eDiscovery Platform Alerting & Monitoring Framework

Executive Summary

This framework provides a unified approach to alerting and monitoring across your eDiscovery platforms (RelativityOne and Reveal AI). Both platforms lack native SIEM integrations, requiring custom polling-based solutions for comprehensive monitoring coverage.

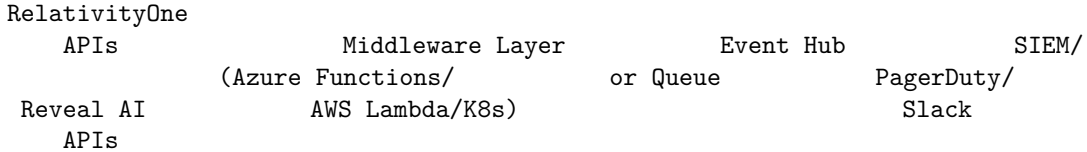
Key Finding: RelativityOne offers a more mature API ecosystem with documented endpoints, while Reveal AI requires 40-60 additional hours of development effort for equivalent monitoring coverage.

Platform Comparison Matrix

Capability	RelativityOne	Reveal AI
Native SIEM Connectors	No	No
Webhook Support	No (Post-Save Event Handlers available)	No
Audit API	Yes (comprehensive)	Limited (export-based)
Push Notifications	Security events only	Email alerts for errors only
Native Email Alerts	Security + Imaging only	Unhandled errors via SMTP
Rate Limits	1,000 req/min (Object Manager)	Not publicly documented
Authentication	Bearer Token / Basic Auth	Session Token / OAuth 2.0

Architecture Overview

Recommended: Middleware Service Pattern



Why Middleware? - Normalizes data formats between platforms - Handles authentication token refresh - Provides abstraction layer for SIEM-specific logic - Enables centralized rate limiting and retry logic - Isolates platform-specific changes

---

Alert Severity Classification

Severity	Response Time	Description	Examples
Critical	Immediate	System failures, security breaches, data loss risk	Job errors, brute force attacks, mass deletions
High	< 1 hour	Significant operational impact	Failed logins, large exports, job errors with partial success
Medium	< 4 hours	Operational concerns, compliance issues	Cancelled jobs, unusual activity patterns
Low	Next business day	Informational, minor issues	Workspace health, index fragmentation

---

Tiered Implementation Plan

Phase 1: Critical Infrastructure (Deploy First)

RelativityOne - Tier 1 APIs

API	Endpoint	Poll Frequency	Alert Conditions
Processing Set Manager	`/Relativity.Processing.Services.IProcessingSetManager/Read/GetProcessingSetAsync`	5 min	Status = Failed/Stopped, EnvironmentErrors present
Production Queue Manager	`/relativity-productions/{version}/productions/queue`	15 min	Errors in queue, Status = Failed/Cancelled

API	Endpoint	Poll Frequency	Alert Conditions
Imaging Job Manager	`/relativity-imaging/{version}/workspaces/{id}/imagingsets/{id}`	1-5 min	Status = Error, Documents with errors > 0
Security Alerts	Native push	N/A	Brute force (50+ failures/hour), login method changes

Reveal AI - Tier 1 Monitoring

Data Source	Polling Method	Poll Frequency	Alert Conditions
NIA Job Database (nia_job)	SQL Query	5 min	Status = 4 (Error)
API Health	HTTP GET `/nia/version`	1 min	Non-200 response, timeout > 5s
Long-Running Jobs	SQL Query	15 min	Status = 2 (InProcess) AND duration > threshold

Phase 2: Security & Compliance

RelativityOne - Tier 2 APIs

API	Poll Frequency	Key Alerts
Audit API	5-15 min	Failed logins > 5 in 10 min, exports > 10K docs, mass deletions
Integration Points Job History	5 min	Status = "Error - Job Failed", "Validation failed"
Structured Analytics	5-10 min	Status = Failed/Cancelled, ErrorMessages present

Reveal AI - Tier 2 Monitoring

Data Source	Poll Frequency	Key Alerts
User Login Report	1 hour (scheduled export)	Failed logins, unusual hours, session anomalies
Document History	30 min	High-volume downloads, after-hours access
Export/Production Jobs	15 min	Large exports, external destinations

Phase 3: Operational Excellence

Platform	Data Source	Poll Frequency	Purpose
RelativityOne	Workspace Manager	15-30 min	Workspace health, resource allocation
RelativityOne	dtSearch Index (Object Manager)	15 min	Build errors, fragmentation
Reveal AI	Tagging Reports	4 hours	Reviewer activity, zero activity detection
Reveal AI	Bulk Update Jobs	10 min	Mass deletions, tag modifications

