Kubescape

by ARMO

Report date: 2025-01-20T13:03:04

Frameworks scanned: ClusterScan (compliance score: 79.48), MITRE (compliance score: 71.50), NSA (compliance score: 61.17)

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	3	40	93%
High	C-0015	List Kubernetes secrets	4	89	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	1	89	99%
High	C-0256	External facing	2	27	93%
High	C-0262	Anonymous access enabled	2	81	98%
High	C-0265	Authenticated user has sensitive permissions	0	89	100%
High	C-0270	Ensure CPU limits are set	9	18	50%
High	C-0271	Ensure memory limits are set	9	18	50%
Medium	C-0002	Prevent containers from allowing command execution	1	89	99%
Medium	C-0007	Roles with delete capabilities	5	89	94%
Medium	C-0013	Non-root containers	12	18	33%
Medium	C-0016	Allow privilege escalation	7	18	61%
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	9	23	61%
Medium	C-0031	Delete Kubernetes events	2	89	98%
Medium	C-0034	Automatic mapping of service account	16	73	78%
Medium	C-0035	Administrative Roles	1	89	99%
Medium	C-0037	CoreDNS poisoning	2	89	98%
Medium	C-0039	Validate admission controller (mutating)	0	0	100%
Medium	C-0044	Container hostPort	0	18	100%
Medium	C-0053	Access container service account	21	63	67%
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	1	89	99%
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	3	89	97%
Medium	C-0260	Missing network policy	9	45	80%
Low	C-0014	Access Kubernetes dashboard	0	107	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	**57**	**293**		**74.85%**

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