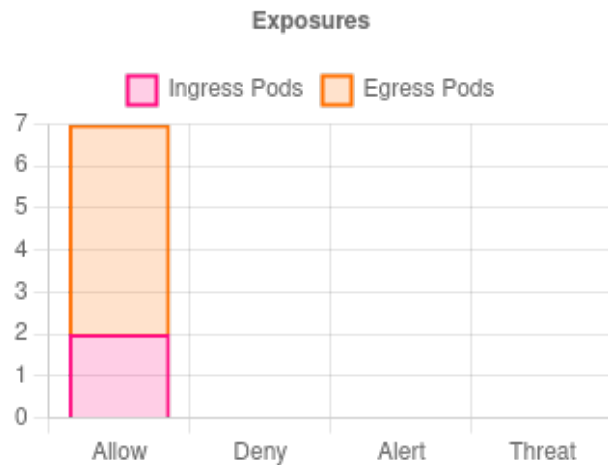# Security Event and Risk Report

Ingress and Egress Exposure

Ingress and Egress exposure and risk summarizes external connections for the cluster. Ingress shows incoming connections by application protocol from outside the cluster, and Egress shows connections by application protocol from pods to any destination outside the cluster. The Mode is the protection mode which the service is in and Action shows allow if a network rule allows it, or deny if it was a violation. How to Use It: Review ingress and egress connections to make sure allowed ones should be allowed, and investigate any that show deny. If shown as a deny but it should be allowed, review the network rules to whitelist the connections.

Ingress

Service	Pods	Vulnerabilities	Policy Mode	External Host (IP)	External Host (FQDN)	Sessions	Applications	Action
etcd.kube-system	1	High:0 Medium:0	Discover	192.168.49.2		1	etcd	Allow
kube-apiserver.kube-system	1	High:0 Medium:0	Discover	192.168.49.2		194		Allow
				192.168.49.1		12		Allow

Egress

Service	Pods	Vulnerabilities	Policy Mode	External Host (IP)	External Host (FQDN)	Sessions	Applications	Action
coredns.kube-system	1	High:0 Medium:0	Discover	10.96.0.1		1		Allow
				192.168.49.1		4	DNS	Allow
etcd.kube-system	1	High:0 Medium:0	Discover	192.168.49.2		1		Allow
kube-apiserver.kube-system	1	High:0 Medium:0	Discover	192.168.49.2		6		Allow
kube-controller-manager.kube-system	1	High:0 Medium:0	Discover	192.168.49.2		5		Allow
storage.kube-system	1	High:0 Medium:0	Discover	10.96.0.1		1		Allow

Critical Run-Time Security Events

No critical run-time security events

Critical Run-Time Security Events show totals for Critical and Warning level events. Only critical run-time security events are summarized.

How to Use It: High volumes of critical events could indicate an attack or a misconfigured service. Investigate to determine if they are coming from the same service or namespace. Updates of services with new application or process behavior could be generating security events and require adding new whitelist rules, or moving the service to Discover mode to learn them.

Top Security Events

Source

No security events

Top security events by Source shows the containers or pods with the most network security events originating from that pods or containers. Security events are including network based detection of suspicious payloads or connections such as DDoS or sql injection etc, network segmentation (whitelist rule) violations, suspicious process or file system incidents.
How to Use It: Review containers with security events to see if there are following phenomena:
1. The container has been exploited to start generating attacks (lateral, east-west movement). If yes, you need to fix them.
2. The containers generating violations to see if they have been compromised and are being used to expand laterally or attempt egress. If connections should be allowed, add a whitelist rule for them.
3. Often a compromised or hacked pod will have multiple process and file system incidents as the hacker tries to install malicious code or vulnerable packages and/or start suspicious processes. Pods can be quarantined or a packet capture started by NeuVector.

