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:

splunk® phantom

EMA™ IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

Table of Contents

Executive Summary

The need for automation in security operations is widely apparent. In EMA's security orchestration, automation, and response (SOAR) research, 52% of participants reported that improving operational efficiency was their top goal for purchase, which was almost 1.5 times higher than the second-highest choice (addressing a personnel shortage). To fill that need, vendors supplying SOAR solutions and platforms have been emerging and expanding. While each vendor has something of a specialty or focal area, all are delivering significant value to their customers.

SOAR is being used to surpass homegrown automations that have been in place for years because they have development teams that specialize in creating integrations for tools commonly used. This research shows that those who have commercial SOAR solutions are much more highly automated than those who are using in-house tools. They are nearly two times more automated, with 47% of the SOAR customers reporting having 76% or more of their tasks automated versus 24% of those using only in-house automations.

On average, SOAR participants are taking 1.3 years to get to the level of automation they desired to achieve at the start of their projects, but also report having achieved ROI in about 11 months. Eighty-three percent of manufacturing, 76% of government and nonprofits, and 66% of infrastructure services organizations all felt they received ROI in one year or less.

Once personnel are able to start using automations and orchestrations, management perceives that the levels of efficiency increase to the point where 23% of senior management felt their personnel were performing at least two levels higher than without SOAR. Sixty-five percent of respondents felt operations staff were performing at least one level higher in perceived skillset.

While EMA does not tout SOAR solutions as a silver bullet, it is very obvious that organizations that make the monetary and time investment in the solutions are getting their money's worth.

Demographics Overview

Scope and Definitions

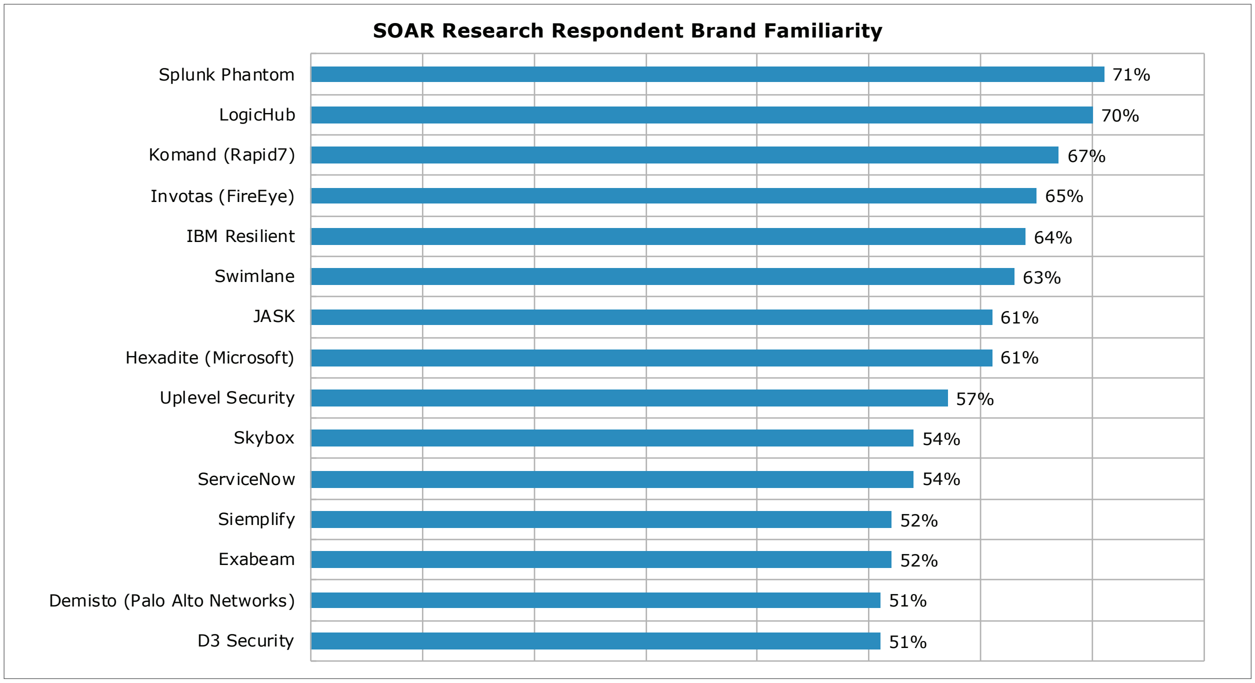
The SOAR report reached over 250 technology professionals from IT and security in both individual contributor and management roles across North America from companies of 500 or more people.

To provide a foundation for the rest of the document, demographic definitions are as follows:

1. Enterprises are organizations that employ 5,000 or more people
2. Small-to-medium enterprises (SMEs) employ at least 1,000 people but do not exceed 4,999
3. Midmarket organizations employed less than between 500 and 999 personnel
4. Graphs labeled as infrastructure services include oil, gas, chemicals, transportation, and telecom
5. Technology Services/Providers include any organization that provides internet access, internet or cybersecurity managed service providers, or IT professional services or consulting

