EXECUTIVE SUMMARY · FOR PLATFORM

3 criticals to fix, 5 warnings. Biggest lever: revoke cluster-admin bindings and drop privileged:true.

SCORE	Δ VS. PRIOR	CRITICAL	WARNINGS	AVG CONFIDENCE
61/100	+13 pts	3	5	0.63

HEADLINE FINDINGS

- CRITICAL `kube-system` Container running with privileged: true 1.00
- CRITICAL `cluster` ServiceAccount bound to cluster-admin 0.67
- WARN `production` No NetworkPolicy in production namespace 0.67
- WARN `production` CPU limits not set 0.67
- WARN `staging` Image uses :latest tag 0.33

AUDIT CONTEXT

Cluster `prod-eu-central`, audited 2026-04-19 22:26. Posture score **61/100** (prior: 48/100). `dump SHA-256: a3f8c21d9e0b4756…`

Findings are fused across **9 scanner(s)**: `kubescape, trivy, kubeaudit, polaris, kube-score, popeye, pod-status, events, service-endpoints`. When multiple independent tools 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 static manifests dumped via `kubectl cluster-info dump`, enriched by optional live/read-only tooling where available. Secrets, JWTs, AWS keys, and PEM blocks are redacted from all evidence excerpts before printing.

FINDINGS · 8 TOTAL · FUSED FROM ALL SCANNERS

Every signal, with source attribution.

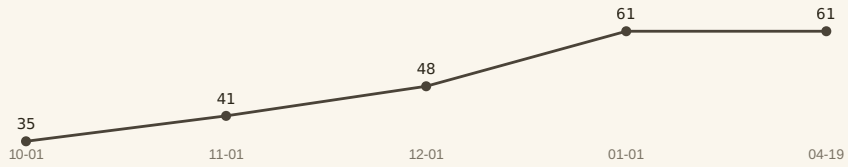
Rows are deduplicated across scanners: when multiple tools independently flag the same `(namespace, resource, issue)`, they collapse into one row. The **Sources** column shows which tools agreed, and **Confidence** reflects how corroborated the finding is — higher bars = more independent tools converged.

ID	SEV	NAMESPACE	RESOURCE	FINDING	SOURCES	CONF
F-01	CRITICAL	kube-system	DaemonSet/node-agent	Container running with privileged: true	kubeaudit kubescape polaris	1.00
F-02	CRITICAL	cluster	ClusterRoleBinding/ci-builder	ServiceAccount bound to cluster-admin	kube-score kubescape	0.67
F-03	WARN	production	Namespace/production	No NetworkPolicy in production namespace	kube-score kubescape	0.67
F-04	WARN	production	Deployment/api-server	CPU limits not set	kube-score polaris	0.67
F-05	WARN	staging	Deployment/frontend	Image uses :latest tag	trivy	0.33
F-06	CRITICAL	production	Deployment/payment-service	CVE-2024-3094 in libxz (CVSS 10.0)	trivy	0.33
F-07	WARN	monitoring	Deployment/prometheus	Container may run as root (runAsNonRoot not set)	kubeaudit polaris	0.67
F-08	WARN	production	Deployment/auth-service	Single replica — no high availability	kube-score popeye	0.67

COMPLIANCE · TREND

Compliance mapping & score trajectory.

SCORE TREND (CONFIDENCE-WEIGHTED)



This audit

61/100

Prior: 48/100

FRAMEWORK MAPPING

Framework references per finding. Full per-framework breakdown on the following pages.

ID	SEV	FINDING	FRAMEWORK REFERENCES	CONF
F-01	CRITICAL	Container running with privileged: true	CIS: 5.2.5 CRA: art.10 SOC2: CC6.6	1.00
F-02	CRITICAL	ServiceAccount bound to cluster-admin	CIS: 5.1.1 CRA: art.13 SOC2: CC6.3	0.67
F-03	WARN	No NetworkPolicy in production namespace	CIS: 5.3.2 CRA: art.13 SOC2: CC6.1	0.67
F-04	WARN	CPU limits not set	CIS: 5.7.1 SOC2: A1.1	0.67
F-05	WARN	Image uses :latest tag	CIS: 5.1.4 CRA: art.13 SOC2: CC8.1	0.33
F-06	CRITICAL	CVE-2024-3094 in libxz (CVSS 10.0)	CRA: art.13 SOC2: CC7.1	0.33
F-07	WARN	Container may run as root (runAsNonRoot not set)	CIS: 5.2.6 CRA: art.10 SOC2: CC6.6	0.67
F-08	WARN	Single replica — no high availability	SOC2: A1.2	0.67

Framework references are indicative and should be reviewed with your compliance team. CIS benchmarks: v1.9 for Kubernetes. CRA = EU Cyber Resilience Act, article references. SOC2 categories map to the CC (Common Criteria) and A1 (Availability) control families.

