Auditing Security Checks

The Auditing Security Checks take a look at auditing configuration for SQL Server databases and instances to ensure logs and events are running and properly setup.

The Auditing Security Checks available on the Configure the Policy section are the following:

Name	Description
C2 Audit Trace Enabled	Determine whether C2 Audit Trace is enabled on the SQL Server.
DISA Audit Configuration	The DISA/NIST specifications require a specific SQL Server trace to exist for auditing SQL Server use. Check to see if there are any traces outside of the existing default trace. Audit specification for DISA tracking to be used in place of a trace if trace does not exist.
Implement Change Data Capture	List databases that have Change Data Capture enabled.
Login Audit Level	Determine whether the SQL Server login auditing configuration is acceptable.
SQL Server Audit is Configured for Logins	SQL Server Audit is configured to record both failed and successful logins. This check is only valid for Enterprise Edition SQL Server 2008 R2 and above.
SQL Server Audit is in use	This check returns the name, status and target file locations of any SQL Server Audits that are on the server. In order for the results to be compliant with GDPR specifications, the audit should be enabled and recording data.