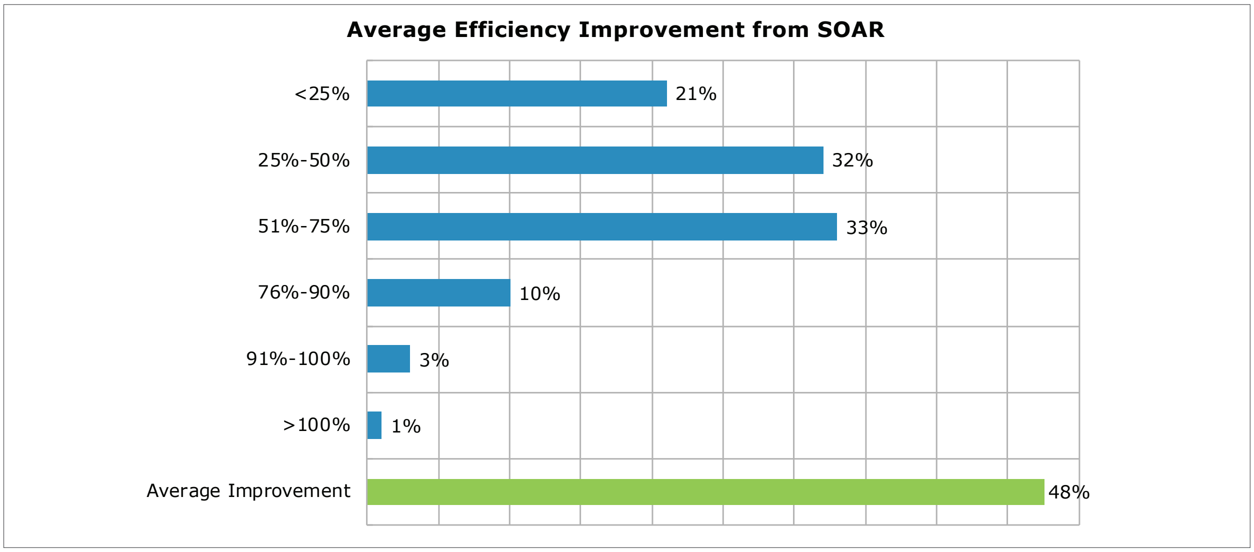
Familiarity with SOAR Vendors

The current SOAR market has no dearth of solutions adding value to the automation and orchestration market. Below is a list of the vendors operating within the space as recognized by respondents. This should give marketers some measure of how effective their marketing strategies have been.



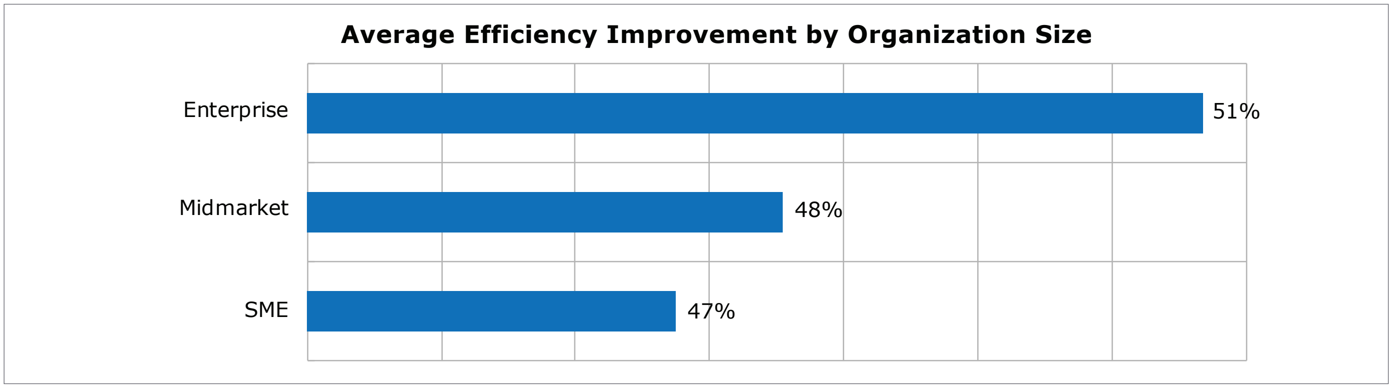
Efficiency Improvements

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[1] 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.