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%	62%	34%	53%	67%	34%
5 of 10 in-scope items touched **5** failing	5 of 8 in-scope items touched **5** failing	10 of 29 in-scope items touched **10** failing	10 of 19 in-scope items touched **10** failing	4 of 6 in-scope items touched **4** failing	14 of 41 in-scope items touched **14** 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.

NIS2 · NIS2 DIRECTIVE

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union

10 in-scope items · **5** touched · **5** failing

ITEM	REQUIREMENT	RELEVANCE	HITS	FINDING IDS
Art.20 · Governance				
20.1	Management bodies approve and oversee risk-management measures	out-of-scope	—	
20.2	Management bodies follow training; employees encouraged similarly	out-of-scope	—	
Art.21 · Cybersecurity risk-management measures				
21.2.a	Policies on risk analysis and information system security	contextual	—	
21.2.b	Incident handling	partial	—	
21.2.c	Business continuity, backup, crisis management, disaster recovery	partial	**2** WARN	F-04, F-08
21.2.d	Supply chain security (including direct suppliers/ service providers)	partial	**2** CRITICAL	F-05, F-06
21.2.e	**Security in acquisition, development and maintenance + vulnerability handling**	**primary**	**5** CRITICAL	F-01, F-03, F-05, F-06, F-07
21.2.f	Policies and procedures to assess effectiveness of measures	contextual	—	
21.2.g	**Basic cyber hygiene and cybersecurity training**	**primary**	**2** CRITICAL	F-01, F-07
21.2.h	Cryptography and, where appropriate, encryption	partial	—	
21.2.i	**Human resources security, access control, asset management**	**primary**	**2** CRITICAL	F-02, F-03
21.2.j	Multi-factor authentication, secured communications, emergency comms	partial	—	
Art.23 · Reporting obligations				
23.1	Significant incidents notified without undue delay	out-of-scope	—	
23.4	Early warning within 24h, incident notification within 72h, final report 1 month	out-of-scope	—	

GDPR · GDPR

Regulation (EU) 2016/679 — General Data Protection Regulation

8 in-scope items · **5** touched · **5** failing

ITEM	REQUIREMENT	RELEVANCE	HITS	FINDING IDS
Art.5 · Principles of processing personal data				
5.1.f	**Integrity and confidentiality — appropriate technical/organisational measures**	**primary**	**4** CRITICAL	F-01, F-02, F-03, F-07
Art.25 · Data protection by design and by default				
25.1	**Appropriate technical and organisational measures implemented by design**	**primary**	**2** CRITICAL	F-02, F-03
25.2	Only personal data necessary for each purpose processed by default	contextual	—	
Art.32 · Security of processing				
32.1.a	Pseudonymisation and encryption of personal data	partial	—	
32.1.b	**Ongoing confidentiality, integrity, availability and resilience**	**primary**	**5** CRITICAL	F-01, F-03, F-06, F-07, F-08
32.1.c	Ability to restore availability and access after incident	partial	—	
32.1.d	**Regular testing and evaluation of effectiveness**	**primary**	**2** CRITICAL	F-05, F-06
32.2	**Risks from destruction, loss, alteration, unauthorised disclosure/access**	**primary**	**1** CRITICAL	F-02
Art.33 · Notification of a personal data breach				
33.1	Notify supervisory authority within 72 hours	out-of-scope	—	

DORA · DORA

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

29 in-scope items · **10** touched · **10** 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**	**1** WARN	F-04
7.d	**Technologically resilient to adequately deal with additional needs under stress**	**primary**	**1** WARN	F-04
Art.8 · Identification				
8.1	Identify, classify and document ICT-supported business functions	partial	—	
8.2	**Identify information and ICT assets, their interconnections**	**primary**	**1** WARN	F-05
8.3	Identify and document all processes dependent on ICT 3rd parties	partial	**1** CRITICAL	F-06
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**	**2** CRITICAL	F-01, F-07
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**	**3** CRITICAL	F-01, F-03, F-07
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** CRITICAL	F-05, F-06
9.4.e	**Physical and logical access control to ICT assets**	**primary**	**4** CRITICAL	F-01, F-02, F-03, F-07
9.4.f	Strong authentication mechanisms + key management	partial	—	
Art.10 · Detection				
10.1	**Detect anomalous activities, including ICT network performance + incidents**	**primary**	—	
10.2	**Multiple layers of control, alert thresholds, criteria**	**primary**	—	
10.3		partial	—	

