

# HOW USING SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE TOOLS MAKES LIFE EASIER... AND MORE DIFFICULT

CONFESSIONS OF SECURITY PROFESSIONALS



AN ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) RESEARCH REPORT SUMMARY

BY DAVID MONAHAN

OCTOBER 2019

SPONSORED BY:



IT AND DATA MANAGEMENT  
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

# Table of Contents

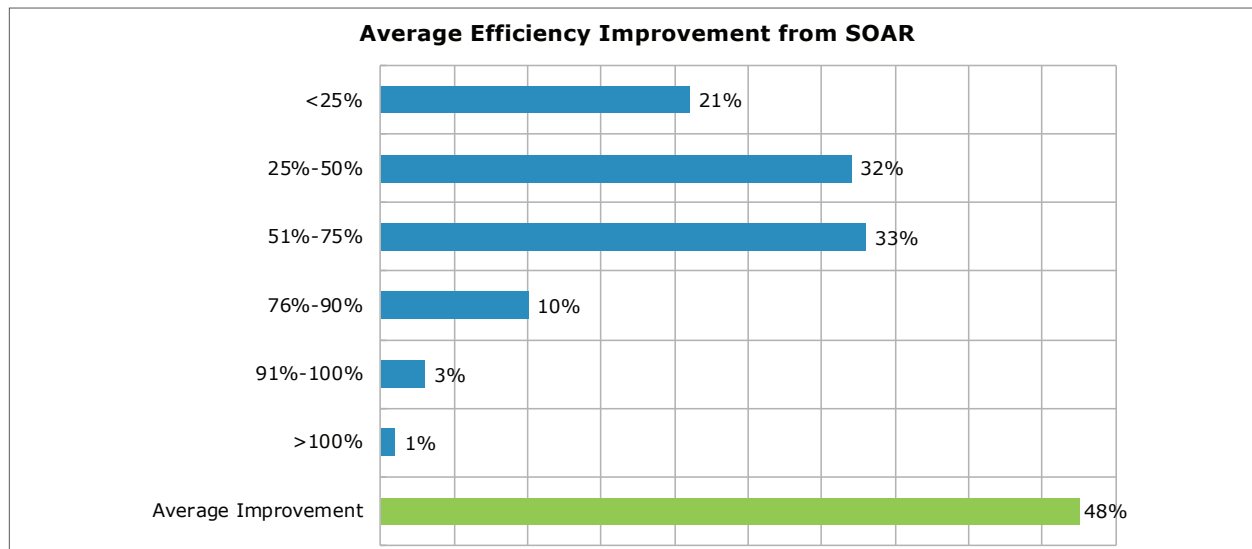
The SOAR Value Proposition .....	1
Efficiency Improvements .....	1
Existing Process Gap Identification .....	2
Problem Diagnosis Accuracy Improvements .....	3
Productivity Improvements.....	5
SOAR and Staffing .....	7
SOAR Investments .....	9
Achieving Return on Investment with SOAR .....	9



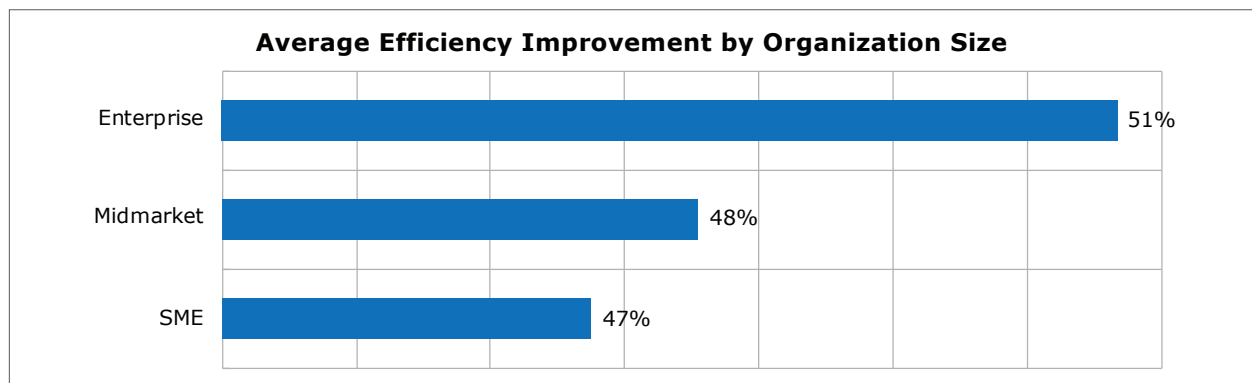
# The SOAR Value Proposition

## Efficiency Improvements

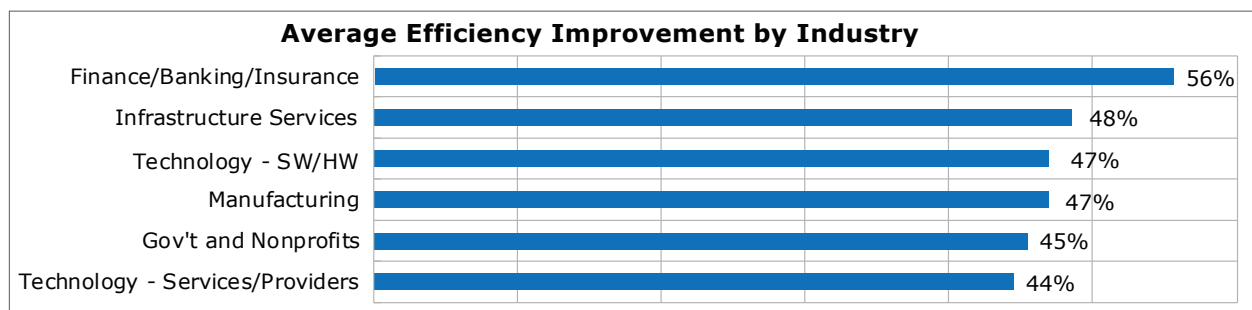
Three of the stated value propositions from SOAR are the improvements in efficiency, productivity, and execution accuracy. Those engaging in SOAR activities, commercial or homegrown, identified huge gains in all three areas. On average, respondents identified a 48% efficiency improvement. Previous EMA research<sup>1</sup> identified that 64% of the security tickets generated per day were not being worked due to lack of manpower (and automation). This level of efficiency gain would drop that percentage significantly, thus reducing risk to each participating organization. SOAR allows many cases that were previously left behind to now be investigated.



Enterprises saw the most efficiency improvements, reaching an average of 51%.



