

NIST CSF 2.0-DE.CM-01-Ex5

DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed
Continuous Monitoring (DE.CM)

Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events

DE.CM-01

Networks and network services are monitored to find potentially adverse events

Ex5

Monitor network communications to identify changes in security postures for zero trust purposes

Compliance Framework References:

CCMv4.0: IVS-03

CCMv4.0: IVS-09

CCMv4.0: LOG-01

CCMv4.0: LOG-03

CCMv4.0: LOG-05

CCMv4.0: LOG-08

CCMv4.0: TVM-02

CCMv4.0: TVM-10

CCMv4.0: UEM-10

CIS Controls v8.0: 13.1

CRI Profile v2.0: DE.CM-01

CRI Profile v2.0: DE.CM-01.01

CRI Profile v2.0: DE.CM-01.02

CRI Profile v2.0: DE.CM-01.03

CRI Profile v2.0: DE.CM-01.04

CRI Profile v2.0: DE.CM-01.05

CRI Profile v2.0: DE.CM-01.06

CSF v1.1: DE.CM-1

CSF v1.1: DE.CM-4

CSF v1.1: DE.CM-5

CSF v1.1: DE.CM-7

SP 800-53 Rev 5.1.1: AC-02

SP 800-53 Rev 5.1.1: AU-12

SP 800-53 Rev 5.1.1: CA-07

SP 800-53 Rev 5.1.1: CM-03

SP 800-53 Rev 5.1.1: SC-05

SP 800-53 Rev 5.1.1: SC-07

SP 800-53 Rev 5.1.1: SI-04

Vendor: CustomRequired

Comments: This would require creating custom queries for the specific zero trust vendor to identify specific properties that may have changed.

UDM Search Query:

None

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