The Ultimate Implementation Guide: **Salesforce Shield Event Monitoring**

*Includes new ChatGPT/LLM prompts

www.spotlightmonitor.com

Salesforce Shield Event Monitoring Implementation Guide

Introduction

This is a practical, step-by-step playbook to plan, implement, and operationalize Salesforce Shield Event Monitoring (the Event Monitoring component of Shield). This guide focuses on Event Log Files (ELFs), Real-Time Event Monitoring (RTEM), and the optional Event Monitoring Analytics App.

Who this guide is for: RevOps/Business Systems, Salesforce Admins/Architects, Security, IT, and Compliance teams who need actionable visibility into Salesforce activity to reduce risk and prove control effectiveness.

How to use this guide: Skim the Executive Summary, confirm scope and roles, then follow the step-by-step plan. Each section includes context, examples, and checklists so you can implement quickly without getting lost in theory.

What you'll walk away with: A working Event Monitoring pipeline (ELFs + Real-Time streams), high-signal detections, dashboards that leaders actually read, and audit-ready evidence of monitoring and incident response.

Salesforce Shield Event Monitoring Implementation Guide

Introduction

This is a practical, step-by-step playbook to plan, implement, and operationalize Salesforce Shield Event Monitoring (the Event Monitoring component of Shield). This guide focuses on Event Log Files (ELFs) and Real-Time Event Monitoring (RTEM).

Who this guide is for: Business Systems/RevOps, Salesforce Admins/Architects, Security, IT, and Compliance teams who need actionable visibility into Salesforce activity to reduce risk and prove control effectiveness.

How to use this guide: Skim the Executive Summary, confirm scope and roles, then follow the step-by-step plan. Each section includes context, examples, and checklists so you can implement quickly without getting lost in theory.

Salesforce Shield Event Monitoring Implementation Guide

1. Purpose & Scope

Implementations succeed when everyone knows what problem we're solving and what is not in scope. This guide narrows the focus to **Event Monitoring** only so your team can deliver tangible outcomes fast, then iterate.
Event Monitoring helps turns Salesforce into a transparent system: you can see who accessed what, when, and how—across UI, API, reports, and custom code. We'll define the boundaries clearly so parallel initiatives (like Shield Platform Encryption or Field Audit Trail) don't slow you down.

In scope: Event Monitoring only — collecting, storing, analyzing, and alerting on user and system activity in Salesforce (e.g., logins, API calls, report exports, page views, Apex execution).

Out of scope: Shield Platform Encryption, DataDetect, and Field Audit Trail (referenced only where relevant to architecture or governance).

2. What Is Event Monitoring?

Think of Event Monitoring as a flight recorder for Salesforce. It continuously emits telemetry about user and system behavior. Historical Event Log Files answer investigative questions ("what happened last Tuesday?"), while Real-Time Event Monitoring answers operational questions ("what's happening right now, and should we act?").

Salesforce Shield Event Monitoring Implementation Guide

Event Monitoring captures detailed telemetry about how users and integrations interact with Salesforce. It provides:

- **Event Log Files (ELFs):** CSV log files generated by Salesforce on a frequent cadence (hourly & 24-hour) for dozens of event types (e.g., Login, API, ReportExport, URI, ApexExecution, LightningExperience). ELFs are retrieved via UI or API and typically cover a recent rolling window.

- **Real-Time Event Monitoring (RTEM):** Near real-time events published as Platform Events (e.g., LoginEventStream, ReportEventStream, URIEventStream, APIEventStream, ApexExecutionEventStream, etc.) so you can alert or take action immediately (Flows, Triggers, or external subscribers).

Key Outcomes: Detect risky behavior, investigate incidents, meet compliance requirements, optimize adoption, and prove control effectiveness.

3. Why It Matters (Business Value)

Before diving into configuration, align on outcomes. Executives care about reduced risk and audit readiness; admins care about fewer surprises and cleaner adoption signals; security cares about closing data-exfiltration blind spots. Event Monitoring serves all three—if you collect the right events, centralize them, and tune alerts to be actionable.

- Security: Detect mass report exports, anomalous logins, API spikes, data exfiltration patterns.

- Compliance: Evidence of monitoring and incident response for frameworks (SOC 2, ISO 27001, SOX, HIPAA, etc.).
- Operational Insight: Identify adoption friction, performance hotspots, and training needs.
- Forensics: Reconstruct timelines during incidents with reliable telemetry.

