EXECUTIVE SUMMARY · FOR PLATFORM

1 critical to fix, 30 warnings. Biggest lever: drop privileged:true.

SCORE	Δ VS. PRIOR	CRITICAL	WARNINGS	AVG CONFIDENCE
14/100	+0 pts	1	30	0.56

HEADLINE FINDINGS

- CRITICAL `kube-system` container "kube-proxy" is privileged 0.33
- WARN `big-monolith` no pods found matching service labels (map[app:hunger-check]) 1.00
- WARN `default` no pods found matching service labels (map[app:build-code]) 1.00
- WARN `default` no pods found matching service labels (map[app:health-check]) 1.00
- WARN `default` no pods found matching service labels (map[app:internal-proxy]) 1.00

AUDIT CONTEXT

Cluster `.test`, audited 2026-05-05 07:55. Posture score **14/100** (prior: 14/100). `dump SHA-256: 6b181a0c2f43426a…`

Findings are fused across **0 scanner source(s)** spanning **0 categories** (`no scanners`). When multiple independent sources flag the same resource with the same issue class, we collapse them into one finding and increase its confidence score (shown as a bar, 0.0–1.0). The posture score is confidence-weighted — low-confidence findings deduct proportionally fewer points.

Scoring per finding: CRITICAL −12 pts, WARN −4 pts, INFO −1 pt, each multiplied by the finding's confidence. Floor 0, ceiling 100.

This audit is based on cluster state collected via Ephemera's `collect-cluster-data.sh` script (read-only `kubectl get` calls), then scanned offline by 0 independent tools. Secrets, JWTs, AWS keys, and PEM blocks are redacted at collection time and again before printing.

FINDINGS · 42 TOTAL · FUSED FROM ALL SCANNERS

Every signal, with source attribution.

Rows are deduplicated across scanners: when multiple tools independently flag the same `(namespace, resource, issue)`, they collapse into one row. The **Sources** column shows which tools agreed, and **Confidence** reflects how corroborated the finding is — higher bars = more independent tools converged.

ID	SEV	NAMESPACE	RESOURCE	FINDING	SOURCES	CONF
F-01	CRITICAL	kube-system	DaemonSet/kube-proxy	container "kube-proxy" is privileged	config scan	0.33
F-02	WARN	big-monolith	Service/hunger-check-service	no pods found matching service labels (map[app:hunger-check])	config scan runtime check	1.00
F-03	WARN	default	Service/build-code-service	no pods found matching service labels (map[app:build-code])	config scan runtime check	1.00
F-04	WARN	default	Service/health-check-service	no pods found matching service labels (map[app:health-check])	config scan runtime check	1.00
F-05	WARN	default	Service/internal-proxy-api-ser…	no pods found matching service labels (map[app:internal-proxy])	config scan runtime check	1.00
F-06	WARN	default	Service/internal-proxy-info-ap…	no pods found matching service labels (map[app:internal-proxy])	config scan runtime check	1.00
F-07	WARN	default	Service/kubernetes-goat-home-s…	no pods found matching service labels (map[app:kubernetes-goat-home])	config scan runtime check	1.00
F-08	WARN	default	Service/metadata-db	no pods found matching service labels (map[app.kubernetes.io/instance:	config scan runtime check	1.00
F-09	WARN	default	Service/poor-registry-service	no pods found matching service labels (map[app:poor-registry])	config scan runtime check	1.00
F-10	WARN	default	Service/system-monitor-service	no pods found matching service labels (map[app:system-monitor])	config scan runtime check	1.00
F-11	WARN	default	Service/wordpress-1776847905	no pods found matching service labels (map[app.kubernetes.io/instance:	config scan runtime check	1.00
F-12	WARN	default	Service/wordpress-1776847905-m…	no pods found matching service labels (map[app.kubernetes.io/component	config scan runtime check	1.00
F-13	WARN	default	Service/wordpress-1776847905-m…	no pods found matching service labels (map[app.kubernetes.io/instance:	config scan runtime check	1.00
F-14	WARN	secure-middleware	Service/cache-store-service	no pods found matching service labels (map[app:cache-store])	config scan runtime check	1.00
F-15	WARN	default	Service/kubernetes	service has no selector specified	config scan	0.85
F-16	WARN	kube-system	Service/kube-dns	no pods found matching service labels (map[k8s-app:kube-dns])	config scan	0.85
F-17	WARN	default	Deployment/wordpress-1776847905	Repeated warning events: Unhealthy (13x)	runtime check	0.33
F-18	WARN	default	Job/batch-check-job	The container "batch-check" is using an invalid container image, "madh	config scan	0.33
F-19	WARN	default	Job/batch-check-job	container "batch-check" does not have a read-only root file system	config scan	0.33

ID	SEV	FINDING	FRAMEWORK REFERENCES	CONF
			CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05	
F-06	WARN	no pods found matching service labels (map[app:internal-proxy])	NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05	1.00
F-07	WARN	no pods found matching service labels (map[app:kubernetes-goat-home])	NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05	1.00
F-08	WARN	no pods found matching service labels (map[app.kubernetes.io/instance:me	NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05	1.00
F-09	WARN	no pods found matching service labels (map[app:poor-registry])	NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05	1.00
F-10	WARN	no pods found matching service labels (map[app:system-monitor])	NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05	1.00
F-11	WARN	no pods found matching service labels (map[app.kubernetes.io/instance:wo	NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05	1.00
F-12	WARN	no pods found matching service labels (map[app.kubernetes.io/component:p	NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1	1.00