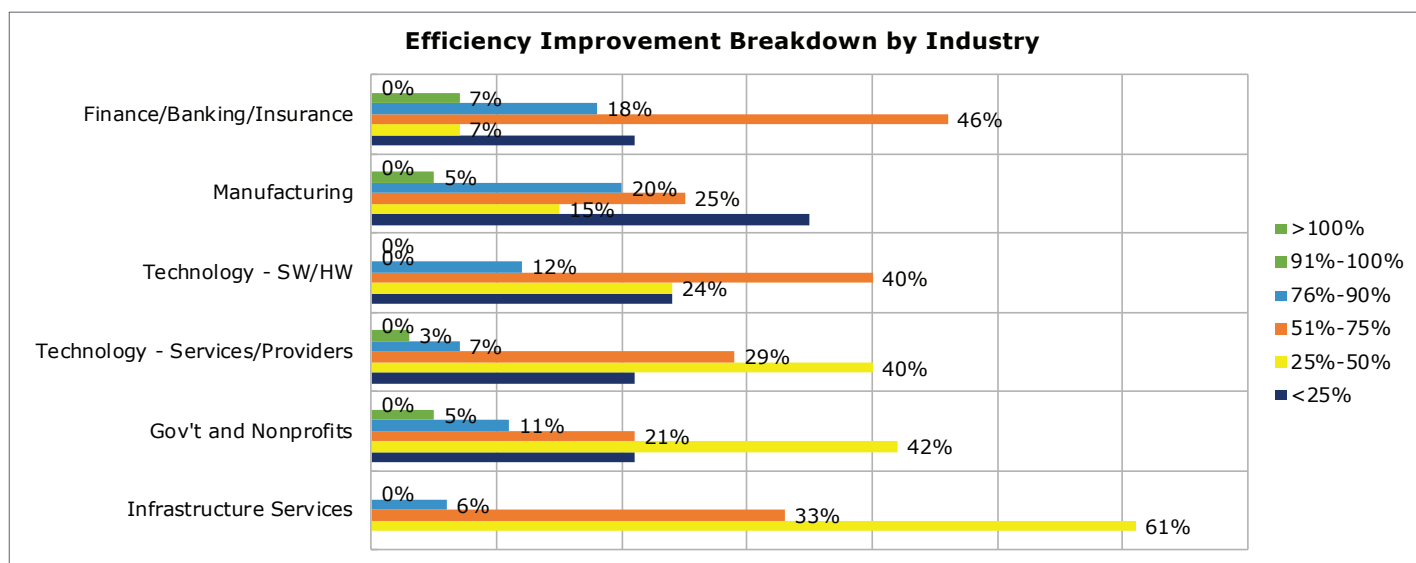
Finance/Banking/Insurance topped the list by industry at 56%. Every identified industry had significant increases.



<sup>1</sup> [A Day in the Life of a Cyber Security Pro](#)



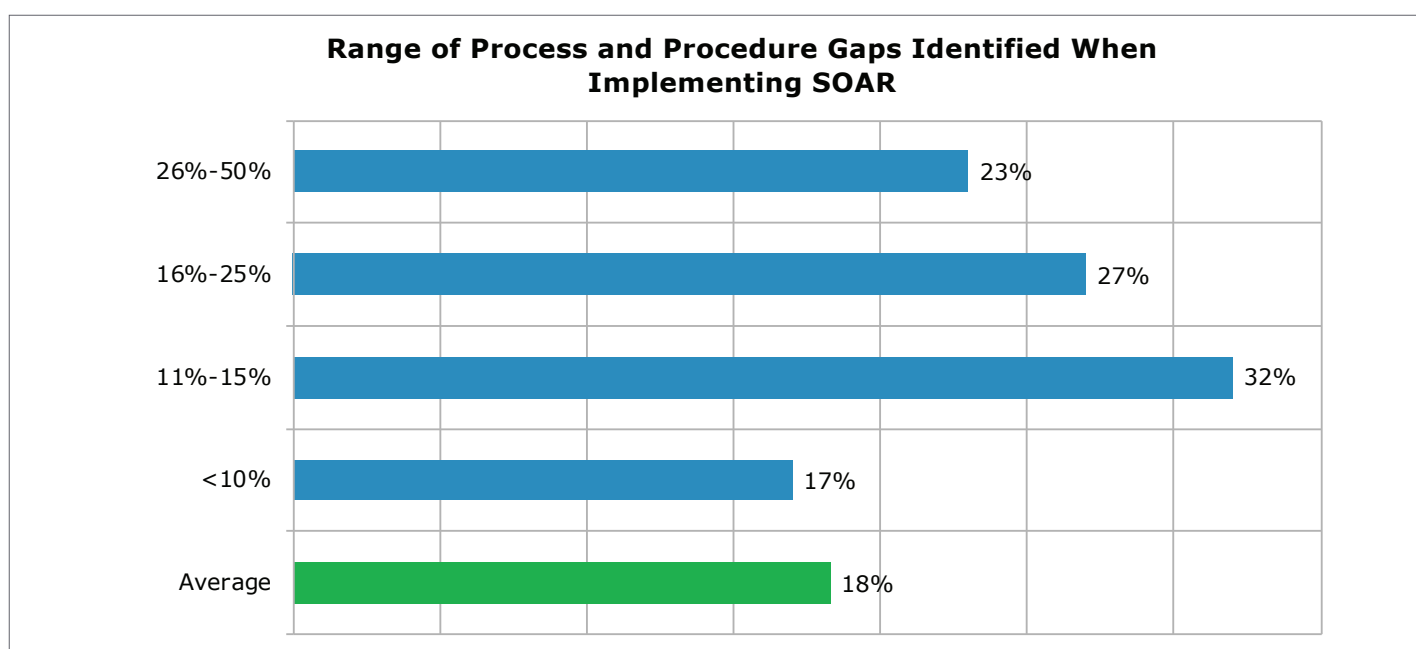
Infrastructure government and technology services and providers saw the most gains in the 25% to 50% improvement range, while finance/banking/insurance and manufacturing saw most of their gains in the 51%-75% improvement.



## Existing Process Gap Identification

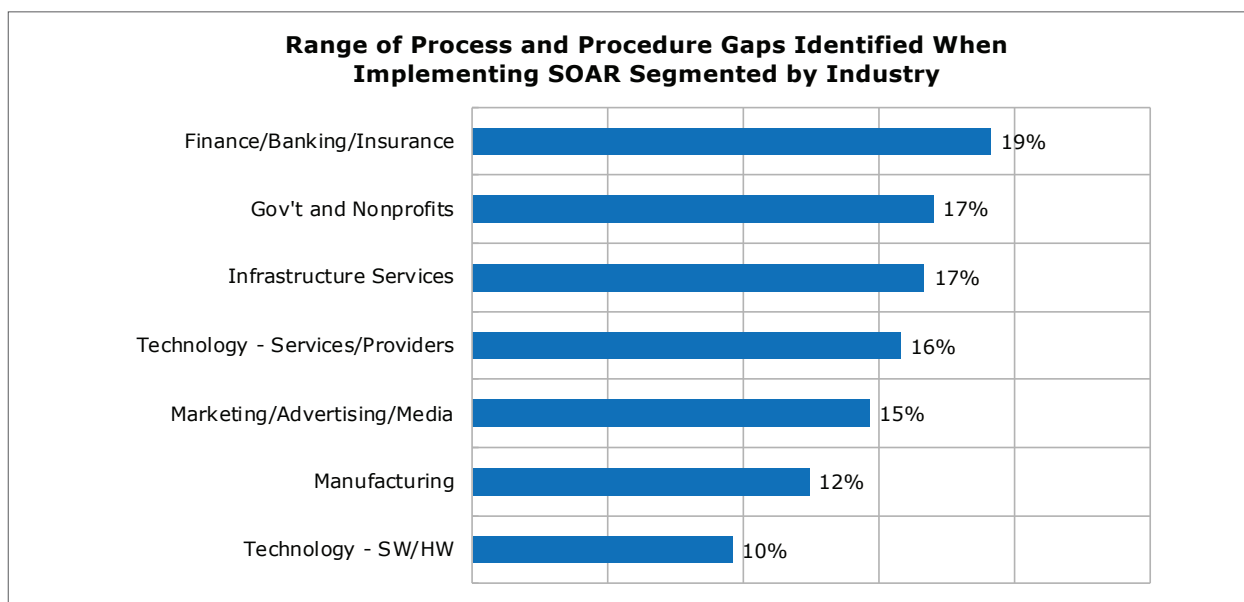
With automation comes the acceleration of outputs. However, just because it's faster does not mean it's better or more accurate. Automating bad processes will just bring bad outcomes faster. One of the unintended benefits of SOAR is discovering where bad processes exist. Whether bad processes and procedures exist because information is out-of-date, incomplete, or totally undocumented, automating an investigation and a response forces updates to occur. Every industry reported SOAR forced that hand and helped them identify those gaps.

