



Hardening SQL Server

Craig Purnell

craig.purnell@gmail.com

PITTSBURGH TECHFEST

@CraigPurnell

About Me

“Data Guy”, Sr. Database Administrator, Consultant & MCT
16 years in IT, all of it in Database Administration & BackOffice ERP Infrastructure

Gardener, Night Photographer, & Boater

 craig.purnell@gmail.com

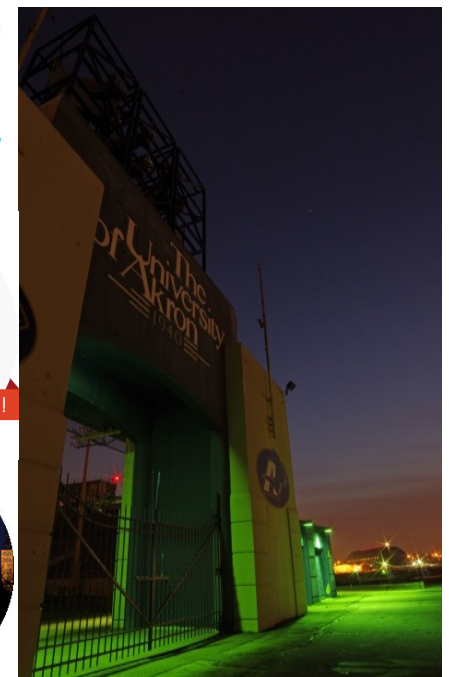
 @CraigPurnell



Program Committee
2011 - 2015



Microsoft
CERTIFIED
Trainer



Survey

- Are you a ?
 - Developer
 - Security Professional
 - DBA
 - Manager
 - Auditor / Compliance Professional
 - Security Consultant

2014, The Year of the Data Breach

- Not bubble gum and marbles anymore
- Organized Crime Online
- Stealing Data for Money
- Do you want to be on the front page?

Intro

- SQL Server Security used to be a joke
 - SQL Slammer (buffer overrun)
 - SQL Spida (DBA laziness)
 - Blank SA password
- Snicker, Snicker 😊 😊
- Slammer was over 12 years ago (I checked)
- We've come a long way, baby...

CVE Vulnerability List

- SQL Server : 75
- DB2 : 105
- mySQL : 243
- Oracle : 390

Microsoft » Sql Server : Vulnerability Statistics

[Vulnerabilities \(75\)](#) [CVSS Scores Report](#) [Browse all versions](#) [Possible matches for this product](#) [Related Metasploit Modules](#)

[Related OVAL Definitions](#) : [Vulnerabilities \(38\)](#) [Patches \(1\)](#) [Inventory Definitions \(15\)](#) [Compliance Definitions \(0\)](#)

[Vulnerability Feeds & Widgets](#)

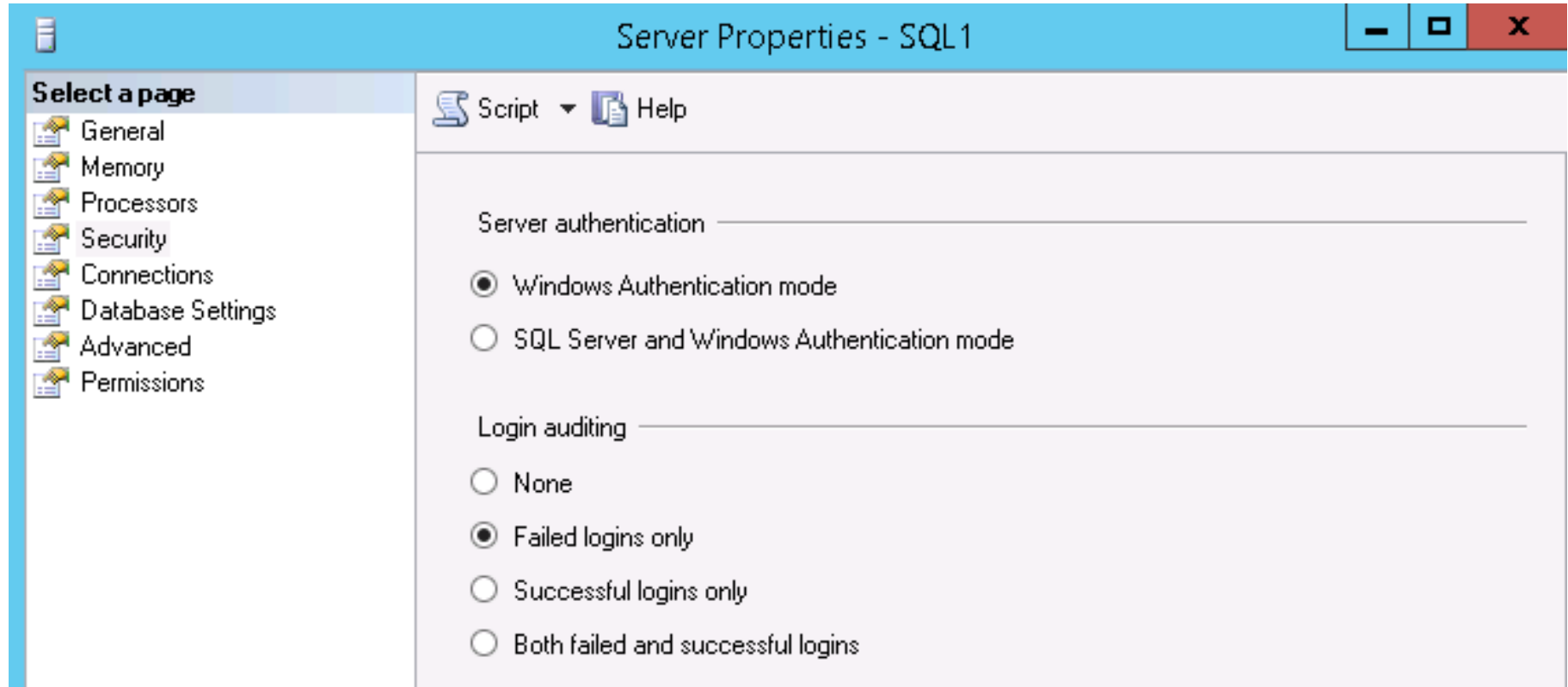
Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF
1999	1	1											
2000	6									1		1	
2001	12	10	9	1								1	
2002	24	5	12	10		2	1					2	
2003	3	1	1	1								1	
2004	1	1		1									
2007	2		1	1									
2008	11	2	10	9	2						1		
2009	8		8	6	3								
2011	1										1		
2012	3		2				1						
2014	2	1					1						
Total	74	21	43	29	5	2	3			1	2	6	
% Of All		28.4	58.1	39.2	6.8	2.7	4.1	0.0	0.0	1.4	2.7	8.1	0.0