ID	SEV	FINDING	FRAMEWORK REFERENCES	CONF
			CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05	
F-13	WARN	no pods found matching service labels (map[app.kubernetes.io/instance:wo	NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05	1.00
F-14	WARN	no pods found matching service labels (map[app:cache-store])	NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05	1.00
F-15	WARN	service has no selector specified	NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05	0.85
F-16	WARN	no pods found matching service labels (map[k8s-app:kube-dns])	NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05	0.85
F-17	WARN	Repeated warning events: Unhealthy (13x)	NIS2: 21.2.b, 21.2.c GDPR: 32.1.b DORA: 11.6 CRA: I.1.2.h CER: 13.1.c ISO27001: A.5.30, A.8.16 SOC2: A1.2 NIST-CSF: DE.CM-09	0.33
F-18	WARN	The container "batch-check" is using an invalid container image, "madhua	NIS2: 21.2.d, 21.2.e GDPR: 32.1.d DORA: 8.2, 9.4.d CRA: I.2.1, I.2.7 ISO27001: A.8.9, A.8.19 CIS-K8s: 6.1.1 SOC2: CC6.8, CC8.1 NIST-CSF: ID.RA-01, GV.SC-05 MITRE: T1525 OWASP-K8s: K02 NSA-CISA: PS-9, UA-4	0.33
F-19	WARN	container "batch-check" does not have a read-only root file system	NIS2: 21.2.e, 21.2.g GDPR: 32.1.b	0.33

ID	SEV	FINDING	FRAMEWORK REFERENCES	CONF
			SOC2: A1.2 NIST-CSF: DE.CM-09	
F-32	INFO	Standalone Job does not specify ttlSecondsAfterFinished	—	0.33
F-33	INFO	container "batch-check" has cpu request 0	NIS2: 21.2.c DORA: 7.c ISO27001: A.8.6 OWASP-K8s: K01	0.33
F-34	INFO	container "batch-check" has memory limit 0	NIS2: 21.2.c DORA: 7.c ISO27001: A.8.6	0.33
F-35	INFO	Standalone Job does not specify ttlSecondsAfterFinished	—	0.33
F-36	INFO	container "hidden-in-layers" has cpu request 0	NIS2: 21.2.c DORA: 7.c ISO27001: A.8.6 OWASP-K8s: K01	0.33
F-37	INFO	container "hidden-in-layers" has memory limit 0	NIS2: 21.2.c DORA: 7.c ISO27001: A.8.6	0.33
F-38	INFO	unhealthyPodEvictionPolicy is not explicitly set	—	0.33
F-39	INFO	unhealthyPodEvictionPolicy is not explicitly set	—	0.33
F-40	INFO	container "kube-proxy" is Privileged hence allows privilege escalation.	NIS2: 21.2.e, 21.2.g GDPR: 32.1.b DORA: 9.2, 9.4.a CRA: I.1.2.b, I.1.2.k ISO27001: A.8.2, A.8.9 CIS-K8s: 5.2.5 SOC2: CC6.1 NIST-CSF: PR.PS-01 MITRE: T1548 OWASP-K8s: K01 NSA-CISA: PS-4	0.33
F-41	INFO	container "kube-proxy" has cpu request 0	NIS2: 21.2.c DORA: 7.c ISO27001: A.8.6 OWASP-K8s: K01	0.33
F-42	INFO	container "kube-proxy" has memory limit 0	NIS2: 21.2.c DORA: 7.c ISO27001: A.8.6	0.33

Framework references are indicative and should be reviewed with your compliance team. Covers: NIS2 (EU 2022/2555), GDPR (EU 2016/679), DORA (EU 2022/2554), CRA (EU 2024/2847), CER (EU 2022/2557), ISO/IEC 27001:2022, MITRE ATT&CK for Containers, OWASP K8s Top 10, and NSA/CISA K8s Hardening Guide v1.2.

Which regulations this cluster speaks to.

Each of the six frameworks below defines dozens or hundreds of requirements, only a subset of which are addressable through Kubernetes cluster state. The percentages show how many of the **in-scope** items (excluding purely organisational/physical controls) are exercised by findings in this report. A high percentage is not good news — it means findings are landing across many control domains.

NIS2	GDPR	DORA	CRA	CER	ISO27001
50%	38%	31%	42%	33%	20%
5 of 10 in-scope items touched **5** failing	3 of 8 in-scope items touched **3** failing	9 of 29 in-scope items touched **8** failing	8 of 19 in-scope items touched **8** failing	2 of 6 in-scope items touched **2** failing	8 of 41 in-scope items touched **7** failing

CIS-K8s	SOC2	NIST-CSF	MITRE	OWASP-K8s	NSA-CISA
14%	29%	21%	19%	30%	28%
6 of 43 in-scope items touched **5** failing	6 of 21 in-scope items touched **6** failing	4 of 19 in-scope items touched **4** failing	4 of 21 in-scope items touched **4** failing	3 of 10 in-scope items touched **3** failing	7 of 25 in-scope items touched **6** failing

The per-framework breakdown on the following pages shows every section and subsection. **Primary** = cluster state is the main source of evidence. Partial = cluster contributes but is insufficient alone. *Contextual* = informs but is not main evidence. *Out of scope* means Kubernetes cannot provide evidence — handled by policies, training, supply chain controls, and incident response processes.

