MYSMARTOPS

Security Assessment Pipeline Outputs

GCP · GKE · IRAP-001

AUTOMATED SECURE ASSURANCE PIPELINE — SAMPLE OUTPUT

Generated by the MySmartOps automated secure assurance pipeline | Control framework: IRAP-aligned (NIST 800-53 control identifiers) | Environment: Google Kubernetes Engine (PROTECTED)

This report is a representative sample of the evidence and narrative produced automatically by the MySmartOps secure assurance pipeline. Security posture is measured continuously across a core set of controls, findings and strengths are gathered from live telemetry, and an assessor-ready narrative is generated for each control — materially reducing manual effort and expediting the IRAP review process.

Assessment summary

16	16	6	0
CONTROLS ASSESSED	STRENGTHS VERIFIED	HIGH-SEVERITY FINDINGS	CRITICAL FINDINGS

The environment demonstrates a strong overall posture with no critical findings. Six high-severity issues are concentrated in account and privilege management, audit logging, and transmission security. The strongest areas are least functionality, authentication, cryptographic key management, and supply-chain protection. The highest-priority actions are to tighten account lifecycle management and restore complete audit coverage.

High-severity findings

CONTROL	SEVERITY	FINDING	RECOMMENDED REMEDIATION
AC-2	HIGH	Cluster-admin bindings over-provisioned	Scope cluster-admin roles to specific namespaces; grant minimum required permissions only.
AC-6	HIGH	Cluster-admin bindings over-provisioned	Replace cluster-admin with namespace-scoped roles.
AU-2	HIGH	Sysdig agent coverage below 100% — audit records missing from unmonitored nodes	Deploy Sysdig as a DaemonSet on all nodes for complete audit coverage.
AU-2	HIGH	Zero Sysdig events in the last 30 days — audit pipeline may be broken	Verify Sysdig agents are connected and forwarding events to Sysdig Secure SaaS.
SC-8	HIGH	Certificates expiring within 30 days	Trigger cert-manager renewal now; set renewBefore=24h for internal certs.
IR-4	HIGH	IR playbooks not reviewed within 90 days	Review and update all IR playbooks; schedule a quarterly review.

Verified strengths

CONTROL	POSITIVE CONTROL CONFIRMED BY TELEMETRY
CM-7	PSA restricted enforced — least-functionality baseline met; zero OPA Gatekeeper violations.
AC-2	Workload Identity fully enabled.
AC-6	Workload Identity at 100% coverage.
IA-2	Workload Identity fully enabled — no static credentials.
IA-5	All KMS keys have a rotation policy configured.
AU-12	100% Sysdig coverage — complete audit record generation.
SC-7	Default-deny firewall and Kubernetes NetworkPolicy both active.
SC-8	Istio mTLS in STRICT mode — all inter-service traffic encrypted.
SC-12	All KMS keys have a rotation policy.
SC-28	etcd encrypted with Cloud KMS CMEK.
SI-3	Sysdig enforce mode on all nodes with 100% coverage.
SI-4	100% monitoring coverage with no unresolved critical events.
SA-11	Security pipeline active with the merge gate enforced.
SA-12	Binary Authorization enforced with 100% signed images.
IR-4	IR playbooks current and tested; automated response active.

Control-by-control narrative

CM-7 — Least Functionality

2 strengths 0 findings

The Least Functionality control (CM-7) is well implemented in the GKE Kubernetes environment. Key metrics demonstrate a strong posture: PSA restricted enforced, zero OPA Gatekeeper violations, and no privileged or root-user pods running. The environment also benefits from enabled auto-upgrades, shielded VMs, and AppArmor-enabled nodes, providing robust protection against misuse of excessive permissions. No critical risks were identified; the assessor recommends periodically reviewing active OPA constraints so they continue to enforce least functionality as the environment evolves.

AC-2 — Account Management

1 finding 1 strength

The posture for Account Management has areas of concern. The high-severity finding of over-provisioned cluster-admin bindings poses a significant risk, as excessive administrator privileges could allow an attacker to gain full control of the environment and potentially access or compromise PROTECTED data. The use of Workload Identity is a positive control, ensuring access is tightly scoped to authorised applications and services. To address the most critical risk, scope cluster-admin roles to specific namespaces and grant the minimum required permissions, limiting the potential impact of a breach.

AC-6 — Least Privilege

1 finding 1 strength

The AC-6 Least Privilege posture has mixed results. The environment has achieved 100% Workload Identity coverage with no root-user pods or exposed service-account keys, but a high-severity risk exists around over-provisioned cluster-admin bindings, which could allow elevated privileges and unauthorised access to PROTECTED data. The most important remediation is to replace the broad cluster-admin role with granular, namespace-scoped roles that provide only the minimum necessary permissions for each workload.

IA-2 — Identification and Authentication

1 strength 0 findings

The environment demonstrates a strong posture for Identification and Authentication. Workload Identity is fully enabled, so all workloads leverage federated identity management rather than static credentials, mitigating the risk of credential theft and unauthorised access to PROTECTED data. No plaintext credentials were detected, further reducing the attack surface. The key recommendation is to continue monitoring for configuration drift from this optimal state.

