SOAR · A FOUR-WEEK TRIAL

Test SOAR on one real question.

A trial on one server and one part of your network, judged by what the people who approve responses can see.

The question a trial should answer is simple: **when SOAR raises an alarm on your own data, can the people who approve responses see how it knows, what it is still unsure about, and exactly what they are being asked to sign?**

In the first week, set SOAR up on one computer at your site (so far it has been tested on a rented computer in a data centre, not on physical hardware) and connect two things: the log-in records from one server and a copy of activity from one part of the network. Name a case owner and the people who approve each level of risk, and keep one recent alarm your team has already closed.

In the second week, test it on something you already understand. Load a recording of network traffic from a past incident and see which unusual connections SOAR flags as leads; for password-guessing, watch the live log-in records. Do not expect one file to replay the whole night. Its rehearsals of a response use a built-in sample network, so treat those as a demonstration.

In the third week, leave it running through quiet hours and messy ones. Check that measured counts stay measured, that leads stay labelled as leads, and that your analysts still make the judgement on each lead.

In the fourth week, sit down with the person who would have been on call at ten past two, and the people who would approve a response. Go through SOAR's cases, proposals and approvals, and the alarm you kept from week one. Ask whether they would have signed on a measured count, a labelled lead and a proposal with an expiry. Then decide whether to expand, narrow, pause or stop, and write down why.

Throughout, remember what SOAR will not do: it will not keep your raw records, search old logs or change live systems. Your team still does all three.

Four weeks is a suggestion; agree the scope and the people involved for your organization.