HOW TO READ THIS

For each framework item, the table shows: the requirement, its Kubernetes relevance, the number of distinct findings that touched it, the highest severity hit, and which finding IDs map to it. Finding IDs link back to the findings table on page 2 so you can trace each compliance gap to a concrete remediation.

This is a technical coverage view, not a compliance attestation. Real compliance requires documented policies, organisational controls, supply chain audits, personnel training, and incident response procedures that a cluster scanner cannot assess. What this report does is surface the Kubernetes-level evidence you can contribute toward each framework's technical requirements.

DORA · DORA

Regulation (EU) 2022/2554 — Digital Operational Resilience Act

29 in-scope items · **9** touched · **8** failing

ITEM	REQUIREMENT	RELEVANCE	HITS	FINDING IDS
Art.5 · Governance and organisation				
5.1	*Management body approves ICT risk management framework*	*out-of-scope*	—	
Art.6 · ICT risk management framework				
6.2	**Strategies, policies, procedures, protocols and tools protecting all ICT assets**	**primary**	—	
6.8	Digital operational resilience strategy within framework	partial	—	
Art.7 · ICT systems, protocols and tools				
7.a	*Appropriate to magnitude of operations*	*contextual*	—	
7.b	**Reliable**	**primary**	—	
7.c	**Sufficient capacity for data processing, peak load, stress**	**primary**	**6** INFO	F-33, F-34, F-36, F-37, F-41, F-42
7.d	**Technologically resilient to adequately deal with additional needs under stress**	**primary**	—	
Art.8 · Identification				
8.1	Identify, classify and document ICT-supported business functions	partial	—	
8.2	**Identify information and ICT assets, their interconnections**	**primary**	**2** WARN	F-18, F-21
8.3	Identify and document all processes dependent on ICT 3rd parties	partial	—	
8.4	*Risk assessment on each major change to infrastructure*	*contextual*	—	
8.7	Assess ICT concentration risk and interdependencies	partial	—	
Art.9 · Protection and prevention				
9.1	**Continuously monitor and control security + functioning of ICT systems**	**primary**	—	
9.2	**Minimise impact of ICT risk via appropriate security tools**	**primary**	**9** CRITICAL	F-01, F-19, F-20, F-22, F-23, F-25 (+3)
9.3	**Design, procure and implement ICT security policies, procedures, protocols, tools**	**primary**	**1** CRITICAL	F-01
9.4.a	**Availability, authenticity, integrity, confidentiality of data**	**primary**	**6** CRITICAL	F-01, F-20, F-23, F-25, F-27, F-40
9.4.b	Security of data in use, in transit, at rest	partial	—	
9.4.c	**Policies preventing information leakage**	**primary**	—	
9.4.d	**Network connection security + software/firmware up to date**	**primary**	**2** WARN	F-18, F-21
9.4.e	**Physical and logical access control to ICT assets**	**primary**	**4** CRITICAL	F-01, F-20, F-23, F-27
9.4.f	Strong authentication mechanisms + key management	partial	—	
Art.10 · Detection				
10.1	**Detect anomalous activities, including ICT network performance + incidents**	**primary**	**15** WARN	F-02, F-03, F-04, F-05, F-06, F-07 (+9)
10.2	**Multiple layers of control, alert thresholds, criteria**	**primary**	—	
10.3	Automated alert mechanisms for staff responsible for response	partial	—	
Art.11 · Response and recovery				

ITEM	REQUIREMENT	RELEVANCE	HITS	FINDING IDS
11.2	Comprehensive ICT business continuity policy	partial	—	
11.4	ICT response and recovery plans: RTO, RPO	partial	—	
11.6	**Redundant ICT capacities with resources, capabilities + functionalities**	**primary**	**6** WARN	F-17, F-24, F-28, F-29, F-30, F-31
Art.12 · Backup policies and procedures, restoration and recovery				
12.1	*Policies specifying scope of data covered by backup*	*contextual*	—	
12.2	*Backup systems able to activate in accordance with backup policies*	*contextual*	—	
12.3	*Restoration and recovery procedures and methods regularly tested*	*contextual*	—	
Art.13 · Learning and evolving				
13.1	*Review ICT-related incidents + root-cause analysis*	*out-of-scope*	—	
Art.14 · Communication				
14.1	*Crisis communication plans enabling responsible disclosure*	*out-of-scope*	—	

