CHECKLIST

CLOUD SECURITY PARTNERS

okta Security Review

Administrative & Org Hardening

1. Identify all Okta orgs (**prod**, **preview**, **sandbox**) and ensure configuration backups exist.
2. Use **read-only admins** for discovery and separate, monitored **break-glass accounts** exempt from lockout.
3. Enumerate **all admin** accounts, remove **stale users**, and validate **least-privilege** role assignments.
4. Enforce **phishing-resistant MFA** for all administrative access.
5. Confirm System Log export to **SIEM**, ensuring auth, admin, policy, and app events are captured.
6. Document **IdP** outage recovery procedures and **break-glass** monitoring protocols.

Identity & Lifecycle Management

7. Validate identity sources (**HR**, **AD**, **SCIM**) and confirm automated provisioning/deprovisioning.
8. Review User Profile Policies (**enrollment**, **identification controls**) and Okta Account Management policies.
9. Identify orphaned or inactive users and ensure terminated accounts **lose** all app access and sessions immediately.
10. Review group rules and external IdP trust relationships to **prevent** privilege creep.
11. Disable self-service registration unless **strictly** required.

Network & Connectivity Security

12. Review number/size of IP ranges; verify broad ranges are **not** used in policy rules.
13. Ensure secure configuration **and** certificate validity.
14. Block traffic from risky geographies and anonymous networks (**TOR**, **VPNs**).
15. Enforce device assurance and posture checks (**FastPass**/**MDM**) to block unmanaged devices.

Authentication & Policy Logic

16. Identify defined IdPs/Authenticators and review Enrollment Policies for **unenrolled** users.
17. Confirm **consistent** MFA enforcement, behavior detection usage, and session/refresh lifetimes.
18. Review **password** complexity, history, exclusions, reset rules, and breach protection.
19. Confirm **no policies** allow single-factor authentication or treat users without a second factor insecurely.
20. Specifically **block** legacy authentication protocols, particularly in Office 365 policies.

Application & API Security

21. Review Application Sign-In Policies, especially the "Default" policy, to ensure **no implicit** allowances.
22. Inventory **all apps** and **API tokens**, removing excessive scopes, unused integrations, and unknown tokens.
23. Review SAML/OIDC settings (**SHA256**, **redirect URIs**) and restrict unnecessary IdP-initiated SSO.
24. Confirm apps inherit global policies **unless** justified, and validate logout/session revocation.
25. Rotate client secrets and review hooks/workflows for **potential** data exposure.

Monitoring & Threat Detection

26. Enable **anomaly detection** for impossible travel, brute force, and risky login patterns.
27. Configure **real-time alerts** for admin changes, MFA resets, token creation, and policy edits.
28. **Validate** rate limits, abuse detection, and System Log retention periods.

Reach out to Cloud Security Partners today for help reviewing your Okta organization.

cloudsecuritypartners.com cloud-security-partners