Event Logs

DCSync Related

Logs related to DCSync Credential attacks. This is a start but needs more filtering as there are tons of 4662 events.

```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">*[System[(EventID=4662)]]</Select>
  </Query>
</QueryList>
```

GPO Drive Map Troubleshooting

Source

```
<QueryList>
  <Query Id="0" Path="Microsoft-Windows-GroupPolicy/Operational">
    <Select Path="Microsoft-Windows-GroupPolicy/Operational">*[System[(EventID='4001')]]</Select>
    <Select Path="Microsoft-Windows-GroupPolicy/Operational">*[System[(EventID='5017')]]</Select>
    <Select Path="Microsoft-Windows-GroupPolicy/Operational">*[System[(EventID='5312')]]</Select>
    <Select Path="Microsoft-Windows-GroupPolicy/Operational">*[System[(EventID='4016')]]</Select>
  </Query>
</QueryList>
```

Recently installed software

This will only show software related installation events that are still stored in the system event log, so be mindful of the date of the last event log entry to know how far back logs are available.

```
Get-WinEvent -ProviderName MsiInstaller | where id -eq 1033 | select TimeCreated,Message | Format-List
```

Windows IP address conflict

```
<QueryList>
  <Query Id="0" Path="System">
    <Select Path="System">*[System[(EventID='4199')]]</Select>
  </Query>
</QueryList>
```

Log example:

```
The system detected an address conflict for IP address 10.X.Y.Z with the system having network hardware address 00-1F-FE-D8-31-00. Network operations on this system may be disrupted as a result.
```

Via PowerShell:

```
$query = @"
<QueryList>
  <Query Id="0" Path="System">
    <Select Path="System">*[System[(EventID='4199')]]</Select>
  </Query>
</QueryList>
"@

$ipConflictEvents = Get-WinEvent -FilterXml $query -Oldest
$ipConflictEvents | Format-Table
```

Windows RDP-Related Event Logs

Source

Below is a consolidated XML query of all of the event ids related in the above document. I have yet to have this actually solve a problem for me as of 5/30/2024. I still need to dive into the details of the individual log entries with different types and data.

```
<QueryList>
  <Query Id="0" Path="System">
    <Select Path="Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational">*</Select>
    <Select Path="Security">*[System[(EventID=4624)]]</Select>
    <Select Path="Security">*[System[(EventID=4625)]]</Select>
    <Select Path="Security">*[System[(EventID=4634)]]</Select>
    <Select Path="Security">*[System[(EventID=4647)]]</Select>
    <Select Path="Security">*[System[(EventID=4778)]]</Select>
    <Select Path="Security">*[System[(EventID=4779)]]</Select>
    <Select Path="System">*[System[(EventID=9009)]]</Select>
  </Query>
</QueryList>
```

#end

Revision #6
Created 30 May 2024 19:05:09 by bluecrow76
Updated 1 November 2024 19:13:19 by bluecrow76