NIST CSF 2.0-PR.IR-01-Ex1

PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used

Technology Infrastructure Resilience (PR.IR)

Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience

PR.IR-01

Networks and environments are protected from unauthorized logical access and usage

Ex1

Logically segment organization networks and cloud-based platforms according to trust boundaries and platform types (e.g., IT, IoT, OT, mobile, guests), and permit required communications only between segments

Compliance Framework References:

CCMv4.0: AIS-04
CCMv4.0: AIS-06
CCMv4.0: DCS-12
CCMv4.0: DSP-10
CCMv4.0: DSP-15
CCMv4.0: IVS-03
CCMv4.0: IVS-05
CCMv4.0: IVS-06
CCMv4.0: IVS-09
CCMv4.0: UEM-05
CCMv4.0: UEM-14
CIS Controls v8.0: 3.12
CIS Controls v8.0: 12.2
CRI Profile v2.0: PR.IR-01
CRI Profile v2.0: PR.IR-01.01
CRI Profile v2.0: PR.IR-01.02
CRI Profile v2.0: PR.IR-01.03
CRI Profile v2.0: PR.IR-01.04
CRI Profile v2.0: PR.IR-01.05
CRI Profile v2.0: PR.IR-01.06
CRI Profile v2.0: PR.IR-01.07
CRI Profile v2.0: PR.IR-01.08
CSF v1.1: PR.AC-3
CSF v1.1: PR.AC-5
CSF v1.1: PR.DS-7
CSF v1.1: PR.PT-4
SP 800-218: PO.5.1
SP 800-53 Rev 5.1.1: AC-03
SP 800-53 Rev 5.1.1: AC-04
SP 800-53 Rev 5.1.1: SC-04
SP 800-53 Rev 5.1.1: SC-05
SP 800-53 Rev 5.1.1: SC-07

Vendor: Agnostic

Comments: Firewall, netflow, and other communications between internal subnets can be demonstrated via log analysis. However, this Example also demonstrates the need to show that only permitted communication is allowed. This can only be done by configuration review.

Note: This rule checks to see if data is routed through a firewall. In order for it to work, a reference list called firewall_log_types must be created. This was tested against a list with the following firewall log types in the list:

PAN_FIREWALL
PAN_PANORAMA
AWS_NETWORK_FIREWALL
AZURE_FIREWALL
BARRACUDA_FIREWALL
CHECKPOINT_FIREWALL
CISCO_ASA_FIREWALL
CISCO_FIREPOWER_FIREWALL
FORCEPOINT_FIREWALL
FORTINET_FIREWALL
PFSENSE
RADWARE_FIREWALL
SONIC_FIREWALL
SOPHOS_FIREWALL
ZSCALER_FIREWALL

UDM Search Query:

```
$e.metadata.log_type IN %firewall_log_types
$sourceIP = $e.principal.ip

$e.principal.ip IN cidr %private_network_IP_ranges
$e.target.ip in cidr %private_network_IP_ranges

$e.security_result.action = "ALLOW"

match:
    $sourceIP

outcome:
    $destinationIP = array_distinct($e.target.ip)
```

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