SQLskills Immersion Event

IEAzure: Azure VMs and Azure SQL Database

Module 7: Azure Security

Tim Radney

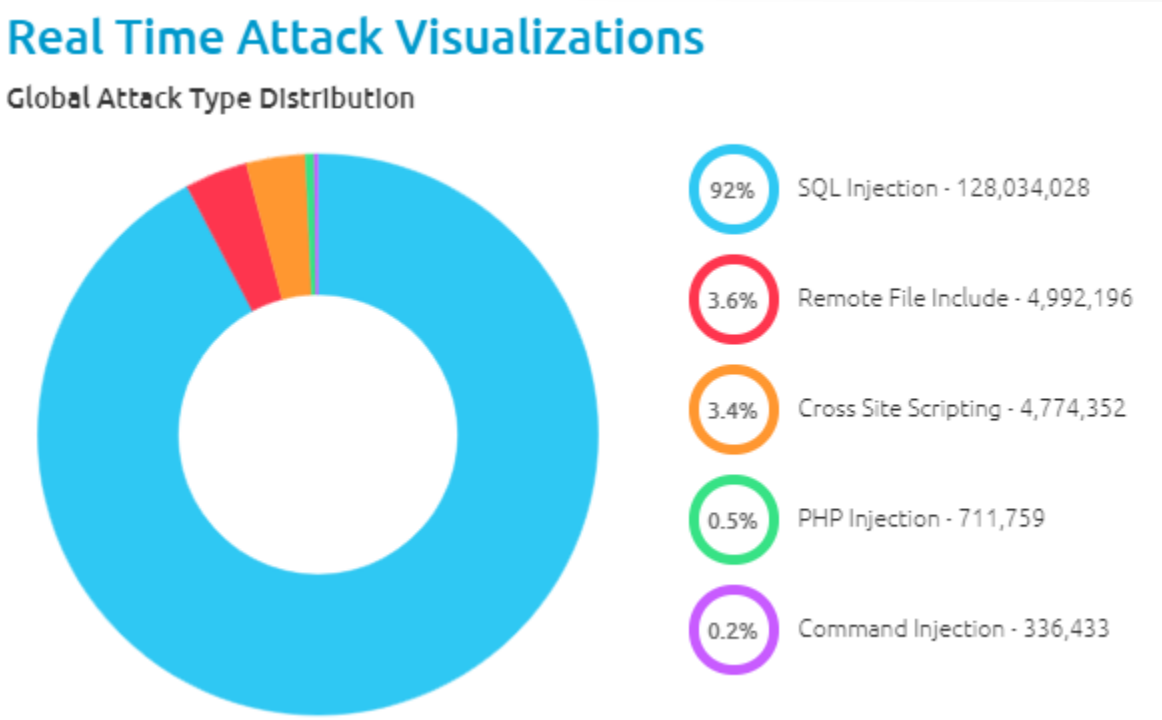
Tim@SQLskills.com

Overview

- Why SQL Server security?
- SQL Server Security Features
- Azure Security Center
- Azure Monitor - Operational Insights
- Log Analytics
- Vulnerability Assessment
- Data Classification and Discovery
- Threat Detection

Why SQL Server Security

- Ransomware
- Spectre / Meltdown
- SQL Injection
- Insider data theft



https://www.akamai.com/us/en/resources/visualizing-akamai/

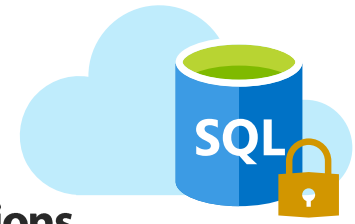
Why SQL Security Intelligence?

No organization is immune to data breaches

- No organization is immune to data breaches and security incidents
- 75% perpetrated by outsiders, while 25% involved internal actors

Common threats

- SQL injection
- Brute force access
- Password cracking
- Credential theft/leak
- Privilege abuse



Common regulations

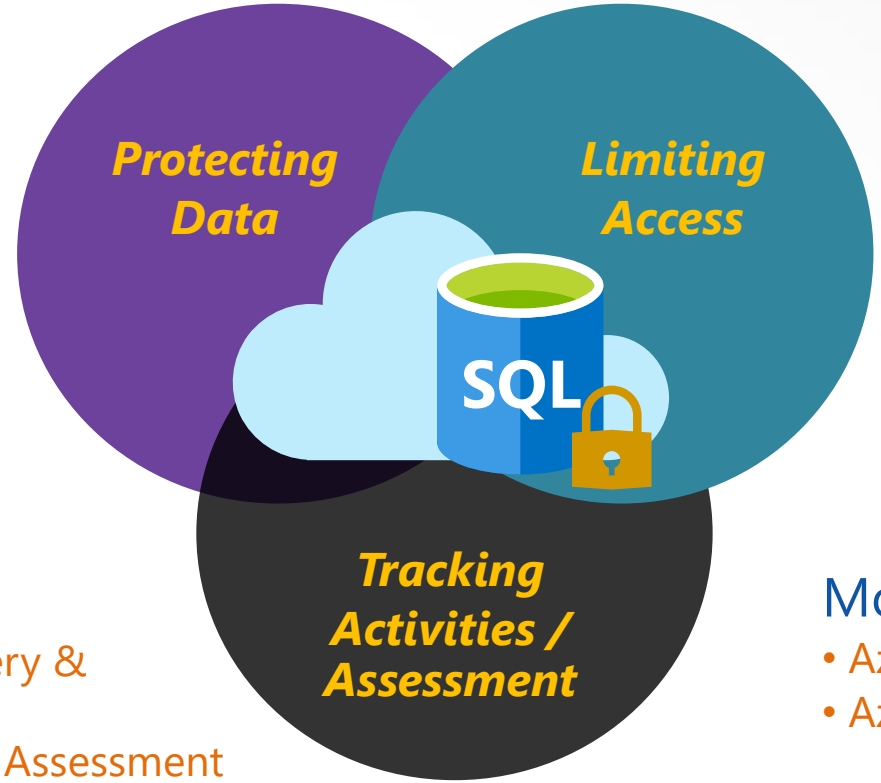
- GDPR (Personal)
- PCI (Payment)
- HIPPA (Health)
- FedRAMP (Government)

Secure your database

1. Discover sensitive data
2. Identify & remediate SQL vulnerabilities
3. Detect & remediate suspicious database activities
4. Meet security regulations requirements

Security Landscape

Available:
- TLS (link)
- TDE
- Dynamic Data Masking
- Always Encrypted
  - Secure Enclaves



Available:
- Row-level Security
- Firewall
- Users & Permissions
- SQL Authentication
- Azure Active Directory Authentication

Available:
- Data Discovery & Classification
- Vulnerability Assessment
- Advanced Threat Detection
- SQL Database Auditing with Power BI
- Azure Activity Log to Event Hubs

