NIST CSF 2.0-PR.AA-04-Ex1

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-04

Identity assertions are protected, conveyed, and verified

Ex1

Protect identity assertions that are used to convey authentication and user information through single sign-on systems

Compliance Framework References:

CCMv4.0: IAM-01
CCMv4.0: IAM-03
CCMv4.0: IAM-16
CRI Profile v2.0: PR.AA-04
CRI Profile v2.0: PR.AA-04.01
SP 800-53 Rev 5.1.1: IA-13

Vendor: Microsoft Azure

Comments: SAML assertions should be able to be discoverable by different authentication and SSO providers. However, this is likely dependent on how well the related parser has been implemented in the SIEM. So, it may require custom queries to discover the necessary evidence.

Note: This is Entra Active DIrectory, and relies on Entra's Conditional Access functionality. This requires an Entra ID P1 or P2 subscription for each user for data to populate.

UDM Search Query:

```
$user = $e.target.user.userid
$user = /.*/
$loginType = $e.extensions.auth.type
$loginType = "SSO"
$e.additional.fields["conditionalAccessStatus"] = "success"

match:
    $user

outcome:
    $applications = array_distinct($e.target.application )
```

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