SignalForge Consulting — Splunk Health Checklist

Use this as a quick-start for your first 30 days.

- Validate forwarder versions and TLS settings
- Normalize high-volume sources (CIM) and deduplicate
- Set KPIs: ingestion errors, license headroom, search concurrency
- Rationalize top 10 detections and triage steps
- Map coverage to ATT&CK and M-21-31 outcomes

Contact: info@signalforgeconsulting.com