Source: <http://www.cvedetails.com/index.php>

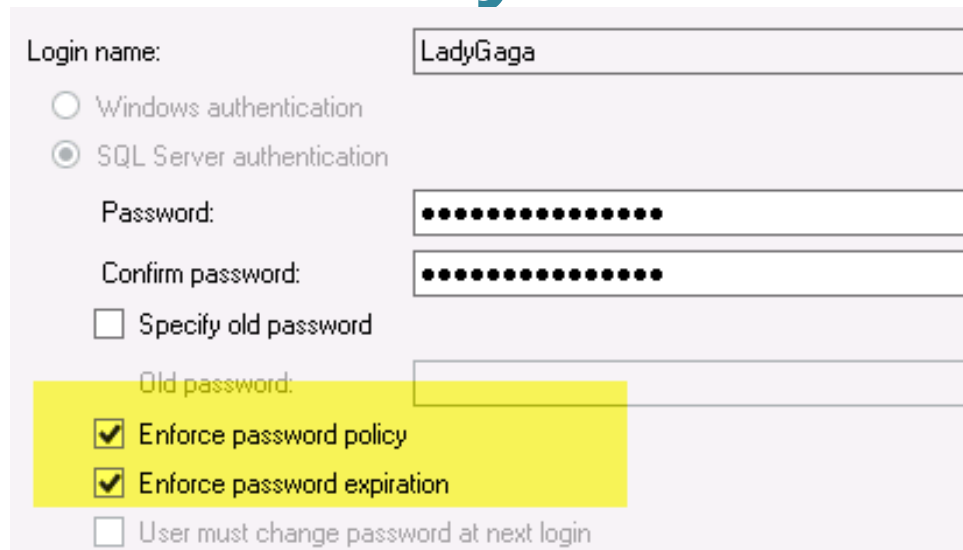
**Most Security Issues are Due to
Misconfiguration or Bad
Application Design**

Use Windows Authentication ¹



If you can....

Enforce Password Expiration/Policy on Mixed Mode



The screenshot shows the 'Log On' dialog box in SQL Server Enterprise Manager. The 'Login name' field contains 'LadyGaga'. Under the 'Authentication' section, 'SQL Server authentication' is selected with a radio button. The 'Password' and 'Confirm password' fields are filled with masked characters (dots). The 'Specify old password' checkbox is unchecked. The 'Old password' field is empty. A yellow highlight box covers the 'Enforce password policy' and 'Enforce password expiration' checkboxes, both of which are checked. The 'User must change password at next login' checkbox is unchecked.

Login name: LadyGaga

☐ Windows authentication
☒ SQL Server authentication

Password:

Confirm password:

☐ Specify old password

Old password:

☒ Enforce password policy
☒ Enforce password expiration

☐ User must change password at next login

- Most compliance authorities decry the use of Mixed Mode
- Most DBAs I know always configure it
- What if the application doesn't support it?
- What if the DBAs don't enforce it?

Mitigating Framework / Best Practices on Mixed Mode

- Monthly account audits
- Audit password strength on SQL logins
- Require password changes on SQL logins
 - 3rd party applications (Yes, you too)

The SA Login

- Equivalent of Administrator in Windows
- When installing SQL Server in Mixed mode, a password is required
- Should never be used for connecting from applications
- Usage violates the “distinct credential per person” guideline
- Forget it even exists

