2021

Cybersecurity INSIDERS

SOAR REPORT

SWIMLANE

INTRODUCTION

The modern IT security team has a lot to handle: Devices around the infrastructure send more alerts than teams can handle, staff burnout leads to trouble retaining talent, and too much time spent on gathering and analyzing information means threat response is too slow and ineffective.

To alleviate this pressure and provide timely and effective threat response, more organizations are adopting security orchestration, automation, and response (SOAR) solutions to automate time-consuming incident response processes.

Specifically, organizations can use SOAR to enhance security operations in three important areas: threat and vulnerability management, incident response, and security operations automation.

The 2021 SOAR Report is based on a comprehensive survey of cybersecurity professionals to uncover the latest trends, use cases, and benefits of SOAR solutions.

Key findings include:

- Virtually all SOAR users find their solution somewhat useful to extremely useful (92%) in improving their organizations' overall security posture. Long term users are most positive in their assessment: 64% of organizations that have been using SOAR for more than 5 years consider their solution extremely useful – double the rate of overall users.
- Most organizations in this survey see significant productivity and efficiency improvements from investing in SOAR. Not surprisingly, the more mature and longer-term users see significantly higher gains, with half of the organizations seeing more than 50% improvement.
- More than half of organizations in this survey report significant benefits of using SOAR that is both quantitative, such as reduced mean time to resolution (70%) or maximizing efficiency of security staff (68%), as well as qualitative, such as optimizing the value and utility of already existing tools (55%). In combination, these benefits can lead to additional improvements, including lower turnover of staff and higher morale.
- Organizations use SOAR for various reasons and use cases, depending on priorities and existing security tools. The most popular use cases include threat intelligence (57%), followed by remediating phishing attacks (56%) and SIEM triage (54%). More and more organizations are looking for automation beyond the traditional security priorities and making good use of what a true automation platform can accomplish.

We want to thank Swimlane for supporting this important research project.

We hope you find this report informative and helpful as you continue your efforts to better manage the growing volume of security alerts by automating time-consuming incident response processes.

Thank you,

Holger Schulze

Holger Schulze

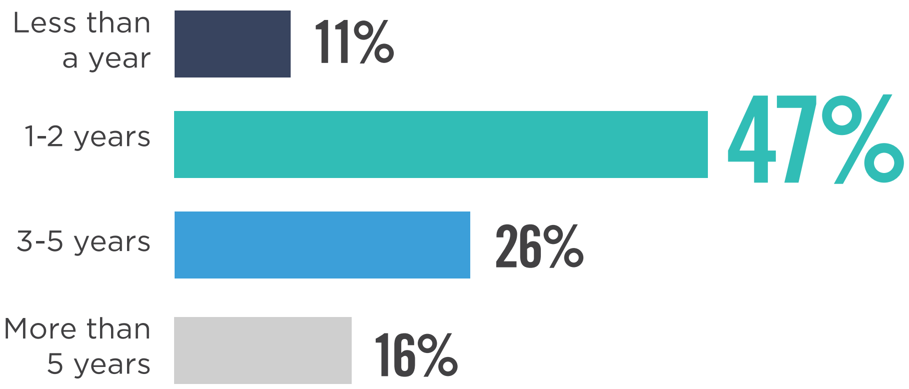
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

SOAR MATURITY

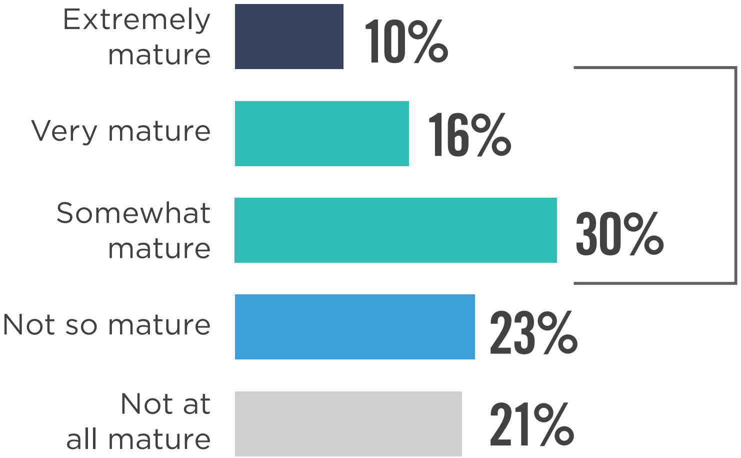
Most organizations in our survey have been using SOAR for between one and two years (47%). Forty-six percent of organizations have been using SOAR for more than 3 years. Only 11% have been using security orchestration, automation and response solutions for less than one year.