4. Prerequisites & Assumptions

- Appropriate licenses for Event Monitoring (or Shield) and API access.
- Integration destination chosen for downstream analysis (e.g., Splunk, Datadog, Sumo, Elastic, Azure/M365 SIEM, GCP/Security Command Center, AWS/Security Lake, Snowflake, BigQuery).
- Core team identified (Security, Salesforce Admin/Architect, RevOps/Business Systems, IT, Compliance, Data/Analytics).
- Data governance decisions: retention, PII minimization, access controls, separation of duties.
- MFA & SSO basics in place to maximize signal quality.

Note: Salesforce retains ELFs for a limited window (commonly ~30 days with Event Monitoring). Confirm the exact retention and cadence for your org and edition.

5. Roles & RACI (Example)

Activity	Admin	Security	Compliance	Data/Analytics	Exec Sponsor
Requirements & Use Cases	R	A	C	C	I
Licensing & Provisioning	R	C	I	I	A
Permissions Model	R	A	C	I	I
ELF Export & Storage	R	A	C	R	I
RTEM Subscriptions/Flows	R	A	C	C	I
SIEM Dashboards & Alerts	C	R	C	R	I
Runbooks & IR Playbooks	C	A	R	C	I
UAT & Sign-off	R	A	A	C	I

A = Accountable, R = Responsible, C = Consulted, I = Informed

6. Reference Architecture Patterns

A) SMB-Friendly (Fast Start)

1. Pull ELFs daily to cloud storage (e.g., S3/GCS/Azure Blob).
2. Load into SIEM/warehouse for dashboards & scheduled alerts.
3. Use a small set of **RTEM** subscriptions for high-risk events (e.g., report exports, logins) → Flow → Slack/Email.

B) Enterprise (Streaming + Data Lake)

1. RTEM → Event Bus (Kafka/Pub/Sub/Event Hubs) → SIEM + SOAR.
2. Scheduled ELF backfill to warehouse/lake for investigations and historical analytics.
3. Transaction Security policies for inline controls (e.g., block large report export outside allowlisted IPs).

Data Flow (Typical)

Salesforce → (RTEM: Platform Events) & (ELF: REST/Tooling API export) → Secure Storage → SIEM/Analytics → Alerts/Playbooks → Ticketing/ChatOps.

7. Data Governance & Security Controls

Minimization: Keep only fields needed for detections and forensics.

- **Access Controls:** Separate roles (Admin vs Security); limit who can see logs.
- **Retention:** Align with policy, legal hold, and storage costs (e.g., 1–3 years in SIEM/warehouse).
- **PII/PHI:** Treat logs as potentially sensitive; apply encryption at rest and transit.
- **Secrets & Keys:** Store API credentials in a vault; rotate on schedule.

8. Step-By-Step Implementation

The fastest path to value is incremental. Don't boil the ocean—stand up a minimal pipeline, prove it catches meaningful issues, then expand coverage. The steps below are ordered so you can deliver visible progress each week and keep stakeholders engaged.

8.1 Plan & Use-Case Definition (1–2 weeks)

1. **Prioritize detections:**
   - Mass **ReportExport** events, especially off-hours or outside corporate IPs.
   - **API** spikes or unusual access by integration users.
   - **Login** anomalies (new countries, failed-then-success, high-risk profiles).
   - **URI** events (sensitive object page views at scale).
   - **ApexExecution** performance and unusual payload patterns.
2. M**ap to compliance controls** (e.g., SOC 2 CC7 Monitoring, SOX ITGC).
3. Define SLAs/OLAs for alert triage, response, and closure.

Salesforce Shield Event Monitoring Implementation Guide

8.2 Licensing & Provisioning

1. Confirm Event Monitoring is provisioned for the target org(s).
2. Validate **permissions** for implementers:
   - View Event Log Files
   - API Enabled
   - Manage Real-Time Event Monitoring (for RTEM)
   - Access to CRM Analytics (if using the Analytics App)

8.3 Enable the Event Monitoring Analytics App (Optional)

1. Install/enable the app in CRM Analytics (formerly Tableau CRM / Einstein Analytics).
2. Run the setup wizard; schedule dataflows.
3. Review prebuilt dashboards and customize KPIs.

