


Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing


🔍


Sign in

Sign up

 OTRF / Set-AuditRule Public

🔔 Notifications

 Fork 23

 Star 88

<> Code

🕒 Issues 1

🔗 Pull requests


🎬 Actions

📁 Projects

🛡 Security

📊 Insights

📁 Files

 c3dec54

🔍

🔍 Go to file

> 📁 images

> 📁 resources

> 📁 rules

> 📁 activedirectory

> 📁 file

> 📁 registry

📄 aad\_connect\_health\_monitorin...

**📄 aad\_connect\_health\_service\_ag...**

📄 aad\_joined\_access\_attempts.yml

📄 autoruns.yml

📄 camera\_microphone\_access.yml

📄 default\_logon\_user\_discovery.y...

📄 environment\_variables\_discover...

📄 etw\_dotnet\_disable.yml

📄 laps.yml

📄 isa.yml

📄 powershell\_engine.yml

📄 powershell\_module\_logging.yml

📄 powershell\_scriptblog\_logging...

📄 powershell\_transcript.yml

📄 runmru\_discovery.yml

📄 sysmon\_config\_discovery.yml

📄 sysmon\_event\_channel\_deletio...

📄 system\_audit\_discovery.yml

📄 system\_policies\_discovery.yml

📄 typed\_urls\_discovery.yml

📄 wef\_subscription\_manager\_dis...


📄 windows\_telemetry\_persistenc...

📄 winlogon\_discovery.yml



📄 LICENSE

📄 README.md

📄 Set-AuditRule.ps1

Set-AuditRule / rules / registry / aad\_connect\_health\_service\_agent.yml 

...


 **Cyb3rWard0g** updated name of aad connect health monitoring agent 0a0c333 · 3 years ago  History


Code


Blame

20 lines (20 loc) · 806 Bytes

Raw







1

title: Azure AD Connect Health Service Agent

2

id: b3068822-704a-43a8-8b6f-970148462c8d

3

status: experimental

4

description: A threat actor might want to read information about the Azure AD connect h

5

references:

6

- https://o365blog.com/post/hybridhealthagent/

7

- https://github.com/Gerenios/AADInternals/blob/master/HybridHealthServices\_utils.p

8

author: Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC R&D

9

date: 2020/06/07

10

rule\_category: registry

11

rule:

12

registry\_paths:

13

- 'HKLM:\SOFTWARE\Microsoft\ADHealthAgent'

14

well\_known\_sid\_type: BuiltinAdministratorsSid

15

rights:

16

- ReadKey

17

inheritance\_flags: ContainerInherit

18

propagation\_flags: None

19

audit\_flags:

20

- Success

Page 1 of 2

