Reveal AI API capabilities for SIEM alerting: A practical assessment

Reveal Data's eDiscovery platform lacks native SIEM integration capabilities, requiring custom polling-based development for security monitoring. Unlike RelativityOne's mature API ecosystem, Reveal AI's public documentation reveals limited external monitoring endpoints, no webhook support, and no native connectors for platforms like Splunk or Sentinel. However, REST APIs, database-level monitoring, and exportable audit reports provide a foundation for custom SIEM integration—albeit with significant development effort.

API architecture requires custom integration approach

Reveal AI exposes multiple API layers, though comprehensive documentation is restricted to authenticated customers. The platform uses a **polling-based architecture** without push notifications, meaning SIEM integration requires scheduled API queries rather than real-time event streaming.

Primary API endpoints available:

API Layer	Base URL Pattern	Purpose	Authentication
Reveal REST API v2	`https://[instance].revealdata.com/rest/api/`	Core operations, projects, documents	Session token (incontrolauthtoken header)
NIA API	`http://[server]:5566/nia/`	Integration services, job orchestration	Internal service authentication
NexLP API (StoryEngine)	`https://[server]/StoryEngineWebApi/api/`	AI/ML analytics operations	OAuth 2.0
Swagger Documentation	`/rest/api-docs/index.html?urls.primaryName=v2`	Interactive API reference	Instance authentication required

Authentication flows through **Keycloak** as the identity broker, supporting OAuth 2.0, SAML 2.0, and OpenID Connect. (Revealdata +2) API access begins with a POST to `/api/v2/login` returning a `loginSessionId` for subsequent requests. (Reveal) (revealdata) **Rate limits are not publicly documented**—direct vendor engagement is required to determine polling thresholds.

Job monitoring relies on database polling and status codes

The NIA (NexLP Integration API) provides the most comprehensive job monitoring capability, using a **12-state status model** stored in backend database tables. (Revealdata) For SIEM alerting, these status values enable detection of failures, stalled jobs, and processing anomalies.

Job status codes for alert logic:

Status Code	Description	Alert Recommendation
0	Created	Informational
1	Submitted	Informational
2	InProcess	Monitor duration thresholds
3	Complete	Success confirmation
4	**Error**	**Critical alert trigger**
5	**Cancelled**	**Warning alert**
6	CancelPending	Informational
7	**Deleted**	**Audit/compliance alert**
8	Modified	Change tracking
9-12	Processing/Deletion job states	Monitor for stuck states

Monitorable job types include AI Document Sync (clustering, threading, entity extraction), Index operations, Export jobs, Production jobs, Bulk Updates, AV Transcription, and Deletion jobs. Direct database queries against nia_job_queue and nia_job tables provide the most reliable monitoring path for on-premise deployments. revealdata Revealdata

The platform supports **email alerts for unhandled errors** via SMTP configuration in NIA.config—this represents the only native alerting mechanism and can feed into SIEM email parsing workflows. revealdata Revealdata

Security and audit capabilities center on exportable reports

Reveal AI tracks user activity extensively for legal defensibility but **lacks a dedicated audit log API** in public documentation. Available audit data requires manual or scheduled extraction through the platform's reporting interface.

User Login Report captures authentication events with start/end dates, user identification, session expiration, and browser close detection— revealdataexportable to Excel format. **Document History** provides per-document audit trails including view start/end times, tag actions, downloads, prints, and modifications with user attribution. revealdata **Tagging Reports** deliver reviewer efficiency metrics, action history with timestamps, and accuracy tracking.

Authentication infrastructure through Keycloak offers potential for **indirect audit log collection**—Keycloak maintains native JSON-formatted audit logs that may be accessible depending on deployment architecture. Revealdata For cloud deployments, this typically requires vendor coordination.

ISO 27001 certification (2024 audit confirmed) indicates formal security controls exist, with additional documentation available through the Trust Center at security.revealdata.com. Reveal Reveal Data SOC 2 status requires direct verification with the vendor.

Critical gaps: No webhooks, no native SIEM connectors

The most significant limitation for SIEM integration is the **complete absence of push-based event delivery**. Reveal AI does not support webhooks, event subscriptions, or callback URL configurations. All monitoring must use polling patterns.

