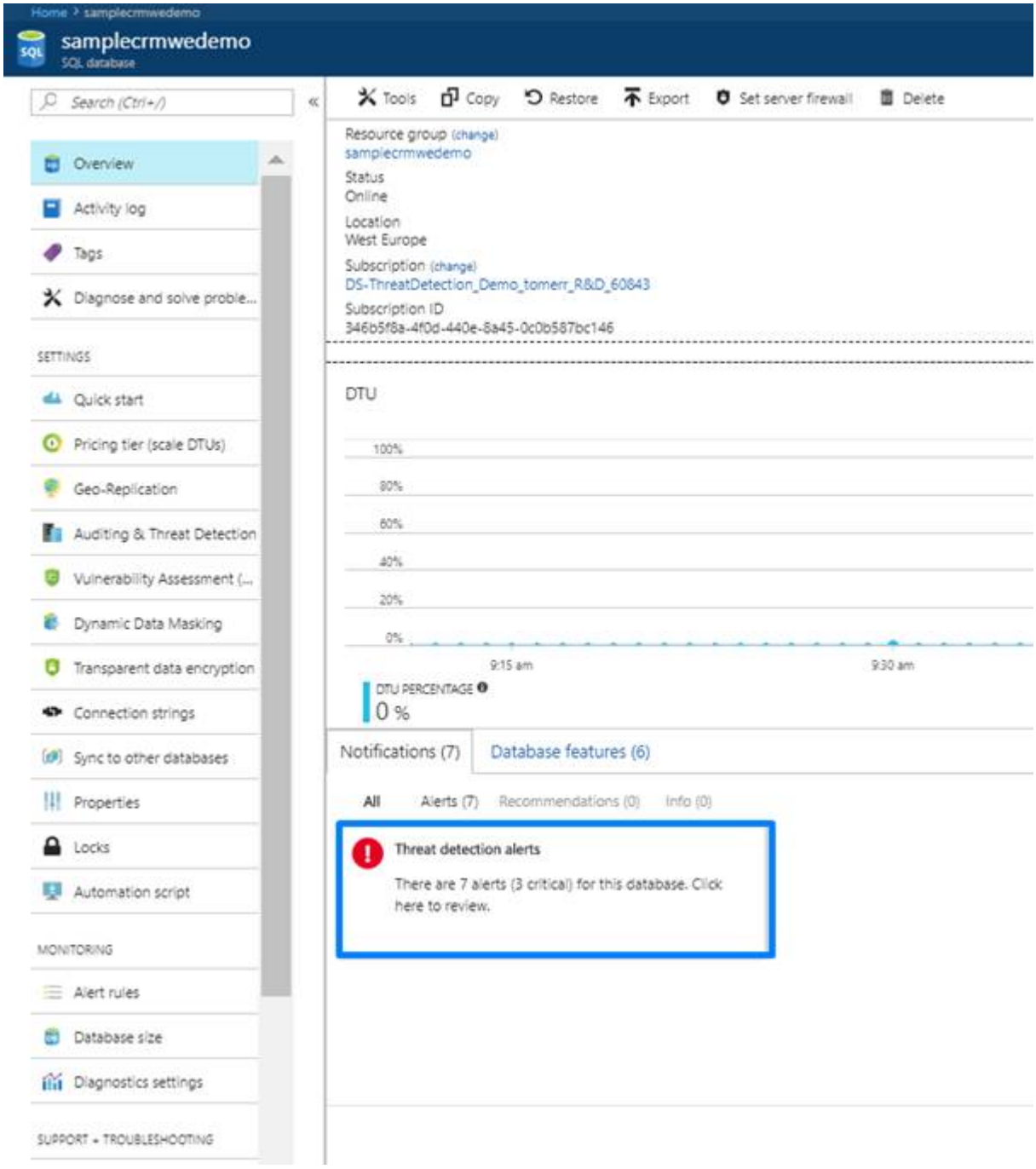
Guide the client to follow below steps to view alert details