Monitoring:
- Azure Security Center
- Azure Advisor and Monitor

Compliance:
- Microsoft Azure Trust Center

SQL Server Security Features

- **Row Level Security**
- **Dynamic Data Masking**
- **Static Data Masking (preview)**
  - Has been temporarily pulled from SSMS
- **Transparent Data Encryption**
- **Always Encrypted**

- **SQL Server Management Studio improvements**
  - Data Classification
  - Vulnerability Assessments

Row Level Security (RLS)

- Protect data privacy by ensuring the right access across rows
- Fine-grained access control over specific rows in a database table
- Help prevent unauthorized access when multiple users share the same tables, or to implement connection filtering in multitenant applications
- Administer via SQL Server Management Studio, Azure Data Studio, or SQL Server Data Tools
- Enforcement logic inside the database and schema is bound to the table

Row Level Security Concepts

- **Predicate function**
  - User-defined inline table-valued function (iTVF) implementing security logic
  - Can be arbitrarily complicated, containing joins with other tables
- **Security predicate**
  - Binds a predicate function to a particular table, applying it for all queries
  - Two types: filter predicates and blocking predicates
- **Security policy**
  - Collection of security predicates for managing security across multiple tables

```
CREATE SECURITY POLICY mySecurityPolicy
       ADD FILTER PREDICATE dbo.fn_securitypredicate(wing, startTime, endTime)
       ON dbo.patients
```

Row Level Security – Security Predicates

- **RLS support two types of security predicates**
  - Filter Predicates silently filter rows available to read operations (SELECT, UPDATE, and DELETE)
  - Block Predicates explicitly block write operations (AFTER INSERT, AFTER UPDATE, BEFORE UPDATE, BEFORE DELETE) that violate predicate
- **Access to row-level data in table is restricted by security predicate defined as inline table-valued function, which is invoked and enforced by security policy**
  - For filter predicates, no indication to application that rows have been filtered from result set; if all rows are filtered, a null set will be returned
  - For block predicates, any operations that violate predicate will fail with error

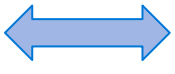
Demo

Row Level Security

Dynamic Data Masking

- Limit sensitive data exposure by obfuscating data to non-privileged users
- On-the-fly obfuscation of data in query results
- Policy-driven on the table and column
- Multiple masking functions available for various sensitive data categories
- Flexibility to define a set of privilege logins for un-masked data access
- By default, database owner is unmasked
- https://msdn.microsoft.com/en-us/library/mt130841.aspx

How Dynamic Data Masking Works




```
ALTER TABLE [Employee] ALTER COLUMN
[SocialSecurityNumber]
ADD MASKED WITH (FUNCTION = 'partial(0,"XXX-XX-",2)')

ALTER TABLE [Employee] ALTER COLUMN [Email]
ADD MASKED WITH (FUNCTION = 'EMAIL()')

ALTER TABLE [Employee] ALTER COLUMN [Salary]
ADD MASKED WITH (FUNCTION = 'RANDOM(1,20000)')

GRANT UNMASK to hrsupervisor
```

Security Officer

```
SELECT [Name],

[SocialSecurityNumber],
       [Email],
       [Salary]
FROM [Employee]
```

non-privileged login

	First Name	Social Security Number	Email	Salary
1	LILA	XXX-XX-XX37	lXX@XXXX.net	8940
2	JAMIE	XXX-XX-XX14	jXX@XXXX.com	19582
3	SHELLEY	XXX-XX-XX28	sXX@XXXX.net	3713
4	MARCELLA	XXX-XX-XX65	mXX@XXXX.net	11572
5	GILBERT	XXX-XX-XX87	gXX@XXXX.net	4487

hrsupervisor login

	First Name	Social Security Num...	Email	Salary
1	LILA	758-10-9637	lila.barnett@comcast.net	1012794
2	JAMIE	113-29-4314	jamie.brown@ntlworld.com	1025713
3	SHELLEY	550-72-2028	shelley.lynn@charter.net	1040131
4	MARCELLA	903-94-5665	marcella.estrada@comcast.net	1040753
5	GILBERT	376-79-4787	gilbert.juarez@verizon.net	1041308

1) Security officer defines dynamic data masking policy in T-SQL over sensitive data in Employee table
2) App user selects from Employee table
3) Dynamic data masking policy obfuscates the sensitive data in the query results

Combine with Row Level Security!

4) Data masking obscures columns, row level security filters rows


```
ALTER TABLE [Employee] ALTER COLUMN
[SocialSecurityNumber]
ADD MASKED WITH (FUNCTION = 'partial(0,"XXX-XX-",2)')

ALTER TABLE [Employee] ALTER COLUMN [Email]
ADD MASKED WITH (FUNCTION = 'EMAIL()')

ALTER TABLE [Employee] ALTER COLUMN [Salary]
ADD MASKED WITH (FUNCTION = 'RANDOM(1,20000)')

GRANT UNMASK to hrsupervisor
```

Security Officer

```
SELECT [Name],

[SocialSecurityNumber],
      [Email],
      [Salary]
FROM [Employee]
```

non-privileged login

	First Name	Social Security Number	Email	Salary
1	LILA	XXX-XX-XX37	lXX@XXXX.net	8940
2	JAMIE	XXX-XX-XX14	jXX@XXXX.com	19582
3	SHELLEY	XXX-XX-XX28	sXX@XXXX.net	3713
4	MARCELLA	XXX-XX-XX65	mXX@XXXX.net	11572
5	GILBERT	XXX-XX-XX87	gXX@XXXX.net	4487

hrsupervisor login

	First Name	Social Security Num...	Email	Salary
1	LILA	758-10-9637	lila.barnett@comcast.net	1012794
2	JAMIE	113-29-4314	jamie.brown@ntlworld.com	1025713
3	SHELLEY	550-72-2028	shelley.lynn@charter.net	1040131
4	MARCELLA	903-94-5665	marcella.estrada@comcast.net	1040753
5	GILBERT	376-79-4787	gilbert.juarez@verizon.net	1041308

DDM On Premises vs. Azure

- **Implementing Data Masking On Premises**
  - Requires a custom solution or SQL Server 2016+
  - Deployment challenges
    - "Trusting" engineers
    - Auditing
  - Prior to DDM, implementing a custom solution could take 40+ hours to implement
  - Implement on 2016 using T-SQL or PowerShell
- **Implementing Data Masking in Azure**
  - Built into the Azure Portal giving column-based recommendations
  - Use PowerShell, Rest API, or the Azure Portal

Demo

Dynamic Data Masking – deeper dive

Static Data Masking

- **Static Data Masking (SQL 2012+ and Azure SQL Database)**
  - Was in Preview and pulled from SSMS in April 2019
  - Will help organizations create sanitized copies of their databases
  - Physical changes are made to the data
    - Static Data Masking for Azure SQL Database and SQL Server | Azure Blog and Updates | Microsoft Azure

