Patch management policy for a SaaS company

SaaS company variant: paste over the same-numbered sections of the general policy

1 Purpose and scope

1.1 This policy covers production and non-production workloads of [Company name]: host operating systems, container base images, application images, libraries and packages, build tooling, managed databases and queues, and employee endpoints.

1.2 For each managed service, the inventory records which patches the provider applies and which the company applies (the shared responsibility line). Provider-applied patches are monitored through [provider notices], not assumed.

3 Asset inventory

3.1 The inventory adds: image name and digest; base image and its source; package manifest or software bill of materials for each release; the pipeline that builds it; runtime location (cluster, region, account).

3.2 Inventory data is read from the cloud provider and the registry by API at least [daily].

4 Severity and patch windows

4.1 Windows follow general policy section 4.3.

4.2 For a container or image, the window ends when a rebuilt image is running in production and the vulnerable image is no longer running, not when the rebuild is merged.

4.3 Third-party and open source components are patched by updating the dependency and rebuilding. The pipeline fails a release that carries a class 1 or class 2 finding unless an exception is recorded.

5 Testing and staging

5.1 Patched images go through the same automated tests as any release. They deploy to [canary percent] of production first, then expand if error rate and latency stay within [thresholds] for [period].

5.2 Rollback is redeployment of the previous image digest.

6 Maintenance windows

6.1 Rolling replacement is the default and needs no customer-visible window. Hosts that cannot be replaced use the standard windows in general policy section 6.

6.2 Live kernel patching, where used, covers only the vulnerabilities its vendor supports. It does not replace the next scheduled reboot or replacement.

8 Reporting and metrics

8.1 Reports add: share of running workloads on an image younger than [30] days; oldest running image age; findings past window by team.

8.2 For each monthly report, export from [system]: the inventory snapshot, the list of changes with test evidence, and the exceptions list. These are the records given to an auditor.