

System Resource Monitoring Service (SysMonSvc) — Design

Purpose: Continuous, low-overhead monitoring of CPU, RAM, Disk, and Network with alerting and artifact collection

Architecture: Collectors (psutil) -> Evaluator (rolling windows & thresholds) -> Alert Builder -> Uploader (REST)

Key Thresholds (defaults):

- CPU Total: warn >70%/5m, critical >90%/1m
- CPU Per-Process: warn >30%/5m, critical >50%/2m
- RAM: warn >75%, critical >90%; Available warn <1GB, crit <500MB; Pagefile warn >70%, crit >85%
- Disk Free: warn <20% or <10GB; critical <10% or <5GB (C: strict)
- Network: errors/drops > 0 (rate-based)

Config: See config/global.default.json and config/sysmon.local.json

Deployment: Run as Windows service via NSSM or console for testing.