Get to SOAR Faster Guide

SOAR has incredible upside. Why has it belly flopped (so far)?

Data sources that are hard to use
If your data comes from a hodgepodge of sources, you're going to have a bad time. It needs to be available (not disabled for performance/political reasons) and ready for ingest (normalized and mapped properly) Otherwise it's garbage in, garbage out.

Data that wasn't built for security
Most network data SOCs use comes from sources — like performance monitoring — that were created for a totally different purpose. This data isn't comprehensive or consistent enough to give you detailed evidence.

Playbooks that don't do enough
Playbooks should automate entire core workflows, not just discrete tasks like threat intelligence lookups or firewall updates. Corelight's comprehensive data makes complex, end-to-end playbooks accessible for any SOC.

Formula for SOAR success

A single data source
Easier to maintain and implement

Expert-crafted playbooks
Elevate everyone's performance

SOAR Platform
Drive process with robust platform

Defender advantage that lasts
To get automation’s full benefits quickly, you need to pair the right data with expert playbooks on a versatile platform. This makes it easier to get SOAR up and running, and enables amazing abilities — like automatically gathering the evidence needed to make the right call.

Here’s a step-by-step example on tackling alert fatigue:

1. Gather the right data to feed your SOAR playbook
   Clear away legacy logging sources and start collecting normalized, security-centric data that contains critical information, and nothing else.

2. Automate away time-consuming, ultimately pointless alerts
   Start by screening out the obvious. For example, consolidate repetitive alerts that all point to the same event, or alerts that can’t lead to an issue, like DNS queries without a response.

3. Package expertise to help your analysts overachieve
   Analyst skill sets and familiarity with tools varies wildly. Give them expert playbooks to take the guesswork out of investigations. You’ll get better quality and precision, while also training your team.

4. Customize playbooks and fine tune alerts
   With the time your team saves, they can hone detections to make them more accurate, or they can build on playbooks and create new ones.

“The most frequently cited barriers to excellence were lack of skilled staff (58%) and the absence of effective orchestration and automation (50%).”

*SANS SOC survey*
Get to SOAR Faster Guide

The right tools make it all possible

A scalable, open, extensible SOAR platform
• Platforms like Splunk Phantom take action in seconds, not hours
• Harness the full power of your existing security investments
• Work smarter, respond faster, and strengthen your defenses

What makes Corelight data different
• Structured, security-centric data that’s precorrelated for SOAR
• Built on Zeek, the global standard for network monitoring for 25 years
• Rich, yet lightweight and storable to deliver great detail, indefinitely
• Easily replace legacy sources, overcoming political and technical hurdles
• Integrates seamlessly with all your existing technology and process

Playbooks created by experts, from Corelight
• Created by elite cybersecurity practitioners with deep experience
• Make every analyst perform better, and more consistently
• Leverages years of tradecraft to get the most out of your data and platform
Fuse signal and evidence for precorrelations
Corelight speeds up SOAR implementation by integrating the open source powerhouses Zeek and Suricata. Because alerts are embedded directly into rich logs, everything’s faster down the line.

Investigate faster with alerts integrated into evidence. Every Suricata alert contains its associated precorrelated Zeek data to bring foundational, standardized evidence all in one place, speeding investigations.


Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com  |  888-547-9497