Rename & Disable SA

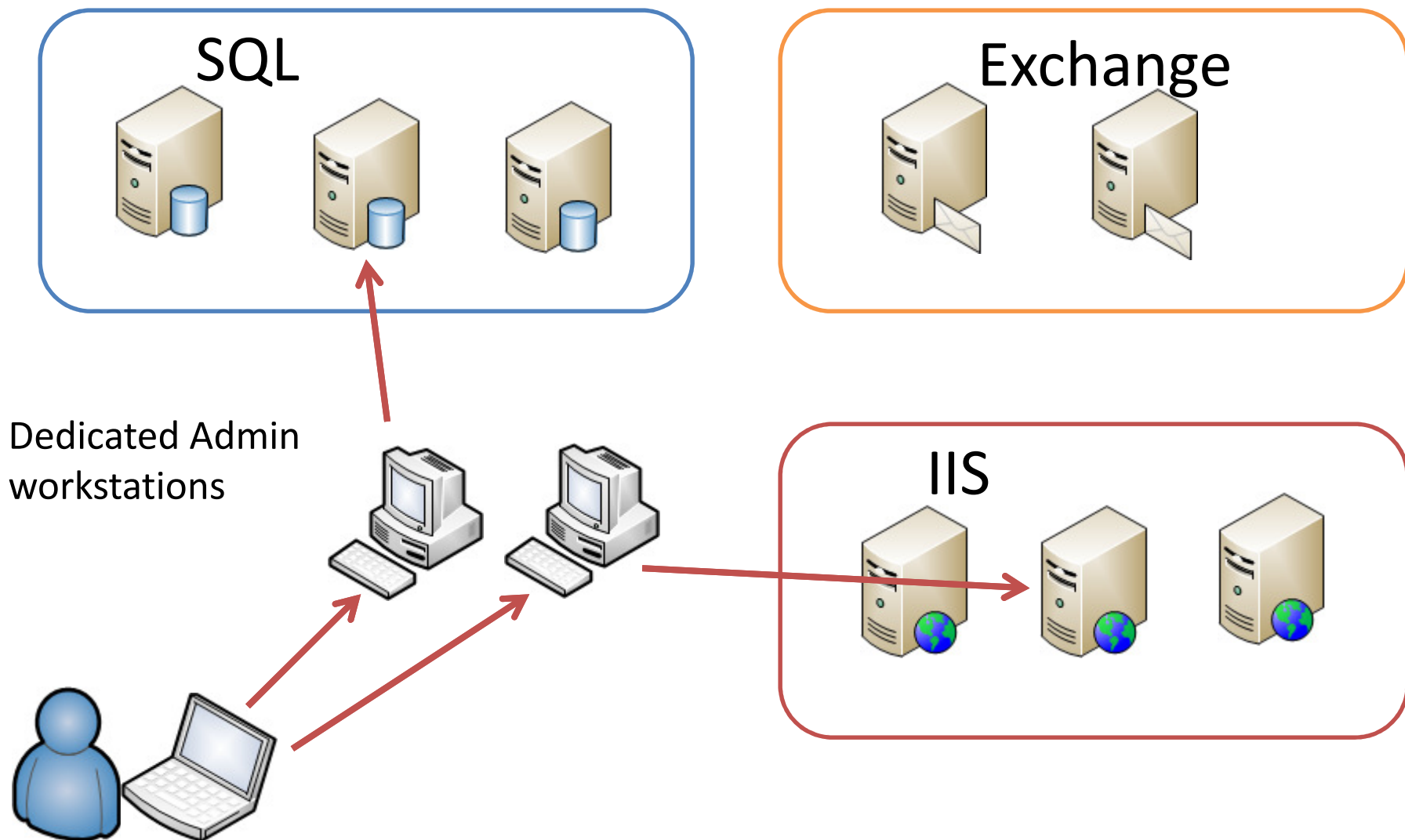
- Easy, low hanging fruit
- To harden your instance, rename the sa account
 - `ALTER LOGIN sa WITH NAME = [essay];`
- Create a honeypot sa
 - `CREATE LOGIN sa WITH PASSWORD = 'h@rdP@ssw0rd!';`
- Disable the sa account
 - `ALTER LOGIN essay DISABLE;`

Two Factor Authentication

- Something you know and something you carry
- Software based apps on smartphones or hard tokens
- Require for IT Admins in Positions of Trust
 - DBA team
 - System Administrators
 - Exchange / Sharepoint Admins
 - Network Admins



Server Zones / Jump Boxes



Encrypt Your Data



“The bottom line is that encryption does work...we need to not think of encryption as an arcane, dark art, but as basic protection for the digital world.”

-Edward Snowden

Your Encryption Toolkit

.NET Crypto API
On the Middle Tier

SQL Server

- Column (Cell) Level
- TDE (Transparent Data Encryption)
- Hashing

EFS (Encrypting File System)

File / Folder

BitLocker (Disk Volume)

SAN (MPIO, HBA, Switch, Drive)

Where to Encrypt?

- Can your DBAs see the data?
 - Default option
- Can your System Admins see the data?
 - Debug memory on the server
- Neither? Encrypt on a App Server
 - Hard to do
 - Key Management
 - Who do you trust?

Encrypting Client Connections^{5a}

- SSL/TLS via SQL Server Native Client
 - Secure Sockets Layer/Transport Layer Security
- IPSEC at the Windows OS level
 - Can be a good solution based on your architecture
 - Complex to set up and configure
- Extended Protection
 - Form of TLS, depending on configuration
- 3rd Party solutions
 - Unisys Stealth