Twenty-three percent of respondents said their organizations found gaps in as many as 50% of their processes. Further investigation revealed that much of these gaps were things that they had never documented before, but many were outdated processes and procedures. All were being run more by tribal knowledge and iterative evolution.





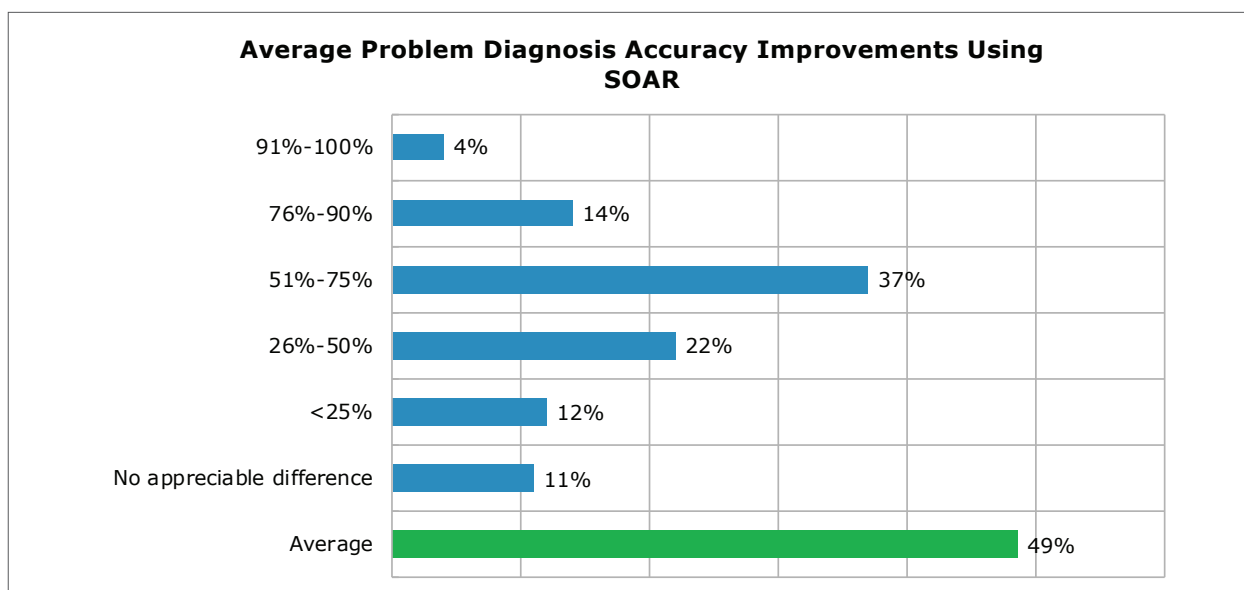
Following is the breakout of gaps identified by industry. An interesting takeaway was identifying that the finance/banking/insurance industry has the highest percentage of gaps. This happens because they have the highest number of processes and procedures documented, and thus the most target-rich environment. When automating, any variance can be significant, so identifying the gaps is critical.



## Problem Diagnosis Accuracy Improvements

If there are errors or gaps in process, errors still occur, but they occur faster and take teams in the wrong direction. Once productivity is improved and process and procedure gaps are addressed, execution accuracy will follow.

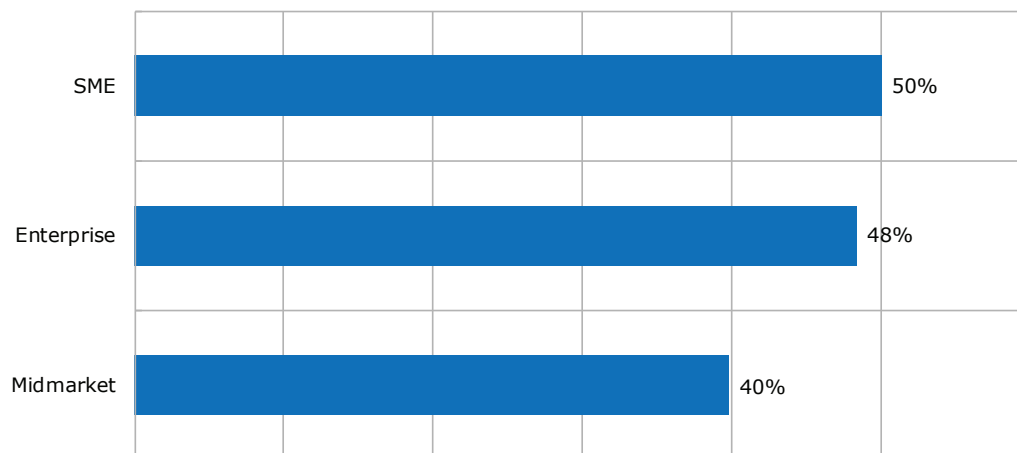
The chart shows how significantly organizations using SOAR were able to improve their problem diagnosis accuracy. On average, respondents indicated a 49% increase in the accuracy of problem diagnosis—very similar to the overall productivity. Previous EMA research<sup>2</sup> identified that 52% of threat alerts were improperly diagnosed by existing systems requiring rework. SOAR both speeds and improves diagnosis. The following chart shows that SME organizations actually benefited the most from this outcome, with a 50% improvement in diagnosis accuracy.



