NIST CSF 2.0-ID.AM-02-Ex1

IDENTIFY (ID): The organization's current cybersecurity risks are understood

Asset Management (ID.AM)

Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy

ID.AM-02

Inventories of software, services, and systems managed by the organization are maintained

Ex1

Maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source, custom applications, API services, and cloud-based applications and services

Compliance Framework References:

CCMv4.0: CCC-04
CCMv4.0: DCS-06
CCMv4.0: DSP-19
CCMv4.0: UEM-02
CCMv4.0: UEM-04
CIS Controls v8.0: 2.1
CRI Profile v2.0: ID.AM-02
CRI Profile v2.0: ID.AM-02.01
CSF v1.1: ID.AM-2
SP 800-221A: MA.RI-1
SP 800-53 Rev 5.1.1: AC-20
SP 800-53 Rev 5.1.1: CM-08
SP 800-53 Rev 5.1.1: PM-05
SP 800-53 Rev 5.1.1: SA-05
SP 800-53 Rev 5.1.1: SA-09

Vendor: Agnostic

Comments: All log data sources can be pulled for applications, hosts, and cloud technologies sending logs. Software names should be able to be ingested if there is a parser as the field about.asset.software.name exists.

Note: The following query is syntatically correct, but there was no data source that correctly parses to the about.asset.software.name UDM field.

UDM Search Query:

```
$software = $e.about.asset.software.name
$software = /.*/

match:
    $software

outcome:
    $softwareVendor = array_distinct($e.about.asset.software.vendor_name)
    $softwareVersion = array_distinct($e.about.asset.software.version)
                                          $softwareDescription          =
array_distinct($e.about.asset.software.description)

order:
    $software
```

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