Destination

Top security events by Destination shows the containers or pods with the most network security events hitting that container. Security events are including network based detection of suspicious payloads or connections such as DDoS or sql injection etc, pods or containers with the most unauthorized connections to them (destination), egress connections out of the cluster which are suspicious are shown as external violations, suspicious process or file system incidents.
How to Use It: Review containers with security events to see if there are following phenomena:
1. The container has been under attack and if the attack has succeeded or damaged the container. If yes, you need to fix them.
2. Top destinations to determine if unauthorized connections are attempted attacks, especially if originating from one client container or from external (ingress). If connection should be allowed, add a whitelist rule for it.
3. Often a compromised or hacked pod will have multiple process and file system incidents as the hacker tries to install malicious code or vulnerable packages and/or start suspicious processes. Pods can be quarantined or a packet capture started by NeuVector.

No security events

Top Vulnerabilities

Pods
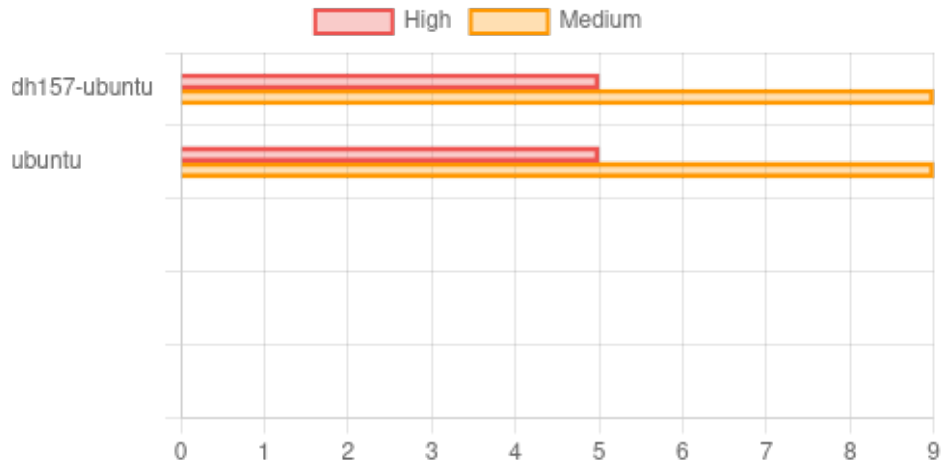
Top incidents by pods shows suspicious process or file system incidents sorted by most incidents by pods.
How to Use It: Often a compromised or hacked pod will have multiple process and file system incidents as the hacker tries to install malicious code or vulnerable packages and/or start suspicious processes. Pods can be quarantined or a packet capture started by NeuVector.

Nodes

Top incidents by nodes shows the worker nodes (hosts) with the highest number of file system or process violations.
How to Use It: Nodes with high incidents can indicate a hacker has gained access and is attempting additional damage, installation, or lateral probing. Review container and host incidents for the node to determine the source, user, and commands used.
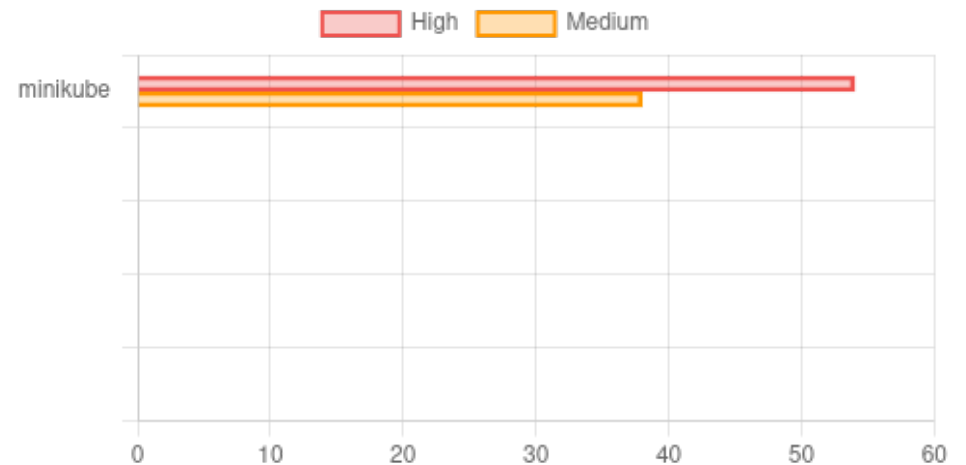
Policy Mode of Services and Pods
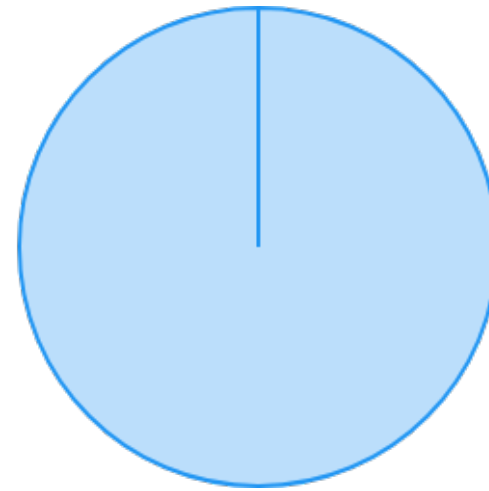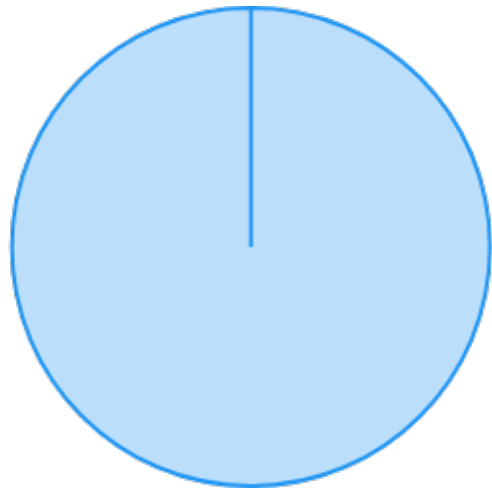
Caution

