Microsoft Audit Logs vs Compliance Alerts for SOC Monitoring

---

1. Overview

This report outlines the key differences, advantages, disadvantages, and recommendations for using Microsoft Audit Logs and Microsoft Compliance Alerts in the context of Security Operations Center (SOC) monitoring.

---

2. Definition and Purpose

Microsoft Audit Logs

- Provide detailed records of all user and administrator activities across Microsoft 365 services.
- Useful for tracking actions such as logins, file access, configuration changes, etc.

Microsoft Compliance Alerts

- Triggered based on specific compliance or security policies configured in Microsoft Purview.
- Designed to notify on suspicious, risky, or policy-violating behavior.

---

3. Key Differences

Attribute	Microsoft Audit Logs	Microsoft Compliance Alerts
Data Source	Microsoft 365 Unified Audit Log (UAL)	Microsoft Purview (Compliance Center)
Primary Use	Activity tracking, investigations	Policy violation detection, real-time alerts

Attribute	Microsoft Audit Logs	Microsoft Compliance Alerts
Data Format	Raw, event-based logs	Structured, policy-based alerts
Trigger Method	Logs all user/admin activities	Fires only when policies are breached
Integration	Supports SIEM integration	Supports alerting systems and workflows
Licensing	M365 E3/E5 (details improve with E5)	Requires M365 E5 or specific add-on licensing
Retention	Up to 1 year (based on license tier)	Retention defined by alert settings

---

4. Pros and Cons

Microsoft Audit Logs

- **Pros:**
  - Detailed, timestamped activity records.
  - Broad visibility across services.
  - Excellent for historical analysis and forensic investigations.
  - Integrates well with SIEMs for event correlation.
- **Cons:**
  - Not real-time; requires manual or scheduled processing.
  - High volume and can be noisy without filtering.
  - Requires parsing and context-building for actionable insights.

Microsoft Compliance Alerts

- **Pros:**
  - Provides real-time detection of compliance or security policy violations.
  - Easy to configure and link to automated workflows or notifications.
  - Useful for detecting insider threats, DLP violations, or unusual behavior.
- **Cons:**
  - Alert coverage limited to configured policies only.
  - Less raw detail compared to audit logs.
  - May produce false positives if rules are not refined.

---

5. Recommendations for SOC Monitoring

Monitoring Need	Recommended Source
Real-Time Threat Detection	Microsoft Compliance Alerts

Monitoring Need	Recommended Source
Threat Hunting / Investigations	Microsoft Audit Logs
Forensics and Root Cause Analysis	Microsoft Audit Logs
Policy Enforcement Monitoring	Microsoft Compliance Alerts
SIEM Event Correlation	Both (Audit for context, Alerts for signal)

6. Conclusion

For a complete SOC monitoring strategy, both Microsoft Audit Logs and Compliance Alerts should be used in tandem. Audit Logs provide the necessary historical detail for investigations and context, while Compliance Alerts offer timely awareness of potential security or compliance issues. Combining both ensures improved visibility, faster response times, and better alignment with security and regulatory requirements.

Revision #2
Created 8 August 2025 08:59:12 by Richmond Abella
Updated 8 August 2025 09:05:17 by Richmond Abella