ITEM	REQUIREMENT	RELEVANCE	HITS	FINDING IDS
	Automated alert mechanisms for staff responsible for response			
Art.11 · Response and recovery				
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**	**1** WARN	F-08
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	—	

CRA · CRA

Regulation (EU) 2024/2847 — Cyber Resilience Act

19 in-scope items · **10** touched · **10** failing

ITEM	REQUIREMENT	RELEVANCE	HITS	FINDING IDS
Annex I.1 · Product cybersecurity requirements				
I.1.1	**Appropriate level of cybersecurity based on risks**	**primary**	—	
I.1.2.a	**Delivered without known exploitable vulnerabilities**	**primary**	**1** CRITICAL	F-06
I.1.2.b	**Secure-by-default configuration**	**primary**	**2** CRITICAL	F-01, F-07
I.1.2.c	Security updates automatic or notified to user	partial	—	
I.1.2.d	**Protection from unauthorised access via authentication/identity controls**	**primary**	**2** CRITICAL	F-02, F-03
I.1.2.e	Confidentiality of stored, transmitted or processed data (encryption)	partial	—	
I.1.2.f	**Integrity of stored, transmitted or processed data**	**primary**	—	
I.1.2.g	Minimise data processed (principle of data minimisation)	contextual	—	
I.1.2.h	**Availability of essential/basic functions, including DoS resilience**	**primary**	**2** WARN	F-04, F-08
I.1.2.i	**Minimise negative impact on availability of services by other devices/networks**	**primary**	**1** WARN	F-04
I.1.2.j	**Limit attack surfaces, including external interfaces**	**primary**	**2** CRITICAL	F-01, F-03
I.1.2.k	**Reduce impact of incidents via exploitation-mitigation techniques**	**primary**	**2** CRITICAL	F-01, F-07
I.1.2.l	Security-related information via recording/ monitoring of internal activity	partial	—	
I.1.2.m	Users can securely delete all data and settings	contextual	—	
Annex I.2 · Vulnerability handling requirements				
I.2.1	**Identify and document vulnerabilities and components (SBOM)**	**primary**	**2** CRITICAL	F-05, F-06
I.2.2	**Address/remediate vulnerabilities without delay**	**primary**	**1** CRITICAL	F-06
I.2.3	**Apply effective/regular tests and reviews of security**	**primary**	—	
I.2.4	Once update addresses issue, share information publicly	out-of-scope	—	
I.2.5	Policy on coordinated vulnerability disclosure	out-of-scope	—	
I.2.6	Facilitate sharing of info about potential vulnerabilities	out-of-scope	—	
I.2.7	Secure distribution mechanism for updates	partial	**1** WARN	F-05
I.2.8	Security patches disseminated without delay + free of charge	contextual	—	

CER · CER DIRECTIVE

Directive (EU) 2022/2557 — Resilience of Critical Entities

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

ITEM	REQUIREMENT	RELEVANCE	HITS	FINDING IDS
Art.12 · Risk assessment by critical entities				
12.1	Risk assessment within 9 months of designation, every 4 years	contextual	—	
12.2	All relevant natural and man-made risks	contextual	—	
Art.13 · Resilience measures of critical entities				
13.1.a	Prevent incidents (incl. disaster risk reduction, climate adaptation)	partial	**4** CRITICAL	F-01, F-03, F-06, F-07
13.1.b	Adequate physical protection of premises and critical infrastructure	out-of-scope	—	
13.1.c	Respond, resist and mitigate consequences of incidents	partial	**2** CRITICAL	F-01, F-03
13.1.d	Recover from incidents (business continuity, alternative supply chains)	partial	**2** WARN	F-04, F-08
13.1.e	Employee security management (access rights, background checks)	partial	**1** CRITICAL	F-02
13.1.f	Raise awareness of the measures among personnel	out-of-scope	—	
Art.14 · Background checks				
14.1	Background checks for persons in sensitive roles	out-of-scope	—	
Art.15 · Incident notification				
15.1	Notify competent authority of significant disruptions	out-of-scope	—	
15.3	Initial notification within 24 hours, detailed report within 1 month	out-of-scope	—	