<sup>2</sup> Ibid

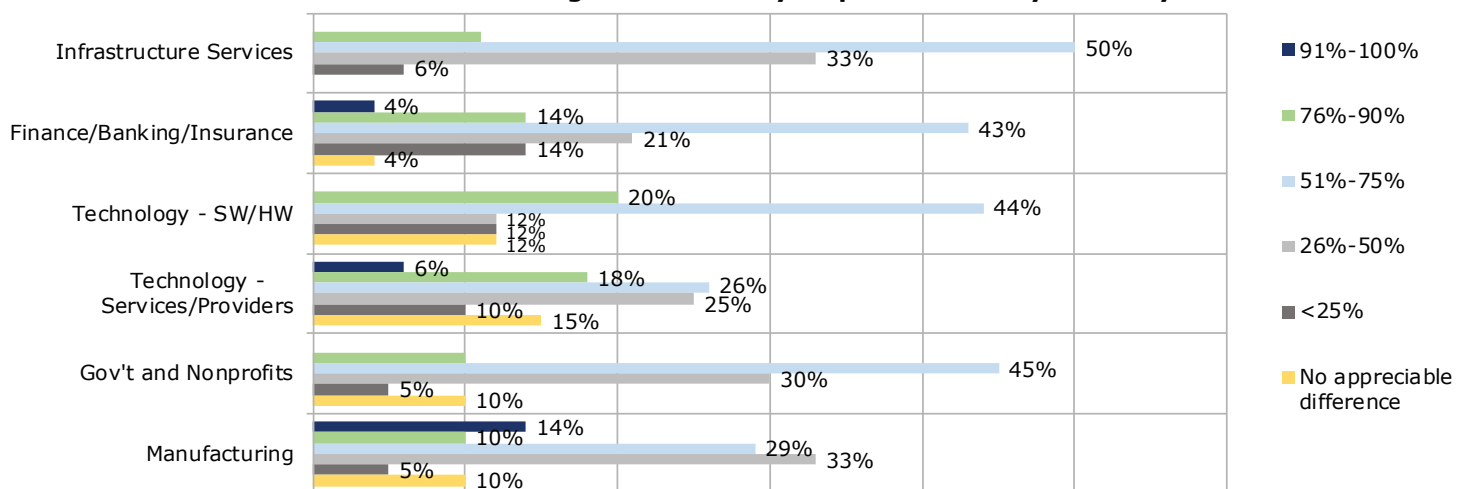
In a breakout by organizational size, SMEs identified the largest diagnosis accuracy improvements (50%). Even at the low end, midmarkets improved by 40%.

**SOAR Problem Diagnosis Accuracy Improvements by Organization Size**



By industry, 50% of infrastructure services saw improvements in the 51% to 75% range. Government, finance/banking/insurance, and technology HW/SW providers all saw similar improvements, while 50% of infrastructure services respondents achieved 50%-75% improvement in problem diagnosis. Fourteen percent of manufacturing respondents improved diagnosis accuracy by 100%.

**SOAR Problem Diagnosis Accuracy Improvements by Industry**

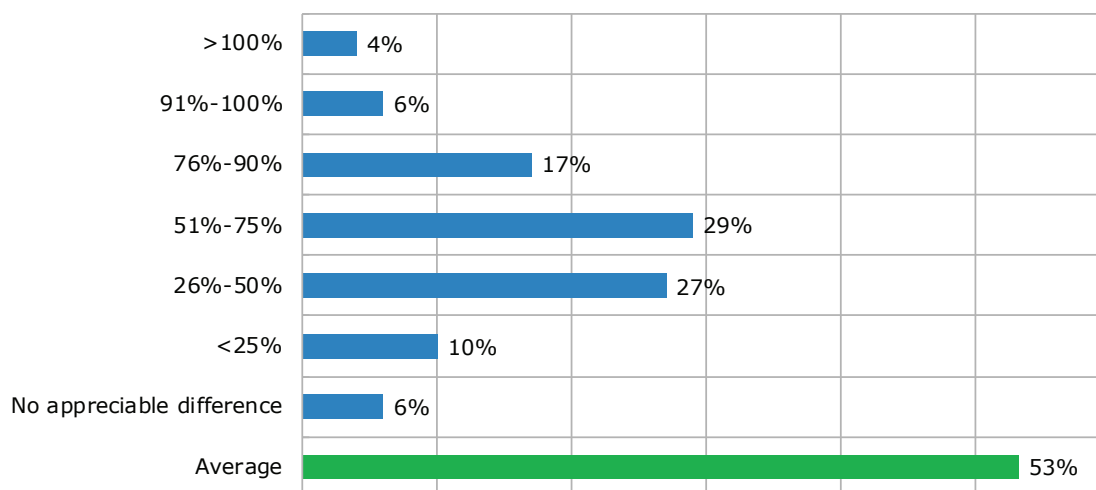


Sixty-four percent of respondents found these improvements to fall in their expected range. While excellent, the question for the next research project is, why did the remaining 37% feel they did not meet expectations?

## Productivity Improvements

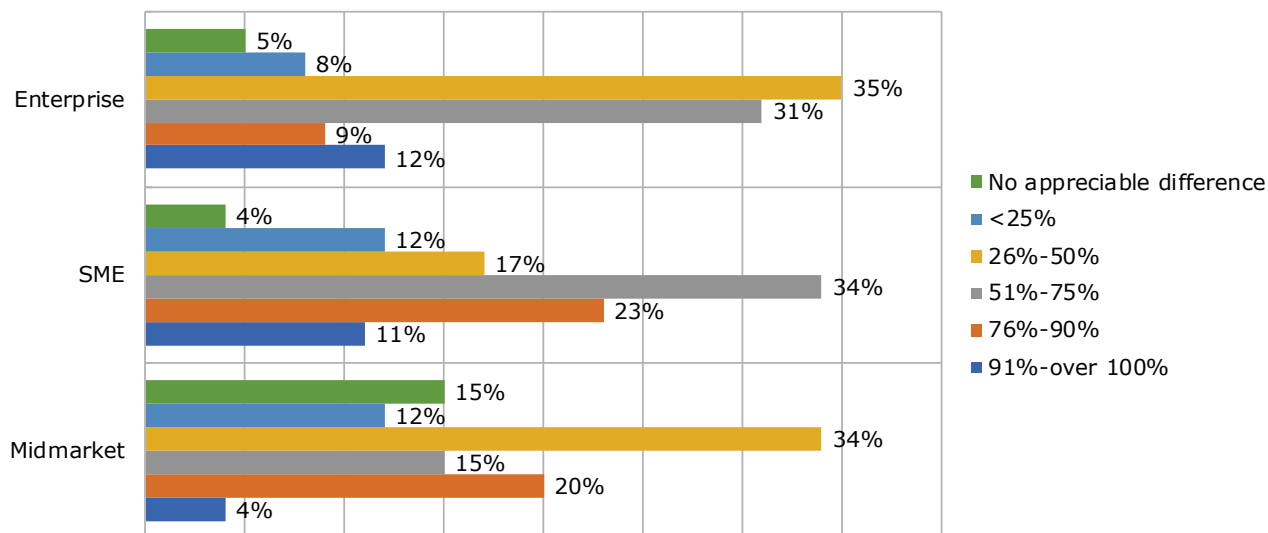
Productivity improvements also fell in similar ranges to efficiency. On average, organizations identified 53% productivity improvements.