How long have you been using your current SOAR solution(s)?



The levels of SOAR maturity are fairly evenly distributed across organizations. Most frequently, organizations consider themselves somewhat mature (30%) in their use of security orchestration, automation and response solutions. Twenty-five percent see themselves as very mature or extremely mature. In contrast, 79% of long-term SOAR users (5+ years) describe themselves as very mature to extremely mature.

How would you describe your organization's maturity in Security Orchestration, Automation and Response (SOAR)?



46%

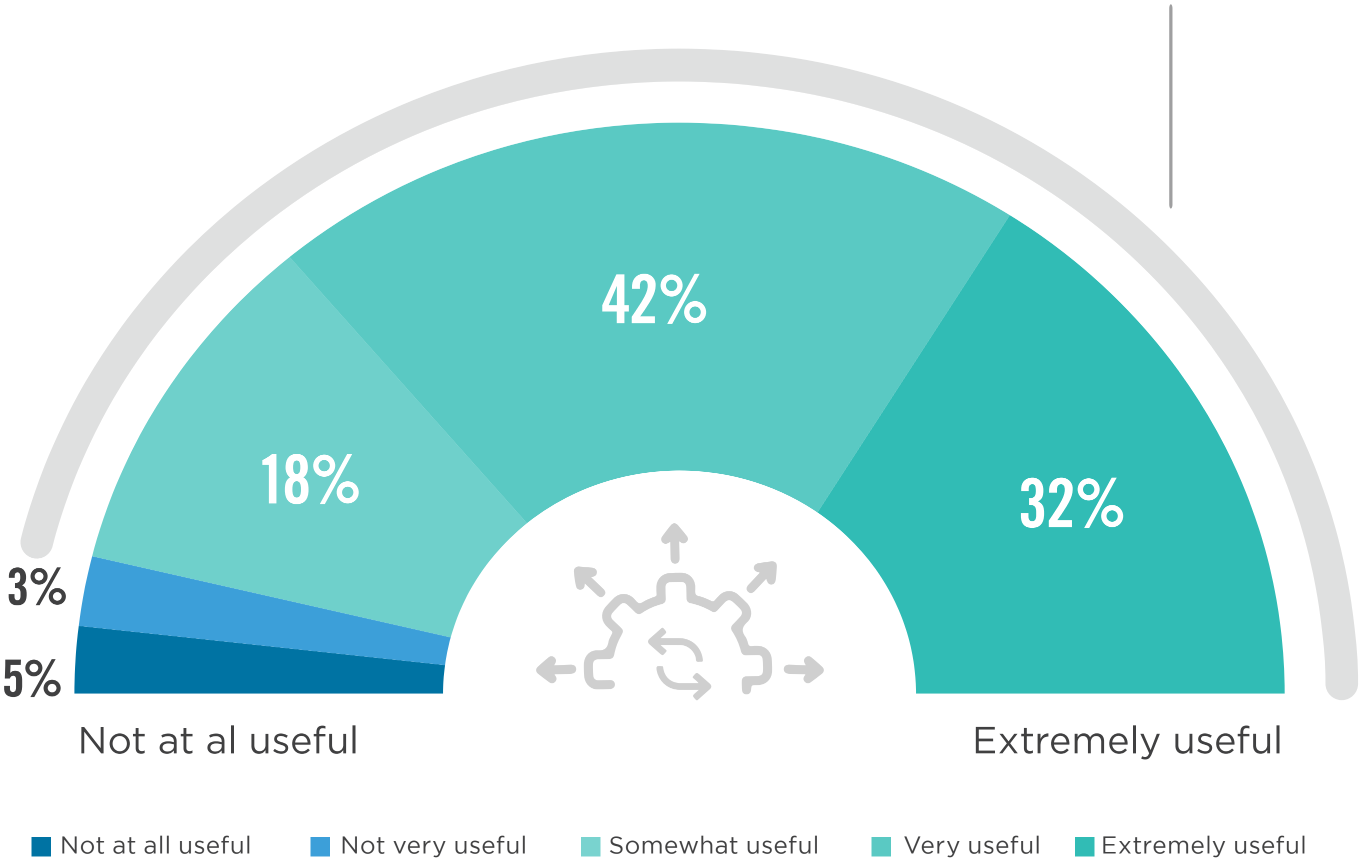
Of organizations consider themselves somewhat mature or very mature in their use of SOAR.