IA-5 — Authenticator Management

1 strength 0 findings

The IA-5 Authenticator Management posture is strong. All four KMS keys have rotation policies configured, ensuring regular key refreshment and mitigating the risk of compromised credentials reaching PROTECTED data. There are no overdue KMS key rotations, exported service-account keys, or disabled KMS keys. The recommendation is to maintain a process that regularly reviews rotation status for any newly added secrets to ensure continued compliance.

AU-2 — Audit Events

2 findings 0 strengths

The AU-2 Audit Events posture is weak, with incomplete Sysdig agent coverage across nodes and no audit events reported in the last 30 days. This is a significant risk: the absence of comprehensive audit logging leaves the environment blind to potential incidents or malicious activity affecting PROTECTED data. The most important remediation is to immediately deploy the Sysdig agent as a DaemonSet across all nodes to ensure complete coverage and reliable forwarding of security events to the Sysdig Secure SaaS platform.

AU-12 — Audit Record Generation

1 strength 0 findings

The environment is achieving full audit record generation, with the Sysdig agent monitoring all three nodes. This provides comprehensive visibility into security-relevant events, a critical requirement for PROTECTED environments. While there were a small number of audit-record violations in the last 30 days, the overall posture is strong. The single most important action is to investigate the root cause of those violations and implement changes to ensure flawless audit record generation.

SC-7 — Boundary Protection

1 strength 0 findings

The environment has a robust boundary-protection posture, with a default-deny firewall and network policy effectively restricting access to sensitive resources. No exposed sensitive ports and no nodes with public IP addresses further strengthen the perimeter. VPC flow logs and strict Istio mTLS provide comprehensive visibility and encryption of network traffic, reducing the risk of unauthorised access to PROTECTED data. The team should consider enabling Private Google Access to further minimise the attack surface.

SC-8 — Transmission Confidentiality and Integrity

1 finding 1 strength

The SC-8 posture is mixed. Istio mTLS is enforced in STRICT mode, ensuring all inter-service traffic is encrypted, but a high-severity issue exists: several certificates expire within 30 days. Expired certificates could cause service disruption and potential data leaks of PROTECTED information flowing between services. The critical action is to trigger an immediate renewal of the expiring certificates, reducing the window of vulnerability and ensuring continuity of secure communications.

SC-12 — Cryptographic Key Management

1 strength 0 findings

The SC-12 posture is positive. The environment maintains four KMS keys, all with an active rotation policy to ensure regular cycling of encryption keys, mitigating long-term exposure of PROTECTED data should a key be compromised. etcd encryption is enabled and no plaintext credentials were detected. No critical risks or overdue rotations were found. The recommendation is continued vigilance in monitoring rotation schedules and extending rotation policies to any newly provisioned keys.

SC-28 — Protection of Information at Rest

1 strength 0 findings

Protection of information at rest is strong. Encryption of the etcd data store using Cloud KMS Customer-Managed Encryption Keys (CMEK) ensures PROTECTED data remains secure even if underlying infrastructure is compromised. There are no findings of concern, and required KMS keys are enabled with no overdue rotations. The recommendation is to regularly review the KMS key rotation schedule for alignment with organisational policy.

SI-3 — Malicious Code Protection

1 strength 0 findings

The environment has a strong malicious-code-protection posture, with Sysdig enforce mode enabled on 100% of nodes and 100% policy coverage. All running containers are subject to robust AppArmor profiles that restrict access and behaviour, mitigating malware execution. With no critical vulnerabilities in container images and Binary Authorization enforced, exposure to malicious code affecting PROTECTED data is very low. The recommendation is to maintain this high level of coverage and enforcement.

SI-4 — Information System Monitoring

1 strength 0 findings

The environment has a robust monitoring posture, with 100% coverage and no unresolved critical events over the past 30 days, providing comprehensive visibility for timely detection and response. Maintaining this high level of monitoring is crucial to protect the confidentiality, integrity, and availability of PROTECTED data. To strengthen further, the team should implement centralised log management and analysis for deeper insight and more advanced threat hunting.

SA-11 — Developer Security Testing

1 strength 0 findings

The SA-11 posture is strong. All repositories have an active security pipeline that blocks unsafe code from merging, and branch protection prevents direct commits. There are no critical security issues open, security scans are frequent, and signed commits are required. To strengthen further, integrate automated code analysis into the security gate to proactively identify and remediate insecure coding practices before they reach production, better protecting PROTECTED data assets.

SA-12 — Supply Chain Protection

1 strength 0 findings

The environment has an excellent supply-chain-protection posture. Binary Authorization is enforced, with 100% of container images signed before deployment, preventing execution of malicious or vulnerable code and mitigating supply-chain attacks against PROTECTED data. All images are scanned for vulnerabilities with no critical CVEs and none from public registries, and SBOM coverage is 100%. The recommendation is to maintain this robust configuration.

IR-4 — Incident Handling

1 finding 1 strength

Incident handling has several strengths: IR playbooks in place, automated response enabled, and fast mean time to detection (8 seconds) and resolution (3 hours). However, the high-severity risk is that these playbooks have not been reviewed within the last 90 days, potentially leaving the environment exposed to evolving threats and delaying response to attacks against PROTECTED data. The most important remediation is to review and update all IR playbooks on a quarterly basis.