ISO27001 · ISO/IEC 27001:2022

ISO/IEC 27001:2022 — Information security management systems

41 in-scope items · **8** touched · **7** failing

ITEM	REQUIREMENT	RELEVANCE	HITS	FINDING IDS
A.5 · Organizational controls (37)				
A.5.1	*Policies for information security*	*out-of-scope*	—	
A.5.2	*Information security roles and responsibilities*	*out-of-scope*	—	
A.5.3	Segregation of duties	partial	—	
A.5.7	*Threat intelligence*	*contextual*	—	
A.5.8	*Information security in project management*	*out-of-scope*	—	
A.5.9	Inventory of information and other associated assets	partial	—	
A.5.10	*Acceptable use of information and assets*	*out-of-scope*	—	
A.5.15	**Access control**	**primary**	—	
A.5.16	**Identity management**	**primary**	—	
A.5.17	Authentication information	partial	—	
A.5.18	**Access rights**	**primary**	—	
A.5.19	Information security in supplier relationships	partial	—	
A.5.20	*Addressing information security in supplier agreements*	*out-of-scope*	—	
A.5.21	Managing information security in the ICT supply chain	partial	—	
A.5.23	**Information security for use of cloud services**	**primary**	—	
A.5.24	Information security incident management planning	partial	—	
A.5.25	Assessment and decision on information security events	partial	—	
A.5.26	*Response to information security incidents*	*out-of-scope*	—	
A.5.27	*Learning from information security incidents*	*out-of-scope*	—	
A.5.29	Information security during disruption	partial	—	
A.5.30	**ICT readiness for business continuity**	**primary**	**6** WARN	F-17, F-24, F-28, F-29, F-30, F-31
A.5.33	Protection of records	partial	—	
A.5.35	*Independent review of information security*	*out-of-scope*	—	
A.5.36	**Compliance with policies, rules and standards for infosec**	**primary**	—	
A.5.37	*Documented operating procedures*	*out-of-scope*	—	
A.6 · People controls (8)				
A.6.1	*Screening*	*out-of-scope*	—	
A.6.2	*Terms and conditions of employment*	*out-of-scope*	—	
A.6.3	*Information security awareness, education and training*	*out-of-scope*	—	
A.6.6	*Confidentiality or non-disclosure agreements*	*out-of-scope*	—	
A.6.7	Remote working	partial	—	
A.6.8	*Information security event reporting*	*out-of-scope*	—	
A.7 · Physical controls (14)				
A.7.1	*Physical security perimeters*	*out-of-scope*	—	
A.7.2	*Physical entry*	*out-of-scope*	—	
A.7.4	*Physical security monitoring*	*out-of-scope*	—	
A.7.8	*Equipment siting and protection*	*out-of-scope*	—	
A.7.9	*Security of assets off-premises*	*out-of-scope*	—	

ITEM	REQUIREMENT	RELEVANCE	HITS	FINDING IDS
A.7.10	*Storage media*	*out-of-scope*	—	
A.7.11	*Supporting utilities*	*out-of-scope*	—	
A.7.12	*Cabling security*	*out-of-scope*	—	
A.7.13	*Equipment maintenance*	*out-of-scope*	—	
A.7.14	*Secure disposal or re-use of equipment*	*out-of-scope*	—	
A.8 · Technological controls (34)				
A.8.1	User endpoint devices	partial	—	
A.8.2	**Privileged access rights**	**primary**	**5** CRITICAL	F-01, F-20, F-23, F-27, F-40
A.8.3	**Information access restriction**	**primary**	—	
A.8.4	*Access to source code*	*out-of-scope*	—	
A.8.5	**Secure authentication**	**primary**	—	
A.8.6	**Capacity management**	**primary**	**6** INFO	F-33, F-34, F-36, F-37, F-41, F-42
A.8.7	Protection against malware	partial	—	
A.8.8	**Management of technical vulnerabilities**	**primary**	—	
A.8.9	**Configuration management**	**primary**	**11** CRITICAL	F-01, F-18, F-19, F-20, F-21, F-22 (+5)
A.8.10	Information deletion	partial	—	
A.8.12	Data leakage prevention	partial	—	
A.8.13	*Information backup*	*contextual*	—	
A.8.14	**Redundancy of information processing facilities**	**primary**	—	
A.8.15	Logging	partial	—	
A.8.16	Monitoring activities	partial	**21** WARN	F-02, F-03, F-04, F-05, F-06, F-07 (+15)
A.8.17	*Clock synchronization*	*out-of-scope*	—	
A.8.18	Use of privileged utility programs	partial	—	
A.8.19	Installation of software on operational systems	partial	**2** WARN	F-18, F-21
A.8.20	**Networks security**	**primary**	—	
A.8.21	**Security of network services**	**primary**	—	
A.8.22	**Segregation of networks**	**primary**	**1** WARN	F-25
A.8.23	*Web filtering*	*out-of-scope*	—	
A.8.24	Use of cryptography	partial	—	
A.8.25	Secure development lifecycle	partial	—	
A.8.26	**Application security requirements**	**primary**	—	
A.8.27	**Secure system architecture and engineering principles**	**primary**	**7** CRITICAL	F-01, F-19, F-20, F-22, F-23, F-26 (+1)
A.8.28	*Secure coding*	*out-of-scope*	—	
A.8.29	**Security testing in development and acceptance**	**primary**	—	
A.8.32	*Change management*	*out-of-scope*	—	
A.8.34	*Protection of information systems during audit testing*	*out-of-scope*	—	

SOC2 · SOC 2 TYPE II

SOC 2 Type II — Trust Services Criteria (AICPA 2017)