Static Data Masking	Dynamic Data Masking
• Happens on a copy of the database • Original data not retrievable • Mask occurs at the storage level • All users have access to the same masked data	• Happens on the original database • Original data intact • Mask occurs on-the-fly at query time • Mask varies based on user permission

Transparent Data Encryption

- **Protects the user database and all of its backups, transaction logs, and tempdb**
- **Improved encryption performance using INTEL's Advanced Encryption Standard (AES) New Instructions (AES-NI) hardware acceleration in Azure**
- **How it works**
  - Azure SQL DB and Managed Instance – on by default
    - Azure manages your keys or Bring Your Own Key - BYOK
  - On-premises – on by choice
    - "2-click user experience" – 2 T-SQL statements
- **Supported on SQL Server 2008+, Azure SQL Database, Azure SQL Managed Instance**

TDE – On Premises vs. Azure

- **Key variables**
  - Number of environments, databases, key rotation requirements
- **Key management challenges**
  - Provisioning, rotation, backup/restore, and DR
- **Total effort to implement on-premises for SQL Server 2014**
  - 400+ hours

- **Azure SQL Database Implementation**
  - On by default, make changes using Azure Portal or PowerShell
- **On-premises or Azure SQL Managed Instance**
  - Implement using T-SQL or PowerShell

Always Encrypted – Types of Encryption

- Randomized – uses a method that encrypts data in a less predictable manner
- Deterministic – uses a method which always generates the same encrypted value for any given plaintext value

```
Randomized Encryption
   Encrypt('123-45-6789') = 0x17cfd50a
   Repeat: Encrypt('123-45-6789') = 0x9b1fcf32
   Allows for transparent retrieval of encrypted data
   but NO operations
   More secure


Deterministic Encryption
   Encrypt('123-45-6789') = 0x85a55d3f
   Repeat: Encrypt('123-45-6789') = 0x85a55d3f
   Allows for transparent retrieval of encrypted data
   AND equality comparison
   (i.e. in WHERE clauses and Joins, DISTINCT, GROUP
   BY)
```

Always Encrypted T-SQL Example

```
CREATE COLUMN MASTER KEY MyCMK
WITH ( KEY_STORE_PROVIDER_NAME = 'MSSQL_CERTIFICATE_STORE',
KEY_PATH = 'Current User / Personal / f2260f28909d21c642a3d8e0b45a830e79a12420' );
```

```
CREATE COLUMN ENCRYPTION KEY MyCEK
WITH VALUES
( COLUMN_MASTER_KEY = MyCMK,
ALGORITHM = 'RSA_OAEP',
ENCRYPTED_VALUE = '0x017000_64003);
```

```
CREATE TABLE Customers (
Customers nvarchar(60) COLLATE Latin1_General_BIN2 ENCRYPTED
WITH (COLUMN_ENCRYPTED_KEY = MyCEK,
ENCRYPTION_TYPE = RANDOMIZED, ALGORITHM = 'AEAD_AES_256_CBC_HMAC_SHA_256'),

SSN varchar(11) COLLATE Latin1_General_BIN2 ENCRYPTED
WITH (COLUMN_ENCRYPTED_KEY = MyCEK,
ENCRYPTION_TYPE = DETERMINISTIC, ALGORITHM = 'AEAD_AES_256_CBC_HMAC_SHA_256'), Age int NULL );
```

Demo

Always Encrypted

Azure Security Center

- **Central hub for monitoring your security status of your resources**
  - Centralizes access to several security tools/features
  - "Single Pane of Glass"
- **Secure score – reviews your security recommendations and prioritizes them for you. This helps you find the most severe vulnerabilities**
- **Security Center mimics the work of a security analyst, reviewing the security recommendations, and applying advanced algorithms to determine the criticality of each recommendation**
- **Gain visibility across your environment to verify compliance**
- **Customize your security policy to focus on what you need – apply the policy to multiple Azure subscriptions**

Azure Security Center Standard tier

- **Protect both Windows and Linux servers**
- **Address vulnerabilities in web applications**
- **Detect anomalous database access and query patterns, SQL injection attacks, and other threats targeting SQL databases in Azure**
  - Threat Detection
- **Receive alerts on suspicious activity as well as recommended actions**
- **Discover, classify, label, and protect sensitive data in your databases**
  - Data Discovery and Classification
- Get a unified view of security across all of your on-premises and cloud workloads, including your Azure IoT solution