Use Certificate for Encryption

Protocols for MSSQLSERVER Properties

Flags Certificate Advanced

☒ General

Force Encryption Yes

Hide Instance No

Force Encryption
Turn on or off encryption for selected server instance

OK Cancel Apply Help

Protocols for MSSQLSERVER Properties

Flags Certificate Advanced

Certificate: View... Clear

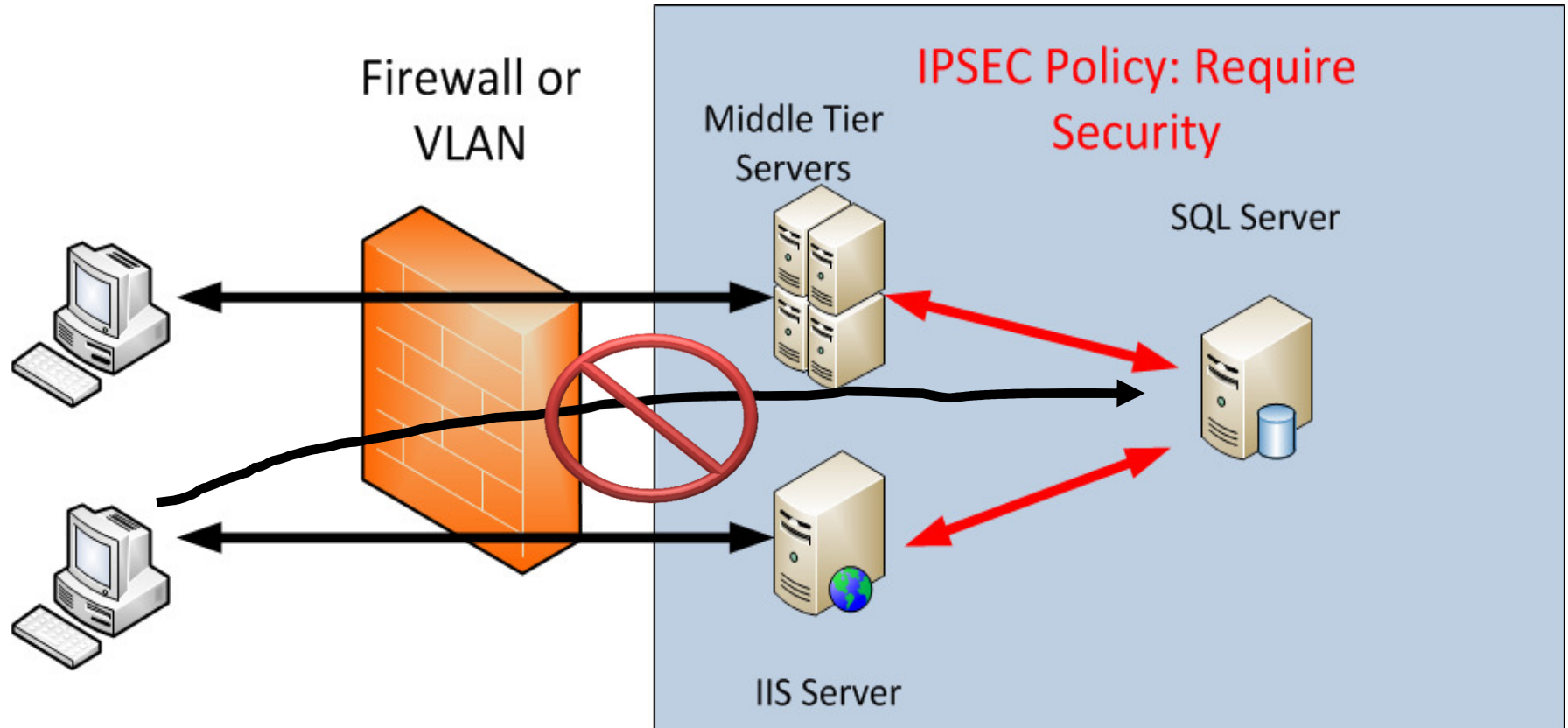
SQL2.ADATUM.COM

Expiration Date	9/14/2015
Friendly Name	
Issued By	COM, ADATUM, ADATUM-CA1-CA
Issued To	SQL2.ADATUM.COM

