THREATIQ | LABS

THREATIQ LABS FIELD NOTES

Why SSO Is Not Logging.

Closing the visibility gap between authentication and security telemetry.

FIELD NOTE #001

THE PROBLEM

SSO Enabled ≠ Security Visibility

Single sign-on is a gate, not a camera. Once someone is through it, SSO can’t tell you what they did next.

What SSO tells you

- Who authenticated
- When they signed in
- Source IP and device
- Whether MFA was satisfied
- Which application was accessed

What SSO can’t tell you

- What they did inside the app
- Which data they viewed or exported
- Admin and privileged actions taken
- Security and configuration changes
- New access or OAuth grants created
- Whether the app even logs at all
- Whether those logs reach the SIEM

THE THREATIQ LABS MINIMUM LOGGING STANDARD

Five things every critical app should log.

Not more data — the right data. If an application can’t produce these, it can’t be defended or audited.

1 Authentication

Establish who got in and how — the baseline for everything else.

EXAMPLE SOURCES Sign-in successes & failures, MFA events, session creation, token issuance.

2 Administrative Activity

Catch privileged actions and abuse — your highest-impact events.

EXAMPLE SOURCES Admin console actions, role & permission changes, tenant/global settings.

3 Security-Relevant User Activity

See what users actually did with data, not just that they arrived.

EXAMPLE SOURCES Record views, exports & downloads, sharing, bulk actions, sensitive API calls.

4 Configuration Changes

Detect drift and tampering before it becomes an incident.

EXAMPLE SOURCES Security policy edits, integration & OAuth grants, logging/SIEM config changes.

5 Validation

Prove the logs actually arrive — a standard you can’t audit isn’t real.

EXAMPLE SOURCES SIEM ingestion checks, source health/heartbeats, coverage-gap alerting.

The test

If you can’t produce these from an application, you cannot investigate it, audit it, or prove what happened. SSO status tells you none of it.

EXECUTIVE ACTIONS

Five questions to ask this week.

Forward these to your application owners and SIEM team. The answers map your real coverage.

1. For our top business-critical apps, which ones send audit logs to the SIEM today — not just SSO sign-in events?
2. If an account were misused after a valid login, could we reconstruct what the user did inside the app?
3. Do we capture administrative and configuration changes across our SaaS and cloud platforms?
4. Who owns confirming a new application produces security logs before it goes live?
5. How do we validate, on an ongoing basis, that expected logs are actually arriving in the SIEM?

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

Want the SSO Logging Validation Checklist, or a second opinion on your coverage?

info@threatiqlabs.com · threatiqlabs.com