EFFECTIVENESS OF SOAR

On average, a majority of users find their SOAR solution very useful (42%) to extremely useful (32%) in improving their organizations' overall security posture. Long term users are overwhelmingly positive in their assessment: 64% of organizations that have been using SOAR for more than 5 years consider their solution extremely useful – double the rate of overall users.

How useful has security orchestration, automation and response (SOAR) been to improving your organization's overall security posture?

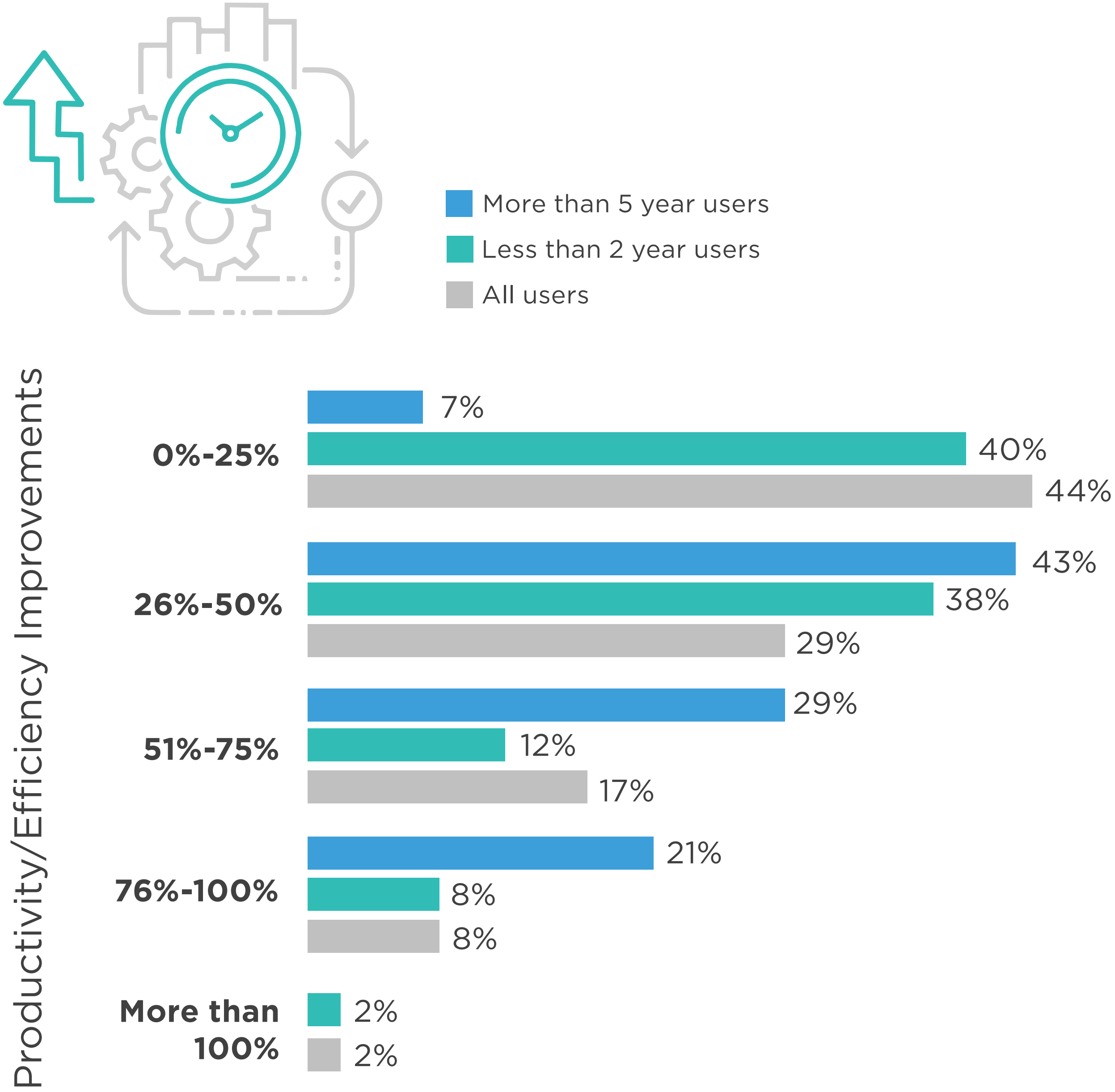
92% Of organizations think SOAR is somewhat to extremely useful.