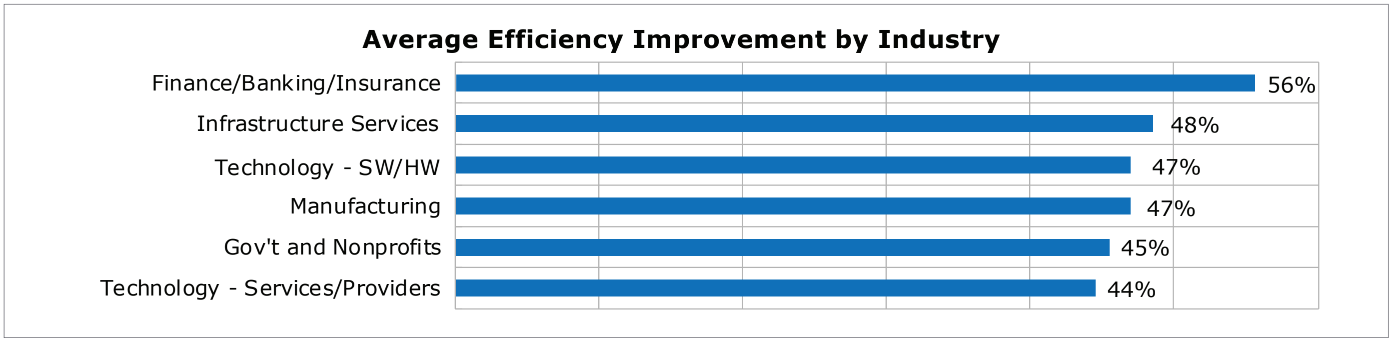


1 A Day in the Life of a Cyber Security Pro

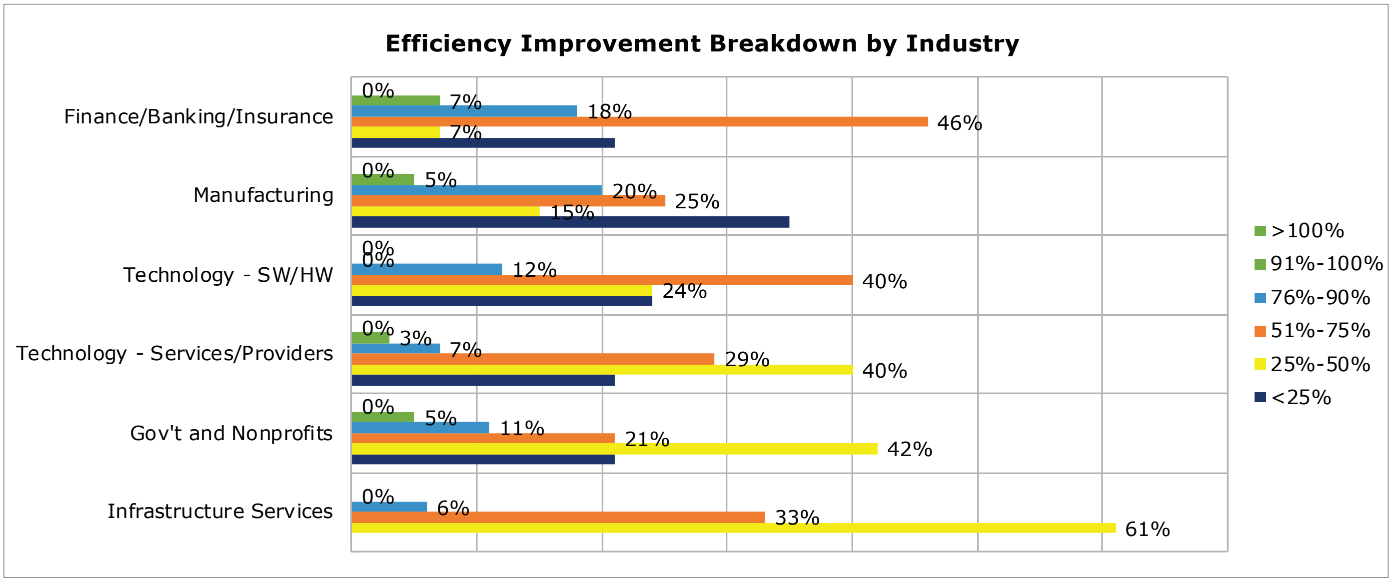
Enterprises saw the most efficiency improvements, reaching an average of 51%.



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



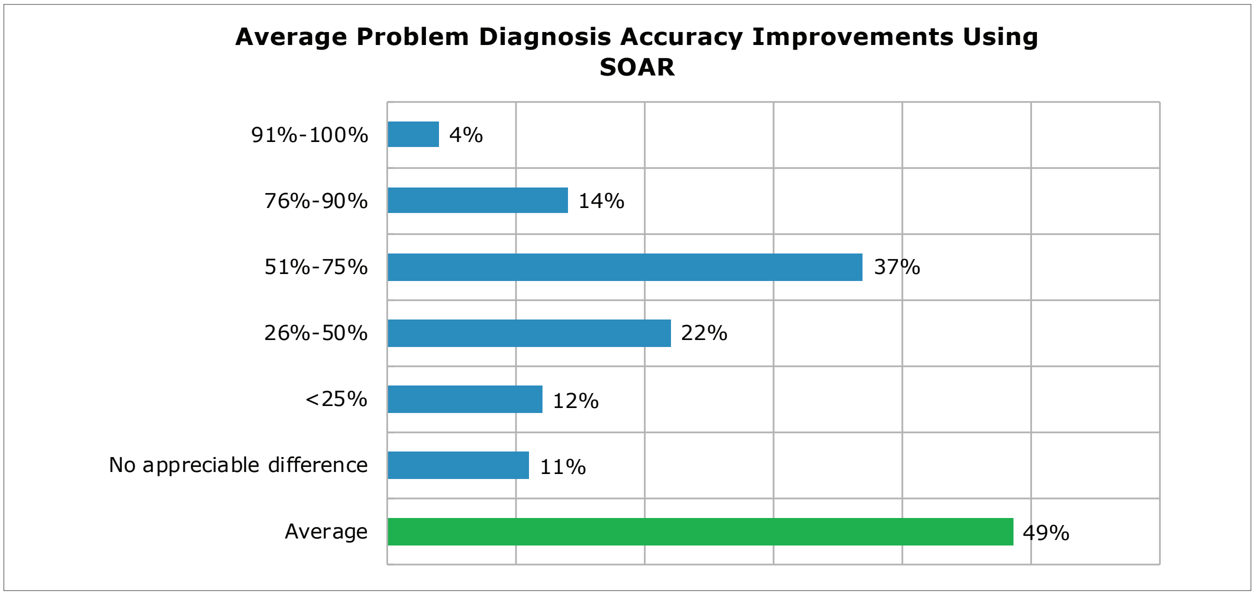
Infrastructure government and technology services and providers saw the most gains in the 25% to 50% improvement range, while finance/banking/insurance and manufacturing saw most of their gains in the 51%-75% improvement.



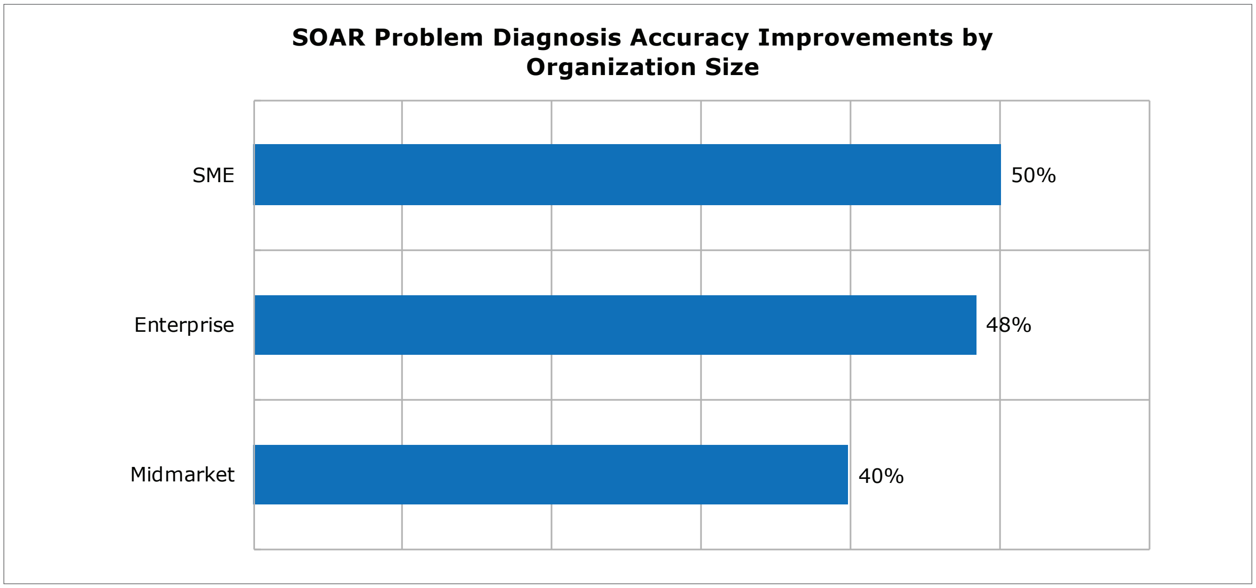
Problem Diagnosis Accuracy Improvements

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[2] 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.