---

Alert Rules Reference

Critical Alerts

```
# RelativityOne - Processing Job Failure
IF EnvironmentErrors != null THEN CRITICAL
IF DataSourceHasJobLevelErrors == true THEN CRITICAL
IF Status == "Failed" OR Status == "Stopped" THEN CRITICAL

# RelativityOne - Security
IF Login_Failed_Count > 50 within 1 hour THEN CRITICAL (Brute Force)
IF Login_Method_Changed THEN CRITICAL
```

```
# Reveal AI - Job Failure
IF nia_job_status == 4 (Error) THEN CRITICAL
IF API_Response_Code != 200 THEN CRITICAL
IF API_Response_Time > 5000ms THEN CRITICAL
```

High Severity Alerts

```
# RelativityOne - Data Exfiltration Risk
IF Export_Document_Count > 10000 THEN HIGH
IF MassDelete_Count > 100 THEN HIGH
IF Permission_Elevation_Detected THEN HIGH

# RelativityOne - Integration Points
IF Job_Status == "Completed with Errors" AND Items_With_Errors > 100 THEN HIGH
IF Job_Status == "Pending" for > 30 minutes THEN HIGH

# Reveal AI - Security
IF After_Hours_Document_Access THEN HIGH
IF Download_Volume > threshold THEN HIGH
IF Bulk_Update_Affected_Count > threshold THEN HIGH
```

Medium Severity Alerts

```
# RelativityOne
IF Job_Status == "Paused" for > 30 minutes THEN MEDIUM
IF dtSearch_Status IN ["Build Error", "Compression Error"] THEN MEDIUM

# Reveal AI
IF nia_job_status == 5 (Cancelled) THEN MEDIUM
IF Reviewer_Zero_Activity for > 4 hours THEN MEDIUM
```

Polling Schedule Summary

Interval	RelativityOne APIs	Reveal AI Sources
1 min	Processing Queue (active jobs)	API Health (`/nia/version`)
5 min	Production Queue, Imaging Sets, Integration Points	Job Failures (nia_job), Bulk Operations
15 min	Audit (security), dtSearch, Structured Analytics	Long-Running Jobs, Data Exports
30 min	Workspace health, general status	Document History
1 hour	Full audit export for compliance	User Login Report

Interval	RelativityOne APIs	Reveal AI Sources
4 hours	-	Tagging Reports / Reviewer Activity

Authentication Configuration

RelativityOne

```
# Bearer Token (Recommended)
curl -X POST "<host>/Relativity/Identity/connect/token" \
  -H "Content-Type: application/x-www-form-urlencoded" \
  -d "grant_type=client_credentials" \
  -d "scope=SystemUserInfo" \
  -d "client_id=<your_client_id>" \
  -d "client_secret=<your_client_secret>"

# Required Headers for All Requests
X-CSRF-Header: -
Content-Type: application/json
Authorization: Bearer <access_token>
```

Reveal AI

```
# Session Token Authentication
POST /api/v2/login
# Returns: loginSessionId

# Required Header for Subsequent Requests
incontrolauthtoken: <loginSessionId>
```

Important: Implement token refresh logic - bearer tokens expire and require renewal.

SIEM Integration Patterns

Splunk

```
# Processing Job Failure Alert
index=ediscovery sourcetype=relativity_processing
| where Status IN ("Failed", "Error", "Paused") OR EnvironmentErrors!=""
| stats count by WorkspaceID, ProcessingSetName, Status
| where count > 0
```

```
# Multiple Failed Logins
index=ediscovery sourcetype=relativity_audit Action="Login Failed"
| stats count by UserName
| where count > 5

# Reveal AI Job Errors
index=ediscovery sourcetype=reveal_jobs
| where nia_job_status=4
| stats count by job_id, job_type, timestamp
```

Datadog

```yaml
# Processing Job Monitor
name: "eDiscovery Processing Job Failure"
type: metric alert
query: "sum(last_5m):sum:ediscovery.processing.errors{*} > 0"
message: "Processing job has failed"
tags:
  - platform:relativityone
  - severity:critical

# Production Queue Monitor
name: "eDiscovery Production Queue Stuck"
type: metric alert
query: "avg(last_15m):avg:ediscovery.production.queue_time{*} > 7200"
message: "Production job stuck in queue for >2 hours"
```

Microsoft SCOM

All monitoring scripts include built-in SCOM integration via Windows Event Log. Enable with `"scom_enabled": true` in config.

