



# SOAR: THE ACKNOWLEDGEMENT THAT ALL OF YOUR CYBERSECURITY PLATFORMS HAVE FAILED

---

WHITEPAPER



## Overview

The cybersecurity marketplace has adapted and yet marginally evolved to meet the changing needs of security operation centers (SOCs) over the past few decades. It seems as though every week there's a new solution introduced.

To stay ahead of the bad actors who have been evolving their techniques right alongside the market, companies find themselves making nearly continual technology and resource investments into security solutions and processes.

For some teams, the result is a patchwork of incompatible, often redundant, tools. These "additive solutions" focus on essential security goals:

- The ability to access historical data made it possible to comply with rapidly changing compliance requirements in an efficient, effective way.
- Aggregating and analyzing network events captured by endpoints and machine-generated data sources to provide greater visibility into network infrastructure challenges.
- Providing search and investigative capabilities.
- Serving as a log collection point.

Ultimately, even teams that invest heavily in a variety of add-on solutions typically find that they remain vulnerable to internal, external, and zero-day threats. For teams stuck in this add-on solution cycle, providing adequate cybersecurity requires a whack-a-mole approach, where another issue pops up as soon as the company invests in a new solution.

This brings us to the most critical question we must ask of legacy cyber threat platforms: Does deploying yet another supplemental technology to stitch failed platforms together really represent a company's best option?

The circular logic of vendors and analysts has become daunting and frustrating to consumers:

1. Select a SIEM to correlate, search, and investigate historical log data.
2. Add an NTA platform because it's prohibitively expensive and functionally inadequate to bring that data into a SIEM.
3. Deploy a UBA vendor for internal threat detection because we don't have the required data or analysis capabilities in either my SIEM or NTA platform.
4. Bring in a 3rd party SOAR platform to somehow make them all work together.
5. Repeat.

***“SOAR is the acknowledgment that all of your other approaches to cybersecurity have failed.”***

- Jeff Shipley, CEO of RAVENii

## The Introduction of the SOAR “Solution”

The latest in an ever-increasing bag of supplemental platforms to address the shortcomings of legacy cyber threat platforms is SOAR (Security Orchestration Automation and Response).

Like its predecessors, SOAR is a cyber bandage designed to address the failed promises and functional inadequacies of legacy (SIEM, NTA and UBA) vendors with yet another layer of additive and arguably unnecessary technology. It’s [yet another “solution”](#) to add to the heap.

In fact, in a [recent survey](#) conducted by Swimlane, cybersecurity professionals stated that the most popular use case for SOAR was as a tool to triage their already existing SIEM solution. See figure 1. “SOAR is just another band-aid for the shortcomings of all of these other products,” says Mike Yelland, Senior Sales Engineer at MixMode.

Take, for example, the primary value prop for SOAR solutions as described by vendors and analysts alike: *To improve, streamline, and enhance the interoperability between multiple, disparate security platforms.*

The presumption then for the value of a SOAR platform is that the previously deployed cybersecurity platforms have failed to address the requirements they were intended to solve. Worse, it presumes that the original goals of the deployment can only be addressed by adding additional supplemental technology and workflow integration to address the deployed product’s functional gaps.

The most concerning aspect of SOAR’s position in the market is that it requires customers to acknowledge that all the additive technology, associated budget, and operational resources invested to date have not fulfilled the promises they have been touted to deliver. “SOAR is the acknowledgment that all of your other approaches to cybersecurity have failed,” says Jeff Shipley, CEO of RAVENii.

## IT Teams Can, and Must, Find Better Solutions

“Even the analyst community will tell customers that SIEM was really designed to meet basic search, investigative, and compliance requirements for machine data. They then state that companies need supplemental “tools” and additional supporting resources for NTA platforms,

Figure 1: What are the key use cases your organization is utilizing SOAR for?



[Swimlane - 2020 SOAR Report](#)

for network traffic analytics, and UBA platforms for user behavior analytics and insider threat detection,” says Coulehan. “Often, when you get to a level of maturity with all three of those platforms, customers recognize that the lack of information sharing between them actually creates more, not less risk to the organization,” he adds. “Unfortunately the objective evidence suggests that the practice of stacking correlative analysis platforms on top of correlative platforms has failed to achieve the desired result, yet continues to be the industry trend.”

“The idea that one can solve critical cyber threat and intelligence issues with yet another add-on platform may benefit the vendor and analyst community, but our customers regularly tell us that they remain exposed, continue to struggle with operational and budgetary constraints, and have had enough with an ineffective and cost prohibitive 4+ vendor model that frankly doesn’t solve our problems or improve our threat posture,” he continues.

So, the central question remains. Is this the best one can expect for a modern SOC, and if so, how much time, money, and personnel are actually required to even theoretically make all of this work? The short answer is, “It won’t meet all your requirements and is too expensive.”

Most customers are surprised to learn that SOAR platforms rely on invoking 3rd party technologies, including next-generation firewalls and endpoint protection platforms via traditional API calls to isolate and quarantine malicious threats and users.

The ability to invoke those API calls is a product of months — sometimes years — of highly manual workflow definition and continuous refinement to create what SOAR vendors call “playbooks.”

