Microsoft®
tech·ed
India | 2009

LEARNING LIVES HERE

Hardening SQL Server

Karthik Bharathy
Program Manager, SQL Server
Microsoft

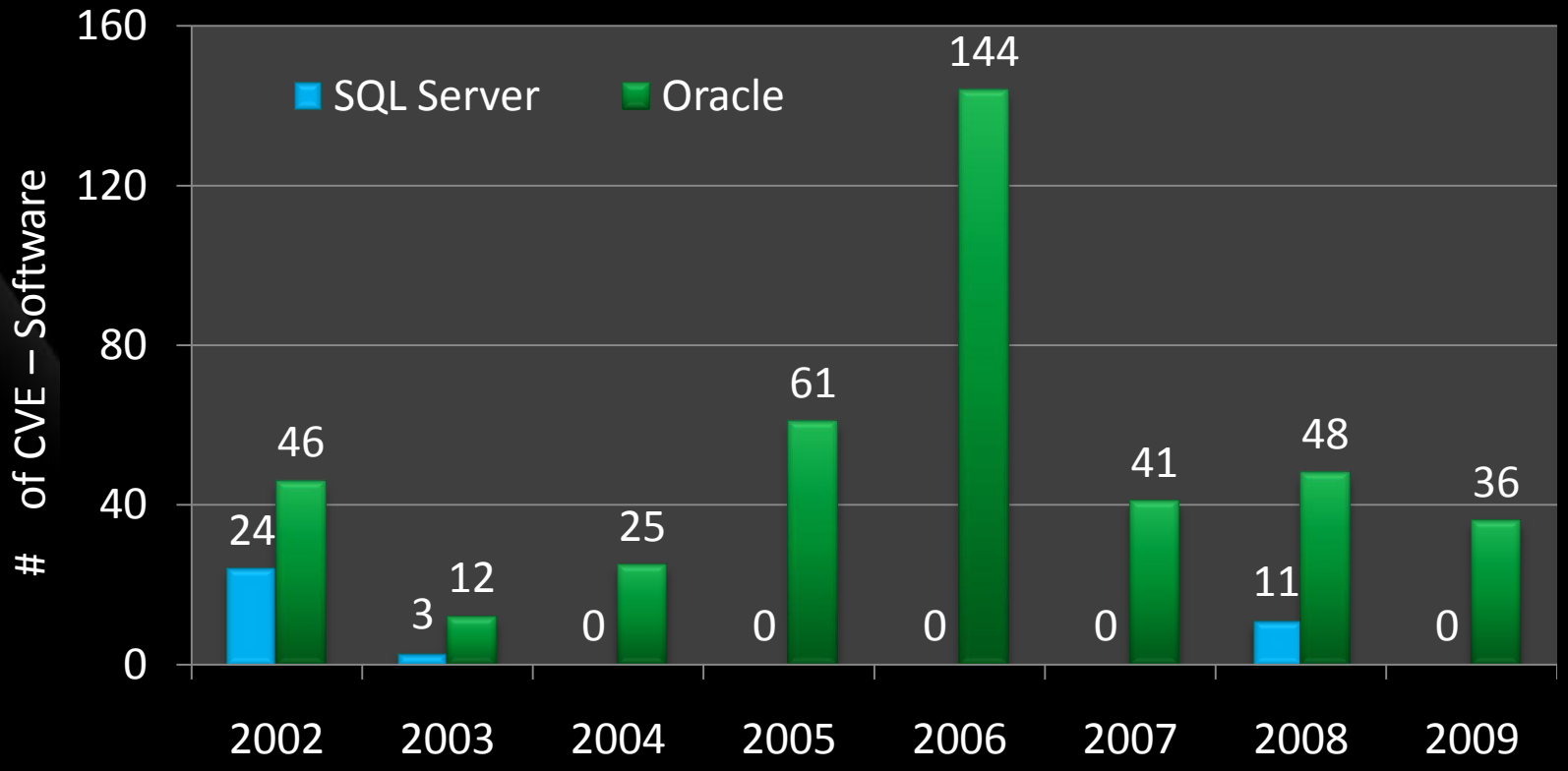
msdn Microsoft Developer Network

Microsoft TechNet

Key Session takeaways

- Understand the many views of SQL Server
- Look at hardening SQL Server
  - At the network level
  - At the access level
  - At the data level
  - At the application level
- Tools and features for hardening
- Best practices