Demo

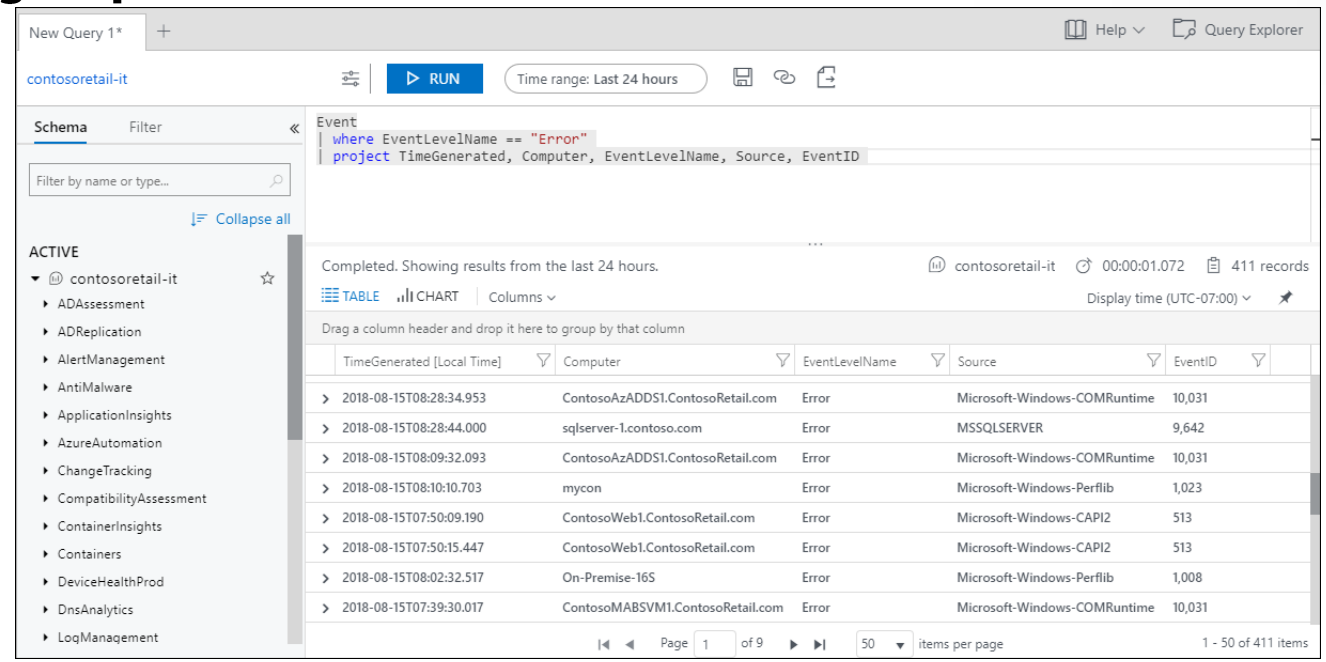
Azure Security Center

Azure Monitor

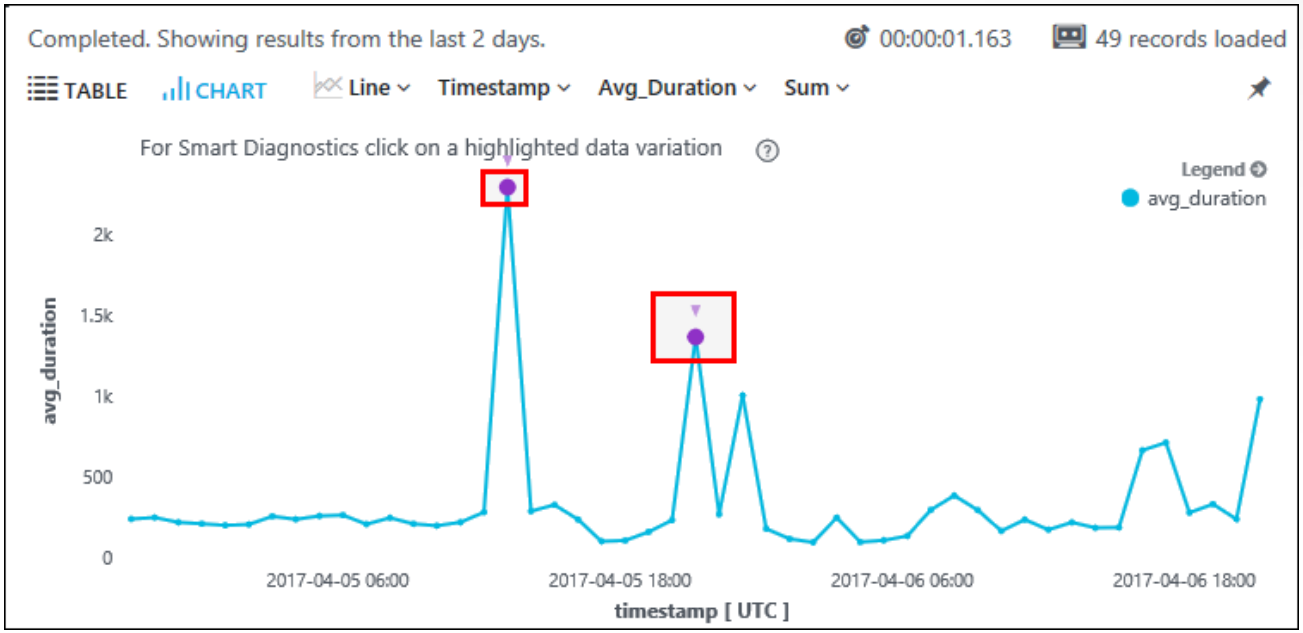
- **Formerly Operational Insights**
- **Central hub for monitoring your applications and infrastructure**
  - Centralizes access to several tools/features
  - "Single Pane of Glass"
- **Monitor and visualize metrics - Metrics**
  - Numerical values available from Azure Resources used to understand the health, operation and performance
- **Query and analyze logs – Log Analytics**
  - Logs are activity logs, diagnostic logs and telemetry from monitoring solutions; Analytics queries assist with troubleshooting and visualizations
- **Setup alert and actions - Alerts**
  - Alerts notify you of critical conditions and potentially take corrective automated actions based upon triggers from logs or metrics

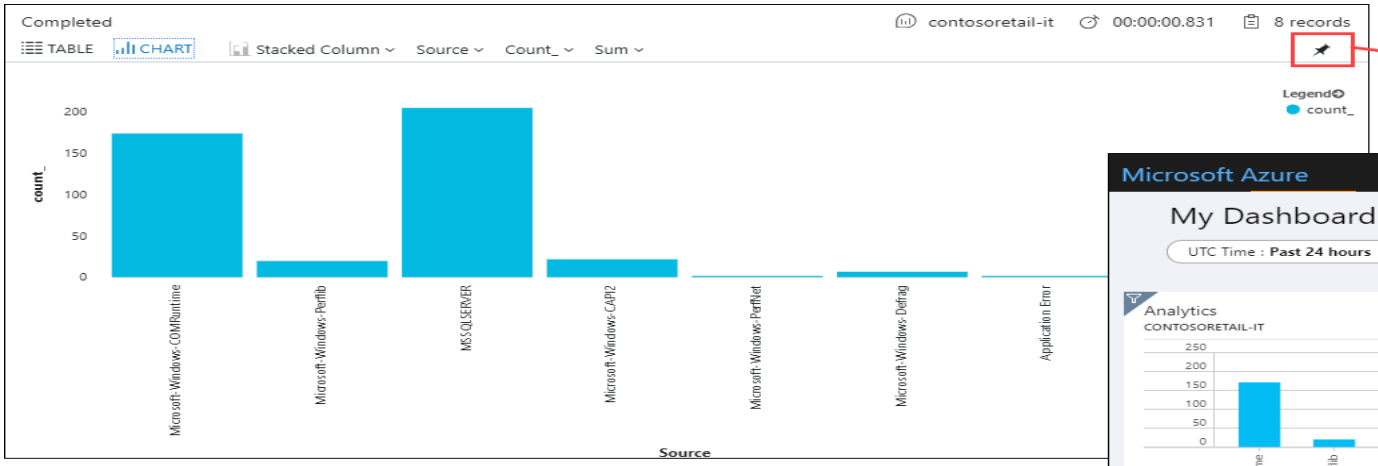
Log Analytics

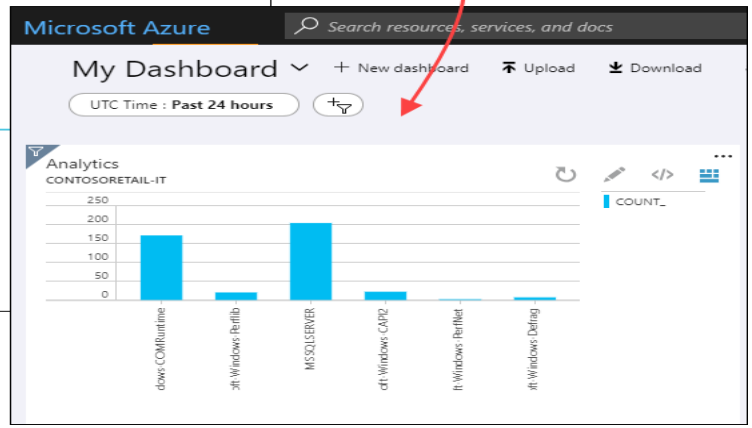
- **Write queries using KQL (Kusto Query Language)**
  - https://www.pluralsight.com/courses/kusto-query-language-kql-from-scratch
- **Intellisense guides query development**
- **Filter, sort, and group results**
- **Apply a time range**
- **Create charts**
  - Column, line, pie, area
- **Save and load queries**
- **Export and share queries**



