

**THE DETAILS** listed below identify the missing security checks for each guideline and will help to give our prospects a “reality check” about potential vulnerabilities that may exist.

Guidelines	Missing Security Checks - Weaknesses	Covered by
<b>Roll your own?</b> <ul style="list-style-type: none"> <li>✓ What are your guidelines based on?</li> <li>✓ How do you know if you are checking for the right components</li> <li>✓ How do you confirm &amp; validate that your security settings are consistent in your SQL Server environment?</li> </ul>	<ul style="list-style-type: none"> <li>✓ Any SQL login have a blank password</li> <li>✓ SQL logins not using password policy</li> <li>✓ SQL logins not using expiration</li> <li>✓ Fixed roles assigned to public to public or guest</li> <li>✓ “sa” account allows blank password</li> <li>✓ xp_cmdshell enabled</li> <li>✓ SQL logins not using password policy</li> <li>✓ Sysadmins own trustworthy databases</li> </ul>	<ul style="list-style-type: none"> <li>– Idera Level-1 or Level-2 or Level-3 depending on environment. We bring a standardization process ,best practices to ensure that the right checks are in place.</li> </ul>
<b>MSBPA - Microsoft Best Practices Analyzer</b> <ul style="list-style-type: none"> <li>✓ Are you currently using this guideline to establish baselines for SQL Server?</li> <li>✓ Are you aware that using this guideline allows “blank” passwords for “ANY” SQL Server account?</li> <li>✓ 20 security checks in total</li> </ul>	<ul style="list-style-type: none"> <li>✓ Public server role has granted permissions</li> <li>✓ Dangerous extended stored procedures</li> <li>✓ Fixed roles assigned to public or guest</li> <li>✓ “sa” account not disabled</li> <li>✓ xp_cmdshell enabled</li> <li>✓ “sa” account allows blank password</li> <li>✓ Any SQL Server account has blank password</li> <li>✓ “sa” account not disabled or renamed</li> <li>✓ Executable file permissions not acceptable</li> <li>✓ Does everyone have read access to system tables</li> </ul>	<ul style="list-style-type: none"> <li>– Idera Level-1 BASIC guideline</li> <li>– MSBPA security checks</li> <li>– Plus additional checks</li> <li>– 37 security checks in total</li> </ul>
<b>CIS - Center for Internet Security</b> <ul style="list-style-type: none"> <li>✓ Are you currently using this guideline to establish baselines for SQL Server?</li> <li>✓ Are you aware that using this guideline leaves your environment open to SQL Injection &amp; Login intrusion?</li> <li>✓ 44 security checks in total</li> </ul>	<ul style="list-style-type: none"> <li>✓ Executables file permissions are not acceptable</li> <li>✓ “sa” account not using password policy</li> <li>✓ “sa” account not disabled</li> <li>✓ Does everyone have read access to system tables</li> <li>✓ Sysadmins own trustworthy databases</li> <li>✓ Public server role has been granted permissions</li> <li>✓ “sysadmin” own databases</li> <li>✓ Data files on system drives</li> <li>✓ Baseline data not being used</li> <li>✓ Does everyone have access to database files</li> </ul>	<ul style="list-style-type: none"> <li>– Idera Level-2 BALANCED guideline {default}</li> <li>– Includes Idera Level-1</li> <li>– MSBPA security checks</li> <li>– CIS security checks</li> <li>– Plus additional checks</li> <li>– 68 security checks in total</li> </ul>
<b>SRR - Security Readiness Review (DISA)</b> <ul style="list-style-type: none"> <li>✓ Are you currently using this guideline to establish baselines for SQL Server?</li> <li>✓ Are you aware that using this guideline leaves your environment open to SQL Injection &amp; Login intrusion?</li> <li>✓ 55 security checks in total</li> </ul>	<ul style="list-style-type: none"> <li>✓ “sa” account not disabled</li> <li>✓ Baseline data not being used</li> <li>✓ “sa” account not using password policy</li> <li>✓ OS version not at an acceptable level</li> <li>✓ Any permissions granted to public server role</li> <li>✓ Required administrative accounts do not exist</li> <li>✓ Sysadmins own trustworthy databases</li> <li>✓ xp_cmdshell proxy account exists</li> <li>✓ Unauthorized users have “ALTER TRACE” permission</li> <li>✓ Are system table updates allowed</li> </ul>	<ul style="list-style-type: none"> <li>– Idera Level-3 STRONG guideline</li> <li>– Includes CIS security checks</li> <li>– Includes MSBPA</li> <li>– Includes SRR</li> <li>– Includes Idera Level-2 BALANCED guideline</li> <li>– Plus additional checks</li> <li>– 84 security checks in total</li> </ul>

## SQL Server Intrusion - In The News !!

**Most Common Methods** - SQL Injection, Blank Passwords, Default Login IDs, Internally Abused Authority

[Common SQL Server Security Issues and Solutions](https://technet.microsoft.com) - Technet.microsoft.com

[Regulatory Agencies Issues Fines for Security Breaches](https://darkreading.com) - Database Security darkreading.com

[Super IT User Breaches HSBC Database](https://darkreading.com) - Database Security darkreading.com