NIST CSF 2.0-PR.AA-04-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-04

Identity assertions are protected, conveyed, and verified

Ex2

Protect identity assertions that are used to convey authentication and user information between federated 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: Agnostic

Comments: SAML assertions should be able to provide this information in logs. However, this will likely take in depth research to discover the necessary logs. Additionally, it is likely this may require a custom query to discover the evidence.

Note: This has been tested with Okta, but should be usable with any SAML IdP.

UDM Search Query:

```
($e.target.application = /SAML/ OR
    $e.target.resource.name = /SAML/ OR
    $e.extensions.auth.type = "SSO" OR
    $e.metadata.product_name = /SSO/ nocase )

$user_id = group($e.principal.user.userid, $e.target.user.userid)

$date = timestamp.get_date($e.metadata.event_timestamp.seconds)

$e.target.application != ""

$e.security_result.action = "ALLOW"

match:
    $user_id

outcome:
    $vendor = array_distinct($e.metadata.vendor_name)
    $application = array_distinct($e.target.application)

order:
    $user_id

limit: 25
```

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