



Report date: 2024-12-25T15:09:09

Framework scanned: WorkloadScan

Severity	Control reference	Control name	Failed resources	All resources	Compliance score
High	C-0012	Applications credentials in configuration files	0	1	100%
High	C-0038	Host PID/IPC privileges	0	1	100%
High	C-0041	HostNetwork access	0	1	100%
High	C-0045	Writable hostPath mount	0	1	100%
High	C-0046	Insecure capabilities	0	1	100%
High	C-0048	HostPath mount	0	1	100%
High	C-0057	Privileged container	0	1	100%
High	C-0270	Ensure CPU limits are set	0	1	100%
High	C-0271	Ensure memory limits are set	0	1	100%
Medium	C-0013	Non-root containers	1	1	0%
Medium	C-0016	Allow privilege escalation	1	1	0%
Medium	C-0034	Automatic mapping of service account	1	2	50%
Medium	C-0044	Container hostPort	0	1	100%
Medium	C-0055	Linux hardening	1	1	0%
Medium	C-0078	Images from allowed registry	0	1	Action Required †
Medium	C-0207	Prefer using secrets as files over secrets as environment variables	0	1	100%
Medium	C-0257	Workload with PVC access	0	3	100%
Medium	C-0260	Missing network policy	0	7	100%
Low	C-0017	Immutable container filesystem	1	1	0%

Resource summary

1

8

71.05%

† Control configurations are empty (docs: <https://kubescape.io/docs/frameworks-and-controls/configuring-controls>)