SOAR · SEE THE ATTACK, AND WHO MUST SIGN THE RESPONSE

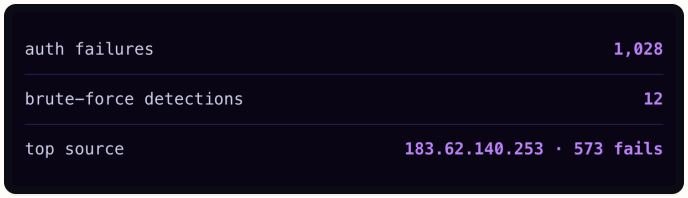
Is this attack real, and who decides what to do?

In the middle of the night, someone on your security team has to decide whether an attack is real and what to do about it. The evidence is scattered across several tools, and the decision often ends up as a chat message. SOAR brings the evidence into one place, puts a proposed response in front of the people your rules name, and records who signed.

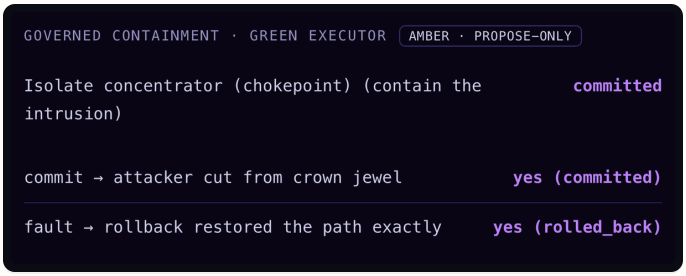
Three short demonstrations

To show how it works, we used SOAR's built-in demonstrations, which play back real, publicly available recordings. In the first, someone was trying to break into a server by guessing passwords. SOAR counted **1,028 failed log-ins from 24 different addresses** and marked the number as measured, because it came straight from the server's own records.

In a second recording, of network traffic, it noticed a computer contacting places it had never contacted before. It looked only at who was talking to whom and how much, never at what was said, and it kept none of the contents. It marked that finding as a lead, not yet confirmed.



The failed log-ins, counted from the server's own records.



A rehearsal on SOAR's sample network, so the names differ from the recordings. Marked as a proposal only.

Its third demonstration shows the response. SOAR drafts one, using AI models that run on your own computers, such as cutting an attacker off from the rest of the network. It rehearses that kind of change on a sample network, a simulation rather than your real one, and forces a failure so the undo can be seen. Then it waits for a person to decide.

Who has to approve depends on how risky you decide the action is. Steps your policy already allows go ahead without a person and are recorded. Riskier ones need one named person, two independent people, or, for anything that could affect safety, the case owner and a process engineer. Every approval a person gives expires, and it is tied to the evidence they saw: if the evidence changes, the approval no longer counts.

SOAR can run on your own computers with no internet connection. It keeps its findings and the record of who approved what, but not your raw data, and it works alongside the tools your team already has rather than replacing them. It does not change your live systems: your team does that. Its own built-in actions are demonstrations.

Next: the manager guide tells this night's story in full, and the evaluation brief describes a four-week trial.