Background



Source: NIST National Vulnerability Database

Notes: Update as of 4/21/2009.
Vulnerabilities are included for SQL Server 2000 , SQL Server 2005 , SQL Server 2008. Oracle (8i, 9i, 9iR2, 10g, 10gR2,11g)
Query for Oracle was run with vendor name: 'Oracle' , and product name: 'any' (all database product name variations were queried) .
Query for Microsoft was run with vendor name: 'Microsoft ' ; product name: 'Microsoft SQL Server'; version name: 'Any'
We are counting NIST CVE – Software Flaws (Each CVE might include more than one Oracle vulnerabilities)

Brief look at history

- SQL Slammer worm (2003)
  - Exploit on UDP port 1434
  - Buffer overflow in service resolution
- Spida worm (2002)
  - Exploit on TCP port 1433
  - Collect system info and email password hash

The many views of SQL Server

I. Network service

SQL Server offers a network service. Attacks on the network and port E.g. Port Sniffing, DoS attack

II. Access service

SQL Server requires login/password to connect and execute queries. Attacks on blank passwords, improper roles/permissions

III. Data service

SQL Server data in mdf, ldf, log files. Attempts to capture data either directly from the host or from backup disk

IV. Application service

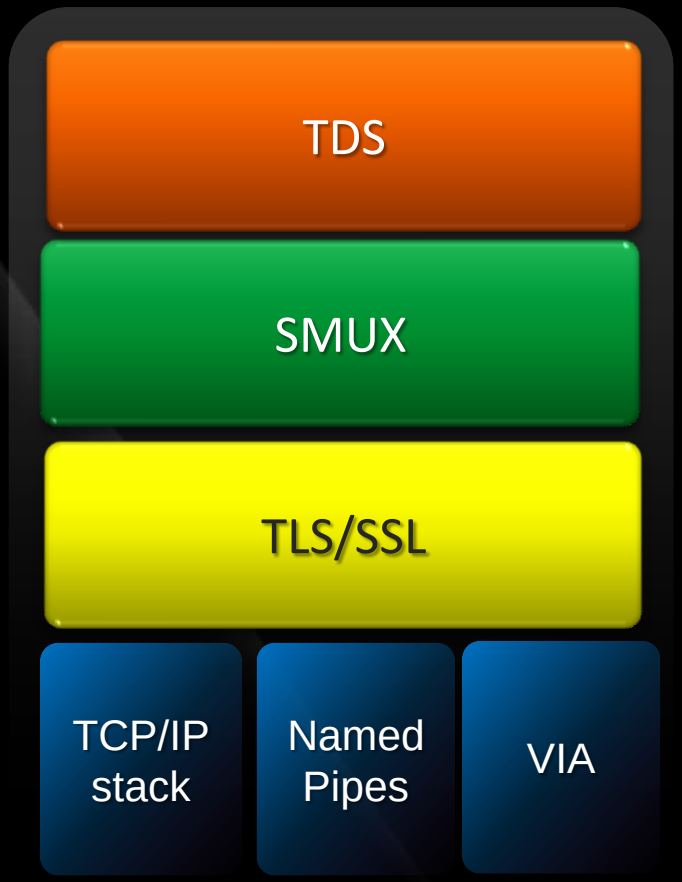
T-SQL queries interact with the instance may be poorly written. E.g. SQL Injection and elevation of privileges

Let’s look at each view….

