NIST CSF 2.0-DE.CM-06-Ex2

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-06

External service provider activities and services are monitored to find potentially adverse events

Ex2

Monitor activity from cloud-based services, internet service providers, and other service providers for deviations from expected behavior

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: 15.2
CIS Controls v8.0: 15.6
CRI Profile v2.0: DE.CM-06
CRI Profile v2.0: DE.CM-06.01
CRI Profile v2.0: DE.CM-06.02
CSF v1.1: DE.CM-6
CSF v1.1: DE.CM-7
SP 800-53 Rev 5.1.1: CA-07
SP 800-53 Rev 5.1.1: PS-07
SP 800-53 Rev 5.1.1: SA-04
SP 800-53 Rev 5.1.1: SA-09
SP 800-53 Rev 5.1.1: SI-04

Vendor: Agnostic

Comments: This could be any query that demonostrates that the SIEM will create alerts for indicators of compromise from cloud provider logs.

The following shows anomalously high number of failed logins within a single hour. More than 2 failed attempts is considered high.

The following query should work on AWS, Azure, Office365, or Google. However, it has only been tested with Azure.

UDM Search Query:

```
($e.about.asset.attribute.cloud.environment = "AMAZON_WEB_SERVICES" or
    $e.about.asset.attribute.cloud.environment = "GOOGLE_CLOUD_PLATFORM" or
    $e.about.asset.attribute.cloud.environment = "MICROSOFT_AZURE" or
                          $e.about.asset.attribute.cloud.environment       =
"UNSPECIFIED_CLOUD_ENVIRONMENT")

$e.metadata.event_type = "USER_LOGIN"
$e.security_result.action = "BLOCK"
$e.principal.ip = $ip
$e.target.user.userid != ""
$e.target.hostname != ""
$e.target.user.userid = $target_user
$e.target.user.userid != "Not Available"
$e.extensions.auth.mechanism             !=             "OTP"             and
$e.target.user.user_authentication_status       !=       "SUSPENDED"       and
$e.target.user.user_authentication_status != "NO_ACTIVE_CREDENTIALS"
not (re.regex($e.target.user.userid, `.*\$`))
not                     $e.security_result.description                     in
%whitelisted_login_failure_reason_codes //This is to eliminate noise cases
like user login attempt with expired login credentials, user is presented
MFA, username does not exist.

match:
    $target_user over 1h

outcome:
    $product = array_distinct($e.metadata.product_name)
    $target_hostname = array_distinct($e.target.hostname)
    $ip_address = array_distinct($ip)
     $anomalous = if(sum(if($e.security_result.action = "BLOCK", 1, 0))>2,
"Yes", "No")
    $anomalous_count = sum(if($e.security_result.action = "BLOCK", 1, 0))
                                                $first_seen             =
timestamp.get_date(min($e.metadata.event_timestamp.seconds))
                                                 $last_seen             =
timestamp.get_date(max($e.metadata.event_timestamp.seconds))

order:
    $anomalous_count desc

limit:
    100
```

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