Native SIEM integration status:

Platform	Integration Status
Splunk	❌ Not available
Microsoft Sentinel	❌ Not available
Datadog	❌ Not available
Elastic/ELK	❌ Not available
QRadar	❌ Not available
Syslog forwarding	❌ Not documented
CEF/LEEF output	❌ Not available

No public status page (status.revealdata.com) exists for platform health monitoring. Internal health visibility is limited to the **Ops Center** administrative interface, which does not expose external APIs.

SIEM integration decision matrix

Based on available capabilities, the following matrix provides polling recommendations, key monitoring fields, and alert configurations for a Reveal AI SIEM framework:

Monitoring Domain	Data Source	Polling Method	Recommended Frequency	Key Fields	Alert Conditions	Severity
Job Failures	NIA database (nia_job)	SQL query / API poll	Every 5 minutes	job_id, nia_job_status, timestamp, error_details	Status = 4 (Error)	Critical
Long-Running Jobs	NIA database (nia_job)	SQL query	Every 15 minutes	job_id, status, start_time, job_type	Status = 2 AND duration > threshold	High
Cancelled Jobs	NIA database (nia_job)	SQL query	Every 15 minutes	job_id, cancelled_by, timestamp	Status = 5 (Cancelled)	Medium
User Authentication	User Login Report	Scheduled export + parse	Every 1 hour	user_id, login_time, logout_time, session_duration	Failed logins, unusual hours, session anomalies	High
Document Access	Document History	API poll or export	Every 30 minutes	doc_id, action_type, performed_by, timestamp	High-volume downloads, after-hours access	High
Data Exports	Export/Production jobs	REST API v2	Every 15 minutes	export_id, user, document_count, destination	Large exports, unusual users, external destinations	Critical
Bulk Operations	Bulk Update jobs	NIA API / database	Every 10 minutes	operation_type, affected_count, user	Mass deletions, tag modifications	High
API Health	NIA API `/nia/version`	HTTP health check	Every 1 minute	response_code, response_time	Non-200 response, timeout > 5s	Critical
Reviewer Activity	Tagging Reports	Scheduled export	Every 4 hours	user, documents_per_hour, active_time	Zero activity, unusual patterns	Medium

---

Implementation recommendations

Tier 1 priorities should focus on job failure detection via direct database monitoring (nia_job table queries for

status code 4) and API availability checks against the `/nia/version` endpoint. These provide the highest-value alerts with lowest implementation complexity.

Tier 2 implementation requires scheduled extraction of User Login Reports and Document History exports, with SIEM parsing rules to normalize CSV/Excel output into standard event formats. For cloud deployments, coordinate with Reveal support to establish automated export delivery or API access to these report datasets.

Tier 3 enhancement involves Keycloak audit log integration if deployment architecture permits—Keycloak provides native JSON-formatted authentication events that can supplement Reveal's user login tracking with real-time authentication failure detection.

For immediate action, contact Reveal Data support (support@revealdata.com) to request: complete REST API documentation including audit endpoints, enterprise logging options not in public documentation, rate limit specifications for polling design, and any roadmap items for webhook or SIEM connector development.

Comparison with RelativityOne capabilities

Unlike RelativityOne's comprehensive SIEM integration framework with documented audit APIs, webhook support, and Splunk/Sentinel connectors, Reveal AI requires **substantially more custom development** for equivalent monitoring coverage. Organizations evaluating both platforms should factor approximately **40-60 hours of additional development effort** for Reveal AI SIEM integration compared to RelativityOne's out-of-box capabilities.

The absence of standardized event formats (CEF, JSON streams) means Reveal integration produces higher ongoing maintenance burden as export formats may change between versions. Consider implementing an abstraction layer in your polling architecture to isolate SIEM logic from Reveal-specific data structures.

Conclusion

Reveal AI's SIEM integration potential exists primarily through its REST API and database-level access, but **requires custom polling infrastructure** rather than native connectors. Job monitoring offers the most actionable SIEM data via NIA status codes, while security/audit monitoring depends on scheduled report extraction. Organizations should prioritize direct vendor engagement to access non-public API documentation and explore enterprise logging options that may exceed publicly available capabilities. The platform is optimized for legal workflow defensibility rather than SOC operations—plan accordingly for the custom development investment required.