Analyzing Data in Log Analytics





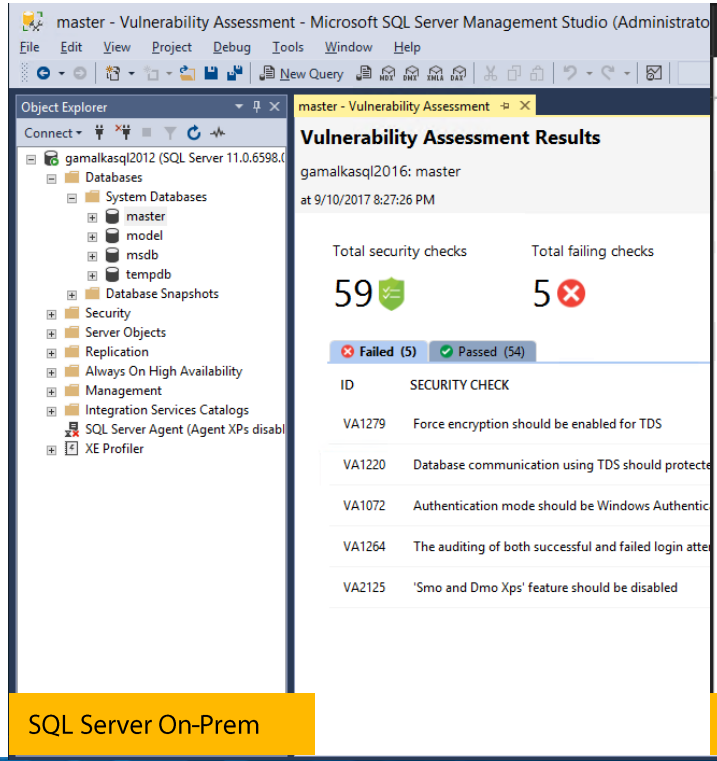


Vulnerability Assessment

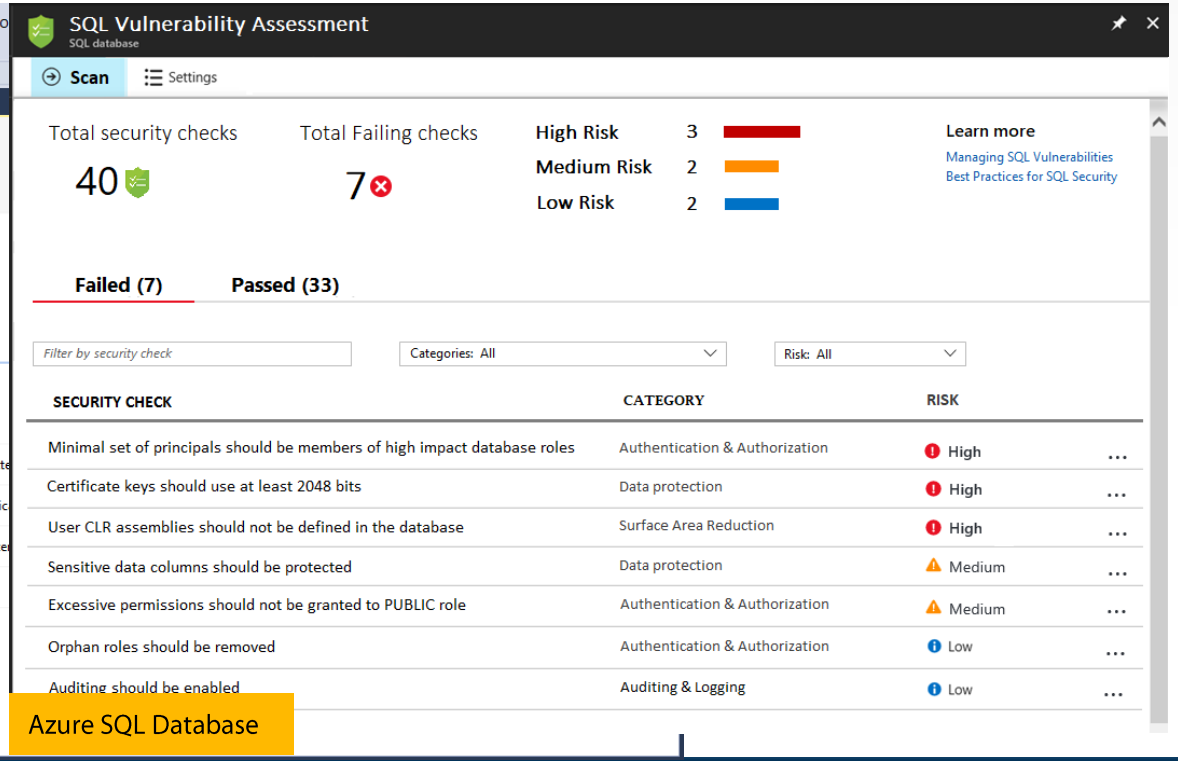
- Your first stop to track and improve the security of SQL Database
- Get visibility by discovering sensitive data and potential security vulnerabilities
- Remediate issues by receiving scheduled actionable steps that help guide you to remediate any gaps and harden your security defenses
- Customize the assessment to your specific environment with configurable policies so you can focus on deviations
- Available in the Azure Portal and SQL Server Management Studio

Vulnerability Assessment

- Just run a scan and discover sensitive data that isn't protected
- Coherent report that helps meet compliance requirements
- SSMS 17.4+