8.4 Event Log Files (ELFs) Export Strategy

1. **Decide cadence:** Daily is typical; increase frequency for high-risk periods.
2. **Choose a method:**
   a. **API (recommended):** Query EventLogFile sObject and download LogFile.
   b. CLI/Script: Use Salesforce CLI, Python, or integration tool.
   c. AppExchange/SIEM connectors: If available, use supported connectors.
3. Store securely (cloud object storage). Partition by EventType/LogDate.
4. Automate loads into SIEM/warehouse; apply schemas and field mappings.

Example SOQL (ELFs):

```
SELECT Id, EventType, LogDate, LogFile, LogFileLength
FROM EventLogFile
WHERE EventType IN ('ReportExport','API','Login','URI')
  AND LogDate = TODAY
```

Example REST (ELFs):

```
# 1) List available ELFs
curl -H "Authorization: Bearer $TOKEN" \

 "$SF_BASE/services/data/vXX.0/query/?
q=SELECT+Id,EventType,LogDate,LogFileLength+FROM+EventLogFile+WHER
E+LogDate=TODAY"

# 2) Download a specific ELF (CSV or JSON depending on your org settings)
curl -H "Authorization: Bearer $TOKEN" \
 "$SF_BASE/services/data/vXX.0/sobjects/EventLogFile/<ELF_ID>/LogFile" -o
event.csv
```

8.5 Real-Time Event Monitoring (RTEM)

1. **Identify streams** to subscribe to (e.g., ReportEventStream, LoginEventStream, APIEventStream, URIEventStream, ApexExecutionEventStream).
2. **Subscribe** via:
    - **Platform Event triggers/Flows:** Build detections in Salesforce (e.g., Flow filters + notifications).
    - **External consumers:** Use CometD or event connectors to your SIEM/SOAR or message bus.
    -
3. **Actions:** Alert (Slack/Email/SMS), create Case/Incident, or invoke SOAR playbooks.

8.7 SIEM/Analytics Integration

1. Parse & normalize fields (e.g., EVENT_TYPE, USER_ID, USERNAME, CLIENT_IP, URI, ROWS_PROCESSED).
2. Correlate with identity (IdP logs), endpoint, and network telemetry.
3. Dashboards: Access monitoring, data egress, API health, adoption trends.
4. Alert rules: Threshold, anomaly, and sequence-based.

8.8 Detections Library (Starter Set)

- Data Exfiltration: Multiple ReportExport by same user within 10 minutes or > X rows.
- API Abuse: API events surge > Y% over baseline for an integration user.
- Privileged Account Login: Admin login from new ASN/country.
- Mass Viewing: URI events > threshold on sensitive objects (e.g., Leads, Opportunities, Cases) in short window.
- Apex Misuse/Perf: ApexExecution with unusual runtime or failures.

8.9 Alerting, Runbooks & Incident Response

1. Route alerts to SecOps queue (Jira/ServiceNow) with priority logic.
2. Create runbooks for top detections (triage steps, queries, comms templates).
3. Escalation matrix and business impact assessment.

9. Test Plan & UAT (Scripted Scenarios)

Treat testing like a dress rehearsal for real incidents. Each scenario exists to verify that events are captured end-to-end, alerts contain enough context for triage, and responders know exactly what to do.

- Login Anomaly: Attempt login from non-standard geo with a privileged user.
- Mass Export: Run several large report exports (admin & standard profiles).

- API Spike: Simulate increased API calls by a test integration user.
- Sensitive Browsing: Rapid page views to sensitive objects.

Acceptance Criteria: Events captured, parsed, surfaced on dashboards, alerts generated with correct context, runbooks executed, tickets created, stakeholders notified, and outcomes documented.

10. Cutover & Rollout Checklist

Cutover isn't just a technical switch—it's a communications moment. Use this checklist to make the new monitoring capability visible: publish dashboards, confirm on-call runbooks, and brief leadership on what will (and won't) generate alerts.

- Licenses verified; permissions assigned
- ELF exports automated & validated
- RTEM subscriptions live with guardrails
- SIEM/warehouse ingest + dashboards published
- Top detections enabled (low false positive rate)
- Runbooks and on-call updated
- Stakeholder training completed
- Executive summary & KPIs defined

11. Ongoing Operations (Day-2)

Event Monitoring is a product, not a project. Assign owners, define SLAs, and review signal quality regularly. A lightweight operating rhythm will keep false positives low and stakeholder trust high.