If need further help, then open ICM to

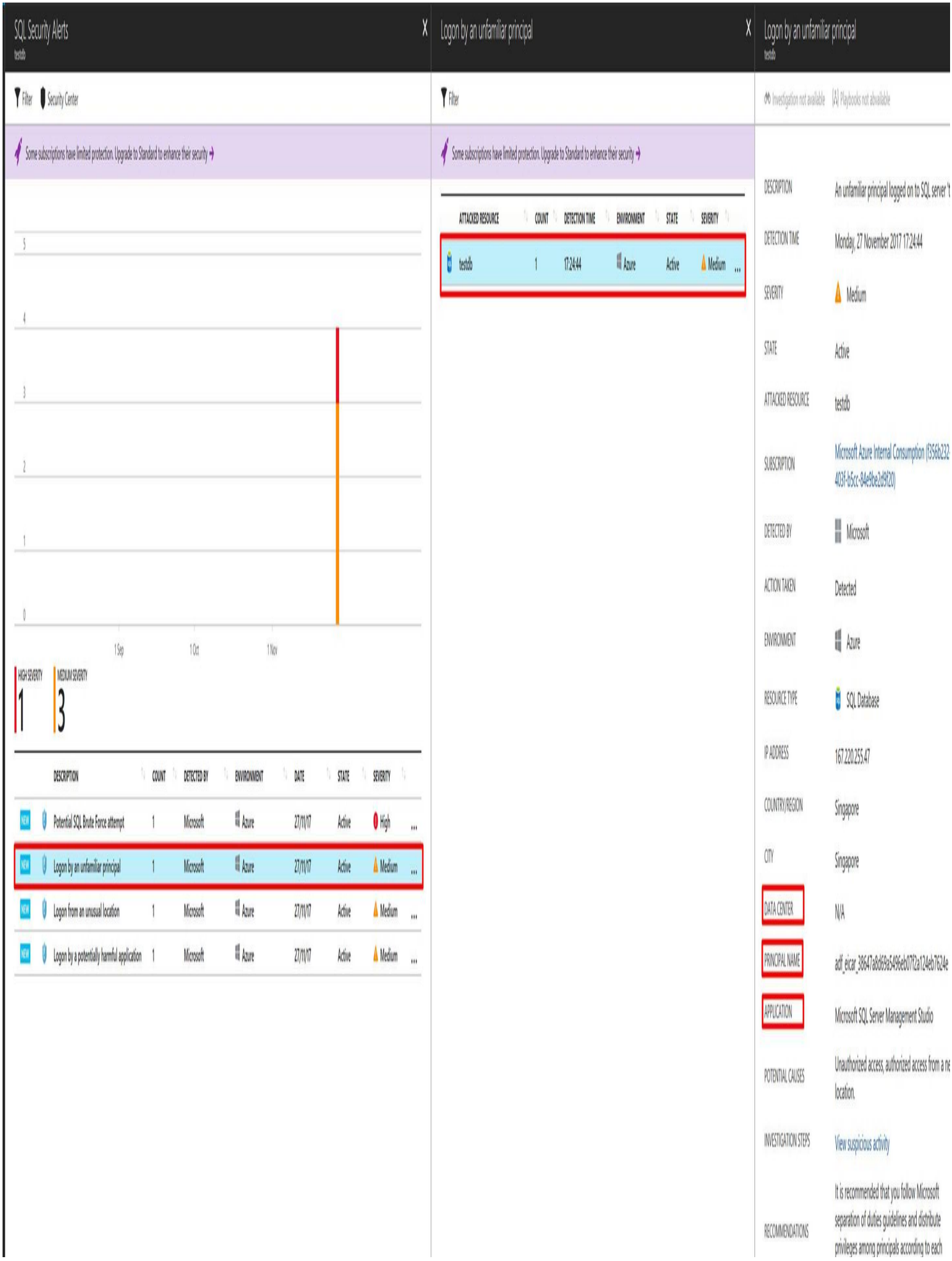
Azure SQL DB | Auditing, Threat Detection, VA, Classification

Step 1. Click **View recent SQL alerts** in the e-mail alert or by clicking on the SQL security tile within database blade in Azure portal top view active threats on the database