ISO27001 · ISO/IEC 27001:2022

ISO/IEC 27001:2022 — Information security management systems

41 in-scope items · **14** touched · **14** 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	**1** CRITICAL	F-02
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**	**1** CRITICAL	F-02
A.5.16	**Identity management**	**primary**	—	
A.5.17	Authentication information	partial	—	
A.5.18	**Access rights**	**primary**	**1** CRITICAL	F-02
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**	**1** CRITICAL	F-06
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**	**1** WARN	F-08
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	—	

ITEM	REQUIREMENT	RELEVANCE	HITS	FINDING IDS
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	—	
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**	**3** CRITICAL	F-01, F-02, F-07
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**	**1** WARN	F-04
A.8.7	Protection against malware	partial	—	
A.8.8	**Management of technical vulnerabilities**	**primary**	**1** CRITICAL	F-06
A.8.9	**Configuration management**	**primary**	**3** CRITICAL	F-01, F-05, F-07
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**	**1** WARN	F-08
A.8.15	Logging	partial	—	
A.8.16	Monitoring activities	partial	—	
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** CRITICAL	F-05, F-06
A.8.20	**Networks security**	**primary**	**1** WARN	F-03
A.8.21	**Security of network services**	**primary**	—	
A.8.22	**Segregation of networks**	**primary**	**1** WARN	F-03
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**	**2** CRITICAL	F-01, F-07
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	—	

REMEDIATION · RUNBOOK

Fix list, copyable, severity-ordered.

3 critical + 5 warning finding(s) below, grouped by issue-class × namespace so duplicate remediations collapse. 0 informational finding(s) are listed on page 2 only. Placeholders (<DEPLOY>, <CTR>, <SVC>) must be substituted. Apply in non-production first and verify with `kubectl diff` before `kubectl apply`.

```
# ═══ CRITICAL ═══

# [1] F-01 · kube-system · Container running with privileged: true
# affects: DaemonSet/node-agent
# flagged by: kubeaudit, kubescape, polaris
kubectl patch daemonset node-agent -n kube-system --type=json -p '[{"op":"remove","path":"/spec/template/
spec/containers/0/securityContext/privileged"}]'

# [2] F-02 · cluster · ServiceAccount bound to cluster-admin
# affects: ClusterRoleBinding/ci-builder
# flagged by: kube-score, kubescape
kubectl delete clusterrolebinding ci-builder
# Create a least-privilege ClusterRole instead

# [3] F-06 · production · CVE-2024-3094 in libxz (CVSS 10.0)
# affects: Deployment/payment-service
# flagged by: trivy
docker build --no-cache -t payment:2.1.1 .
kubectl set image deployment/payment-service payment=registry.internal/payment:2.1.1 -n production

# ═══ WARN ═══

# [4] F-03 · production · No NetworkPolicy in production namespace
# affects: Namespace/production
# flagged by: kube-score, kubescape
kubectl apply -f - <<EOF
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: default-deny
  namespace: production
spec:
  podSelector: {}
  policyTypes: [Ingress, Egress]
EOF

# [5] F-04 · production · CPU limits not set
# affects: Deployment/api-server
# flagged by: kube-score, polaris
kubectl set resources deployment api-server -n production --limits=cpu=500m,memory=512Mi

# [6] F-05 · staging · Image uses :latest tag
# affects: Deployment/frontend
# flagged by: trivy
# Pin to a specific digest:
kubectl set image deployment/frontend nginx=nginx:1.25.4@sha256:abc123 -n staging

# [7] F-07 · monitoring · Container may run as root (runAsNonRoot not set)
# affects: Deployment/prometheus
# flagged by: kubeaudit, polaris
# Add to container securityContext:
runAsNonRoot: true
runAsUser: 65534

# [8] F-08 · production · Single replica — no high availability
# affects: Deployment/auth-service
# flagged by: kube-score, popeye
kubectl scale deployment auth-service --replicas=2 -n production
# Also add a PodDisruptionBudget
```

Re-run the scan pipeline after remediation (`./run-scans.sh && python3 k8s_audit_report.py`) — the score, trend line, and confidence distribution all update on the next pass.