NIST CSF 2.0-PR.AA-05-Ex2

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

Identity Management, Authentication, and Access Control (PR.AA)

Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access

PR.AA-05

Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties

Ex2

Take attributes of the requester and the requested resource into account for authorization decisions (e.g., geolocation, day/time, requester endpoint's cyber health)

Compliance Framework References:

CCMv4.0: CCC-04
CCMv4.0: CEK-10
CCMv4.0: CEK-11
CCMv4.0: CEK-12
CCMv4.0: CEK-13
CCMv4.0: CEK-14
CCMv4.0: CEK-15
CCMv4.0: CEK-16
CCMv4.0: CEK-17
CCMv4.0: CEK-18
CCMv4.0: CEK-19
CCMv4.0: CEK-20
CCMv4.0: CEK-21
CCMv4.0: IAM-01
CCMv4.0: IAM-03
CCMv4.0: IAM-04
CCMv4.0: IAM-05
CCMv4.0: IAM-06
CCMv4.0: IAM-07
CCMv4.0: IAM-08
CCMv4.0: IAM-09
CCMv4.0: IAM-10
CCMv4.0: IAM-11
CCMv4.0: IAM-12
CCMv4.0: IAM-16
CCMv4.0: IVS-03
CCMv4.0: IVS-06
CCMv4.0: LOG-02
CCMv4.0: LOG-04
CCMv4.0: LOG-09
CCMv4.0: UEM-05
CCMv4.0: UEM-14
CIS Controls v8.0: 3.3
CIS Controls v8.0: 6.8
CRI Profile v2.0: PR.AA-05
CRI Profile v2.0: PR.AA-05.01
CRI Profile v2.0: PR.AA-05.02
CRI Profile v2.0: PR.AA-05.03
CRI Profile v2.0: PR.AA-05.04

CSF v1.1: PR.AC-1
CSF v1.1: PR.AC-3
CSF v1.1: PR.AC-4
SP 800-218: PO.5.2
SP 800-218: PS.1.1
SP 800-53 Rev 5.1.1: AC-01
SP 800-53 Rev 5.1.1: AC-02
SP 800-53 Rev 5.1.1: AC-03
SP 800-53 Rev 5.1.1: AC-05
SP 800-53 Rev 5.1.1: AC-06
SP 800-53 Rev 5.1.1: AC-10
SP 800-53 Rev 5.1.1: AC-16
SP 800-53 Rev 5.1.1: AC-17
SP 800-53 Rev 5.1.1: AC-18
SP 800-53 Rev 5.1.1: AC-19
SP 800-53 Rev 5.1.1: AC-24
SP 800-53 Rev 5.1.1: IA-13

Vendor: Microsoft Azure

Comments: 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.

Note: Query is specific to Entra ID.

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