SQL Server On-Prem



Azure SQL Database

Demo

Review vulnerability assessments in SSMS and the Azure Portal

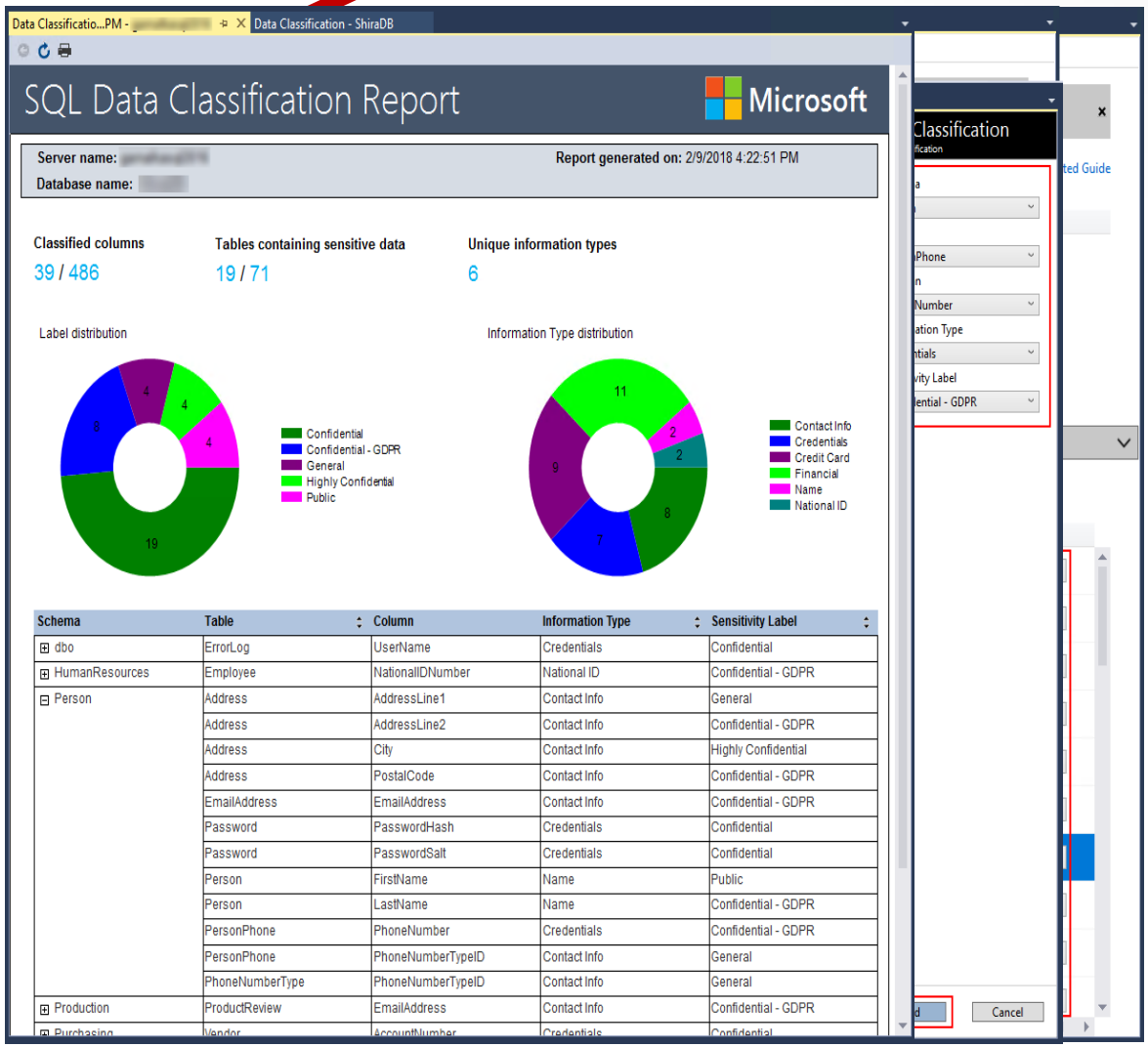
Data Discovery and Classification

- Provides advanced capabilities built into Azure SQL Database for discovering, classifying, labeling, and protecting the sensitive data within your databases
- Helps improve your organizations information protection stature
- Helps meet data privacy standards and regulatory requirements
- Can audit and alert on anomalous access to sensitive data

Data Discovery and Classification

- **Discovery and recommendations**
  - The classification engine in Azure scans your database and identifies columns containing potentially sensitive data
  - You can then review and apply necessary classification recommendations via the portal
  - This is NOT a deep scan of data within your database
- **Labeling**
  - Sensitivity classification labels can be tagged on columns using new classification metadata attributes introduced into the SQL Engine
  - These labels can be used for auditing
- **Query result set sensitivity**
  - Sensitivity of a query result set is calculated in real time for auditing
- **Visibility**
  - Classification state can be viewed in the Azure Portal or downloaded in Excel

SQL Data Discovery and Classification (17.5+)



- New tool built into SQL Server Management Studio (SSMS)
- For discovering, classifying, labeling and reporting the sensitive data
  - (Financial, healthcare, PII, etc.)
- Helping meet data privacy standards and regulatory compliance requirements, such as GDPR
- Controlling access to and hardening the security of databases/columns containing highly sensitive data
- Data Discovery & Classification is supported for SQL Server 2008 and later

Demo

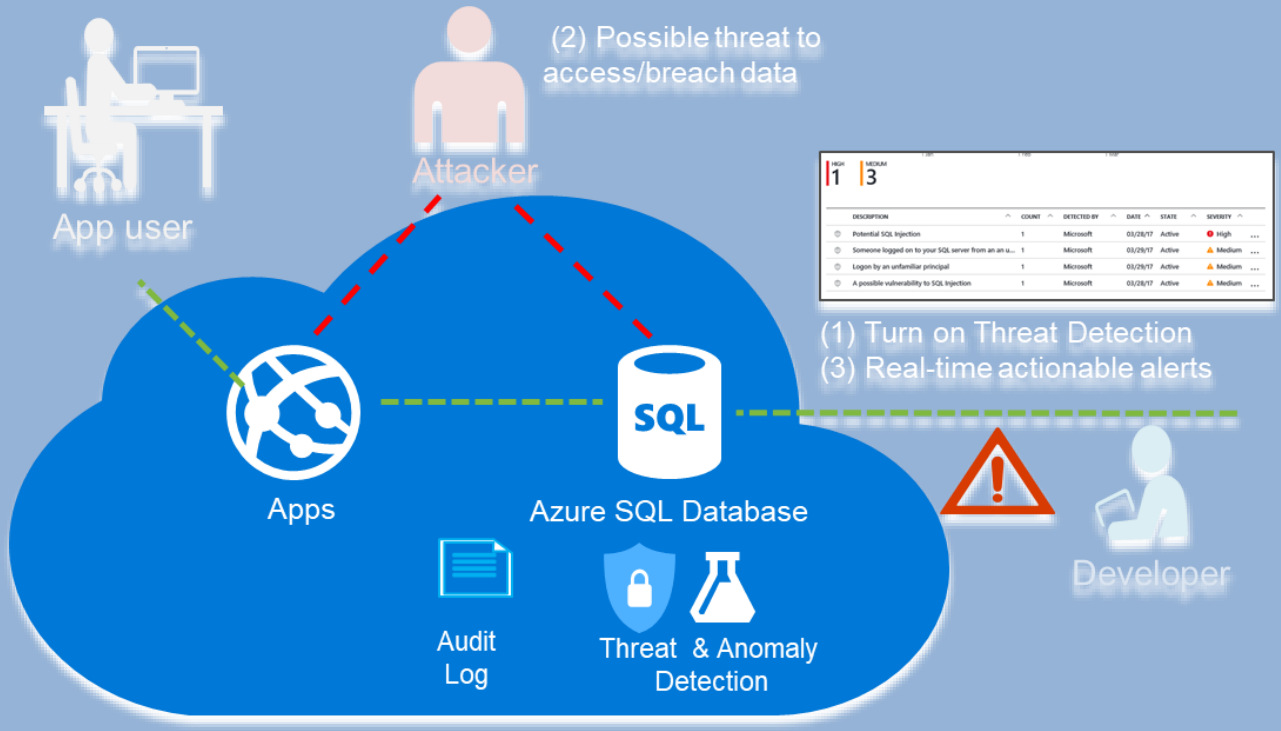
Data Discovery and Classification in SSMS and Azure