- Daily: Ingest health checks; alert queue triage.
- Weekly: False-positive review; rules tuning; top anomalies review.
- Monthly: Metrics reporting to leadership; control attestation for audit.
- Quarterly: Use-case refresh, license/feature review; tabletop exercises.

12. Compliance Mapping (Examples)

Auditors don't just want data—they want evidence that you watch it and respond. Use these mappings to tie detections and runbooks to specific controls so your monitoring story is crisp in reviews.

- SOC 2 / ISO 27001: Monitoring, logging, incident response, access management.
- SOX: Detective control for changes/data access tied to financial reporting.
- HIPAA/GLBA/FERPA: Audit trail and monitoring for access to regulated data.

13. Metrics & KPIs

- Coverage: % priority event types ingested (ELF + RTEM).
- MTTD/MTTR: Mean time to detect/respond for top use cases.
- Alert Quality: True-positive rate, suppression effectiveness.
- Adoption: Reduction in risky behaviors; policy exceptions closed.
- Operational Health: Ingest latency, data freshness, pipeline success rate.

14. Common Pitfalls & How To Avoid Them

Every successful rollout shared the same discipline: start narrow, measure results, and expand. The pitfalls below are real patterns—we've included the antidotes so you don't repeat them.

- Only ELFs, No Real-Time: Add RTEM for high-risk detections.
- No Storage Plan: Define retention & archive from day one.
- Unparsed Logs: Normalize fields early; maintain a schema dictionary.
- Noise Overload: Start with 5–8 high-value detections; iterate.
- No Runbooks: Every alert type needs a triage playbook.

15. Event Types (Indicative Cheat Sheet)

(Exact availability depends on edition and org settings; confirm in your environment.)

- **Access & Auth:** Login, Logout, LightningLogin, LoginAs.
- **Data Egress:** ReportRecordsExported, BulkApiResultDownload, DataExportJob, ContentTransfer.
- **API & Dev:** API, BulkAPI, MetadataAPI, ApexExecution, ApexCallout.
- **UI Activity:** URI,, ListView, Search.
- **Analytics/Other:** CRM Analytics (Wave) usage events.

16. Query Cookbook

Top ELF in last 24h:

```
SELECT EventType, COUNT(Id)
FROM EventLogFile
WHERE LogDate = TODAY
GROUP BY EventType
ORDER BY COUNT(Id) DESC
```

Report exports by user (last 7 days):

```
SELECT Id, EventType, LogDate, LogFileLength
FROM EventLogFile
WHERE EventType = 'ReportExport'
  AND LogDate = LAST_N_DAYS:7
```

17. Transaction Security Policy Examples (Optional)

1. Mass Export Off-Network:
   - Condition: ReportExport and ROW_COUNT > 10,000 and NOT IN ALLOWLIST_IP
   - Action: Block and Alert Security

2. Privileged Login From New Country:
   - Condition: Login for Profile IN ('System Administrator') and COUNTRY not in allowlist
   - Action: Alert + require step-up as applicable

3. API Spike By Integration User:
   - Condition: API > baseline + 200% in 10 min window
   - Action: Alert + create SOAR ticket

18. Incident Playbooks (Templates)

Report Export Anomaly

1. Validate user, time, and IP; check VPN/SSO context.
2. Correlate with recent HR changes or tickets.
3. If high-risk objects included, notify data owner & legal.
4. Contain: Temporarily disable user/report access if policy allows.
5. Document and close with lessons learned.

API Abuse Suspected

1. Identify integration user and connected app.
2. Review scopes, recent deployments, and IP origins.
3. Rate-limit or revoke tokens per policy; open incident.
4. Coordinate with app owner; implement compensating controls.

19. Project Plan & Timeline (Example 6 Weeks)

Timeboxing forces decisions. Use this schedule to create momentum and clear milestones. If your environment is complex, treat weeks as phases and keep the sequence intact.

Week 1: Kickoff, requirements, architecture, access.
Week 2: ELF pipeline live to storage; initial SIEM parsing.
Week 3: RTEM subscriptions; Slack/Email routing; Analytics App enabled.
Week 4: Dashboards & top 5 detections; runbooks drafted.
Week 5: UAT scripts; policy tuning; training sessions.
Week 6: Production cutover; executive readout; backlog for phase 2.