- Highlight the *Concepts*
- Understand the *Tools* used
- *Demo* features in SQL Server 2008
- Summarize the *Best Practices*

I. Network service

Concepts



Tabular Data Stream

Session MUX protocol for MARS

Network Channel Encryption

Network Transport

Network service

SQL Server Tools

- SQL Scan: scans individual computer, a Windows domain, or a range of IP addresses for SQL Server 2000 and MSDE 2000
- SQL Check: scans the computer on which it is running for instances of SQL Server 2000 and MSDE 2000
- SQL Server Critical Update: Detect and update vulnerable files through a wizard
- Other 3rd party tools

Network service
Lock down

- Verify instance patch level
- Disable unused features DatabaseMail, XPCmdShell
- Prefer Windows mode Authentication
- Revoke permissions not needed for user
- Remove sample databases

LEARNING LIVES HERE

demo

Lock down SQL Server

Karthik Bharathy
Program Manager
Microsoft

msdn Microsoft Developer Network

Microsoft TechNet

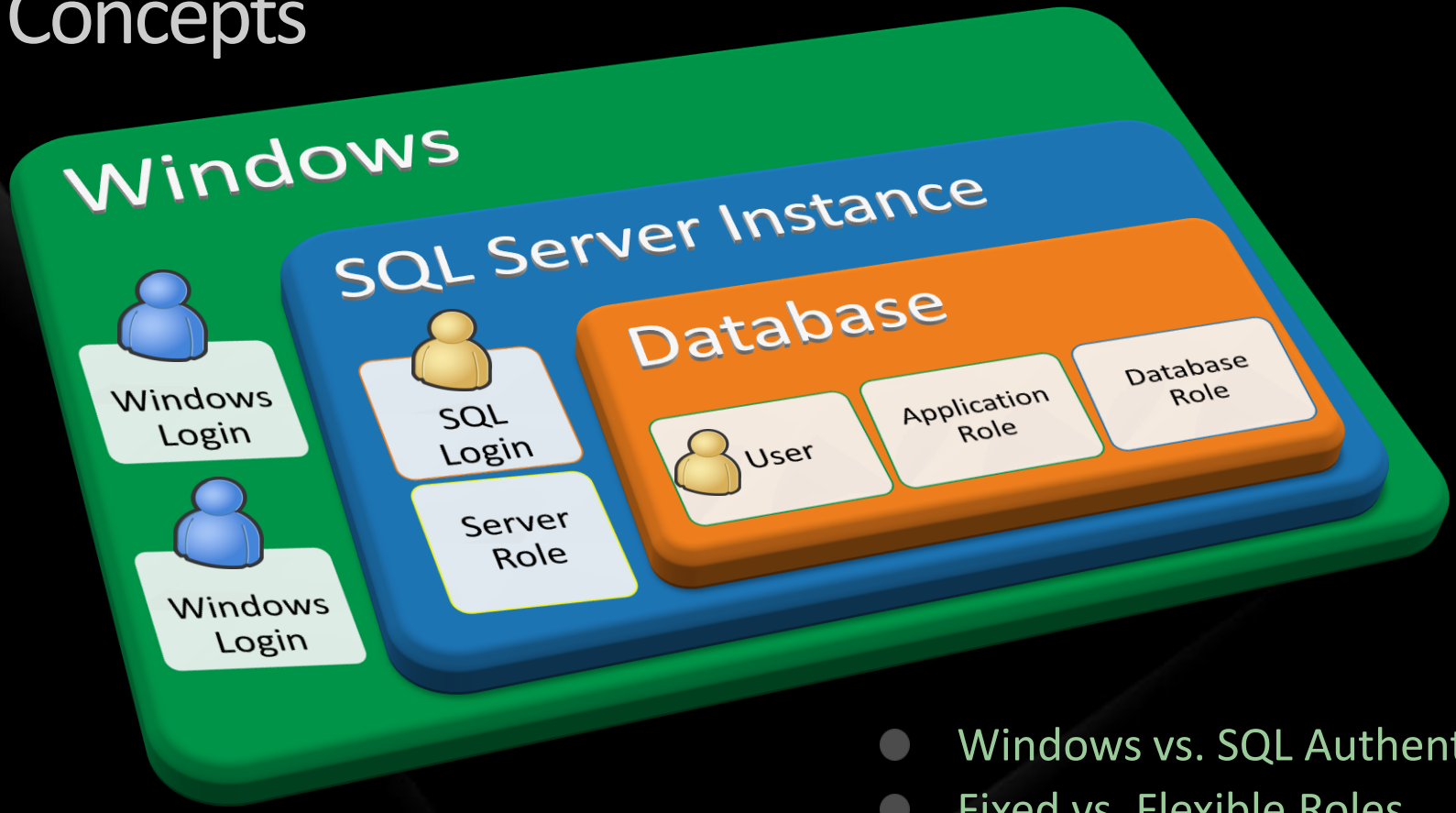
Network service

Best Practices

- Ensure patch level is up-to-date
- Use TCP/IP as the preferred network protocol
- Not exposing TCP/IP ports over the Internet
- Using SSL encrypted communication
- Disabling protocols that are not required
- Lock down SQL Server

