

# NIST CSF 2.0-RS.MI-01-Ex1

RESPOND (RS): Actions regarding a detected cybersecurity incident are taken  
Incident Mitigation (RS.MI)

Activities are performed to prevent expansion of an event and mitigate its effects

## RS.MI-01

Incidents are contained

### Ex1

Cybersecurity technologies (e.g., antivirus software) and cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) automatically perform containment actions

#### Compliance Framework References:

CCMv4.0: CEK-19

CCMv4.0: CEK-20

CCMv4.0: IVS-09

CCMv4.0: SEF-02

CCMv4.0: UEM-09

CRI Profile v2.0: RS.MI-01

CRI Profile v2.0: RS.MI-01.01

CSF v1.1: RS.MI-1

SP 800-53 Rev 5.1.1: IR-04

Vendor: Agnostic

Comments: Logs from the cybersecurity technology will typically describe the action that was taken in response to the threat. In many cases the query would need to be specific to the technology. However, we'll try to construct a general query for antivirus responses.

Note: The current version of the query checks for either SentinelOne or Crowdstrike. However, adding other vendor names is trivial as long as they are known (they can be added to the regex filter for `$e.metadata.vendor_name`).

## UDM Search Query:

```
$hostname = $e.principal.hostname  
$hostname = /.*/  
$hostname != ""
```

```
$e.metadata.vendor_name = /SentinelOne|CrowdStrike/ nocase  
($e.security_result.action = "BLOCK" OR  
  $e.security_result.action = "QUARANTINE" OR  
  $e.security_result.action = "ALLOW_WITH_MODIFICATION")
```

```
$e.security_result.action != "UNKNOWN_ACTION"
```

```
match:  
  $hostname
```

```
outcome:  
  $vendor_name = array_distinct($e.metadata.vendor_name)  
  $security_action = array_distinct($e.security_result.action)  
  $categories = array_distinct($e.security_result.category)  
  $occurrences = count($e.metadata.id)
```

```
order:  
  $occurrences desc
```

```
limit: 25
```

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