USM Anywhere Log Source Review Checklist

Section 1: Inventory & Coverage

🔴	**Build a complete log source inventory**
	List every source you intend to ingest (firewalls, AD, endpoints, cloud, SaaS, applications). Compare against what is actually arriving in USM Anywhere. Any gap is a blind spot.
🔴	**Identify sources without native AlienApp connectors**
	Applications lacking a native connector are the most common ingestion failure. Flag each one and confirm whether a custom parser, syslog forwarder, or API pull is in place.
🔴	**Confirm sensor placement covers critical traffic**
	Verify sensors sit on network segments generating the most security-relevant traffic perimeter, critical server VLANs, and cloud egress. Misplaced sensors miss everything that matters.

Section 2: Ingestion Health

🟡	**Check for silent ingestion failures**
	Confirm each log source has reported in the last 24 hours. A source that has quietly stopped sending is worse than one never configured; it creates false confidence.
🟡	**Review parsing accuracy on your top 5 sources**
	Sample real events and confirm fields (source IP, user, action, outcome) are extracting correctly. Broken parsing means broken correlation.
🟡	**Validate time synchronisation across all sources**
	Timestamp drift between sources destroys correlation accuracy. Confirm NTP is enforced on every log emitter.

Section 3:Directive & Alert Quality

🔵	**Audit directives against actual threat coverage**
	Map your active directives to your priority threats (MITRE ATT&CK). Identify techniques with no coverage.
🔵	**Measure alert volume and false positive rate**
	Track alerts per day per analyst. If analysts are drowning, tuning is overdue and a poorly written rule can overwhelm the sensor or fill storage.
🔵	**Suppress known-good activity**
	Backup windows, vulnerability scans, and scheduled jobs generate predictable noise. Confirm these are suppressed so genuine signals surface.

Section 4:Retention & Evidence

🟢	**Retention & Evidence**
	Check your searchable data window against your audit requirements (ISO 27001, PCI DSS, UK GDPR). If you need data beyond the search window, confirm the retrieval process is documented and tested.
	Next Step:
	Score yourself:
	10/10 = Well-tuned.
	6–9 = Tuning required
	Below 6 = Your SIEM is running blind.

Need help? Kootek Consulting's certified USM Anywhere advisors provide reactive and proactive support, log source onboarding, directive tuning, and incident investigation.

W: www.kootek.co.uk
E: support@kootek.co.uk
T: 02080581605

LevelBlue
Certified Security Engineer