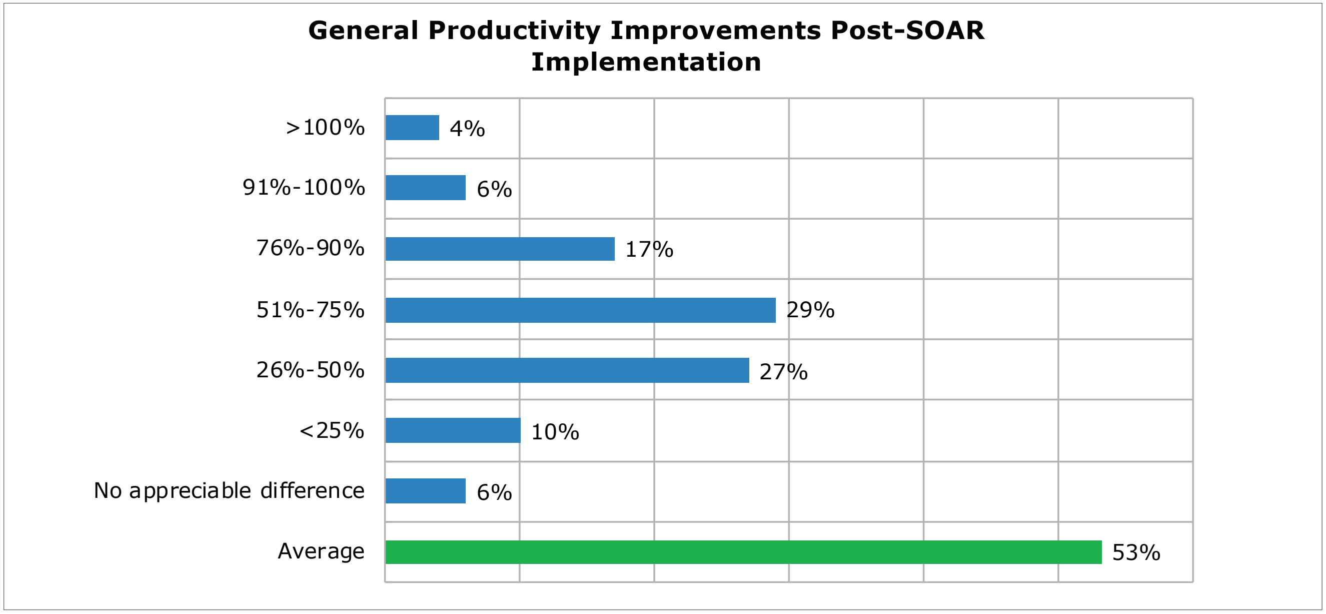
In a breakout by organizational size, SMEs identified the largest diagnosis accuracy improvements (50%). Even at the low end, midmarkets improved by 40%.