II. Access service

Concepts

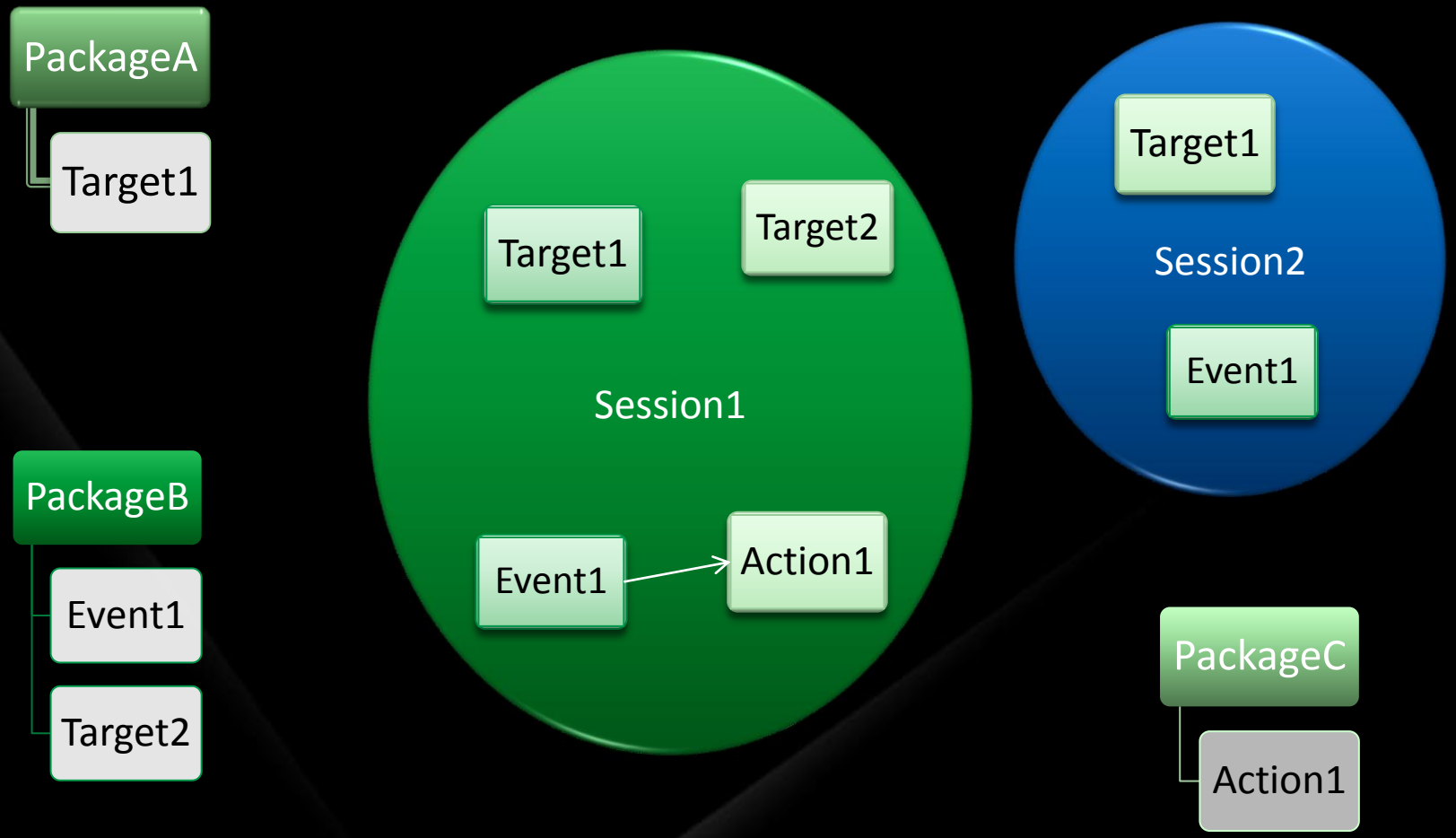


- Windows vs. SQL Authentication
- Fixed vs. Flexible Roles
- Users and Application Role
- Statement vs. Object permissions

Access service
SQL Server 2008 Tools

- XEvent: scalable and configurable asynchronous eventing infrastructure