21 in-scope items · **6** touched · **6** failing

ITEM	REQUIREMENT	RELEVANCE	HITS	FINDING IDS
CC6 · Logical and Physical Access Controls				
CC6.1	**Logical access security over protected information assets**	**primary**	**5** CRITICAL	F-01, F-20, F-23, F-27, F-40
CC6.2	Prior to system access, credentials are registered and authorized	partial	—	
CC6.3	**Access to protected information assets is based on authorization**	**primary**	—	
CC6.6	**Logical access security measures against threats from outside boundaries**	**primary**	**1** WARN	F-25
CC6.7	Restricts transmission, movement and removal of information	partial	—	
CC6.8	**Prevents or detects against unauthorized or malicious software**	**primary**	**6** CRITICAL	F-01, F-18, F-19, F-21, F-22, F-26
CC7 · System Operations				
CC7.1	**Detection and monitoring procedures for security events**	**primary**	—	
CC7.2	**Monitoring of system components for anomalies (incidents)**	**primary**	**15** WARN	F-02, F-03, F-04, F-05, F-06, F-07 (+9)
CC7.3	Evaluation of identified events to determine incidents	partial	—	
CC7.4	Procedures to respond to identified security incidents	partial	—	
CC7.5	**Identification and resolution of vulnerabilities**	**primary**	—	
CC8 · Change Management				
CC8.1	**Changes to infrastructure and software are authorized and managed**	**primary**	**2** WARN	F-18, F-21
A1 · Availability				
A1.1	**Processing capacity maintained to meet availability commitments**	**primary**	—	
A1.2	**Environmental protections, software, data-backup for recovery**	**primary**	**6** WARN	F-17, F-24, F-28, F-29, F-30, F-31
A1.3	Recovery plan testing	partial	—	
C1 · Confidentiality				
C1.1	**Confidential information is protected during processing and storage**	**primary**	—	
C1.2	Confidential information is disposed of in accordance with objectives	partial	—	
PI1 · Processing Integrity				
PI1.1	Obtains or generates, uses and communicates relevant quality info	partial	—	
PI1.2	System processing is complete, valid, accurate, timely	partial	—	
PI1.4	Inputs are processed completely, accurately and timely	partial	—	
PI1.5	Outputs are reviewed for completeness and accuracy	partial	—	

NIST-CSF · NIST CSF 2.0

NIST Cybersecurity Framework 2.0 — voluntary cybersecurity risk management guidance

19 in-scope items · **4** touched · **4** failing

ITEM	REQUIREMENT	RELEVANCE	HITS	FINDING IDS
GV · Govern				
GV.SC-05	Supply chain risk management requirements in agreements	partial	**2** WARN	F-18, F-21
ID · Identify				
ID.AM-01	Inventories of hardware managed by the organization are maintained	partial	—	
ID.AM-02	**Inventories of software, services managed by the organization**	**primary**	—	
ID.RA-01	**Vulnerabilities in assets are identified, validated and recorded**	**primary**	**2** WARN	F-18, F-21
PR · Protect				
PR.AA-01	**Identities and credentials are issued, managed, verified, revoked**	**primary**	—	
PR.AA-02	Identities are proofed and bound to credentials based on context	partial	—	
PR.AA-03	**Users, services and hardware are authenticated**	**primary**	—	
PR.AA-05	**Access permissions, entitlements and authorizations — least privilege**	**primary**	—	
PR.DS-01	**Confidentiality, integrity and availability of data-at-rest protected**	**primary**	—	
PR.DS-02	**Confidentiality, integrity and availability of data-in-transit protected**	**primary**	—	
PR.IR-01	**Networks and environments are protected from unauthorized access**	**primary**	—	
PR.PS-01	**Configuration management practices established and applied**	**primary**	**9** CRITICAL	F-01, F-19, F-20, F-22, F-23, F-25 (+3)
PR.PS-02	**Software maintained, replaced and removed**	**primary**	—	
DE · Detect				
DE.CM-01	**Networks and network services are monitored for anomalous events**	**primary**	—	
DE.CM-06	External service provider activity and services are monitored	partial	—	
DE.CM-09	**Computing hardware and software are monitored for anomalies**	**primary**	**21** WARN	F-02, F-03, F-04, F-05, F-06, F-07 (+15)
RS · Respond				
RS.MA-02	Incidents are categorized, prioritized and escalated	partial	—	
RC · Recover				
RC.RP-01	Recovery plan is executed during or after an incident	partial	—	
RC.RP-03	Integrity of backups and assets is verified before use for restoring	partial	—	