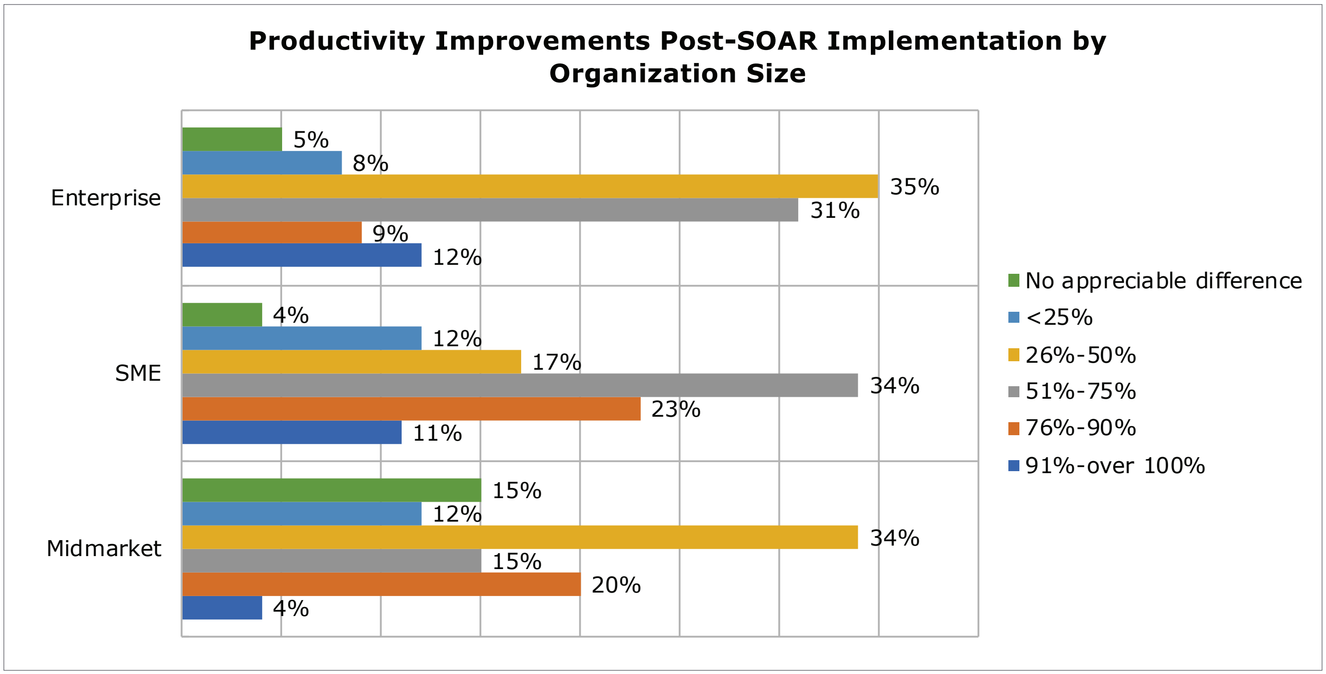
2 Ibid

Productivity Improvements

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

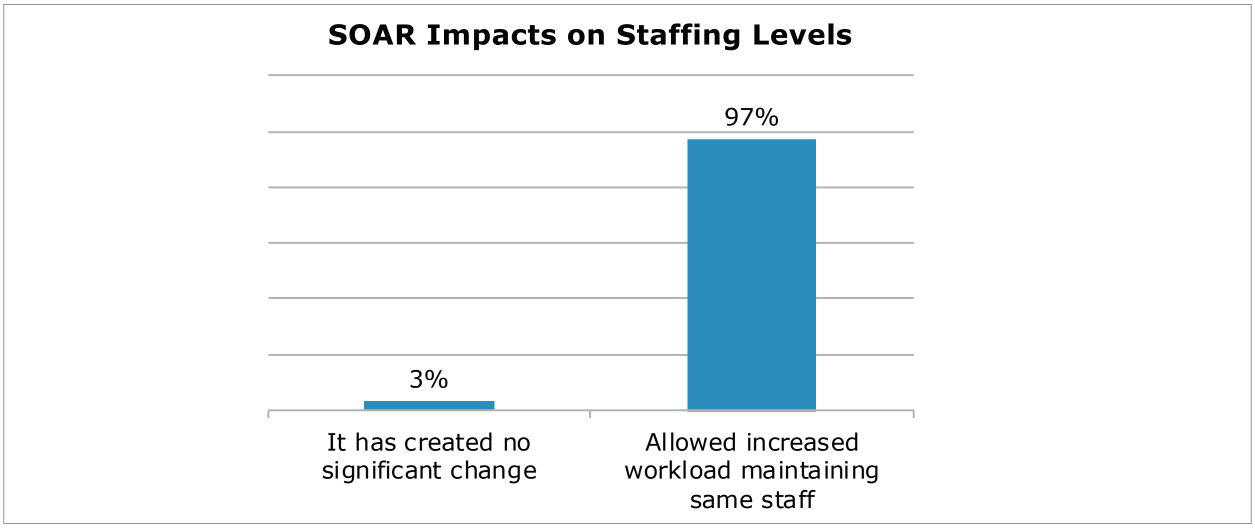


Segmented by organization size, 23% of the SME group saw a 76% to 90% productivity improvement and 12% of Enterprises saw 91% to over 100% productivity improvements.

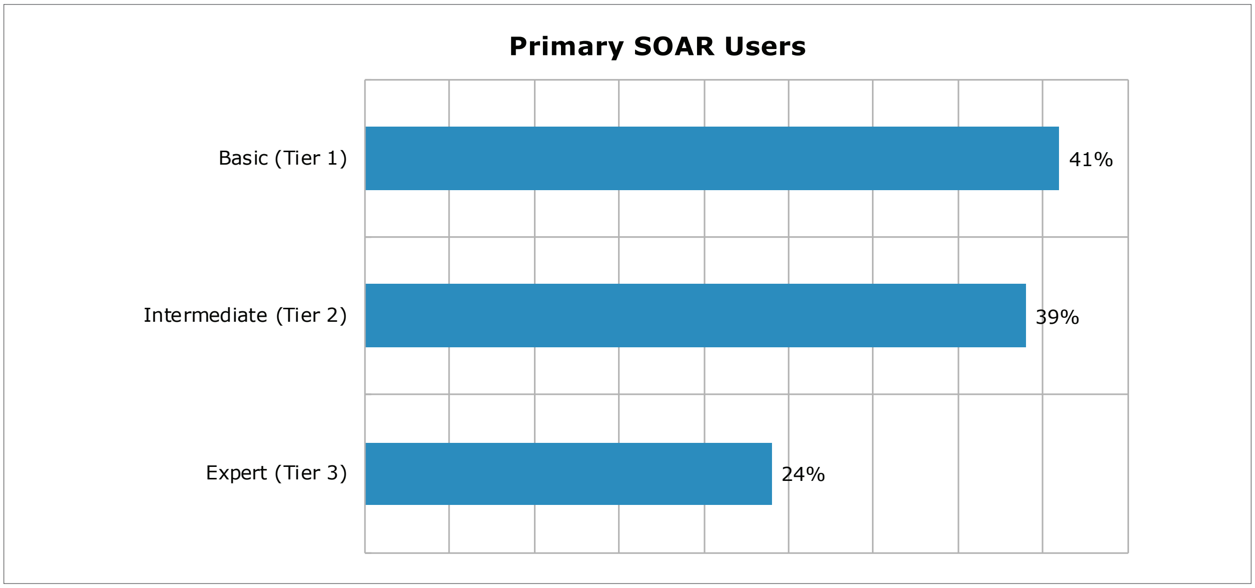


SOAR and Staffing

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.