Expiration Date

OK Cancel Apply Help

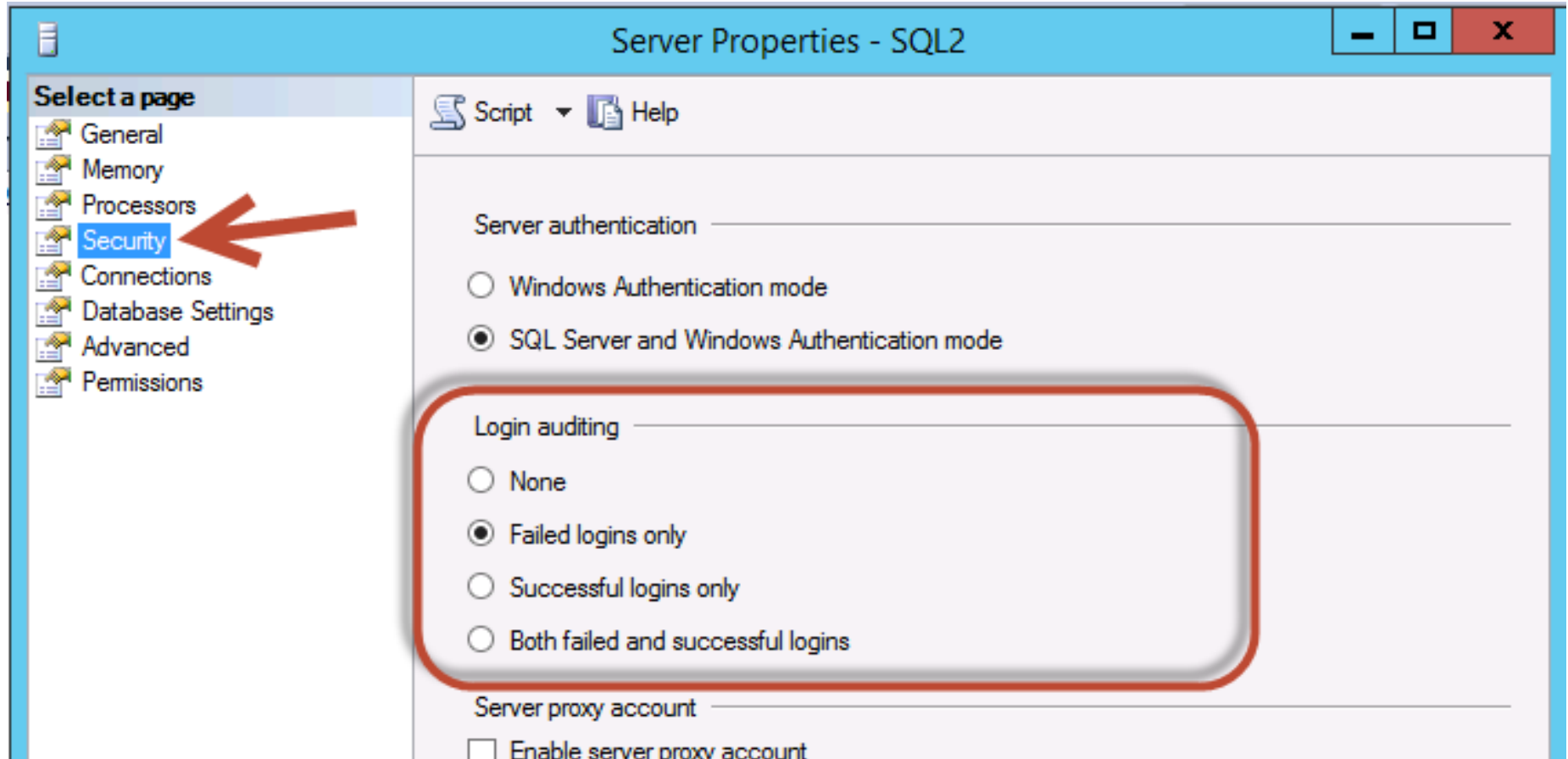
IPSEC with Screened Network



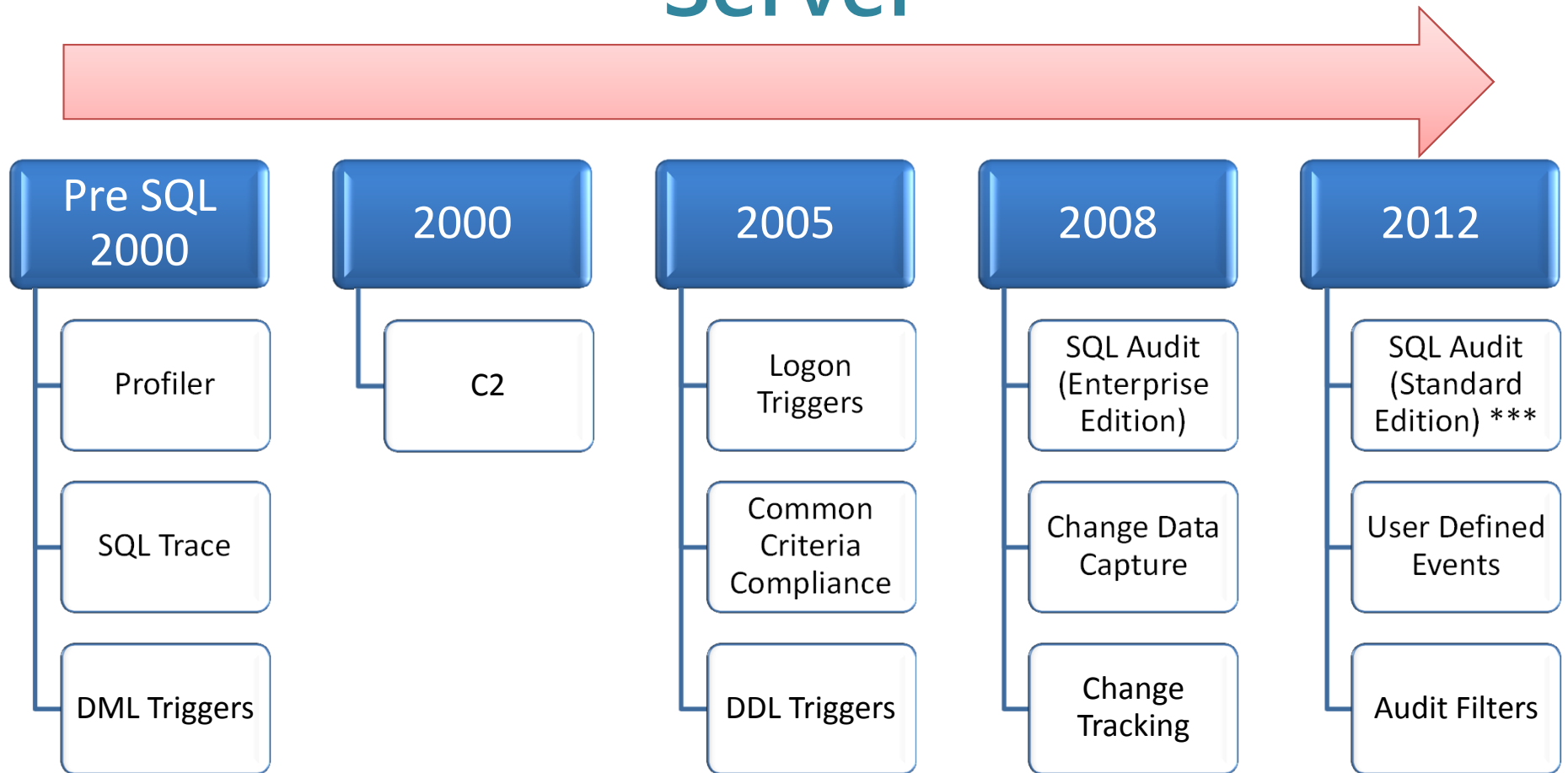
Turn On Auditing

- Track User Events
 - Schema changes
 - CREATE/ALTER/DROP object
 - Data changes
 - INSERT/UPDATE/DELETE
 - Table / View accesses
 - SELECT
- Security Events
 - LOGIN / LOGOUT server
 - CREATE / ALTER / DROP
 - DATABASE/LOGIN/USER/anything
 - Many, many more
- Determine unused Logins / Users
- Review Changes to the Server over time