NSA-CISA · NSA/CISA K8S HARDENING

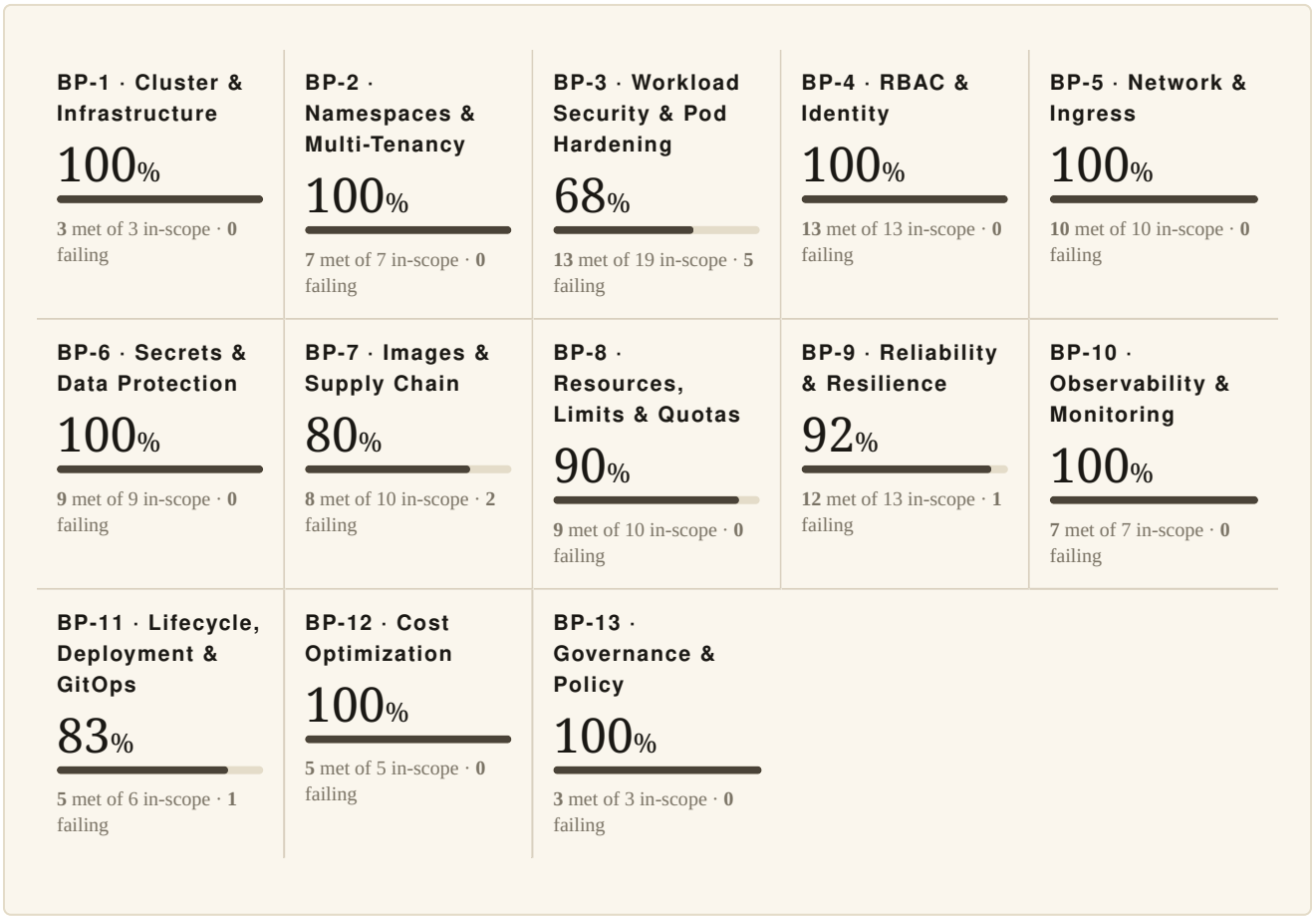
NSA/CISA Kubernetes Hardening Guide v1.2 — US government K8s security baseline

25 in-scope items · **7** touched · **6** failing

ITEM	REQUIREMENT	RELEVANCE	HITS	FINDING IDS
PS · Pod Security				
PS-1	**Run containers as non-root user**	**primary**	**3** WARN	F-20, F-23, F-27
PS-2	**Set immutable / read-only root filesystem**	**primary**	**3** WARN	F-19, F-22, F-26
PS-3	**Disallow privileged containers**	**primary**	**1** CRITICAL	F-01
PS-4	**Disallow privilege escalation**	**primary**	**1** INFO	F-40
PS-5	**Drop unnecessary Linux capabilities**	**primary**	—	
PS-6	**Block hostPath volumes and host namespaces (network/PID/IPC)**	**primary**	**1** WARN	F-25
PS-7	**Apply seccomp / AppArmor / SELinux profiles**	**primary**	—	
PS-8	**Enforce Pod Security Admission baseline minimum**	**primary**	—	
PS-9	Use admission control for image scanning	partial	**2** WARN	F-18, F-21
NS · Network Separation and Hardening				
NS-1	**Default-deny NetworkPolicies in every namespace**	**primary**	—	
NS-2	*Use a CNI plugin that supports NetworkPolicy*	*out-of-scope*	—	
NS-3	Restrict access to the control plane with firewall rules	partial	—	
NS-4	**Encrypt all traffic with TLS (cluster + ingress)**	**primary**	—	
NS-5	**Encrypt etcd at rest with a KMS provider**	**primary**	—	
NS-6	**Avoid NodePort and LoadBalancer services where unnecessary**	**primary**	—	
AA · Authentication and Authorization				
AA-1	**Disable anonymous authentication**	**primary**	—	
AA-2	*Use strong user authentication (OIDC / IAM, MFA)*	*out-of-scope*	—	
AA-3	**RBAC enabled and least-privilege ServiceAccounts**	**primary**	—	
AA-4	**Disable automounting of ServiceAccount tokens by default**	**primary**	—	
AA-5	**Restrict cluster-admin and wildcard permissions**	**primary**	—	
LT · Audit Logging and Threat Detection				
LT-1	**Enable Kubernetes API audit logging**	**primary**	—	
LT-2	Persist audit logs centrally; tamper-evident	partial	—	
LT-3	**Audit policy logs RBAC, secret, and pod-exec events**	**primary**	—	
LT-4	*Runtime threat detection (Falco / Tetragon / similar)*	*out-of-scope*	—	
LT-5	*Monitor for environment-specific anomalies*	*out-of-scope*	—	
UA · Upgrading and Application Security Practices				
UA-1	**Apply security patches and upgrades promptly**	**primary**	—	
UA-2	Run vulnerability scans and penetration tests periodically	partial	—	
UA-3	Remove unused components and services from the cluster	partial	—	
UA-4	Enforce image-signing or trust policies	partial	**2** WARN	F-18, F-21

Operational practices the cluster is following.

