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_discove...
    - etw_dotnet_disable.yml
    - laps.yml
    - lsa.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_monitoring_agent.yml

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

Code Blame 20 lines (20 loc) · 805 Bytes Raw

```yaml
title: Azure AD Connect Health Monitoring Agent
id: e6393e38-6c3e-4bce-8696-3d72d37c2ec2
status: experimental
description: A threat actor might want to read information about the endpoint Microsoft
references:
    - https://o365blog.com/post/hybridhealthagent/
    - https://github.com/Gerenios/AADInternals/blob/master/HybridHealthServices_utils.p
author: Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research), MSTIC R&D
date: 2020/08/25
rule_category: registry
rule:
    registry_paths:
        - 'HKLM:\SOFTWARE\Microsoft\Microsoft Online\Reporting\MonitoringAgent'
    well_known_sid_type: BuiltinAdministratorsSid
    rights:
        - ReadKey
    inheritance_flags: None
    propagation_flags: None
    audit_flags:
        - Success
```