SOC Budget Planning for 2027: Focus on Analyst Time, Not Only Spend



An article on 2027 SOC budgeting argues the main loss is analyst time. It cites ANY.RUN's estimate of 450 hours recoverable per 1,000 investigated alerts through faster analysis and IOC research.

- The article frames SOC budget pressure as a problem of lost analyst time rather than total spend.
- ANY.RUN estimates teams could recover 450 analyst hours per 1,000 investigated alerts.
- The estimated savings come from faster threat analysis and IOC research.
- Manual investigations, repeated checks and unnecessary escalations are named as the main drains on resources.
- The excerpt available does not detail the five priorities in the headline.

What the article says

An article published by The Hacker News on 2027 SOC budget planning asks whether the real problem is not how much a security operations centre spends, but how much analyst time it loses. It points to manual investigations, repeated checks and unnecessary escalations as continuing drains on resources.

The piece cites an estimate from ANY.RUN that SOC teams could recover 450 analyst hours for every 1,000 investigated alerts. According to that estimate, the gain comes from faster threat analysis and faster research into indicators of compromise (**IOC**).

How to read it

The figure is a vendor estimate, and the available excerpt gives no method or assumptions behind it. It should be treated as a prompt for internal measurement, not as a benchmark for your own SOC. The excerpt also does not list the five priorities named in the headline, so we do not summarise them here.

The underlying point is still useful for budget cycles. Headcount and tooling costs are visible, while time spent on repetitive triage is harder to see and is rarely tracked as a cost line.

Practical takeaway

Before requesting additional budget for 2027, a SOC lead can first establish where analyst hours actually go. Evidence from your own alert handling will make any request, whether for tooling, staffing or process change, easier to defend to finance and risk committees.

What to do now

1. Measure how many analyst hours your SOC spends per investigated alert, split by triage, enrichment and escalation.
2. Identify repeated manual checks and unnecessary escalations in recent cases and list candidates for process change.
3. Review how your team researches IOCs and whether that step can be made faster or more consistent.
4. Treat vendor savings estimates such as 450 hours per 1,000 alerts as hypotheses and test them against your own data before budgeting.
5. Tie 2027 budget requests to measured time savings and risk reduction so finance and risk committees can assess them.