Services in Discover mode are still learning and white-listing network behavior and will not have network segmentation turned on.

Caution

Move services into Monitor or Protect mode as soon as possible after reviewing Network Rules.

Policy Mode Service View summarizes the number and ratio of container services in each mode Discover, Monitor and Protect. The Pod View shows the number and ratio by the number of pods (each service can deploy multiple pods).

How to Use It: Services and Pods in Discover mode are still learning and whitelisting network behavior and will don't have network segmentation turned on. Move services and pods into Monitor or Protect mode as soon as possible after reviewing Network Rules.

Application Protocols Detected and Protected by Layer 7 Network Rules

Application Conversations
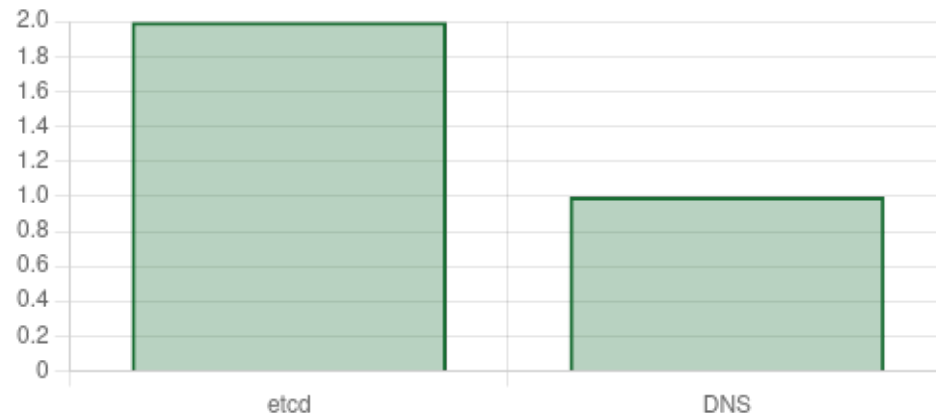
Application Protocols by Application conversations shows the number of conversations detected for each application protocol shown. For each of these, a application layer (Layer 7) network rule has was created to whitelist the connection. The category Others means protocols other than known protocols such as non-standard TCP connections.
How to Use It: Review the protocol list to make sure all common application protocols are detected and whitelisted.

Application Volume

Application Protocols by Volume shows the network activity level detected for each application protocol.
How to Use It: When running test traffic or in production review the activity to assess whether it looks like normal traffic patterns. High activity could indicate an attack, data breach, or misconfiguration of the application.