

Forum: [Hack Forums](#)

Thread: [Building a Small SIEM Lab That Produces Alerts Worth Reading](#)

watsica12 - *October 19, 2026, 2:23 am*

I want to build a small security monitoring lab without turning it into an expensive infrastructure project. Wazuh looks approachable for collecting endpoint events, while Security Onion provides a broader environment for network-security monitoring. My goal is to generate benign test activity, collect the relevant events, and see whether the resulting alerts are understandable and actionable.

One thing I want to avoid is measuring success by the number of alerts generated. A system that produces hundreds of noisy notifications without useful context isn't necessarily providing better security. I'd rather begin with a handful of detections, understand what evidence triggered each one, and improve the rules based on observed results.

For those who have built SIEM labs, which log sources did you ingest first? How do you distinguish normal administrative activity from events that deserve investigation? I'd also like to hear how you test detection rules with repeatable scenarios and document the expected alert, relevant fields, and possible false positives.