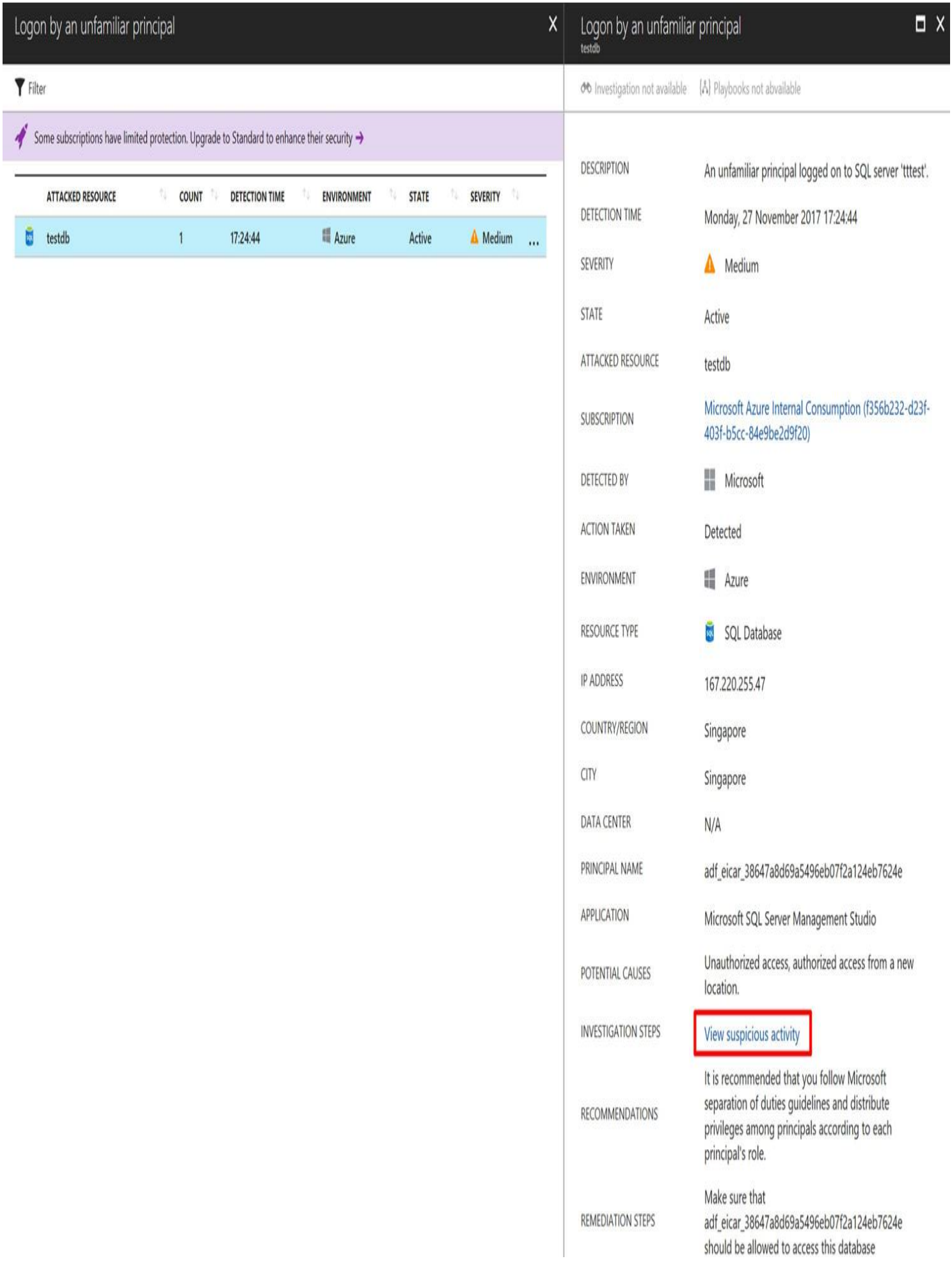

Azure SQL database
Suspicious database activity on server 'tttest', coming from a potentially harmful application ''.
View recent SQL alerts
Access details
Subscription f356b232-d23f-403f-b5cc-84e9be2d9f20
Server tttest
Database testdb
IP Address 167.220.255.47
Principal name ad*****
Application
Country/region Singapore
Date November 27, 2017 09:24:44 UTC
Investigation View suspicious activity
Potential causes Penetration testing, malicious activity
Recommendations It is recommended that you inspect the database audit logs around the time of the event to validate whether this activity is expected.
It is also recommended that you enforce the use of strong passwords and do not re-use them across multiple databases and lock down your firewall as tightly as possible.




Step 2. Click on a **specific alert** provides additional details and actions for investigating and preventing similar threats in the future including the full unfamiliar **Principal** , **Application name** and **Azure Data center** that have accessed your database.