20. Acceptance Checklist (Sign-Off)

- ELFs and RTEM both operational
- Detections producing actionable alerts (≥70% true positive)
- Dashboards published and adopted by SecOps & Admins
- Runbooks approved by Security & Compliance
- Evidence pack prepared for audit (screens, configs, tickets)

21. Next Steps & Enhancements

Once the foundation is live, resist the urge to add dozens of rules. Instead, expand coverage intentionally: one new use case at a time, reviewed with stakeholders, with a runbook for each.

- Expand detections (role changes, permission set grants, connected app scope changes).
- Integrate with Transaction Security for enforcement.
- Add UEBA/anomaly modeling on historical ELFs.
- Link to change management (deployments vs anomalies).

Conclusion

Start with a small, high-value set of detections, wire them to real people and real workflows, and publish dashboards that tell a simple story: we can see what matters, and we act when it matters. As the program matures, fold in Transaction Security for enforcement, enrich events with identity context, and grow historical analytics for trend insight and audits.
If you adopt the mindset that “monitoring is a product,” you’ll avoid shelfware, build trust with security and compliance, and give business leaders the visibility they’ve been asking for.

Salesforce Shield Event Monitoring Implementation Guide

Bonus - ChatGPT/ LLM Prompts!

Below are copy-paste-ready prompt templates you can use with ChatGPT or other LLMs to accelerate your Salesforce Shield Event Monitoring implementation.

Replace the placeholders in [brackets] with your own information.

IMPORTANT: Do not paste sensitive production data, credentials, secrets, or raw logs containing PII/PHI into public LLMs.

1. Planning & Use-Case Prioritization

PROMPT:
You are a Salesforce security architect.

Our organization has:
- Industry: [INDUSTRY]
- Salesforce users: [# USERS]
- Key data types: [PII / PHI / Financial / IP / Other]
- Compliance frameworks: [SOC 2, SOX, HIPAA, ISO 27001, etc.]

We are implementing Salesforce Shield Event Monitoring.

Based on this context:
1. List the top 8–10 highest-risk Salesforce user behaviors we should monitor.
2. Map each behavior to relevant Event Monitoring event types.
3. Rank them by risk and priority.
4. Identify which should be real-time vs ELF-based.

2. Event Type & Coverage Validation

PROMPT:
Act as a Salesforce Shield Event Monitoring expert.

Here are the Event Monitoring event types we plan to ingest:
[PASTE EVENT TYPES]

Here are our primary risk concerns: [LIST RISKS]

Please:
1. Identify coverage gaps.
2. Recommend additional event types.
3. Explain what each event type helps detect.

3. Detection Logic & Alert Design

PROMPT:
You are designing Salesforce Shield Event Monitoring detections.

Detection goal: [DESCRIBE GOAL]

Event type(s): [EVENT TYPES]

Constraints:
- Minimize false positives
- Alert only when action is required
- Business hours: [HOURS]

Provide:
1. Detection logic (plain English)
2. Threshold guidance
3. False positive risks
4. Alert severity

4. Incident Response Runbooks

PROMPT:
You are a security operations lead.

Create a runbook for:
[ALERT NAME]

Include:
1. Triage steps
2. Validation questions
3. Required Salesforce data
4. Containment actions
5. Escalation criteria
6. Audit documentation

5. Alert Tuning & Noise Reduction

PROMPT:
You are reviewing a noisy alert.

Alert description:
[DESCRIBE ALERT]

Provide:
1. Root cause of noise
2. Tuning recommendations
3. Suppression logic
4. Alternative signals

Salesforce Shield Event Monitoring Implementation Guide

Appendix A: Permissions Quick Reference

- View Event Log Files
- API Enabled
- Manage Real-Time Event Monitoring

Appendix B: Useful Links to Maintain Internally

- Runbook folder
- SIEM dashboards
- Flow/Trigger packages
- Key reports & saved searches

Implementation Tip:

Start small (5–8 detections) and iterate every two weeks. Treat Event Monitoring as a security product with its own backlog, SLAs, and owners — not a one-time setup.

Contact Us

brian@spotlightmonitor.com | www.spotlightmonitor.com