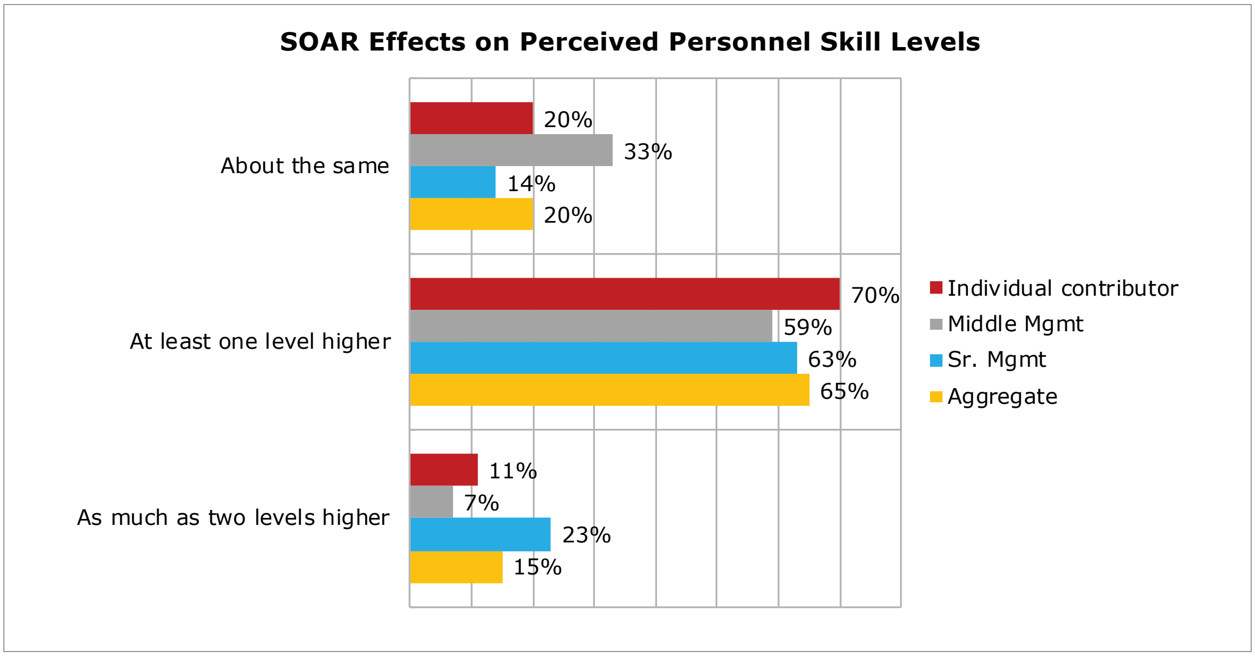


EMA asked respondents, when organizations purchase SOAR, what level of technical skill or performance are they aiming at using it? Is it meant as a frontline augmentation to give the initial trouble receivers basic information, or is it meant to be used by a higher skill level for trouble resolution, 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.

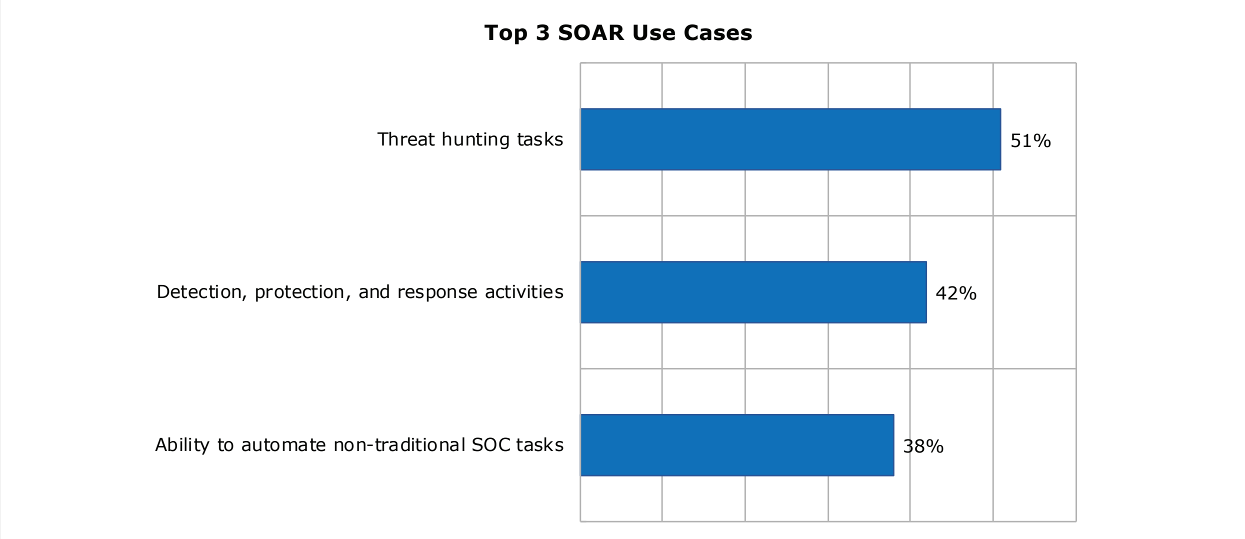


SOAR Investments

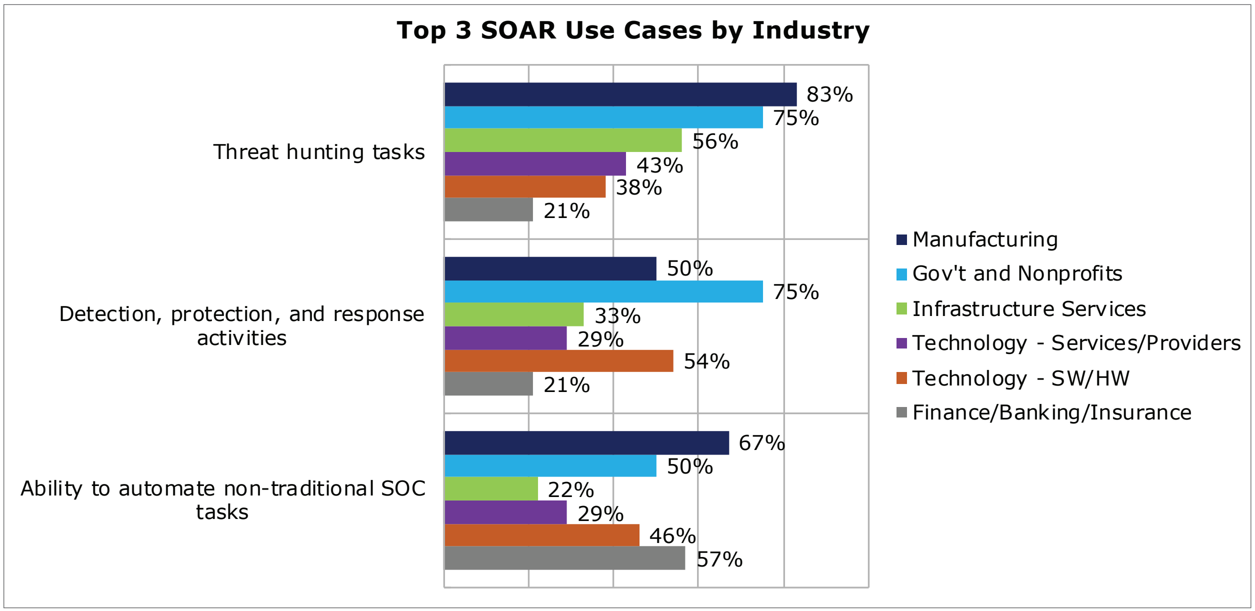
Investing in SOAR tools is not an inexpensive proposition. However, it shows significant opportunity for security operations improvement. It is not a silver bullet. Getting it up and operational to the point it returns value and ROI takes work and resources. Following, EMA points out the most valuable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

Use Cases and Integrations for SOAR

While threat hunting data enrichment only scored in the top 10 use cases for SOAR, threat hunting tasks scored first for 51% of respondents. The most interesting item was that the third-highest rank was the ability to automate non-traditional SOC activities. It's good to know organizations are thinking outside the box to expand value in as many areas as possible.



