D3 SECURITY ☎ 1-800-608-0081 www.d3security.com sales@d3security.com

SOAR-NATIVE SOC

WHY TO START WITH SOAR FROM DAY 1

Many believe that SOAR (security orchestration, automation, and response) platforms are for more mature SOCs. The truth is that building a "SOAR-native SOC"—building your new SOC with a SOAR platform from Day 1—makes good sense from both a business and logistical perspective.

If you already have some detection tools (e.g. NIDS, EDR, SIEM) and ad hoc processes, and are transforming those elements into a formal SOC, now is an optimal time to learn how to leverage a SOAR platform's capabilities to overcome limited resources and an increasingly hostile threat landscape.

ORCHESTRATE

1. Quick-Start Playbooks
If you have ad hoc processes, you can configure them into your SOAR platform to standardize steps for consistency.

If you are open to improving your existing processes with guidance from industry best practices, out-of-the-box Playbooks give you a strong template to implement your own incident response and triage protocols, following industry standards such as NIST.

AUTOMATE

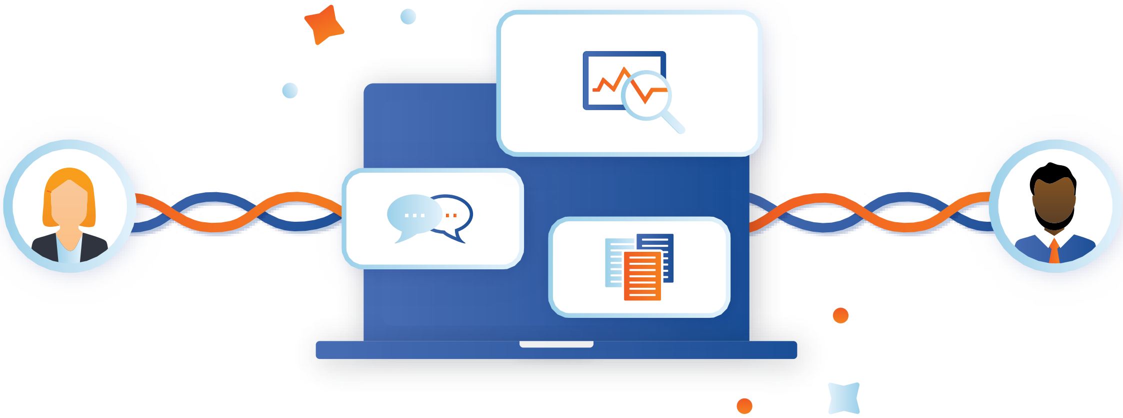
2. Inject Human Expertise & Maximize your Time
In a new SOC, you already juggle multiple roles and cannot afford to lose time on low-level actions such as copying and pasting between multiple tools and windows.

Focus your time on the tasks that require human experience and expertise by automating data collection and enhancement, intervening only where appropriate to efficiently make well-informed decisions.

3. Process Documentation & Improvement
One of the biggest challenges in IT security operations is capturing, retaining, and retrieving team knowledge.

As you evolve existing practices into continually improving Playbooks and Standard Operating Procedures (SOPs), a SOAR platform's automatic history tracking can improve the quality and speed of your procedures and documentation.

By logging all trials, errors, and successes, you avoid the time and hassle of pausing or back-tracking to manually record each step, forgetting important details, or making unintentional errors. As it's easier to review and eliminate unnecessary steps, improvement becomes systematic.



RESPOND

4. Investigative Case Management

IT security operations' core function is to *investigate*—log data, event alerts, incidents, and more. Related Events, Incidents, and Cases should be analyzed together rather than across multiple incompatible systems.

An investigative Case Management system built into a SOAR platform is a valuable enhancement that helps you identify subtle clues or early indicators of repeat offenders, suspicious actors, targeted assets missed during vulnerability assessments, and other applicable entities, all to help create stronger cases of evidentiary value.

5. Secure, Efficient Collaboration

SOCs handle sensitive data that needs to be seen or hidden depending on the need for collaboration.

A SOAR platform with granular, role-based Access Control Levels helps your teams securely collaborate on cases—regardless of job function—and conveniently share the right data with the right people, all in the same system.

6. Fast-Track Training & On-Boarding

As your SOC grows and new analysts join, you need to train your new recruits without compromising the integrity of your processes or slowing your incident response time.

With guided Playbooks, a SOAR platform acts as a 24/7 mentor, walking new analysts through your SOPs step-by-step to ensure consistency, learning, and confidence.

DEMONSTRATE YOUR BUSINESS VALUE

7. Manage Performance & Prove ROI

Security operations teams of today's leading businesses are no longer considered cost centers. They are expected to demonstrate their business value in money saved for the organization. A SOAR platform helps you maintain a "living business case" for your SOC.

How much time does each analyst spend to identify, contain, and eradicate an incident? What is the dollar value of the damage that the SOC has prevented? How many person-hours have you saved via automation? Tracking and reporting performance metrics in a SOAR platform helps you clearly and visually communicate your business value and focus on improvements.

8. Professional Consultation

Your goal is to make the technology work for you, not for you to spend your time working in the nuts-and-bolts of the technology.

With increasingly complex enterprise applications, vendor-specific configurability options, and an evolving threat landscape, a SOAR vendor's in-house CISSPs, business analysts, and project managers can save you significant time and hassle by helping you evolve your existing processes into replicable workflows and translate your business problems into a scalable business solution.