Successful/Failed Logins

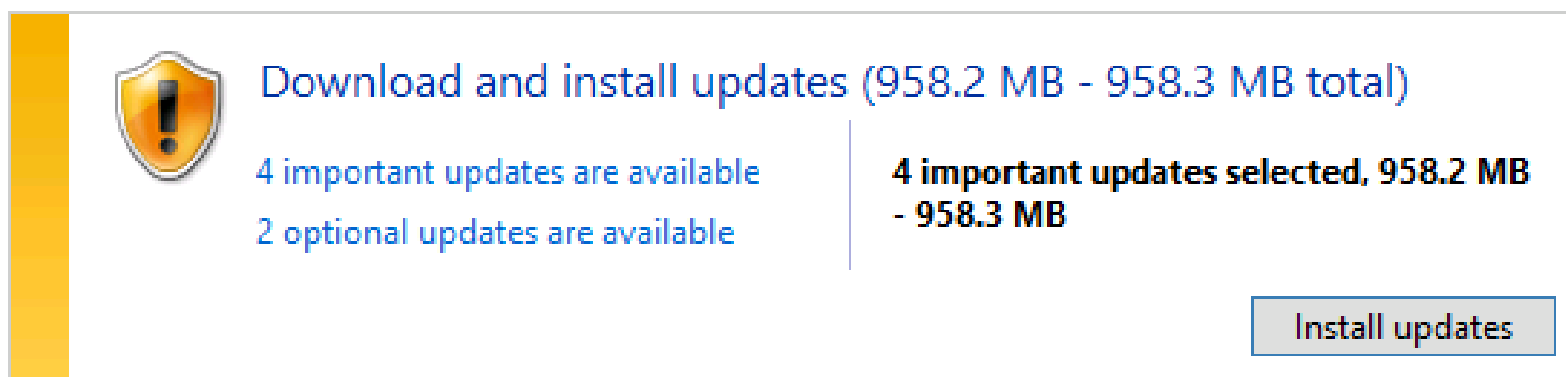


Evolution of Auditing in SQL Server



Patch Your Servers

Windows Update



A screenshot of a Windows Update notification window. It features a yellow vertical bar on the left and a shield icon with an exclamation mark. The main text reads 'Download and install updates (958.2 MB - 958.3 MB total)'. Below this, it states '4 important updates are available' and '2 optional updates are available'. To the right, it says '4 important updates selected, 958.2 MB - 958.3 MB'. At the bottom right, there is a button labeled 'Install updates'.

Download and install updates (958.2 MB - 958.3 MB total)

4 important updates are available
2 optional updates are available

4 important updates selected, 958.2 MB
- 958.3 MB

Install updates

Most recent check for updates: Today at 3:16 PM

Updates were installed: 7/6/2014 at 7:13 PM.

You receive updates: For Windows only.

- Don't forget to patch Java and Flash
- If it's not there, you don't have to patch it...

Do Vulnerability Scanning ^{7b}

- Rapid 7 NEXPOSE Community Edition (Free)
- Nessus Pro Eval (7 day trial)
- Others...

**Get written authorization
from management before
scanning on your network**










Random Administrator Passwords⁸

- **ALL** Server Infrastructure (not just SQL Server)
- Why?
- Pass – the - Hash attack
- What about the Client Side?
 - Administrator disabled out of the box since Vista
 - May be on via provisioning








Turn on the Firewall

The screenshot shows the 'Windows Firewall with Advanced Security' window in Windows 7. The title bar is blue and contains the text 'Windows Firewall with Advanced Security'. Below the title bar is a menu bar with 'File', 'Action', 'View', and 'Help'. The main content area has a blue header with 'Windows Firewall'. Below this is a breadcrumb navigation bar showing 'Control Panel > All Control Panel Items > Windows Firewall'. On the left side, there is a sidebar with links: 'Control Panel Home', 'Allow an app or feature through Windows Firewall', 'Change notification settings', 'Turn Windows Firewall on or off', 'Restore defaults', 'Advanced settings', and 'Troubleshoot my network'. The main content area has a heading 'Help protect your PC with Windows Firewall' followed by a paragraph: 'Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.' Below this is a table with three rows representing different network types: 'Domain networks' (Connected), 'Private networks' (Not connected), and 'Guest or public networks' (Not connected). Each row has a green shield icon on the left and a status indicator on the right. The 'Domain networks' row is expanded, showing details about the firewall state and active domain networks.

Help protect your PC with Windows Firewall	
Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.	
 Domain networks	Connected 
Networks at a workplace that are attached to a domain	
Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active domain networks:	 ADATUM.COM
Notification state:	Do not notify me when Windows Firewall blocks a new app
 Private networks	Not connected 
 Guest or public networks	Not connected 

Install and Configure Antivirus¹⁰

- Most Corporate Security Teams will Require A/V
- Set to Exclude:
 - *.mdf, *.ldf, *.ndf, *.bak, *.trn, *.sqlaudit, *.trc
- Important: Exclude SQLROOT folder

Name	Date modified	Type
 Backup	11/14/2013 10:50 ...	File folder
 Binn	5/31/2013 12:01 PM	File folder
 DATA	10/31/2014 10:02 ...	File folder
 FTData	5/31/2013 11:57 AM	File folder
 JOBS	3/5/2011 1:37 PM	File folder
 Log	6/11/2015 7:13 PM	File folder
 repldata	3/5/2011 1:37 PM	File folder

A/V SQL Server Links

- How to choose antivirus software to run on computers that are running SQL Server
 - <https://support.microsoft.com/en-us/kb/309422>
- Antivirus software that is not cluster-aware may cause problems with Cluster Services
 - <https://support.microsoft.com/en-us/kb/250355>
- Performance and consistency issues when certain modules are loaded into SQL Server address space ***
 - <https://support.microsoft.com/en-us/kb/2033238>
- Best Practices and Recommendations for A/V and SQL Server
 - http://blogs.technet.com/technet_blog_images/b/sql_server_sizing_ha_and_performance_hints/archive/2014/01/16/sql-server-and-anti-virus-best-practices-recommendations-for-exclusion-lists-for-anti-virus-scanner.aspx

Minimize Attack Surface

- SQL Server Configuration Manager (Local)
 - SQL Server Services
 - SQL Server Network Configuration
- SQL Native Client 11.0 Configuration
 - SQL Server Network Configuration
- Protocols for MSSQLSERVER
 - Protocols for SQLEXPRESS
- SQL Native Client 11.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled



Name	State	Start Mode	Log On As
SQL Full-text Filter Daemon Launcher (MSSQLSERVER)	Running	Manual	NT AUTHORITY\LOCALSERVICE
SQL Server (MSSQLSERVER)	Running	Manual	LocalSystem
SQL Server Browser	Stopped	Other (Boot, System...)	NT AUTHORITY\LOCALSERVICE
SQL Server Agent (MSSQLSERVER)	Stopped	Manual	LocalSystem