**General Productivity Improvements Post-SOAR Implementation**



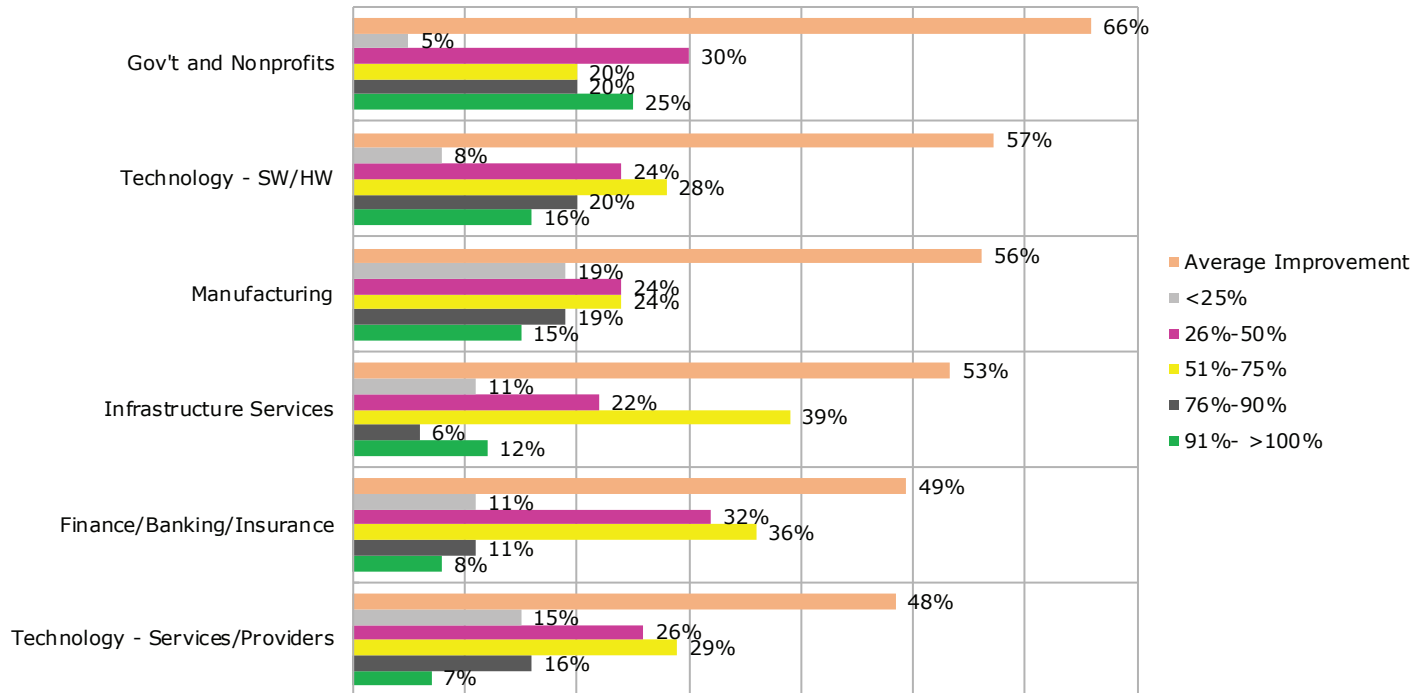
Segmented by organization size, 23% of the SME group saw a 76% to 90% productivity improvement and 12% of Enterprises saw 91% to over 100% productivity improvements.

**Productivity Improvements Post-SOAR Implementation by Organization Size**



The next chart depicts both the range of productivity improvements and the average improvement by industry. Government saw the largest average improvement with 68%. Government is known to be one of the most process-heavy organization groups, so this must be a product of the efficiency and productivity improvements and the process gap closures.

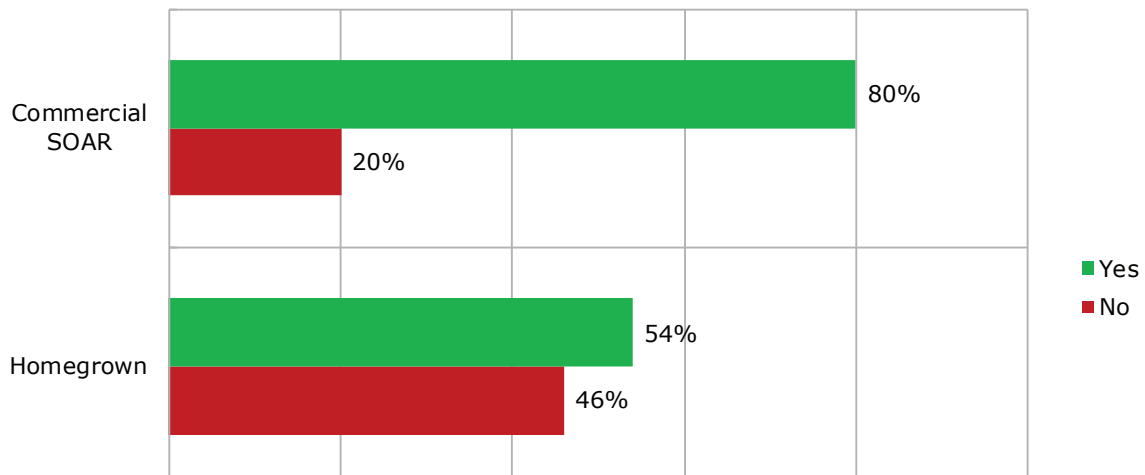
### Productivity Improvements Post-SOAR Implementation by Industry



One of the comparisons made was analyzing how responses from those with commercial SOAR implementations differed from those using homegrown automations and orchestrations.

The following chart shows 80% commercial SOAR users felt this met their expectations compared to the homegrown SOAR implementations that, 36 points lower, was at 54%. Commercial SOAR met expectations 1.5 times more often than in-house SOAR in the area of productivity improvements.

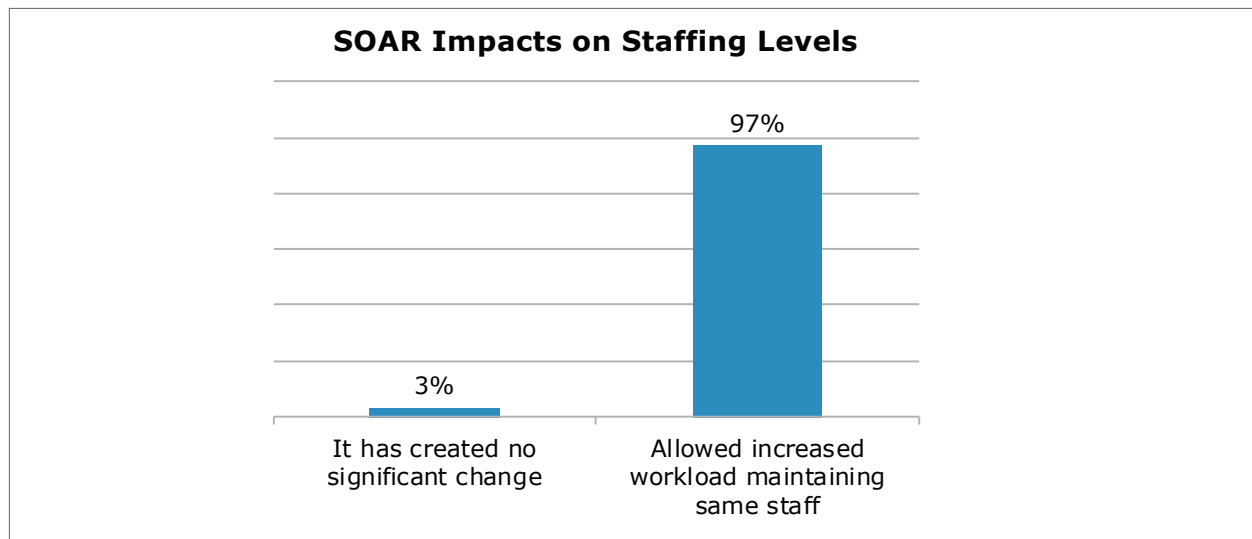
### Commercial SOAR vs. Homegrown Automations Meeting Productivity Expectations



