NIST CSF 2.0-DE.CM-03-Ex3

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-03

Personnel activity and technology usage are monitored to find potentially adverse events

Ex3

Continuously monitor deception technology, including user accounts, for any usage

Compliance Framework References:

CCMv4.0: LOG-01
CCMv4.0: LOG-03
CCMv4.0: LOG-05
CCMv4.0: LOG-08
CCMv4.0: TVM-10
CIS Controls v8.0: 10.7
CRI Profile v2.0: DE.CM-03
CRI Profile v2.0: DE.CM-03.01
CRI Profile v2.0: DE.CM-03.02
CRI Profile v2.0: DE.CM-03.03
CSF v1.1: DE.CM-3
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: AU-13
SP 800-53 Rev 5.1.1: CA-07
SP 800-53 Rev 5.1.1: CM-10
SP 800-53 Rev 5.1.1: CM-11

Vendor: CustomRequired

Comments: Deception technologies are vendor specific and require specific queries. The most common deception technology is Thinkst Canary.

A subscription to Thinkst is required, but unavailable for a UDM.

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