THREATIQ | LABS

THREATIQ LABS · ONE-PAGE CHECKLIST

SSO Logging Validation Checklist

Confirm an application produces — and your SIEM actually receives — security telemetry beyond sign-in.

Companion to Field Note #001 · "Why SSO Is Not Logging." Any unchecked box is a visibility gap.

APPLICATION _____ REVIEWED BY _____ DATE _____

1 · Authentication

- [ ] Sign-in successes and failures are logged
- [ ] MFA challenges and results are captured
- [ ] Session creation / token issuance recorded
- [ ] These events reach the SIEM (verified)

2 · Administrative Activity

- [ ] Admin / privileged console actions are logged
- [ ] Role and permission changes are captured
- [ ] Tenant / global config changes recorded
- [ ] Admin activity reaches the SIEM with user ID

3 · Security-Relevant User Activity

- [ ] Data access / record views logged where needed
- [ ] Exports, downloads, and bulk actions captured
- [ ] Sharing / external-access events recorded
- [ ] Sensitive API calls are logged and forwarded

4 · Configuration Changes

- [ ] Security policy changes are logged
- [ ] Integration / OAuth grant creation captured
- [ ] Logging / SIEM-forwarding changes are logged
- [ ] Changes attributable to a specific user

5 · Validation

- [ ] SIEM confirmed receiving each expected source
- [ ] Source health / heartbeats alert on silence
- [ ] Volume baselines exist to detect log drops
- [ ] Named owner signs off before go-live
- [ ] Coverage re-checked on a schedule

Score your coverage

Every box checked = defensible coverage.
Any box empty = a blind spot to close now.

SSO proves someone got in. Logging tells you what they did next.

info@threatiqlabs.com · threatiqlabs.com