- SQL Server 2008 Auditing: unified box wide solution to audit DDL for configuration and management purpose

XEvent Session



LEARNING LIVES HERE

demo

Capturing events using XEvent

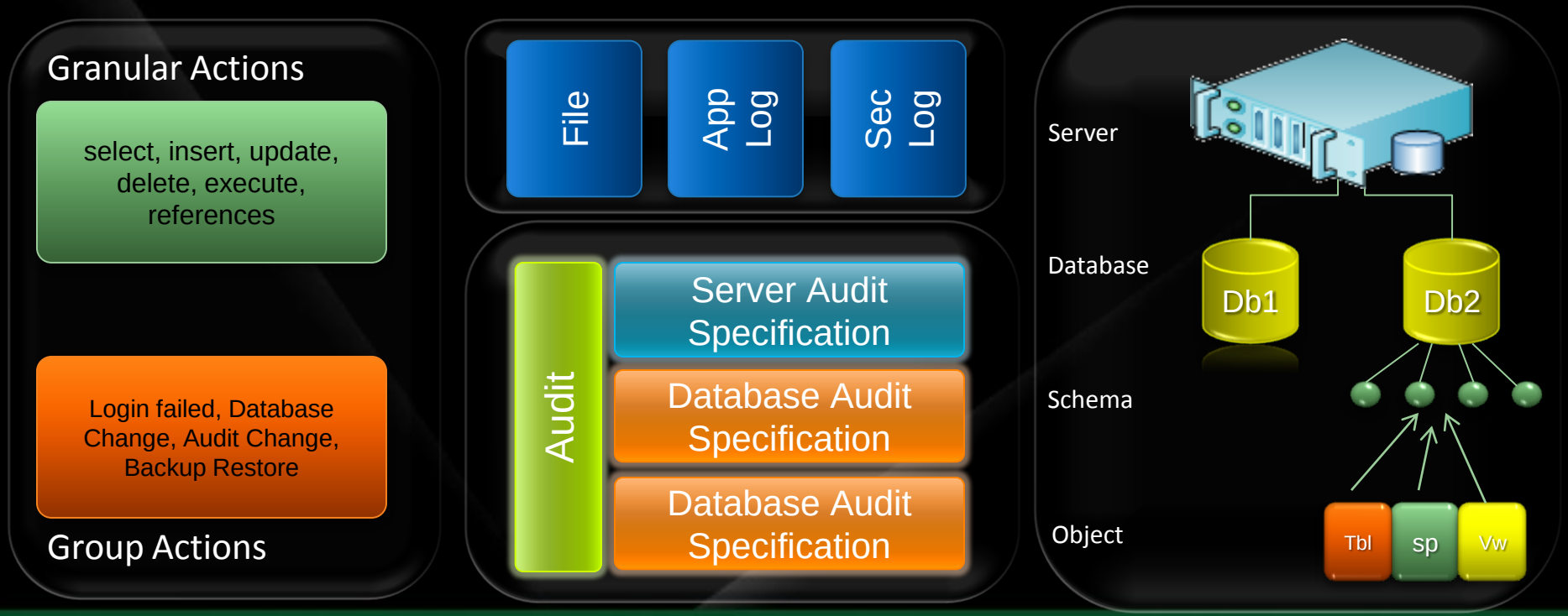
Karthik Bharathy
Program Manager
Microsoft

