Kubescape

by ΔRMO

Frameworks scanned: ClusterScan (compliance score: 81.93), MITRE (compliance score: 72.92), NSA (compliance score: 61.12)

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	38	316	88%
High	C-0015	List Kubernetes secrets	29	129	78%
High	C-0038	Host PID/IPC privileges	4	167	98%
High	C-0041	HostNetwork access	6	167	96%
High	C-0045	Writable hostPath mount	5	167	97%
High	C-0046	Insecure capabilities	0	167	100%
High	C-0048	HostPath mount	7	167	96%
High	C-0057	Privileged container	3	167	98%
High	C-0059	CVE-2021-25742-nginx-ingress-snippet-annotation-vulnerability	0	1	100%
High	C-0088	RBAC enabled	0	0	100%
High	C-0187	Minimize wildcard use in Roles and ClusterRoles	4	129	97%
High	C-0256	External facing	0	338	100%
High	C-0262	Anonymous access enabled	1	123	99%
High	C-0265	Authenticated user has sensitive permissions	0	129	100%
High	C-0270	Ensure CPU limits are set	142	167	15%
High	C-0271	Ensure memory limits are set	139	167	17%
Medium	C-0002	Prevent containers from allowing command execution	4	129	97%
Medium	C-0007	Roles with delete capabilities	12	129	91%
Medium	C-0013	Non-root containers	156	167	7%
Medium	C-0016	Allow privilege escalation	135	167	19%
Medium	C-0020	Mount service principal	0	167	100%
Medium	C-0021	Exposed sensitive interfaces	0	0	100%
Medium	C-0030	Ingress and Egress blocked	158	172	8%
Medium	C-0031	Delete Kubernetes events	5	129	96%
Medium	C-0034	Automatic mapping of service account	167	285	41%
Medium	C-0035	Administrative Roles	4	129	97%
Medium	C-0037	CoreDNS poisoning	9	129	93%
Medium	C-0039	Validate admission controller (mutating)	2	2	0%
Medium	C-0044	Container hostPort	0	167	100%
Medium	C-0053	Access container service account	52	99	47%
Medium	C-0054	Cluster internal networking	29	36	19%
Medium	C-0055	Linux hardening	137	167	18%
Medium	C-0058	CVE-2021-25741 - Using symlink for arbitrary host file system access.	0	0	100%
Medium	C-0063	Portforwarding privileges	4	129	97%
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	5	129	96%
Medium	C-0260	Missing network policy	158	321	51%
Low	C-0014	Access Kubernetes dashboard	0	296	100%
Low	C-0017	Immutable container filesystem	151	167	10%
Low	C-0026	Kubernetes CronJob	32	32	0%
Low	C-0036	Validate admission controller (validating)	2	2	0%
Low	C-0042	SSH server running inside container	1	81	99%
Low	C-0068	PSP enabled	0	0	100%

Resource summary			**337**	**983**	**69.45%**

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