Review members of Fixed Server¹²

Roles

- SYSADMIN = Administrators Group
 - No permission checking
 - They can get you fired
 - Worse yet, they can get your CIO fired
- SecurityAdmin + Privilege escalation = Sysadmin
- Auditors usually have a problem with Sysadmin

Disable xp_cmdshell

13

- Allow you to obtain “OS Shell” access to Windows
- Nearly everyone agrees it’s a massive security hole
- Many of the compliance white papers specifically mention it

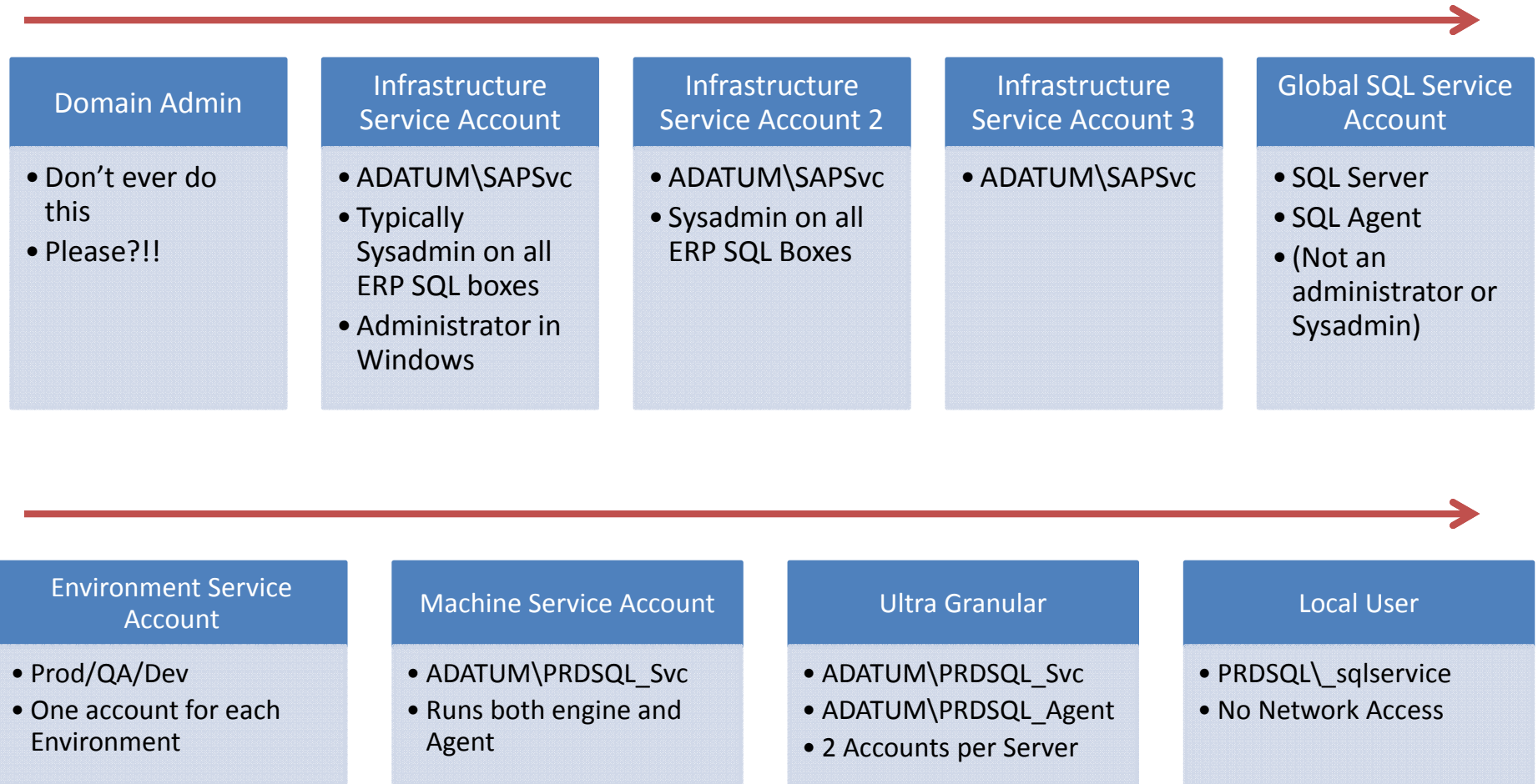
xp_cmdshell, Today

- 10 years ago, xp_cmdshell was relevant and useful to DBAs; *even with it's serious security concerns*
- Today, not so much...
- Why?
 - PowerShell, with and without remoting
 - Central Management Server
 - CLR

Service Account Overprivilege14

- Very common in the wild
- Domain Admin? Please no, Please no
- Local Administrators Group?
 - Common misconception, but not needed
- SQL Agent in Local Admin?
 - Documentation is Misleading
- Normal Domain User
- SQL Server 2008 R2, Virtual Accounts
- SQL Server 2012+, you can use MSA

