NIST CSF 2.0-ID.RA-01-Ex1

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

Risk Assessment (ID.RA)

The cybersecurity risk to the organization, assets, and individuals is understood by the organization

ID.RA-01

Vulnerabilities in assets are identified, validated, and recorded

Ex1

Use vulnerability management technologies to identify unpatched and misconfigured software

Compliance Framework References:

CCMv4.0: AIS-05
CCMv4.0: AIS-07
CCMv4.0: TVM-01
CCMv4.0: TVM-03
CCMv4.0: TVM-05
CCMv4.0: TVM-06
CCMv4.0: TVM-07
CCMv4.0: TVM-08
CCMv4.0: TVM-09
CCMv4.0: TVM-10
CIS Controls v8.0: 7.1
CRI Profile v2.0: ID.RA-01
CRI Profile v2.0: ID.RA-01.01
CRI Profile v2.0: ID.RA-01.02
CRI Profile v2.0: ID.RA-01.03
CSF v1.1: ID.RA-1
CSF v1.1: PR.IP-12
CSF v1.1: DE.CM-8
SP 800-218: PO.5.2
SP 800-221A: MA.RI-3
SP 800-53 Rev 5.1.1: CA-02
SP 800-53 Rev 5.1.1: CA-07
SP 800-53 Rev 5.1.1: CA-08
SP 800-53 Rev 5.1.1: RA-03
SP 800-53 Rev 5.1.1: RA-05
SP 800-53 Rev 5.1.1: SA-11(02)
SP 800-53 Rev 5.1.1: SA-15(07)
SP 800-53 Rev 5.1.1: SA-15(08)
SP 800-53 Rev 5.1.1: SI-04
SP 800-53 Rev 5.1.1: SI-05

Vendor: Agnostic

Comments: This requires a vulnerability scanning technology that can upload vulnerability results to SecOps. For example: Tenable.io or Qualys.

UDM Search Query:

```
$vulnerability = $e.about.asset.vulnerabilities.name
$vulnerability = /.*/

match:
    $vulnerability

outcome:
    $hostname = array_distinct($e.about.asset.hostname)
    $vendor = array_distinct($e.about.asset.vulnerabilities.vendor)
    $severity = array_distinct($e.about.asset.vulnerabilities.severity)
                                                    $lastScan              =
timestamp.get_date(max($e.about.asset.vulnerabilities.last_found.seconds))

order:
    $hostname
```

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