msdn Microsoft Developer Network

Microsoft TechNet

SQL Server Auditing

- Specifications
- Scope
- Actions
- Target



LEARNING LIVES HERE

demo

Access checks using SQL Server Auditing

Karthik Bharathy
Program Manager
Microsoft

msdn Microsoft Developer Network

Microsoft TechNet

Access service
Best Practices

- Enable Audits on SQL Server access, failed logins
- Strong sa passwords
- Prefer Windows Authentication over SQL Authentication
- Restrict PUBLIC role
- Consider no guest access on production boxes

III. Data service

Concepts

- SQL Server data store mdf, ndf, ldf files
- SQL Server logs from audit, database mail, maintenance plans
- SQL Policy files

Data service
SQL Server 2008 Tools

- Transparent Data Encryption:
  - Encryption and Decryption at the database level using Database Encryption Key (DEK)
  - Transparent to the user application
- Extensible Key Management
  - Encryption key is stored and managed on an external device (Hardware Storage Module)
  - Encryption Decryption by HSM

demo

Data encryption using TDE

Karthik Bharathy
Program Manager
Microsoft

msdn Microsoft Developer Network

Microsoft TechNet

Data service

Best Practices

- Drop sample databases
- Built-in encryption functions
- T-SQL Procedure encryption
- Database encryption
- Extensible Key Management

IV. Application service
Concepts

- SQL Injection: Injecting vulnerable SQL code into an application query

- Types
  - Incorrectly escaped quotes
  - Time delays during execution
  - Conditional errors

SQL Injection sample code

```
' or 1=1 --

' union select @@VERSION

declare @query varchar (8000)
set @query =
0x73656C656374202A2066726F6D207379732E7365727665725F7072696E636970616C
732077686572652074797065206696E20282753272C27552729
exec(@query)

--select * from sys.server_principals where type in ('S','U')

select 1/0 from sys.server_principals where type in ('S','U')
and name='admin'
```

Application service
Best Practices

- Validate data passed as query input
  - Escape single quotes
- Use parameterization
- Check query strings composed on a ad-hoc basis
  - Use stored procedures
- Use tools like Microsoft Source Code Analyzer for SQL Injection
- Configure error reporting

Summary

- Take advantage of SQL Server 2008 security features
- Understand the different levels of threat in your environment
- Not every tool and configuration may be necessary
- Finally, note the chain is as strong as the weakest link

આભાર

ধন্যবাদ

நன்றி

ధన్యవాద

Thank You!

ಧನ್ಯವಾದಗಳು

ధన్యవాదాలు

ധന്യവാദ

ਧੰਨਵਾਦ

നിങ്ങൾക്ക് നന്ദി

question & answer

msdn Microsoft Developer Network

Microsoft TechNet

Related Content

Breakout Sessions (session codes and titles)

Interactive Theater Sessions (session codes and titles)

Hands-on Labs (session codes and titles)

Hands-on Labs (session codes and titles)

Track Resources

Resource 1

Resource 2

Resource 3

Resource 4

Microsoft®

Your potential. Our passion.™