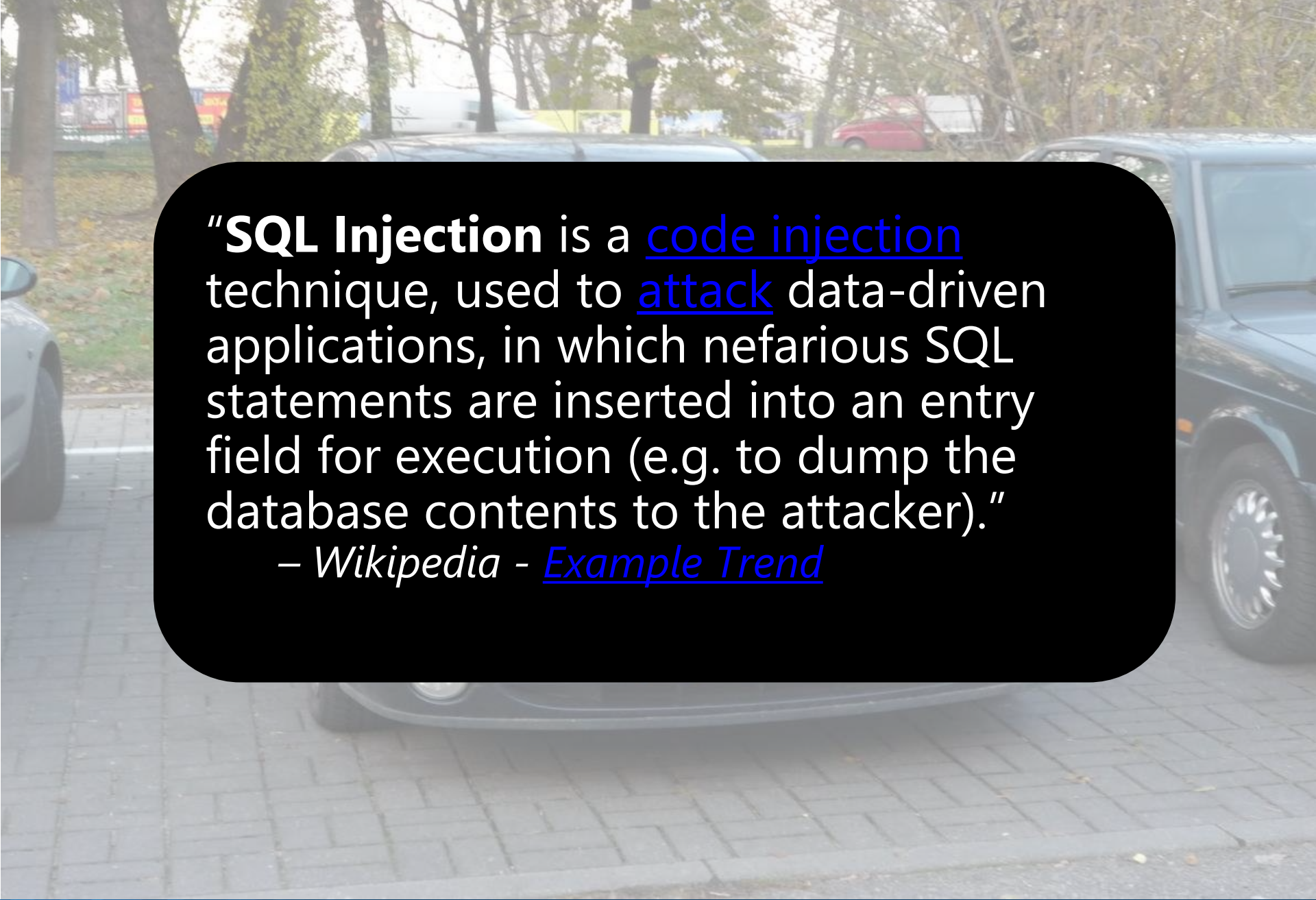
Azure Defender

- SQL injection
- Unusual database access patterns
- Potential risks / vulnerabilities
- Actionable alerts which recommend how to investigate and remediate
- Just turn it on
- Very low cost, $15/server/month, first 60 days for free

Azure Defender

- SQL injection
- Unusual database access patterns
- Potential risks / vulnerabilities





"**SQL Injection** is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker)."

– Wikipedia - Example Trend

Demo

SQL Server Injection Attacks, step through Advanced Threat Detection

What's the Best Bet? (Cover Your Bases)

- **TLS/SSL – uses encryption to protect the transfer of application data**
- **Use TDE to protect data at rest and tempdb**
- **Use Row Level Security and DDM to limit and protect data specifics**
- **Always Encrypted (with enclaves) to protect data in motion**
  - If you cannot use Always Encrypted, leverage DDM
- **Audit sensitive columns – If you can enough to DDM/Encrypt..**
  - Consider 3rd party solutions for auditing large environments with alrerting
- **Use static data masking on any non-production purposed copy of your data, being aware of the data risk levels – when available**
- **Use vulnerability assessments to regularly implement a security health check**

Microsoft Guidance with Spectre and Meltdown

To take advantage of available protections, follow these steps to get the latest updates for both software and hardware:

1. **Make sure your antivirus software is up to date**
2. **Keep your device up to date by turning on automatic updates**
3. **Check that you've installed the latest Windows operating system security update from Microsoft. If automatic updates are turned on, the updates should be automatic, but you should still confirm**
4. **Install any firmware updates from your device manufacturer**

Note: Customers who only install the latest security updates will not be fully protected.
You will need to update both your hardware and your software to fix this vulnerability.