Event Sources: - `RelativityOne-Monitor` - All RelativityOne events (Event IDs 1000-1599) - `RevealAI-Monitor` - All Reveal AI events (Event IDs 2000-2299)

Event ID Mapping:

Monitor	Base ID	OK	WARNING	HIGH	CRITICAL
Telemetry Agent	1000	1000	1002	1003	1004
Billing Agent	1100	1100	1102	1103	1104
Worker Health	1200	1200	1202	1203	1204
Job Queue	1300	1300	1302	1303	1304
Security Audit	1400	1400	1402	1403	1404
Alert Manager	1500	1500	1502	1503	1504
Reveal API Health	2000	2000	2002	2003	2004
Reveal Job Monitor	2100	2100	2102	2103	2104

Monitor	Base ID	OK	WARNING	HIGH	CRITICAL
Reveal Export	2200	2200	2202	2203	2204

SCOM Management Pack Rules:

```
<!-- Alert on Critical events -->
<Rule ID="eDiscovery.Critical.Alert">
  <DataSource>
    <EventLog>Application</EventLog>
    <EventSource>RelativityOne-Monitor</EventSource>
    <EventID>1004,1104,1204,1304,1404,1504</EventID>
  </DataSource>
  <WriteAction>
    <AlertSeverity>Critical</AlertSeverity>
  </WriteAction>
</Rule>
```

Escalation Procedures

Severity-Based Response

Severity	Initial Response	Escalation Path	SLA
Critical	Immediate investigation	On-call engineer → Team Lead → Vendor Support	15 min response
High	Prompt investigation	Assigned engineer → Team Lead	1 hour response
Medium	Scheduled review	Assigned engineer	4 hour response
Low	Batch processing	Weekly review	Next business day

Vendor Contacts

Platform	Support Contact	Use Case
RelativityOne	support@relativity.com	Critical alerts, stuck jobs
Reveal AI	support@revealdata.com	API documentation, rate limits

Implementation Checklist

Week 1-2: Foundation

- ☐ Set up middleware service (Azure Functions/AWS Lambda)
- ☐ Configure RelativityOne API authentication (Bearer tokens)
- ☐ Configure Reveal AI API authentication (Session tokens)
- ☐ Implement Processing Set Manager polling
- ☐ Implement Production Queue Manager polling
- ☐ Set up SIEM data ingestion pipeline

Week 3-4: Critical Monitoring

- ☐ Deploy Reveal AI job failure monitoring (nia_job table)
- ☐ Configure Imaging Job Manager alerts
- ☐ Set up API health checks for both platforms
- ☐ Implement critical alert notifications (PagerDuty/Slack)
- ☐ Test and tune alert thresholds

Week 5-6: Security & Audit

- ☐ Enable RelativityOne Security Center notifications
- ☐ Implement Audit API polling for security events
- ☐ Configure Reveal AI user login report extraction
- ☐ Set up Integration Points Job History monitoring
- ☐ Deploy failed login and data exfiltration alerts

Week 7-8: Operational Maturity

- ☐ Add Structured Analytics monitoring
- ☐ Implement dtSearch index health checks
- ☐ Configure Reveal AI document access monitoring
- ☐ Set up Workspace health monitoring
- ☐ Create operational dashboards
- ☐ Document runbooks for common alert scenarios

Ongoing

- ☐ Fine-tune thresholds based on baseline data
- ☐ Review and update alert rules quarterly
- ☐ Conduct alert fatigue assessments
- ☐ Update documentation for platform API changes

Key Considerations

1. **No Native Webhooks**: Both platforms require polling - plan infrastructure accordingly
2. **Rate Limits**:
   - RelativityOne Object Manager: 1,000 requests/minute
   - Reveal AI: Contact vendor for specifications
3. **Token Management**: Implement automatic token refresh for bearer tokens
4. **Workspace Iteration**: Most RelativityOne APIs require iterating across workspaces; use `workspaceID = -1` for instance-level queries where supported
5. **Data Normalization**: Reveal AI export formats (CSV/Excel) require parsing; implement abstraction layer
6. **Reveal AI Limitations**: Budget 40-60 additional development hours compared to RelativityOne

---

Appendix: Status Code Reference

RelativityOne Processing States

- `Staging` → `Preparing files` → `Submitting` → `Processing` → `Completed`
- Error states: `Failed`, `Stopped`, `Completed with Errors`

Reveal AI Job Status Codes

Code	Status	Alert Action
0	Created	Informational
1	Submitted	Informational
2	InProcess	Monitor duration
3	Complete	Success
4	Error	**Critical Alert**
5	Cancelled	Warning
6	CancelPending	Informational
7	Deleted	Audit/Compliance
8	Modified	Change tracking
9-12	Processing/Deletion	Monitor for stuck

RelativityOne Integration Points Status

Status	Meaning	Alert
Pending	Waiting for agent	Warning if > 30 min
Validation	Being validated	Info
Validation failed	Config error	**Critical**
Processing	Running	Info
Completed	Success	None
Completed with Errors	Item-level errors	High
Error - Job Failed	Job-level failure	**Critical**

Document Version History

Version	Date	Author	Changes
1.0	2024-11-29	-	Initial framework based on platform assessments