Tasktop Hub Cloud Architecture and Operations

This document is provided in addition to the documentation available in the Tasktop Trust Centre at https://www.tasktop.com/trust

Deployment Architecture Overview

Tasktop Integration Hub Cloud is deployed as a single tenanted application with isolated processing and databases per customer. Each customer application is deployed in a private firewalled network and is isolated from other customers. Each of the instances is accessed through a unique subdomain.

Backup Policy

Tasktop Integration Hub and Keycloak databases are backed up multiple times per day using a combination of database snapshots (1x/day) and database exports (4x/day). Backups are retained for up to 30 days.

Log Retention Policy

Tasktop Integration Hub logs, Keycloak logs, system logs, and load balancer logs are retained for up to 1 year for security audit purposes.

Penetration Testing

Penetration tests are conducted once per year by a reputable third party security firm. This firm provides a letter of attestation confirming that Tasktop Integration Hub Cloud is free from critical and high severity security issues.

Incident Response Plan

Included is an extract from our Security Incident Response Plan. The plan is reviewed at least annually. Tasktop performs table top exercises on a regular basis.

Static Scanning

Tasktop conducts static analysis of our code base regularly. Static analysis is used to evaluate source code against known bad coding practices, as well as common vulnerabilities as defined in the industry best practice documents such as OWASP Top 10, SANS CWE Top 25, and similar.

Dynamic Scanning

Tasktop conducts dynamic web application scanning of Tasktop Integration Hub product regularly. These scans are conducted with a configuration that tests for common vulnerabilities as defined in the industry best practice documents such as OWASP Top 10, SANS CWE Top 25, and similar.

Component Analysis

Tasktop Integration Hub 3rd party components and libraries are scanned regularly to assess for known security vulnerabilities. This approach aggregates public security vulnerability data through a 3rd party provider and compares it with the components used in our assembled product to ensure that known vulnerabilities are found and addressed in a timely manner.