Unverschlüsselte LDAP-Verbindungen finden

Eventlog XML zum importieren

"Ldap_insecure.xml"

```
<ViewerConfig><QueryConfig><QueryParams><Simple><Channel>Directory
Service</Channel><EventId>2886,2887,2888,2889</EventId><RelativeTimeInf
o>0</RelativeTimeInfo><BySource>False</BySource></Simple></QueryParams>
<QueryNode><Name LanguageNeutralValue="LDAP Signing Events">LDAP
Signing Events</Name><Description>All events related to LDAP signing on
Domain Controllers</Description><QueryList><Query Id="0"
Path="Directory Service"><Select Path="Directory
Service">*[System[(EventID=2886 or EventID=2887 or EventID=2888 or
EventID=2889)]]</Select></Query></QueryList></QueryNode></QueryConfig><
ResultsConfig><Columns><Column Name="Level" Type="System.String"
Path="Event/System/Level" Visible="">190</Column><Column
Name="Keywords" Type="System.String"
Path="Event/System/Keywords">70</Column><Column Name="Date and Time"
Type="System.DateTime" Path="Event/System/TimeCreated/@SystemTime"
Visible="">240</Column><Column Name="Source" Type="System.String"
Path="Event/System/Provider/@Name" Visible="">235</Column><Column
Name="Event ID" Type="System.UInt32" Path="Event/System/EventID"
Visible="">150</Column><Column Name="Task Category"
Type="System.String" Path="Event/System/Task"
Visible="">151</Column><Column Name="User" Type="System.String"
Path="Event/System/Security/@UserID">50</Column><Column
Name="Operational Code" Type="System.String"
Path="Event/System/Opcode">110</Column><Column Name="Log"
Type="System.String" Path="Event/System/Channel">80</Column><Column
Name="Computer" Type="System.String"
Path="Event/System/Computer">170</Column><Column Name="Process ID"
Type="System.UInt32"
Path="Event/System/Execution/@ProcessID">70</Column><Column
Name="Thread ID" Type="System.UInt32"
Path="Event/System/Execution/@ThreadID">70</Column><Column
Name="Processor ID" Type="System.UInt32"
Path="Event/System/Execution/@ProcessorID">90</Column><Column
Name="Session ID" Type="System.UInt32"
Path="Event/System/Execution/@SessionID">70</Column><Column
Name="Kernel Time" Type="System.UInt32"
Path="Event/System/Execution/@KernelTime">80</Column><Column Name="User
Time" Type="System.UInt32"
Path="Event/System/Execution/@UserTime">70</Column><Column
Name="Processor Time" Type="System.UInt32"
Path="Event/System/Execution/@ProcessorTime">100</Column><Column
Name="Correlation Id" Type="System.Guid"
Path="Event/System/Correlation/@ActivityID">85</Column><Column
Name="Relative Correlation Id" Type="System.Guid"
Path="Event/System/Correlation/@RelatedActivityID">140</Column><Column
```

```
Name="Event Source Name" Type="System.String"
Path="Event/System/Provider/@EventSourceName">140</Column></Columns></R
esultsConfig></ViewerConfig>
```

EventID 2887 deutet auf unverschlüsselte Verbindungen hin, die Anzahl in den letzten 24 Stunden steht im Eventlog.

```
 # Enable Simple LDAP Bind Logging
Reg Add HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics /v "16 LDAP
Interface Events" /t REG_DWORD /d 2
```

```
 # Disable Simple LDAP Bind Logging.
Reg Add HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics /v "16 LDAP
Interface Events" /t REG_DWORD /d 0

Note: You may need replace the double quotes after copy+paste.
```