RETURN ON SOAR

Most organizations in our survey see productivity and efficiency improvements from using SOAR. Organizations can realize significant productivity gains from implementing SOAR and dramatically improve efficiencies by adding orchestration and automation and reducing manual processes.Not surprisingly, the more mature and longer-term users see significantly higher productivity and efficiency gains, with half of users seeing more than 50% improvement.

What overall productivity and efficiency improvements from using SOAR have you seen in your organization's security operations (on average)?



SOAR BENEFITS

The organizations in this survey report benefits of using SOAR that are both quantitative, such as reduced mean time to resolution (70%) or maximizing efficiency of security staff (68%), as well as qualitative, such as optimizing the value and utility of already existing tools (55%). In combination, these benefits can lead to bigger improvements including lower turnover of staff and higher morale.

▶ What ROI impact do you consider most important to justify investment in SOAR solutions?

70%
Reduce mean time to resolution

68%
Maximize staff efficiency

55%
Optimize value of existing tools

36%
Overall cost savings

Other 8%

INVESTMENT DRIVERS

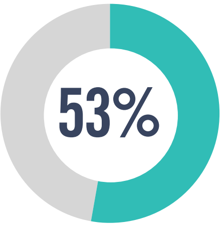
Organizations report a number of drivers that motivate their decision to invest in SOAR solutions. Most frequently mentioned is the need to reduce the time to respond, contain and remediate threats (59%). This is closely followed by the need to improve triage quality and speed (56%) and an increase in the volume of threats facing organizations (55%).

What are the key drivers for your decision to invest in SOAR solution(s)?

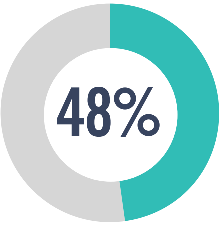
59%
Need to reduce the time to respond, contain and remediate

56%
Need to improve triage quality and speed

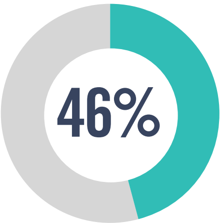
55%
Increase in volume of threats



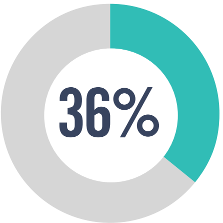
Need for centralized view of threat intelligence



Need to reduce mundane or repetitive routine work for security team



Evolution of threats



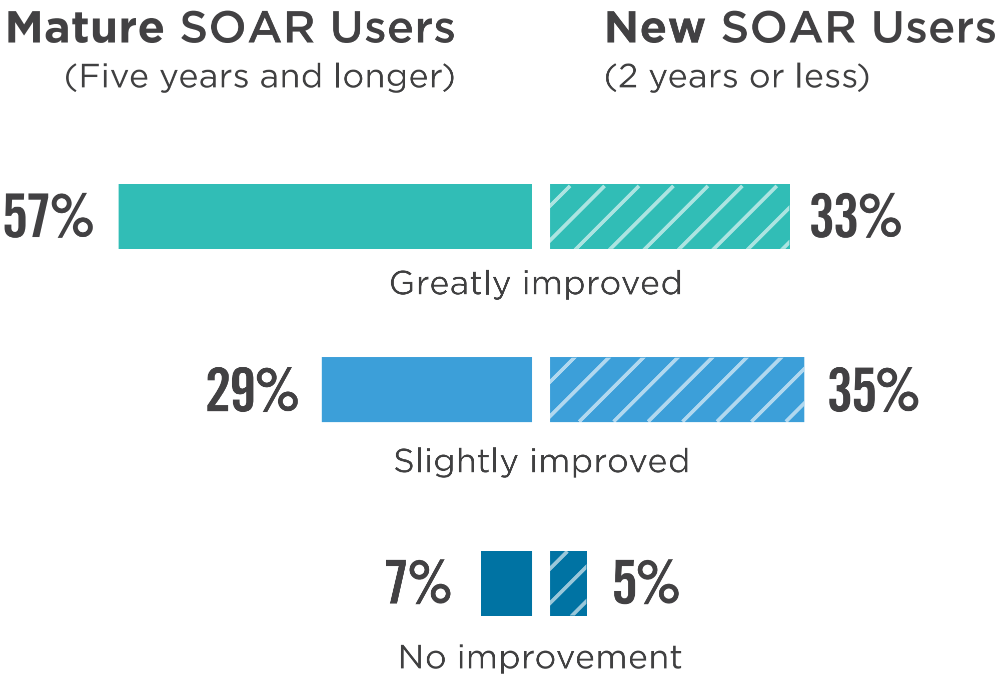
Staff shortages

Other 5%

ALERT TRIAGE QUALITY AND SPEED

A majority of long-term SOAR users (57%) report that the solution has greatly improved the alert triage quality and speed. That's in comparison to 33% among overall SOAR user organizations.