Platform/Service Security

- Microsoft assumes a breach…
- Enhanced monitoring of their Azure assets
- Collection of low-fidelity anomalous activity (automated hunting)
- Monitoring PERF for traits of crypto currency mining
- A large set of other detections that Microsoft doesn't talk about publicly

- Attack team, SQL Red Team, tries to get in, gain a foothold, escalate privileges, and maintain persistence
- SQL Blue Team practices defense-in-depth

- When Microsoft detects something, e.g., failed login attempts, they defend
- If it involves a customer, they will notify, most of the time it's the customer's own security and compliance scanners

Data Breaches

- **A data breach occurs when a cybercriminal successfully infiltrates a data source and extracts sensitive information**
- **Security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual or team**
- **What are the causes of a data breach?**
  - Weak and stolen credentials
  - Theft of a corporate asset
  - Application vulnerabilities
  - Phishing attack
  - Insider threats

SolarWinds

- December 2020
- Global
- Major breaches
- Give hackers access to thousands of companies and government offices that used its products.
- Ongoing

Capital One Cyber Incident

- July 2019
- Financial
- 100+ Million individuals' data
- An outside individual gained unauthorized access and obtained certain types of personal information about Capital One credit card customers and individuals who had applied for our credit card products
- Customers data from 2005 – 2019
- 140k US Social Security numbers
- 1M Canadian Social Insurance numbers
- 80k bank account numbers

Ecuador

- September 2019
- Government
- 20+ Million individuals' data
- Unsecured server run by an Ecuadorian marketing and analytics firm
- Full names, dates of birth, national identity card numbers, tax identification numbers, employment information, names of family members, and much more
- Nearly everyone in Ecuador

TJX Companies, Inc

- December 2006
- Retail Giant
- 94 Million credit cards exposed
- A group of hackers took advantage of a weak data encryption system and stole credit card data during a wireless transfer between two Marshall's stores in Miami

Heartland Payment Systems

- March 2008
- Finance and Insurance
- 134 Million credit cards exposed through SQL injection to install spyware on Heartland's data systems
- At the time of the breach, Heartland was processing 100 million payment card transactions per month for 175k merchants. Most small to mid-sized retailers

VeriSign

- August 2010
- Network Security and Software
- Undisclosed information stolen
- Security experts are unanimous in saying that the most troubling thing about the VeriSign breach in which hackers gained access to privileged systems and information, is the way the company handled it.

RSA Security

- March 2011
- Network Security and Software
- 40 Million employee records stolen
- The impact of the cyberattack that stole information on the security giant's authentication tokens is still being debated

Sony's PlayStation Network

- April 2011
- Entertainment
- 77 Million PlayStation Network accounts hacked; estimated losses of $171 million while the site was down for a month
- This is viewed as the worst gaming community data breach of all-time. Of more than 77 million accounts affected, 12 million had unencrypted credit card numbers

Adobe

- October 2013
- Network Security and Software
- 38 Million user records
- The company originally reported that hackers had stolen nearly 3 million encrypted customer credit card records, plus login data for an undetermined number of user accounts

Target Stores

- December 2013
- Retail Giants - Credit/Debit Card
- Information and contact information of up to 110 million people compromised
- The breach actually began before Thanksgiving, but was not discovered until several weeks later. The retail giant initially announced that hackers had gained access through a third-party HVAC vender to its point-of-sale (POS) payment card readers, and had collected about 40 million credit and debit card numbers.

eBay

- May 2014
- E-commerce
- 145 Million users compromised
- User account hack- the online auction giant reported a cyberattack which exposed names, addresses, dates of birth, and encrypted passwords of all of its 145 million users

JP Morgan Chase

- July 2014
- Finance and Insurance
- 76 Million households and 7 million small businesses
- The largest bank in the nation was the victim of a hack during the summer of 2014 that compromised the data of more than half of all US households. The data breach is considered one of the most serious intrusions into an American corporation's information system and one of the largest data breaches in history

JPMorganChase 

iCloud

- August 2014
- Entertainment – Cloud Storage
- 500 private photos
- The images of various celebrities, mostly women, were posted on the imageboard 4chan, and later disseminated by other users on websites around the world. The images were obtained via the online storage offered by Apple's iCloud platform. The attack was a targeted attack on uses names, passwords and security questions by means of phishing and brute-force guessin

Home Depot

- September 2014
- Home Improvement
- Credit/debit card information
- 56 million customers affected
- Exploit of self-checkout terminals

Anthem

- February 2015
- Finance and Insurance
- Theft of personal information of up to 78.8 million current and former customers
- The second-largest health insurer in the US, formerly known as WellPoint, stated a cyberattack had exposed the names, addresses, SSN, date of birth, and employment history of customers

Office of Personnel Management

- June 2015
- US Government
- Final estimate of 21.5 million records stolen
- Includes records of people who had undergone background checks, but who were not necessarily current or former government employees. One f the largest data breaches of government data in the history of the US. PII data such as SSN as well as names, dates, places of birth, and addresses

Adult Friend Finder

- October 2016
- Social Networking
- 412.2 Million accounts
- User account hack – hackers collected 20 years of data on six databases that included names, email addresses and passwords

Uber

- October 2016
- Transportation Network
- User Account Hack
- 57 million users and 600k drivers personal data exposed
- Two hackers were able to get names, email addresses, and mobile phone numbers of 57M users and drivers license numbers for 600k drivers.

Equifax

- July 2017
- Finance and Insurance
- Credit Card
- Personal information including SSN, birth dates, addresses, and in some cases driver's' license numbers of 143 million consumers. 209k consumers also had their credit card data exposed

Ticketfly - Eventbrite

- May 2018
- Event Management
- 26 million user accounts
- Personal information to include customers names, addresses, emails, and phone numbers

BMO and Simplii

- May 2018
- Bank of Montreal and Simplii Financial
- Finance and Insurance
- As many as 90k total customers may be affected.
- Both banks are still grappling with the fallout from apparent data breaches

Social Networking

- Yahoo
- 2013 – 2014
- 3 BILLION user accounts
- Real names, email addresses, dates of birth, and phone numbers

- Facebook
- 2016 -2018
- Cambridge Analytica scandal – 50 million users data confirmed ‘at risk’

Key Takeaways

- SQL Server injection attacks are the top attacks attempted
- Microsoft provides us with numerous tools to help protect our environments
- Protecting our data assets require more than just the DBA
- Hardening the environment is the first step, detecting anomalies within the system is the ultimate goal

Review

- We discuss why SQL Server security is important
- SQL Server Security feature overview
- You learned about the Azure Security Center window
- We covered the Azure Monitor which was Operational Insights
- We discussed Log Analytics and KQL
- Vulnerability Assessments can be performed within Azure and SSMS
- Although in preview Data Classification and Discovery can help identify sensitive data
- We looked at Threat Detection and discussed how this is a must for any organization