SQL Security Alerts
testdb
Filter
Security Center
Some subscriptions have limited protection. Upgrade to Standard to enhance their security
5
4
3
2
1
0
1 Sep
1 Oct
1 Nov
HIGH SEVERITY
1
MEDIUM SEVERITY
3
DESCRIPTION
COUNT
DETECTED BY
ENVIRONMENT
DATE
STATE
SEVERITY
Potential SQL Brute Force attempt 1 Microsoft Azure 27/11/17 Active High
Logon by an unfamiliar principal 1 Microsoft Azure 27/11/17 Active Medium
Logon from an unusual location 1 Microsoft Azure 27/11/17 Active Medium
Logon by a potentially harmful application 1 Microsoft Azure 27/11/17 Active Medium
Logon by an unfamiliar principal
Filter
Some subscriptions have limited protection. Upgrade to Standard to enhance their security
ATTACKED RESOURCE
COUNT
DETECTION TIME
ENVIRONMENT
STATE
SEVERITY
testdb 1 17:24:44 Azure Active Medium
Logon by an unfamiliar principal
testdb
Investigation not available
Playbooks not available
DESCRIPTION
An unfamiliar principal logged on to SQL server 't
DETECTION TIME
Monday, 27 November 2017 17:24:44
SEVERITY
Medium
STATE
Active
ATTACKED RESOURCE
testdb
SUBSCRIPTION
Microsoft Azure Internal Consumption (f356b232-403f-b5cc-84e9be2d9f20)
DETECTED BY
Microsoft
ACTION TAKEN
Detected
ENVIRONMENT
Azure
RESOURCE TYPE
SQL Database
IP ADDRESS
167.220.255.47
COUNTRY/REGION
Singapore
CITY
Singapore
DATA CENTER
N/A
PRINCIPAL NAME
adf_eicar_38647a8d69a5496eb07f2a124eb7624e
APPLICATION
Microsoft SQL Server Management Studio
POTENTIAL CAUSES
Unauthorized access, authorized access from a ne
location.
INVESTIGATION STEPS
View suspicious activity
RECOMMENDATIONS
It is recommended that you follow Microsoft
separation of duties guidelines and distribute
privileges among principals according to each


Step 3. Click on the **View suspicious Log** to open SQL audit log records around the time of the event, making it easy to find the SQL statements that were executed (who accessed, what he did and when). As the owner of the database you are the only one that can determine if this was legitimate or malicious access by inspecting the nature of the database activities that were recorded in the SQL audit log around the time of the event.


Logon by an unfamiliar principal
Filter
Some subscriptions have limited protection. Upgrade to Standard to enhance their security
ATTACKED RESOURCE
COUNT
DETECTION TIME
ENVIRONMENT
STATE
SEVERITY
testdb
1
17:24:44
Azure
Active
Medium
Logon by an unfamiliar principal
testdb
Investigation not available
Playbooks not available
DESCRIPTION
An unfamiliar principal logged on to SQL server 'tttest'.
DETECTION TIME
Monday, 27 November 2017 17:24:44
SEVERITY
Medium
STATE
Active
ATTACKED RESOURCE
testdb
SUBSCRIPTION
Microsoft Azure Internal Consumption (f356b232-d23f-403f-b5cc-84e9be2d9f20)
DETECTED BY
Microsoft
ACTION TAKEN
Detected
ENVIRONMENT
Azure
RESOURCE TYPE
SQL Database
IP ADDRESS
167.220.255.47
COUNTRY/REGION
Singapore
CITY
Singapore
DATA CENTER
N/A
PRINCIPAL NAME
adf_eicar_38647a8d69a5496eb07f2a124eb7624e
APPLICATION
Microsoft SQL Server Management Studio
POTENTIAL CAUSES
Unauthorized access, authorized access from a new location.
INVESTIGATION STEPS
View suspicious activity
RECOMMENDATIONS
It is recommended that you follow Microsoft separation of duties guidelines and distribute privileges among principals according to each principal's role.
REMEDIATION STEPS
Make sure that adf_eicar_38647a8d69a5496eb07f2a124eb7624e should be allowed to access this database

## Classification

Root cause path -

Workload performance/Other/Uncoded

### How good have you found this content?