NIST CSF 2.0-DE.AE-03-Ex1

DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed

Adverse Event Analysis (DE.AE)

Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents

DE.AE-03

Information is correlated from multiple sources

Ex1

Constantly transfer log data generated by other sources to a relatively small number of log servers

Compliance Framework References:

CCMv4.0: LOG-03
CCMv4.0: LOG-05
CCMv4.0: SEF-05
CRI Profile v2.0: DE.AE-03
CRI Profile v2.0: DE.AE-03.01
CRI Profile v2.0: DE.AE-03.02
CSF v1.1: DE.AE-3
SP 800-53 Rev 5.1.1: AU-06
SP 800-53 Rev 5.1.1: CA-07
SP 800-53 Rev 5.1.1: PM-16
SP 800-53 Rev 5.1.1: IR-04
SP 800-53 Rev 5.1.1: IR-05
SP 800-53 Rev 5.1.1: IR-08
SP 800-53 Rev 5.1.1: SI-04

Vendor: Agnostic

Comments: The UDM query will show multiple servers and the quantity of log events that they have been sent over a period of time.

Note: This is an indiscriminant query that will find all log sources, the number of distinct "principal.hostnames" sending logs, and the total number of events sent by that log source type.

UDM Search Query:

```
$log_types = $e.metadata.log_type
$log_types = /.*/

match:
    $log_types

outcome:
    $count_principal_hosts = count_distinct($e.principal.hostname)
    $events_count = count_distinct($e.metadata.id)

order:
    $log_types
```

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