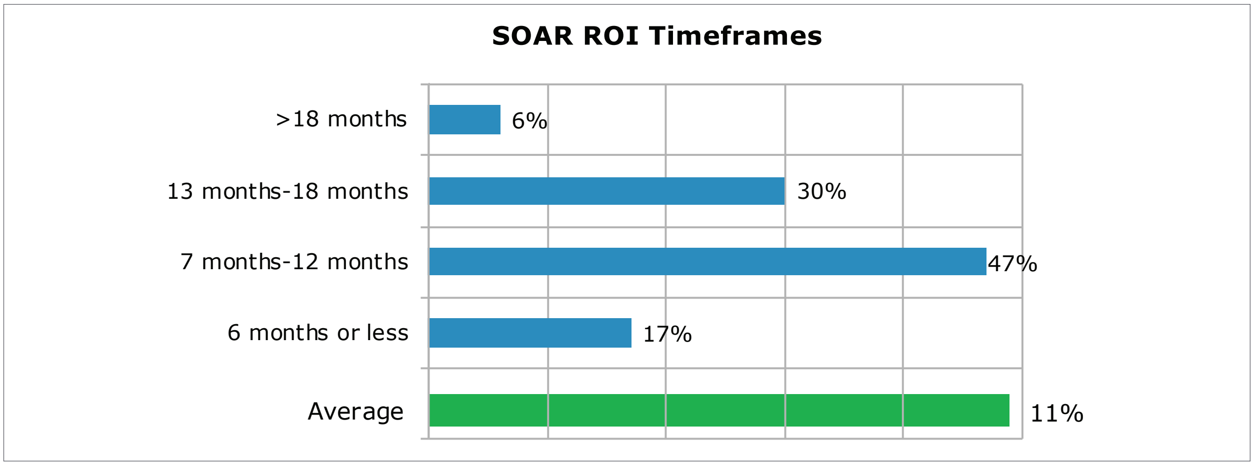
When dissecting the data by industry, there were some variations. Eighty-three percent of manufacturing organizations focus on threat hunting, while only 21% of financial organizations do the same. Fifty-seven percent of finance/banking/insurance groups identified focus on automating non-traditional SOC tasks. Fifty-four percent of technology SW/HW providers focused on detection, protection, and response, while government was evenly split between threat hunting and detection, protection and response activities.



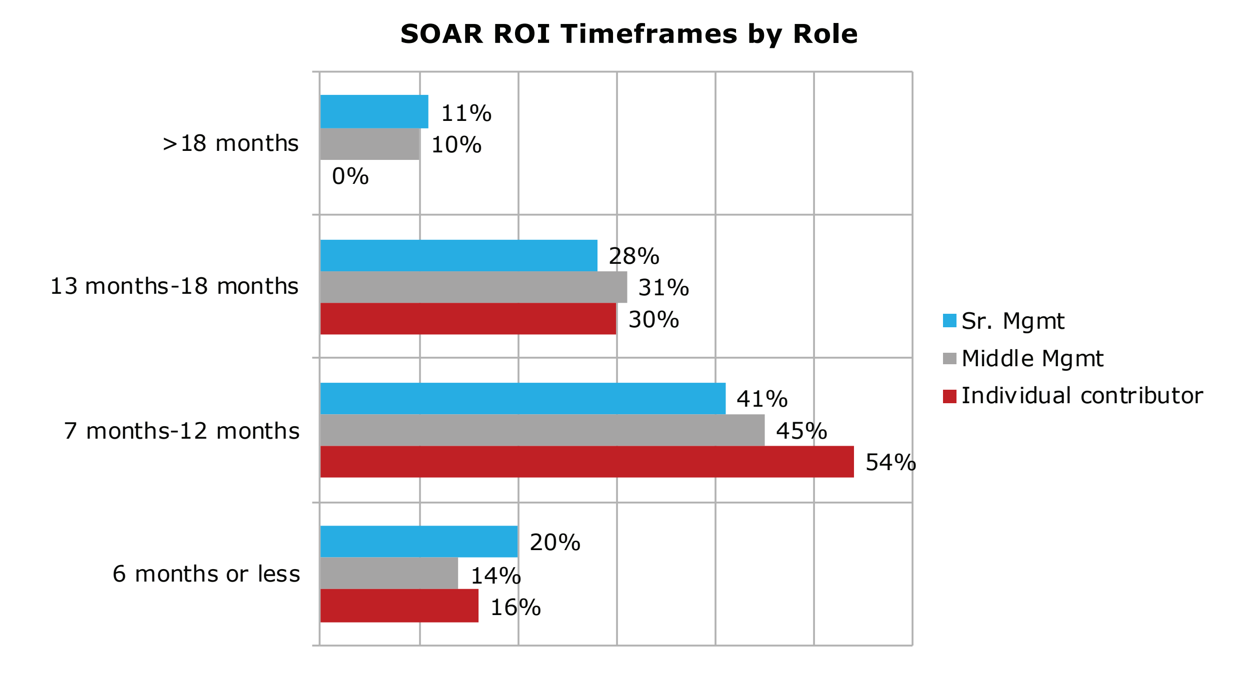
Achieving Return on Investment with SOAR

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.