Service Accounts Extremes



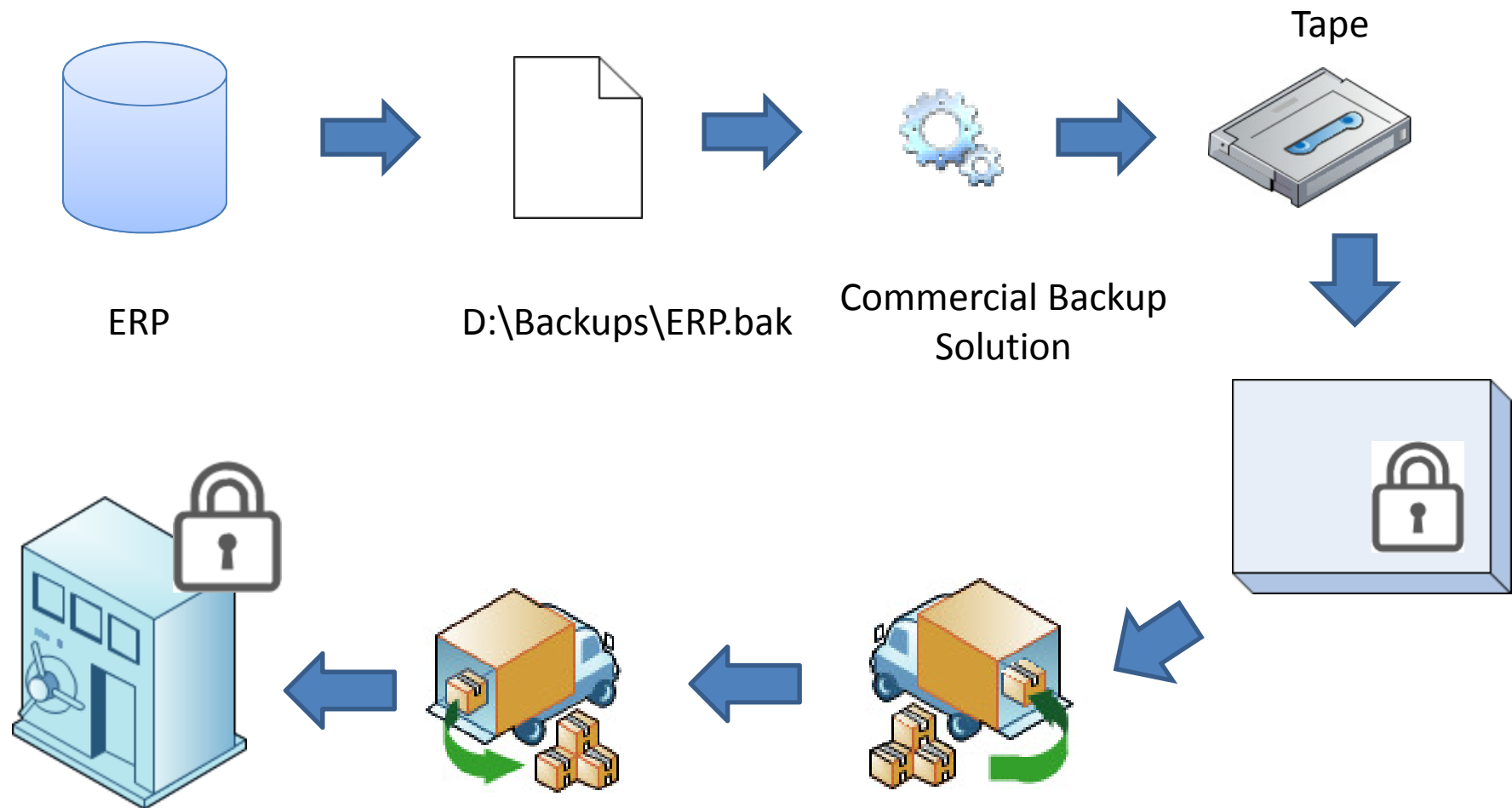
Domain Account Abuse and Misuse

- Password age policy (never expire)
- Password security (put it into Excel)
- Sharing of the password among admins
 - Auditability?
- What happens when someone leaves?
- Abuse and Misuse
 - Sharing across servers
 - Scope Abuse: Using it for things other than SQL Server (!)
 - Documenting / tracking where it is used and WHY?
 - Interactive Logins on Servers

New Options for Service Accounts

- Automatic Password Management
 - Really!
- Virtual Account
 - Managed Local Account
 - NT SERVICE\<instancename>
 - Windows Server 2008 R2 +
 - SQL Server 2012 +
 - Now the Default
- Managed Service Account (MSA)
 - Create in AD
 - DOMAIN\Accountname\$
- Group Managed Service Accounts (gMSA)
 - 1 account , many servers (think failover cluster)
 - Not officially supported for SQL Server

Review Backup Security 15



Any Problems with this?



- Are you encrypting your backups?
- Where?
- Who has access to the tapes?
- Who has access to the Backup Console?
- If disk-based SAN backup, who has access to the SAN?
- Who has access to the box?
- Is the truck secure?

<http://imgarcade.com/1/alfred-e-neuman-what-me-worry-poster/>

Backup Encryption

- Encrypted Backups: New in SQL Server 2014
- Previously a Side Effect of TDE
 - “You got it whether you wanted it or not”
- 3rd Party Backup software
 - Dell Litespeed
 - Idera SQLSafe
 - Red Gate SQL Backup
 - Commvault

Secure your Dev/QA

- Dev and QA are typically not as secure as Production
- Who has access?
- Is there PII or PHI data in those databases?
- Are you obfuscating sensitive data?

Wrap Up

- SQL Server is Secure out of the Box
- Most of the problems come with misconfiguration & poorly written applications
- Last line of defense against the bad guys

Thank You

Please don't forget to fill out an evaluation

Contact Information:



@CraigPurnell



<http://www.craigpurnell.com>




<http://www.linkedin.com/in/craigpurnell>



<http://about.me/craigpurnell>

Virtual Labs



Microsoft Virtual Labs:
SQL Server

Average star rating ★★★★★
Rate this lab ☺ ★★★★★

Lab Name: Exploring organizational security and auditing in SQL Server 2014

Lab Description: In this lab you will learn how to use SQL Server Audit, Contained Database authentication, user-defined server roles and new permissions.

System Requirements: <http://go.microsoft.com/?linkid=9834500>

Job Role: IT Pro

Lab Type: Virtual Hands on labs

[Get Started](#)

- Exploring organizational security and auditing in SQL Server 2014

Learn how to use SQL Server Audit, Contained Database authentication, user-defined server roles and new permissions.

<http://go.microsoft.com/?linkid=9852217>