NIST CSF 2.0-PR.AA-03-Ex3

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-03

Users, services, and hardware are authenticated

Ex3

Periodically reauthenticate users, services, and hardware based on risk (e.g., in zero trust architectures)

Compliance Framework References:

CCMv4.0: DCS-08
CCMv4.0: IAM-01
CCMv4.0: IAM-02
CCMv4.0: IAM-14
CCMv4.0: IAM-16
CCMv4.0: IVS-03
CCMv4.0: UEM-05
CCMv4.0: UEM-06
CCMv4.0: UEM-14
CRI Profile v2.0: PR.AA-03
CRI Profile v2.0: PR.AA-03.01
CRI Profile v2.0: PR.AA-03.02
CRI Profile v2.0: PR.AA-03.03
CSF v1.1: PR.AC-3
CSF v1.1: PR.AC-7
SP 800-218: PO.5.2
SP 800-53 Rev 5.1.1: AC-07
SP 800-53 Rev 5.1.1: AC-12
SP 800-53 Rev 5.1.1: IA-02
SP 800-53 Rev 5.1.1: IA-03
SP 800-53 Rev 5.1.1: IA-05
SP 800-53 Rev 5.1.1: IA-07
SP 800-53 Rev 5.1.1: IA-08
SP 800-53 Rev 5.1.1: IA-09
SP 800-53 Rev 5.1.1: IA-10
SP 800-53 Rev 5.1.1: IA-11

Vendor: Agnostic

Comments: Evidence would likely need to be acquired by configuration review. However, it should be possible to verify that entities are reauthenticated peridiocally via the logs.

Note: Current version creates a row per user, and then has a list of all applications and the total count of ALLOW eventsf ro USER_LOGIN. This does NOT separate each application for login count to be shown per application.

UDM Search Query:

```
$user = $e.target.user.userid
$user = /.*/
$e.metadata.event_type = "USER_LOGIN"
$e.security_result.action = "ALLOW"

match:
    $user over 24h

outcome:
    $targetApplication = array_distinct($e.target.application)
    $timesAuthenticated = count($e.target.application)

limit:  100
```

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