During this process, SOAR vendors downplay the common customer misconception that the O (“Orchestration”) and the A (“Automation”) in SOAR are adjectives for the R (“Response”).

That assumption is categorically incorrect. SOAR technology is neither designed nor intended to independently execute, orchestrate and automate response or remediation.

SOAR platforms are designed as workflow tool sets capable of automating information sharing and correlating data and events between legacy silos, applications and incomplete data sources. However, they are reliant on third party platforms and human operators to take action.

“SOAR is designed to stitch together disparate platforms and data sources that don’t play well together, but that’s not how they are sold,” explains Coulehan. “Vendors and analysts propagate the idea that somehow, theoretically, the creation of playbooks and workflow processes across disparate vendor platforms is going to deliver an improved or automated response to the most serious threats and vulnerabilities, which has not proven valid in today’s environment.”

In Swimlane’s [2020 SOAR Report](#), 68 percent of cybersecurity professionals also stated that the most valuable functionality of their SOAR platform is its ability to optimize existing tools (i.e. SIEM, NDR, and EDR). See figure 2. This implies that without such tools, their SOAR wouldn’t be able to perform its most important function. Still not convinced? Consider [Gartner’s own definition](#), which states that a SOAR platform “informs decisions by correlating the output of siloed processes and technologies.”

**Figure 2: What ROI impact do you consider most important to justify investment in SOAR solutions?**



# 68%

Optimize value  
of existing tools

[Swimlane - 2020 SOAR Report](#)



## The SOC Reckoning

What are companies really gaining when they take on SOAR? At a high level, SOAR and legacy platforms are falling far short of their promises. SOCs are left with several pivotal questions:

- Do we really need yet another platform to inform decisions by correlating information between redundant systems?
- Wasn't that the original intent of a SIEM or similar log management and correlation platforms?
- If the deployment of SIEM, NTA, UBA and other cyber threat platforms has proven ineffective, should we be exploring options to leverage a fully integrated, modern SOC platform that could outperform the functional requirements of legacy SIEM, NTA and UBA?
- Can't we eliminate the need to automate, orchestrate, or integrate limited value platforms?
- Wouldn't the value of a SOAR platform diminish if the requirement for multiple legacy tools (SIEM+NTA+XDR+UBA, etc.) is addressed with a single, purpose-built cybersecurity AI platform?
- Can't we do better than this patchwork of tools?

Here's the good news. There is a viable alternative to checking boxes on the typical components in a program and watching those systems fail while those systems also blow out your budget [MixMode can help](#).

## Modern Security Issues Require Modern Solutions

A [jumble of ineffective, incomplete, extremely expensive platforms](#) that don't meet the fundamental challenges faced by enterprise SOC teams in the early 2020s is not sustainable.

As other [vendors](#) have continued introducing inadequate solutions into the marketplace and signing up clients for lengthy, murky service contracts, MixMode has been leveraging cutting-edge technology to revolutionize enterprise security.

## How MixMode Works

Third-wave, unsupervised AI is the cornerstone of the MixMode single-platform solution. Instead of tacking on yet another additive band-aid solution, MixMode empowers teams to replace their failing systems with technology that works in a fundamentally different way.

Rather than applying a rules-based approach, where first or second-wave AI responds to predefined parameters, MixMode is a responsive, ever-evolving network resident. Instead of comparing new network behaviors to a set of expected behaviors, MixMode can differentiate between problematic and safe behavior by developing a true understanding of the network's baseline behavior.

In a week, MixMode establishes a [baseline of behavior](#) across an entire network, both on-prem and in the cloud. Over time, the software is so adept that it can begin to predict expected behavior and limit flagging to truly questionable behaviors and vulnerabilities. The result is a SOC team that can focus on important tasks rather than chasing down an endless list of alerts created by first- and second-wave, rules-based AI.

When security teams can turn to a singular, powerful solution for network security — one that is not reliant on ongoing updates — they can turn to other matters at hand, safe in the knowledge that anomalous behavior will be detected in real-time and stopped or flagged appropriately.



[www.mixmode.ai](http://www.mixmode.ai)

+1 (858) 225-2352 | [info@mixmode.ai](mailto:info@mixmode.ai) | © 2021 MixMode, Inc.

## About MixMode

MixMode is a next-generation, AI-powered cybersecurity platform focused on solving two primary issues for the Security Operations Center: providing next-generation threat detection, surfacing zero-day attacks and improving false-positive alert fatigue. MixMode allows security teams to dramatically increase productivity and efficiency while significantly decreasing the wasted time, effort, and resources associated with legacy cybersecurity tools.

MixMode's AI intelligently creates and updates the network baseline, then provides security teams with sophisticated functionality like predictive attack detection, 95% false-positive alert reduction, and all the tools necessary to investigate a threat. SOC teams can easily integrate MixMode into their security stack to dramatically reduce the investigation time, cost, and expertise required to respond to persistent threats, malware, insider attacks, and nation-state espionage efforts. MixMode's core AI algorithm is patented and was utilized over the past 20 years on projects for DARPA and the DoD. MixMode is headquartered in Santa Barbara, CA.