Report date: 2025-03-18 14:37:27

Frameworks scanned: ClusterScan (compliance score: 83.43), MITRE (compliance score: 78.97), NSA (compliance score: 72.13)

Severity	Control reference	Control name	Failed resources	All resources	Compliance score
Critical	C-0005	API server insecure port is enabled	0	0	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	1	15	93%
High	C-0015	List Kubernetes secrets	8	10	20%
High	C-0038	Host PID/IPC privileges	0	7	100%
High	C-0041	HostNetwork access	0	7	100%
High	C-0045	Writable hostPath mount	0	7	100%
High	C-0046	Insecure capabilities	0	7	100%
High	C-0048	HostPath mount	0	7	100%
High	C-0057	Privileged container	0	7	100%
High	C-0059	CVE-2021-25742-nginx-ingress-snippet-annotation-vulnerability	0	0	100%
High	C-0088	RBAC enabled	0	0	100%
High	C-0187	Minimize wildcard use in Roles and ClusterRoles	2	10	80%
High	C-0256	External facing	1	13	92%
High	C-0262	Anonymous access enabled	0	6	100%
High	C-0265	Authenticated user has sensitive permissions	0	10	100%
High	C-0270	Ensure CPU limits are set	7	7	0%
High	C-0271	Ensure memory limits are set	7	7	0%
Medium	C-0002	Prevent containers from allowing command execution	2	10	80%
Medium	C-0007	Roles with delete capabilities	4	10	60%
Medium	C-0013	Non-root containers	7	7	0%
Medium	C-0016	Allow privilege escalation	0	7	100%
Medium	C-0020	Mount service principal	0	7	100%
Medium	C-0021	Exposed sensitive interfaces	0	0	100%
Medium	C-0030	Ingress and Egress blocked	7	7	0%
Medium	C-0031	Delete Kubernetes events	3	10	70%
Medium	C-0034	Automatic mapping of service account	7	14	50%
Medium	C-0035	Administrative Roles	2	10	80%
Medium	C-0037	CoreDNS poisoning	5	10	50%
Medium	C-0039	Validate admission controller (mutating)	0	0	100%
Medium	C-0044	Container hostPort	0	7	100%
Medium	C-0053	Access container service account	10	10	0%
Medium	C-0054	Cluster internal networking	0	0	100%
Medium	C-0055	Linux hardening	0	7	100%
Medium	C-0058	CVE-2021-25741 - Using symlink for arbitrary host file system access.	0	0	100%
Medium	C-0063	Portforwarding privileges	2	10	80%
Medium	C-0066	Secret/etcd encryption enabled	0	0	100%
Medium	C-0067	Audit logs enabled	0	0	100%
Medium	C-0188	Minimize access to create pods	2	10	80%
Medium	C-0260	Missing network policy	7	15	53%
Low	C-0014	Access Kubernetes dashboard	0	17	100%
Low	C-0017	Immutable container filesystem	0	7	100%
Low	C-0026	Kubernetes CronJob	0	0	100%
Low	C-0036	Validate admission controller (validating)	0	0	100%
Low	C-0042	SSH server running inside container	0	0	100%
Low	C-0068	PSP enabled	0	0	100%
Resource summary			**25**	**44**	**76.36%**

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