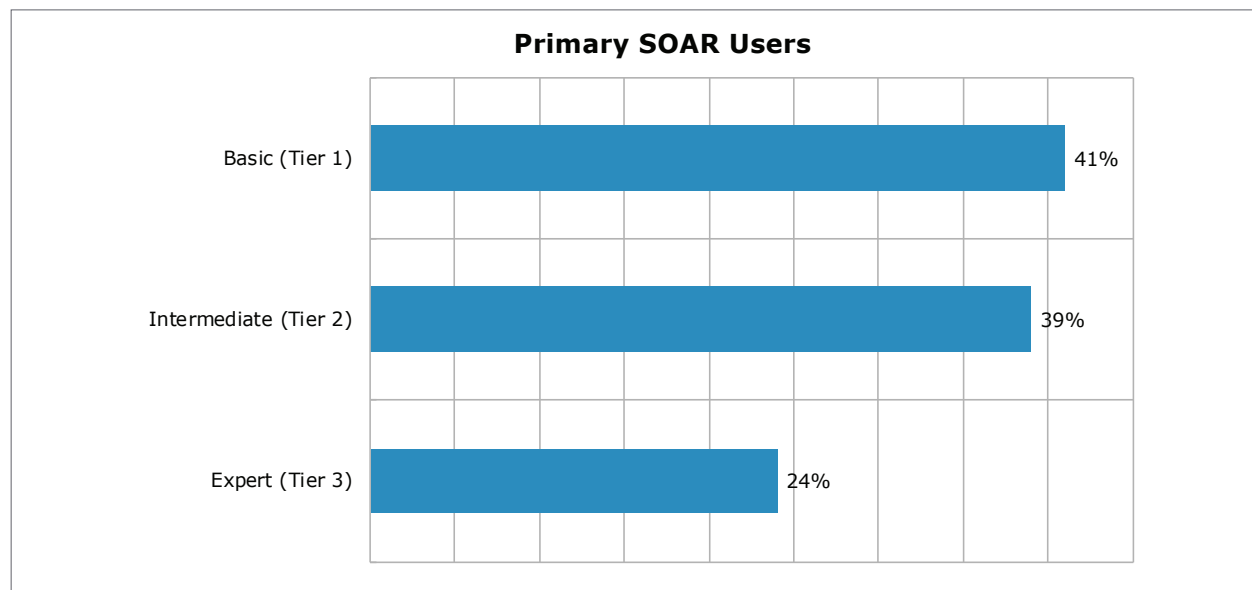


## SOAR and Staffing

Much of the reason why SOAR allows for doing more with the same staff has been discussed focusing on the business, so this section focuses on additional staff impacts.

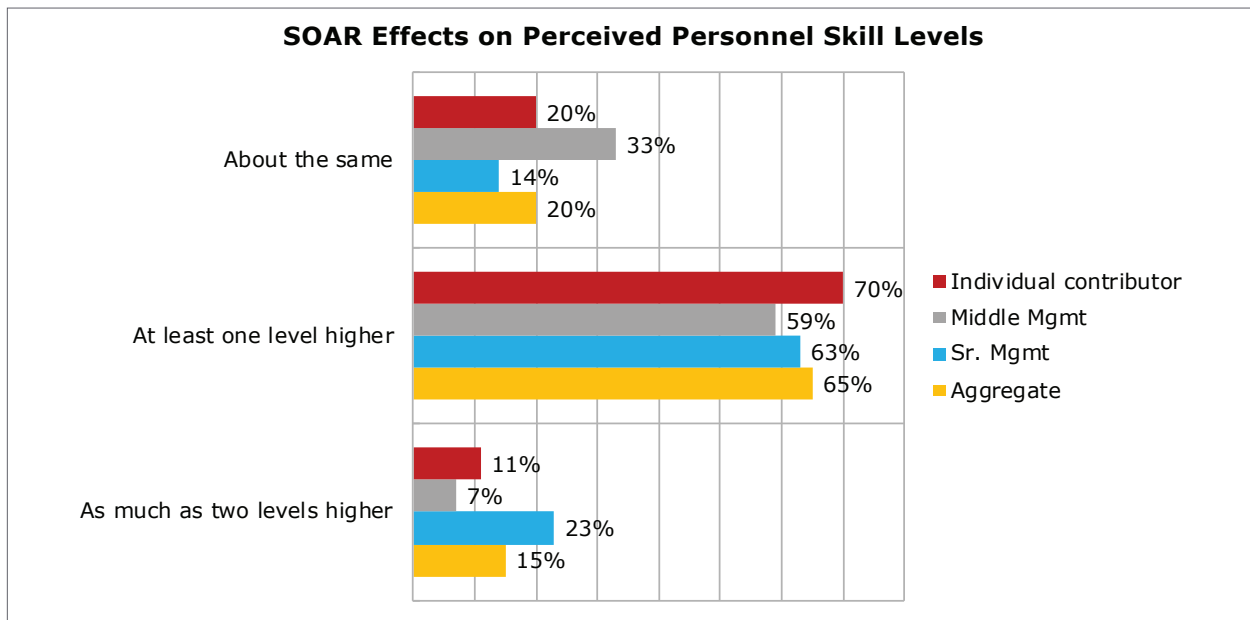


EMA asked respondents, when organizations purchase SOAR, what level of technical skill or performance are they aiming at using it? Is it meant as a frontline augmentation to give the initial trouble receivers basic information, or is it meant to be used by a higher skill level for trouble resolution, etc.? The truth, as expected, is all of the above. Due to its nature, and based upon how the implementers design it to be used in their workflows, it can support users at every level—trouble investigation, threat hunting, or incident response. It really depends on where the orchestration starts in the process.

