NIST CSF 2.0-PR.PS-04-Ex1

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

Platform Security (PR.PS)

The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability

PR.PS-04

Log records are generated and made available for continuous monitoring

Ex1

Configure all operating systems, applications, and services (including cloud-based services) to generate log records

Compliance Framework References:

CCMv4.0: IAM-16
CCMv4.0: LOG-01
CCMv4.0: LOG-02
CCMv4.0: LOG-03
CCMv4.0: LOG-04
CCMv4.0: LOG-05
CCMv4.0: LOG-07
CCMv4.0: LOG-08
CCMv4.0: LOG-10
CCMv4.0: LOG-11
CCMv4.0: LOG-12
CCMv4.0: LOG-13
CIS Controls v8.0: 8.2
CRI Profile v2.0: PR.PS-04
CRI Profile v2.0: PR.PS-04.01
CRI Profile v2.0: PR.PS-04.02
CRI Profile v2.0: PR.PS-04.03
CSF v1.1: PR.PT-1
SP 800-218: PO.3.3
SP 800-53 Rev 5.1.1: AU-02
SP 800-53 Rev 5.1.1: AU-03
SP 800-53 Rev 5.1.1: AU-06
SP 800-53 Rev 5.1.1: AU-07
SP 800-53 Rev 5.1.1: AU-11
SP 800-53 Rev 5.1.1: AU-12

Vendor: Agnostic

Comments: Each device and the corresponding logs can be listed for reviewing against a standard inventory. Similarly, all cloud service logs will be listed as well. Comparison afterwards may require manual review as a spreadsheet.

Note: This needs to be tested against a source that has NXLog sending multiple log types.

UDM Search Query:

```
$host = $e.principal.hostname
$host = /.*/

match:
    $host

outcome:
    $logtypes = array_distinct($e.metadata.log_type)
```

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