This section measures the cluster against **168** practitioner best practices distilled from the kubernetes.io security and configuration guides, the OWASP Kubernetes cheat sheet, the CIS Kubernetes Benchmark, vendor production checklists (Wiz, Sysdig, Palark, Pulumi, Devtron, learnk8s) and the OPA Gatekeeper + Kyverno policy libraries. Of these, **115** are auto-checkable from cluster state — the rest are organisational practices that must be evidenced elsewhere.



Per-category breakdown follows. **Met** = the practice is in scope, no findings hit it. **Failing** = at least one CRITICAL or WARN finding evidences it is not being followed. **Out-of-scope** items are hidden from the per-category tables — they appear in `legal/kubernetes-best-practices-checklist.md` with the organisational evidence they require.

BP-3 · WORKLOAD SECURITY & POD HARDENING

Pod securityContext, capabilities, host-namespace isolation, SA hygiene

19 in-scope items · **13** met · **5** failing

ITEM	PRACTICE	RELEVANCE	HITS	FINDING IDS
3.1	**`privileged: false` on every container**	**primary**	**1** CRITICAL	F-01
3.2	**`allowPrivilegeEscalation: false` on every container**	**primary**	**1** INFO	F-40
3.3	**`runAsNonRoot: true` (or `runAsUser > 0`) on every container**	**primary**	**3** WARN	F-20, F-23, F-27
3.4	**`readOnlyRootFilesystem: true`; writable paths via `emptyDir` only**	**primary**	**3** WARN	F-19, F-22, F-26
3.5	**`capabilities.drop: ["ALL"]`; capabilities re-added explicitly**	**primary**	—	
3.6	**Forbid dangerous caps (NET_ADMIN, SYS_ADMIN, …)**	**primary**	—	
3.7	**`hostNetwork: false`**	**primary**	**1** WARN	F-25
3.8	**`hostPID: false`**	**primary**	—	
3.9	**`hostIPC: false`**	**primary**	—	
3.10	**No `hostPath` mounts to sensitive paths**	**primary**	—	
3.11	**`seccompProfile.type: RuntimeDefault` (or custom) on every container**	**primary**	—	
3.12	**AppArmor / SELinux profile annotation set per workload**	**primary**	—	
3.13	Unsafe sysctls blocked	partial	—	
3.14	**`automountServiceAccountToken: false` unless workload calls API**	**primary**	—	
3.15	No `kubectl exec` / debug containers in production unless audited	partial	—	
3.16	Non-root build user in the Dockerfile (defence in depth)	partial	**3** WARN	F-20, F-23, F-27
3.17	*Dedicated runtime sandbox (gVisor / Kata) for high-risk workloads*	*out-of-scope*	—	
3.18	**No naked Pods — workloads created via Deployment / StatefulSet**	**primary**	—	
3.19	**Use Deployments instead of bare Pods for stateless apps**	**primary**	—	
3.20	**Deny pods that mount the container runtime socket**	**primary**	—	

BP-4 · RBAC & IDENTITY

Authn / authz, ServiceAccount hygiene, cluster-admin minimisation

13 in-scope items · **13** met · **0** failing

ITEM	PRACTICE	RELEVANCE	HITS	FINDING IDS
4.1	**RBAC enabled (`--authorization-mode=Node,RBAC`)**	**primary**	—	
4.2	**Cluster-admin bound to ≤2 named subjects post-bootstrap**	**primary**	—	
4.3	**No wildcard verbs/resources in any Role / ClusterRole**	**primary**	—	
4.4	**Cluster-wide `secrets` read access restricted to platform controllers**	**primary**	—	
4.5	**`escalate`/`bind`/`impersonate` verbs granted only when needed**	**primary**	—	
4.6	**`pods/exec`, `pods/portforward`, `pods/attach` restricted**	**primary**	—	
4.7	**Each workload has a dedicated `ServiceAccount` (never `default`)**	**primary**	—	
4.8	**`automountServiceAccountToken: false` at the SA level when unused**	**primary**	—	
4.9	Bound, projected, short-lived SA tokens — no long-lived `Secret`-backed tokens	partial	—	
4.10	`system:masters` not used outside cluster bootstrap / break-glass	partial	—	
4.11	*External OIDC / IAM identity provider for human cluster access*	*out-of-scope*	—	
4.12	*MFA enforced for every human cluster identity*	*out-of-scope*	—	
4.13	*Quarterly access review; offboarding revokes grants ≤24h*	*out-of-scope*	—	
4.14	RBAC inventory tooling run on every audit	partial	—	
4.15	**`NodeRestriction` admission plugin enabled**	**primary**	—	
4.16	**Anonymous access disabled on the API server**	**primary**	—	