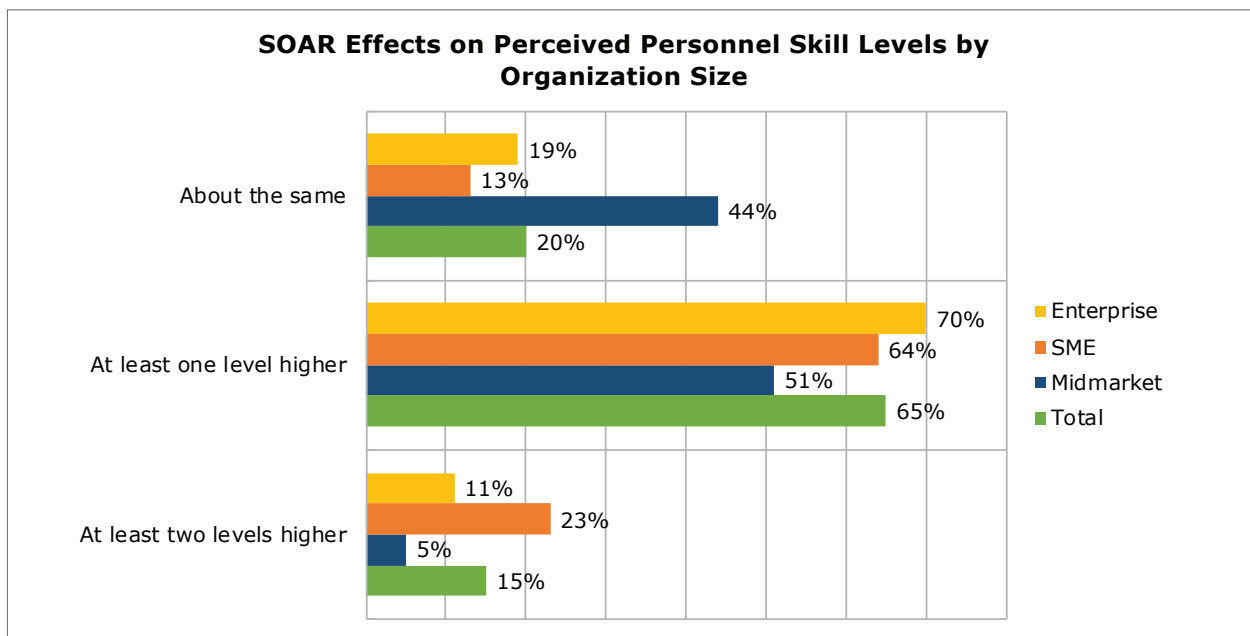


A highly useful benefit of implementing SOAR is the perceived improvement in personnel skill level. This perception is based on the efficiency and productivity improvements through automating the data-gathering process. A tier-one skill level associate does not usually have the skill to know how to quickly locate all of the telemetry and artifacts in uncommon or more complex cases, thus time is lost. With automations and orchestrations doing the heavy lifting in these cases, the increased efficiency makes those personnel appear to be more prepared and/or competent. This happens all the way up the skill chain.

Just over 65% of respondents said their perception of personnel performance increased by at least one level. On average, 15% of participants said they felt personnel performed at two levels higher. Most importantly, 23% of senior management felt their personnel were performing at least two levels higher.



Evaluating the same question by company size, just over half of the midmarket companies (those with less than 1,000 personnel) felt that their personnel received a boost of one level, but 44% said they didn't see any improvement. It is clear that the smaller the company and thus the fewer or less complex automations deployed, the lower the perceived increase in employee improvement.



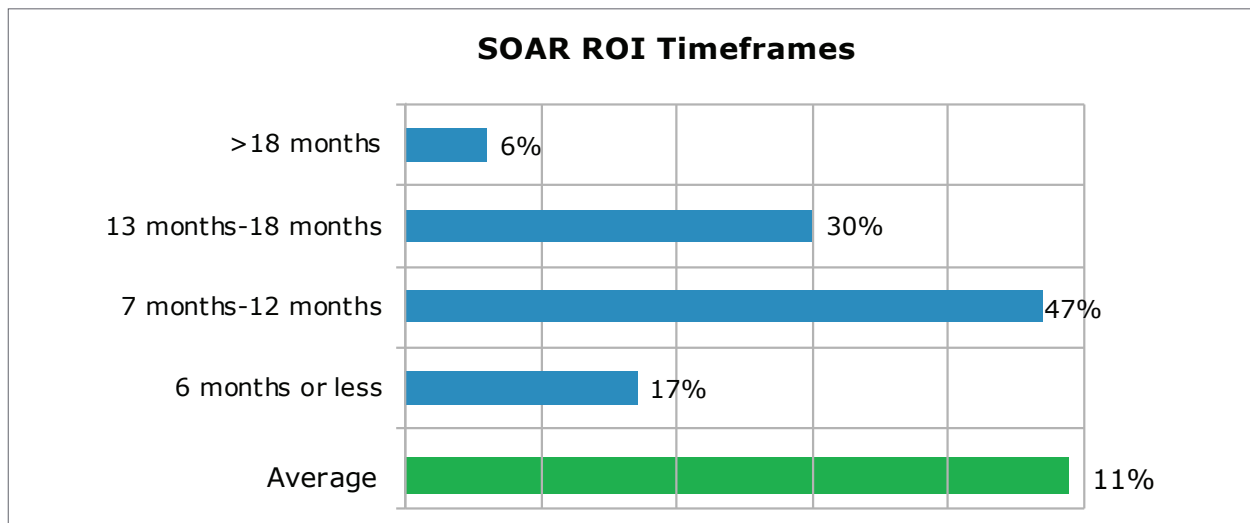
# SOAR Investments

Investing in SOAR tools is not an inexpensive proposition. However, it shows significant opportunity for security operations improvement. It is not a silver bullet. Getting it up and operational to the point it returns value and ROI takes work and resources. Following, EMA points out ROI assessments from clients.

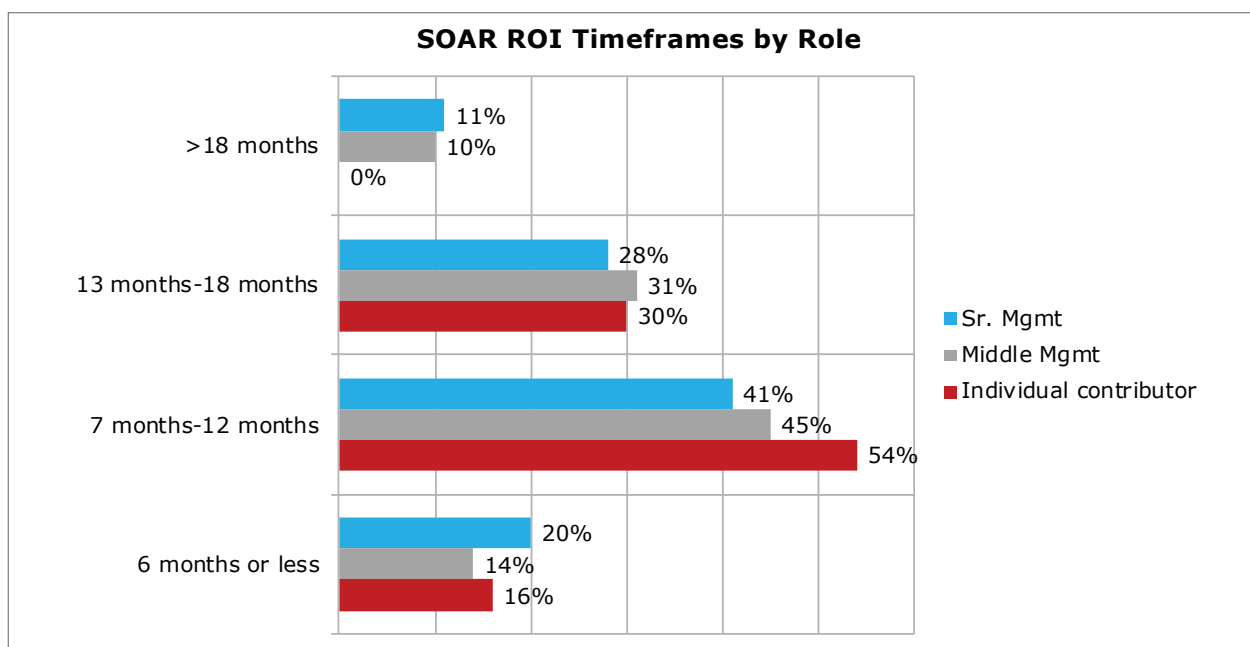
## Achieving Return on Investment with SOAR

As with any significant expenditure, decision makers and authorizers ask how long it will take to get the return on investment (ROI). Normally, U.S. businesses are far more aggressive and impatient on ROI, and range between one and three years.

