



Report date: 2024-12-06T16:38:37

Frameworks scanned: ClusterScan (compliance score: 79.04), MITRE (compliance score: 71.78), NSA (compliance score: 57.43)

Severity	Control reference	Control name	Failed resources	All resources	Compliance score
Critical	C-0005	API server insecure port is enabled	0	1	100%
Critical	C-0069	Disable anonymous access to Kubelet service	0	0	Action Required †
Critical	C-0070	Enforce Kubelet client TLS authentication	0	0	Action Required †
High	C-0012	Applications credentials in configuration files	6	39	85%
High	C-0015	List Kubernetes secrets	3	81	96%
High	C-0038	Host PID/IPC privileges	0	18	100%
High	C-0041	HostNetwork access	4	18	78%
High	C-0045	Writable hostPath mount	2	18	89%
High	C-0046	Insecure capabilities	1	18	94%
High	C-0048	HostPath mount	3	18	83%
High	C-0057	Privileged container	2	18	89%
High	C-0059	CVE-2021-25742-nginx-ingress-snippet-annotation-vulnerability	0	0	100%
High	C-0088	RBAC enabled	0	1	100%
High	C-0187	Minimize wildcard use in Roles and ClusterRoles	0	81	100%
High	C-0256	External facing	2	27	93%
High	C-0262	Anonymous access enabled	2	74	97%
High	C-0265	Authenticated user has sensitive permissions	0	81	100%
High	C-0270	Ensure CPU limits are set	12	18	33%
High	C-0271	Ensure memory limits are set	12	18	33%
Medium	C-0002	Prevent containers from allowing command execution	0	81	100%
Medium	C-0007	Roles with delete capabilities	3	81	96%
Medium	C-0013	Non-root containers	12	18	33%
Medium	C-0016	Allow privilege escalation	10	18	44%
Medium	C-0020	Mount service principal	0	18	100%
Medium	C-0021	Exposed sensitive interfaces	0	0	100%
Medium	C-0030	Ingress and Egress blocked	12	19	37%
Medium	C-0031	Delete Kubernetes events	1	81	99%
Medium	C-0034	Automatic mapping of service account	17	69	75%
Medium	C-0035	Administrative Roles	0	81	100%
Medium	C-0037	CoreDNS poisoning	1	81	99%
Medium	C-0039	Validate admission controller (mutating)	0	0	100%
Medium	C-0044	Container hostPort	2	18	89%
Medium	C-0053	Access container service account	14	56	75%
Medium	C-0054	Cluster internal networking	4	9	56%
Medium	C-0055	Linux hardening	10	18	44%
Medium	C-0058	CVE-2021-25741 - Using symlink for arbitrary host file system access.	0	0	100%
Medium	C-0063	Portforwarding privileges	0	81	100%
Medium	C-0066	Secret/etcd encryption enabled	1	1	0%
Medium	C-0067	Audit logs enabled	1	1	0%
Medium	C-0188	Minimize access to create pods	2	81	98%
Medium	C-0260	Missing network policy	12	40	70%
Low	C-0014	Access Kubernetes dashboard	0	99	100%
Low	C-0017	Immutable container filesystem	10	18	44%
Low	C-0026	Kubernetes CronJob	0	0	100%
Low	C-0036	Validate admission controller (validating)	1	1	0%
Low	C-0042	SSH server running inside container	0	4	100%
Low	C-0068	PSP enabled	1	1	0%

Resource summary

48

269

72.99%

† This control is scanned exclusively by the Kubescape operator, not the Kubescape CLI. Install the Kubescape operator: <https://kubescape.io/docs/install-operator/>.