OEE IntelliSuite - Logging and SIEM Guidance

Security monitoring guidance. Updated 2026-11-03.

1. Purpose and scope

This guide explains how to review IntelliSuite logs and metrics and integrate them with your security information and event management (SIEM) system. OEE IntelliSuite will work with your IT team to accommodate your SIEM requirements.

The IntelliSuite product includes the components described below. Confirm which are installed, how they are reached, who may access them, and which security controls are in place with your IT team. This guide does not establish that any particular service, log source, account, network path or security control is configured or working at your site.

2. The local monitoring stack

The IntelliSuite product includes a local monitoring stack built from standard open components:

- Grafana is the web interface used to view and query data.
- Loki stores log records: text messages from services, with their fields.
- Prometheus stores metrics: numeric measurements sampled over time, such as counts and rates.
- Tempo stores traces, which show how one request moved through several services.
- Grafana Alloy is the collector. It receives telemetry from IntelliSuite services and writes it to Loki, Prometheus and Tempo.

Logs and metrics are different. Use Loki to read what a service reported. Use Prometheus to see how a value changed over time. Neither one is, on its own, a security audit trail.

Source basis: the product source defines these components and provisions the Grafana data sources for Prometheus, Loki and Tempo. It also sets default retention periods for each store. Verify for your installation: that the stack is deployed, where Grafana can be reached from, who holds accounts and roles, and what retention your organization needs. The default settings in the source are a starting point. They are not suitable for production use until your access and security requirements are applied.

3. Providing access

1. Your IT team and IntelliSuite confirm where Grafana runs and the address users will reach it at, and agree whether it is reachable only from your network.
2. Agree access with the authorized owners. Before granting it, configure and validate Grafana authentication and access controls. Test that each reader has only the agreed permissions and cannot administer or write unless separately authorized.
3. Choose one non-sensitive, representative log source and a short time window. In Grafana Explore, select the Loki data source, choose the service, set the time range, and confirm that records appear with the expected fields.
4. Check a sample record together: timestamp, time zone, field names, and whether any field holds sensitive data.
5. Agree the SIEM path together (see section 4), with a named owner on each side.
6. Run an end-to-end test: a known event from a source service should appear in the SIEM within the agreed time. Document the result.

4. Getting data into the SIEM

OEE IntelliSuite will work with your IT team to establish a connection to your SIEM. The teams will agree the event sources, format and transport. Depending on the SIEM, approaches to evaluate include OTLP, syslog, file transfer and API pull. The integration must be verified for your installation.

The product includes an optional OTLP-over-HTTP exporter that can send logs, metrics and traces to a second endpoint. The source deployment configuration has specific transport and authentication requirements; compatibility with your SIEM or an intermediary must be established. The teams must agree the endpoint, data scope, encryption and access method, then configure and test the full path before relying on it.

Integration: the optional OTLP exporter provides one possible path. The teams will select and test the path that fits your SIEM and security requirements.

5. Production edit history (separate from logs)

Pulse provides an edit history for supported production-data edits in its application database, displayed on the Pulse edit log page. Entries can include the edit time, device, item type, description, changed values and editor identity when available.

When authentication is off, the editor may be unknown. This is business history, not a complete security audit trail. We have not verified forwarding these records to Loki or a SIEM.

6. What you can monitor, and what to verify

Choose monitoring by source, and rely only on items confirmed during onboarding.

- Identity events such as sign-in failures or account lockouts may be available from your identity provider, if configured. Confirm coverage with your IT team.
- Application events such as local permission changes, sign-in failures, data exports and configuration changes require separate coverage checks. The source reviewed does not establish these as recorded security events; verify their actual sources and coverage.
- Operational health such as service failures, gaps in telemetry, and unusual volume can be monitored through logs and metrics, where verified during onboarding.
- Business edits can be reviewed in the Pulse edit log page, if that feature is present in your release.

No comprehensive catalogue of security log events or event identifiers has been verified. Event names, identifiers, schema, retention and automatic forwarding must be confirmed during onboarding. This guide is onboarding guidance. It is not evidence that any particular event is captured, retained or forwarded.

7. Onboarding checklist

Agree and verify each item with your IT team.

1. Owners: a named person at your organization and at IntelliSuite for logs, access and the SIEM connection.
2. Reader access: named accounts, roles, and the approval process for changes.
3. Network and transport: the allowed network paths, and how traffic is encrypted and authenticated.
4. Timestamps and fields: a sample of real records, with time zone and field names checked.
5. Retention: how long each store keeps data on each side, and who deletes it.
6. Sensitive data: which fields must be filtered or excluded before data leaves the site.

7. Alert thresholds: which conditions alert, and the agreed threshold values.

8. End-to-end test: a known event traced from source to SIEM, with the result recorded.

9. Responsibility and escalation: who responds to an alert, how it escalates, and the agreed response times.

10. Change control: how configuration changes are requested, approved and recorded.

OEE IntelliSuite. Confirm the installation and log coverage with your IT team.