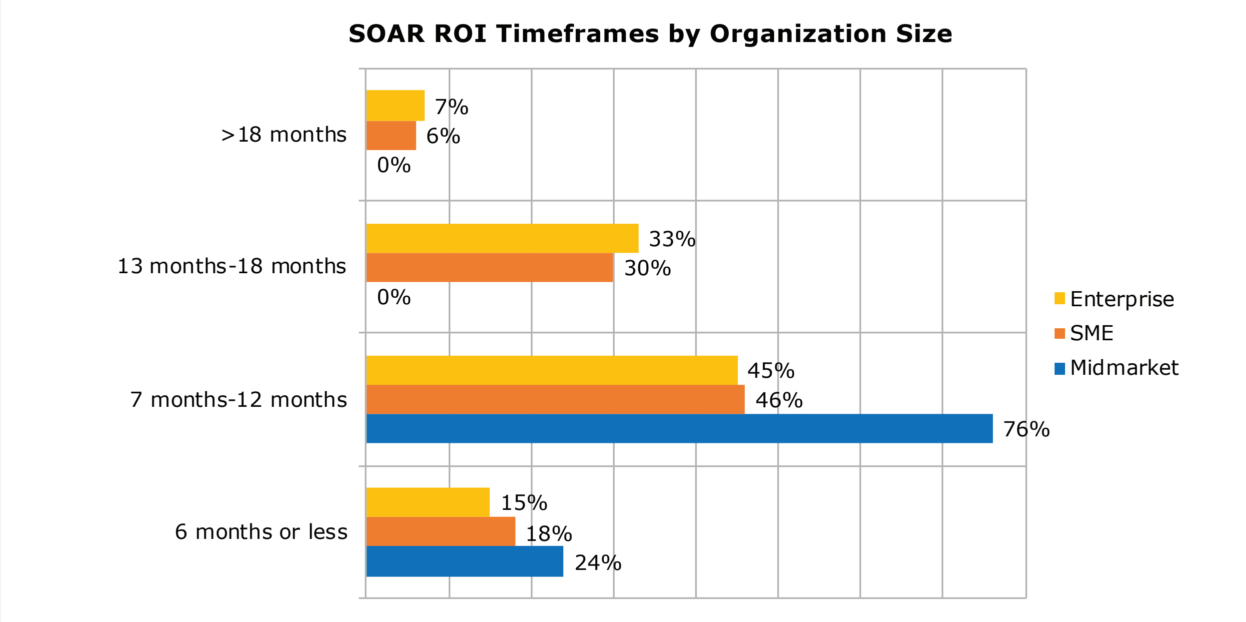
In the next chart, SOAR participants identified their estimated time for ROI. Sixty-four percent indicated ROI was achieved for them in 12 months or less with an average of 11 months. This is within the minimums most organizations expect.



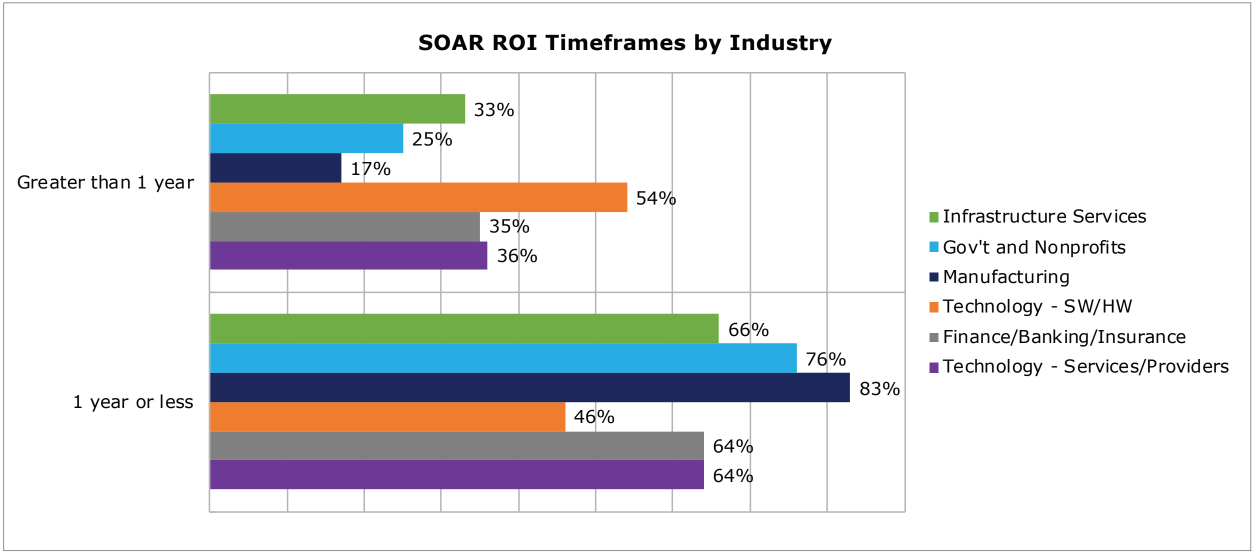
Interestingly, senior management was most conservative in their estimates. Twenty percent indicated they thought ROI was achieved in six months or less and none of the individual contributors felt it took longer than 18 months to achieve ROI.



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.



Conclusion

While in-house automations are a necessity and have been much of the operations glue up to this point, SOAR should not be discounted because in-house automation is in place. SOAR can advance, augment, and even displace in-house automations based on the implementation strategy the organization decides to follow.

SOAR solutions and platforms, whether pure play or functional within other platforms, deliver productivity, efficiency, value, and ROI in a number of ways. None of the respondents in the survey indicated that they had not received value and benefit from their investment.

SOAR does require a significant time investment to fully realize its potential. Its flexibility is its strength and its weakness. Solution providers have out-of-the-box integrations, and most allow administrators to create their own integration for tools that are not yet included. The complexity of that effort varies by vendor.

SOAR keeps increasing in value over time. All of the respondents said that after implementation, they could understand the scope of what their chosen SOAR solution could do for them and they had developed additional automations and orchestrations to implement. Seventy-two percent of the infrastructure services participants said they had identified 10-20 additional automations and orchestrations to implement. Fifty percent of the finance/banking/insurance group said they identified more than 20 additional use cases after implementation.

SOAR may or may not remain a standalone toolset, but in either case, it provides value now and will provide even greater value in the future.

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 or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3898.092519