NIST CSF 2.0-PR.IR-01-Ex4

PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used

Technology Infrastructure Resilience (PR.IR)

Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience

PR.IR-01

Networks and environments are protected from unauthorized logical access and usage

Ex4

Check the cyber health of endpoints before allowing them to access and use production resources

Compliance Framework References:

CCMv4.0: AIS-04
CCMv4.0: AIS-06
CCMv4.0: DCS-12
CCMv4.0: DSP-10
CCMv4.0: DSP-15
CCMv4.0: IVS-03
CCMv4.0: IVS-05
CCMv4.0: IVS-06
CCMv4.0: IVS-09
CCMv4.0: UEM-05
CCMv4.0: UEM-14
CIS Controls v8.0: 3.12
CIS Controls v8.0: 12.2
CRI Profile v2.0: PR.IR-01
CRI Profile v2.0: PR.IR-01.01
CRI Profile v2.0: PR.IR-01.02
CRI Profile v2.0: PR.IR-01.03
CRI Profile v2.0: PR.IR-01.04
CRI Profile v2.0: PR.IR-01.05
CRI Profile v2.0: PR.IR-01.06
CRI Profile v2.0: PR.IR-01.07
CRI Profile v2.0: PR.IR-01.08
CSF v1.1: PR.AC-3
CSF v1.1: PR.AC-5
CSF v1.1: PR.DS-7
CSF v1.1: PR.PT-4
SP 800-218: PO.5.1
SP 800-53 Rev 5.1.1: AC-03
SP 800-53 Rev 5.1.1: AC-04
SP 800-53 Rev 5.1.1: SC-04
SP 800-53 Rev 5.1.1: SC-05
SP 800-53 Rev 5.1.1: SC-07

Vendor: Microsoft Azure

Comments: This requirement is very similar to PR.AA-05 Ex2, may be able to be satisfied by evidence from that Subcategory/Example. As such, the description is duplicated here, and this is shown as a linked query. Should there be other queries that are more specific, they will listed. In either case, it is recommended to used the evidence from the linked query in addition to any support queries listed here.

Description for PR.AA-05 Ex2: Evidence should be available based on the type of authenication log. For example, it would be expected to see this type of validation information in log types like Microsoft Entra

Conditional Access as it tests specifically for qualifying conditions to ensure and entity may access a device or service.

UDM Search Query:

```
$user = $e.target.user.userid
$user = /.*/
$e.additional.fields["conditionalAccessStatus"] = "success"

match:
    $user

outcome:
    $applications = array_distinct($e.target.application )
    $country = array_distinct($e.principal.location.country_or_region)
    $state = array_distinct($e.principal.location.state)
                                                    $compliant              =
array_distinct(if($e.principal.asset.attribute.labels["isCompliant"]        =
"true", "true", "false"))
```

10-20-2024

hostname	destip	count
calm-orion-8112	207.3.50.185	7088
loud-blaze-4706	37.198.57.90	875
eager-glyph-3607	41.249.102.22	3152
tough-zephyr-6801	162.195.41.129	8183
keen-bear-2972	18.240.44.191	9823
warm-fox-0927	42.28.42.216	9220
lively-lion-7689	191.95.195.233	5858
calm-glyph-5246	178.93.96.212	8215
nifty-meteor-5590	112.40.225.248	4566
rich-ember-2213	129.112.53.246	1836

09-20-2024

hostname	destip	count
calm-orion-8112	207.3.50.185	7088
loud-blaze-4706	37.198.57.90	875
eager-glyph-3607	41.249.102.22	3152
tough-zephyr-6801	162.195.41.129	8183
keen-bear-2972	18.240.44.191	9823
warm-fox-0927	42.28.42.216	9220
lively-lion-7689	191.95.195.233	5858
calm-glyph-5246	178.93.96.212	8215
nifty-meteor-5590	112.40.225.248	4566
rich-ember-2213	129.112.53.246	1836

08-20-2024

hostname	destip	count
calm-orion-8112	207.3.50.185	7088
loud-blaze-4706	37.198.57.90	875
eager-glyph-3607	41.249.102.22	3152
tough-zephyr-6801	162.195.41.129	8183
keen-bear-2972	18.240.44.191	9823
warm-fox-0927	42.28.42.216	9220
lively-lion-7689	191.95.195.233	5858
calm-glyph-5246	178.93.96.212	8215
nifty-meteor-5590	112.40.225.248	4566
rich-ember-2213	129.112.53.246	1836