BP-7 · IMAGES & SUPPLY CHAIN

Image pinning, scanning, signing, SBOM, registry hygiene

10 in-scope items · **8** met · **2** failing

ITEM	PRACTICE	RELEVANCE	HITS	FINDING IDS
7.1	**Production images pinned by `@sha256:` digest**	**primary**	—	
7.2	**No `:latest` (or unset) tag in any production manifest**	**primary**	**2** WARN	F-18, F-21
7.3	**`imagePullPolicy: Always` for re-pushable tags**	**primary**	—	
7.4	Allow-listed registries only — block `docker.io/*` wildcards	partial	—	
7.5	Image vulnerability scan gates promotion to prod	partial	—	
7.6	CRITICAL CVEs block deploy; HIGH CVEs require ticket + SLA	partial	—	
7.7	Image signatures verified at admission (Cosign / Notation)	partial	—	
7.8	SBOM generated and stored for every production image	partial	—	
7.9	*Multi-stage builds; minimal base (`scratch` / `distroless` / `alpine`)*	*out-of-scope*	—	
7.10	*No build tools, shells, or package managers in the runtime image*	*out-of-scope*	—	
7.11	OCI metadata labels populated	partial	—	
7.12	*`.dockerignore` excludes `.git`, secrets, build artefacts, and tests*	*out-of-scope*	—	
7.13	*Vulnerability remediation SLA documented (CRIT ≤7d, HIGH ≤30d)*	*out-of-scope*	—	
7.14	*Coordinated Vulnerability Disclosure policy published*	*out-of-scope*	—	
7.15	*Private registry with retention + replication*	*out-of-scope*	—	
7.16	Image promotion uses commit-SHA tags or semver — never floating tags	partial	**2** WARN	F-18, F-21

BP-8 · RESOURCES, LIMITS & QUOTAS

Right-sizing, capacity, headroom, ResourceQuota / LimitRange

10 in-scope items · **9** met · **0** failing

ITEM	PRACTICE	RELEVANCE	HITS	FINDING IDS
8.1	**Every container has CPU and memory `requests`**	**primary**	**6** INFO	F-33, F-34, F-36, F-37, F-41, F-42
8.2	**Every container has memory `limits`**	**primary**	—	
8.3	**CPU `limits` set only when isolation is required**	**primary**	—	
8.4	Requests sized via profiling / load testing / VPA	partial	—	
8.5	**Aggregate requests across all workloads ≤80% of node-pool allocatable**	**primary**	—	
8.6	**`LimitRange` provides defaults so missing fields don't slip through**	**primary**	—	
8.7	**`ResourceQuota` per namespace caps total CPU / memory / pod count**	**primary**	—	
8.8	Ephemeral storage requests + limits set for scratch-writing workloads	partial	—	
8.9	Default `StorageClass` defined; PVCs always reference one	partial	—	
8.10	Node pools sized so a single node loss does not breach quota	partial	—	

BP-11 · LIFECYCLE, DEPLOYMENT & GITOPS

GitOps, IaC, admission policy, progressive delivery, upgrades

6 in-scope items · **5** met · **1** failing

ITEM	PRACTICE	RELEVANCE	HITS	FINDING IDS
11.1	*All manifests in version control; no out-of-band `kubectl apply`*	*out-of-scope*	—	
11.2	*Two-person review rule for prod-targeting PRs*	*out-of-scope*	—	
11.3	*GitOps controller (Argo CD / Flux) reconciles desired state*	*out-of-scope*	—	
11.4	Manifest linting in CI	partial	—	
11.5	Policy-as-Code admission (Kyverno / OPA Gatekeeper)	partial	—	
11.6	*Progressive delivery for high-blast-radius services*	*out-of-scope*	—	
11.7	*Deployment strategy chosen per workload*	*out-of-scope*	—	
11.8	*Rollback path tested; `kubectl rollout undo` rehearsed*	*out-of-scope*	—	
11.9	**Deprecated-API detection before upgrade**	**primary**	—	
11.10	**Removed-API findings always block upgrade**	**primary**	—	
11.11	Standard recommended labels populated	partial	—	
11.12	*ConfigMap / Secret hot-reload configured*	*out-of-scope*	—	
11.13	*Kustomize / Helm with environment overlays*	*out-of-scope*	—	
11.14	*Production data never used unmasked in lower environments*	*out-of-scope*	—	
11.15	Image tag carried as commit SHA so every deploy is traceable	partial	**2** WARN	F-18, F-21

BP-12 · COST OPTIMIZATION

Right-sizing, idle workloads, autoscaling, node-pool strategy

5 in-scope items · **5** met · **0** failing

ITEM	PRACTICE	RELEVANCE	HITS	FINDING IDS
12.1	**Right-size requests against observed usage**	**primary**	—	
12.2	**Identify and shut down idle workloads**	**primary**	—	
12.3	**Top-N most expensive namespaces reviewed monthly**	**primary**	—	
12.4	*Spot / preemptible node pools for fault-tolerant batch / dev*	*out-of-scope*	—	
12.5	*Committed-use / savings-plan discounts for steady workloads*	*out-of-scope*	—	
12.6	Cluster Autoscaler / Karpenter scales node pool down at low traffic	partial	—	
12.7	*Region selection considers data-egress and regulation, not just price*	*out-of-scope*	—	
12.8	Avoid CPU limits where throttling worsens latency	partial	—	
12.9	*Monitoring stack cost is itself tracked*	*out-of-scope*	—	

```
# flagged by: config scan
# Set readOnlyRootFilesystem to true in the container securityContext.

# [11] F-27 · kube-system · container "kube-proxy" is not set to runAsNonRoot
# affects: DaemonSet/kube-proxy
# flagged by: config scan
# Set runAsUser to a non-zero number and runAsNonRoot to true in your pod or container securityContext.
Refer to https://kubernetes.io/docs/tasks/configure-pod-container/security-context/ for details.
```

Re-run the scan pipeline after remediation. The score, trend line, and confidence distribution all update on the next pass.