Report date: 2025-02-08T03:36:52

Framework scanned: NSA

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	1	83	99%
High	C-0038	Host PID/IPC privileges	2	26	92%
High	C-0041	HostNetwork access	2	26	92%
High	C-0046	Insecure capabilities	1	26	96%
High	C-0057	Privileged container	0	26	100%
High	C-0059	CVE-2021-25742-nginx-ingress-snippet-annotation-vulnerability	0	0	100%
High	C-0270	Ensure CPU limits are set	19	26	27%
High	C-0271	Ensure memory limits are set	15	26	42%
Medium	C-0002	Prevent containers from allowing command execution	2	97	98%
Medium	C-0013	Non-root containers	14	26	46%
Medium	C-0016	Allow privilege escalation	4	26	85%
Medium	C-0030	Ingress and Egress blocked	20	33	39%
Medium	C-0034	Automatic mapping of service account	25	89	72%
Medium	C-0035	Administrative Roles	2	97	98%
Medium	C-0044	Container hostPort	0	26	100%
Medium	C-0054	Cluster internal networking	3	8	63%
Medium	C-0055	Linux hardening	4	26	85%
Medium	C-0058	CVE-2021-25741 - Using symlink for arbitrary host file system access.	0	0	100%
Medium	C-0066	Secret/etcd encryption enabled	1	1	0%
Medium	C-0067	Audit logs enabled	1	1	0%
Low	C-0017	Immutable container filesystem	4	26	85%
Low	C-0068	PSP enabled	1	1	0%
	Resource summary		**51**	**258**	**64.74%**

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