

Lessons Learned

The lessons I've learned from building basic security monitoring without a SIEM product.

- **You don't need a SIEM product to have a SIEM.** The function, collect, centralize, analyze, alert, is achievable with the system logger, a few scripts, and a scheduler. The expensive product buys scale, correlation, and team workflow that a small environment does not need. Build the function from what you have, and spend nothing.
- **Monitor categories, not everything.** Watching every log line buries the signal that matters under the volume that does not. Choose the categories that reveal the most trouble; authentication, boundary events, health, critical severity, a few service-specific signals, and accept that you are deliberately not watching the rest. High-value coverage that stays relevant beats total coverage that becomes noise.
- **Noise is the enemy.** A monitoring system dies when its alerts stop being trusted, and they stop being trusted when too many of them do not matter. Tune aggressively toward fewer, more meaningful alerts. Requiring a condition to persist before firing, keeping thresholds where real problems live, resisting the urge to add more checks, all of it serves the goal that every alert should be worth reading.
- **Watch for silence, not just alarms.** This is the failure unique to monitoring. A monitor that has silently stopped looks identical to a healthy environment. Watch for the absence of logs you expect, confirm the checks are running, and test the alerting path deliberately now and then. Never treat "no alerts" as proof that all is well without confirming the monitor is still watching.
- **Start simple.** Cron and a mail command are a complete alerting layer, and adding no attack surface is a feature. Reach for a heavier automation platform only when you genuinely want its orchestration and are willing to secure it. The simplest thing that delivers the alert is usually the right thing.

Revision #1

Created 2026-07-31 22:52:28 UTC by Chris Landis

Updated 2026-07-31 22:55:48 UTC by Chris Landis