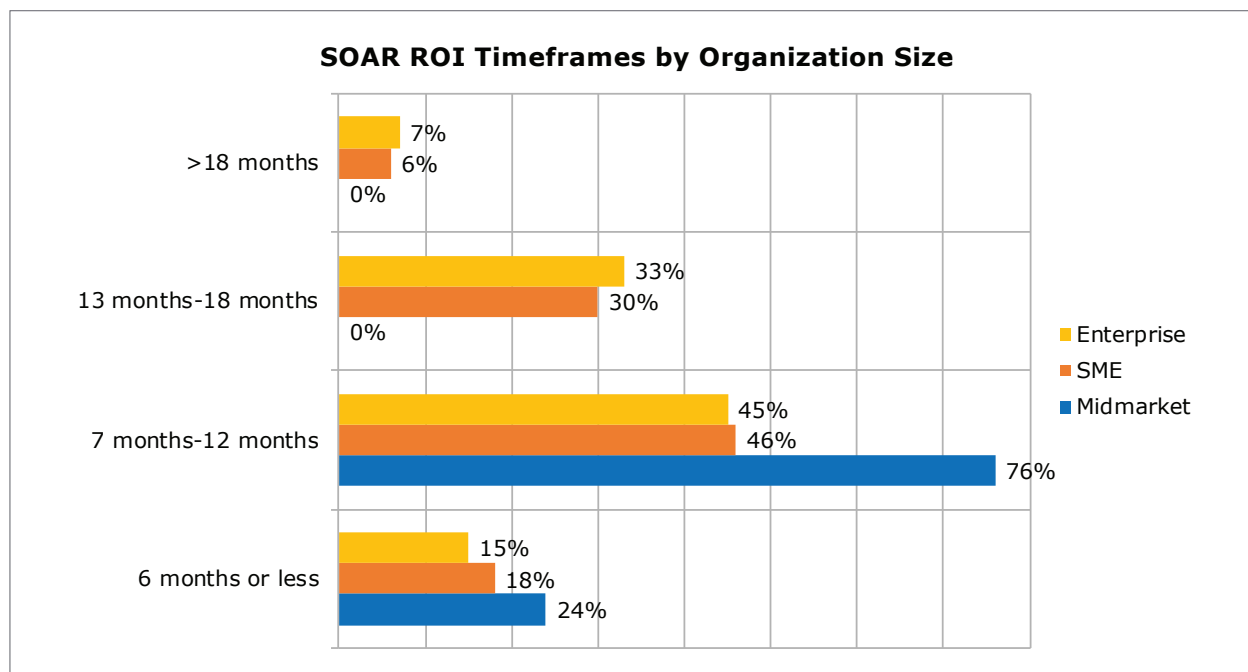
In the next chart, SOAR participants identified their estimated time for ROI. Sixty-four percent indicated ROI was achieved for them in 12 months or less with an average of 11 months. This is within the minimums most organizations expect.



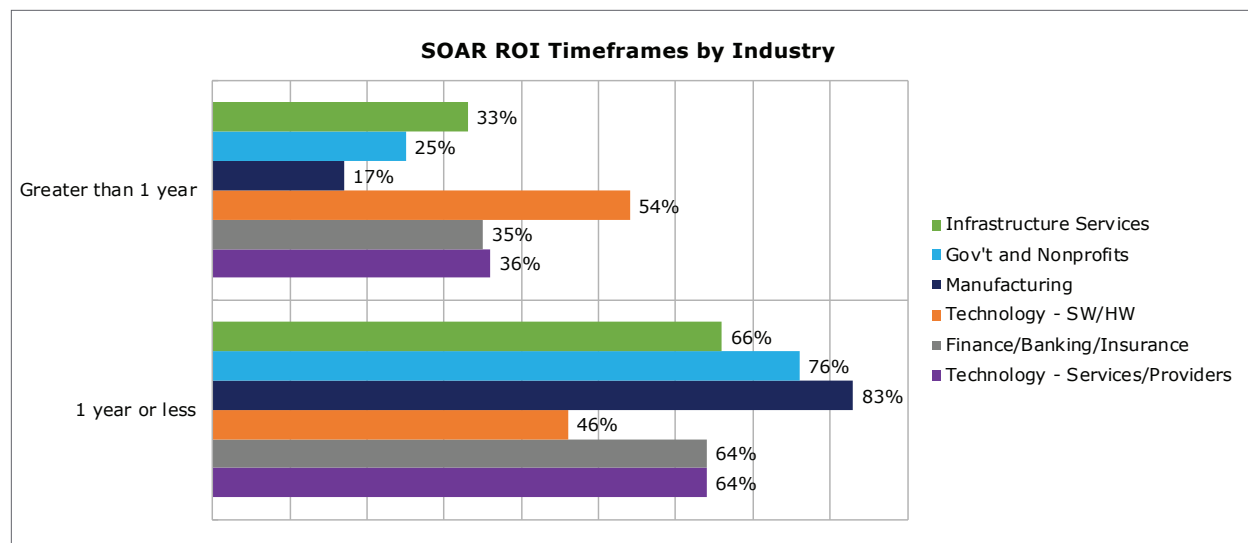
Interestingly, senior management was most conservative in their estimates. Twenty percent indicated they thought ROI was achieved in six months or less and none of the individual contributors felt it took longer than 18 months to achieve ROI.



When broken down by organization size, all of the midmarket respondents said it took them less than 12 months to achieve ROI, with 76% in the 7-12-month category. The midmarkets had fewer automations and felt they had lower productivity and efficiency gains, but also felt they met their ROIs faster than the Enterprises and SMEs.



Lastly, segmented by industry, 83% of manufacturing felt they met their ROI requirements in less than one year. On the contrary, 54% of technology SW/HW providers and 35% of finance/banking/insurance organizations felt it took them more than one year to meet their ROI goals for SOAR.



### About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates® (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at [www.enterprisemanagement.com](http://www.enterprisemanagement.com) or [blog.enterprisemanagement.com](http://blog.enterprisemanagement.com). You can also follow EMA on [Twitter](#), [Facebook](#), or [LinkedIn](#).

---

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2019 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

### Corporate Headquarters:

1995 North 57th Court, Suite 120  
Boulder, CO 80301

**Phone:** +1 303.543.9500

**Fax:** +1 303.543.7687

[www.enterprisemanagement.com](http://www.enterprisemanagement.com)

3898.091619