How has using a SOAR solution changed alert/alarm triage quality and speed for your organization?

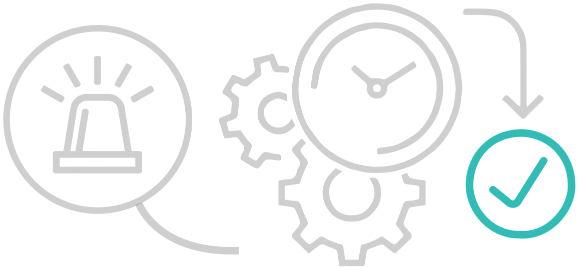


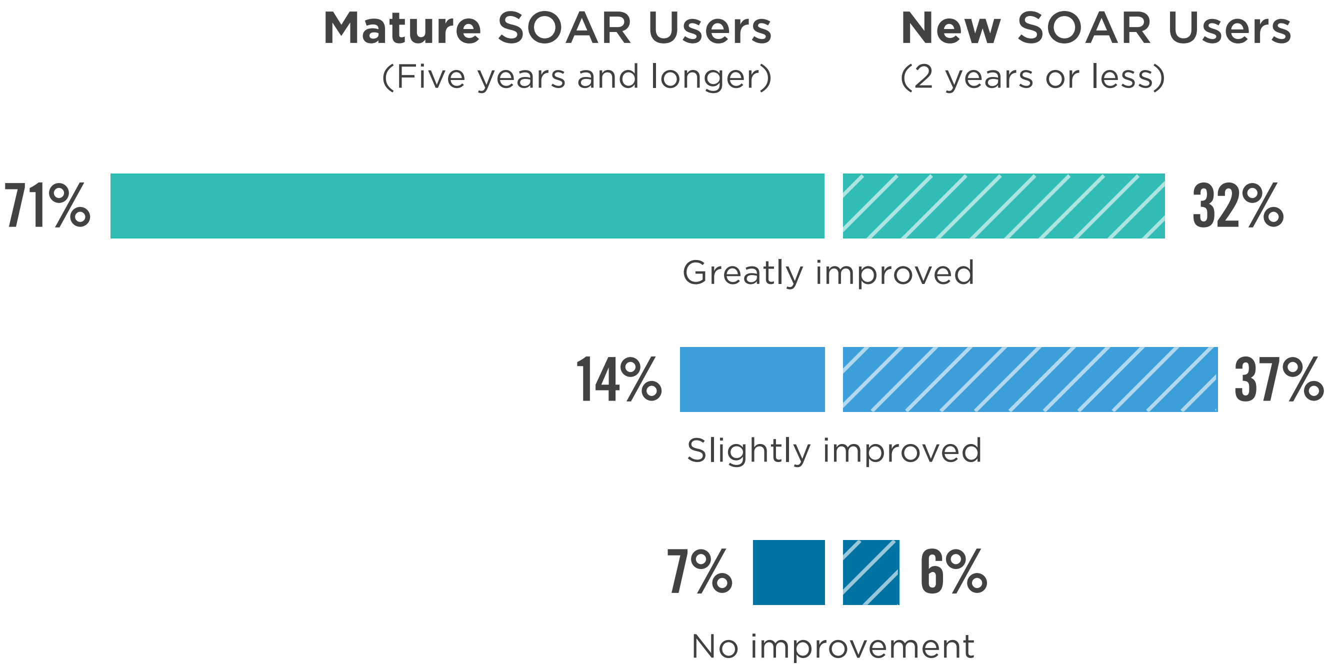
Mature SOAR users not sure 7% | New SOAR users not sure 27%

SPEED OF REMEDIATION

A majority of long-term SOAR users (71%) report that the solution has greatly improved the time to respond, contain and remediate incidents for their organization. That's in comparison to 32% among overall SOAR user organizations.

How has using a SOAR solution reduced the time to respond, contain and remediate incidents for your organization?



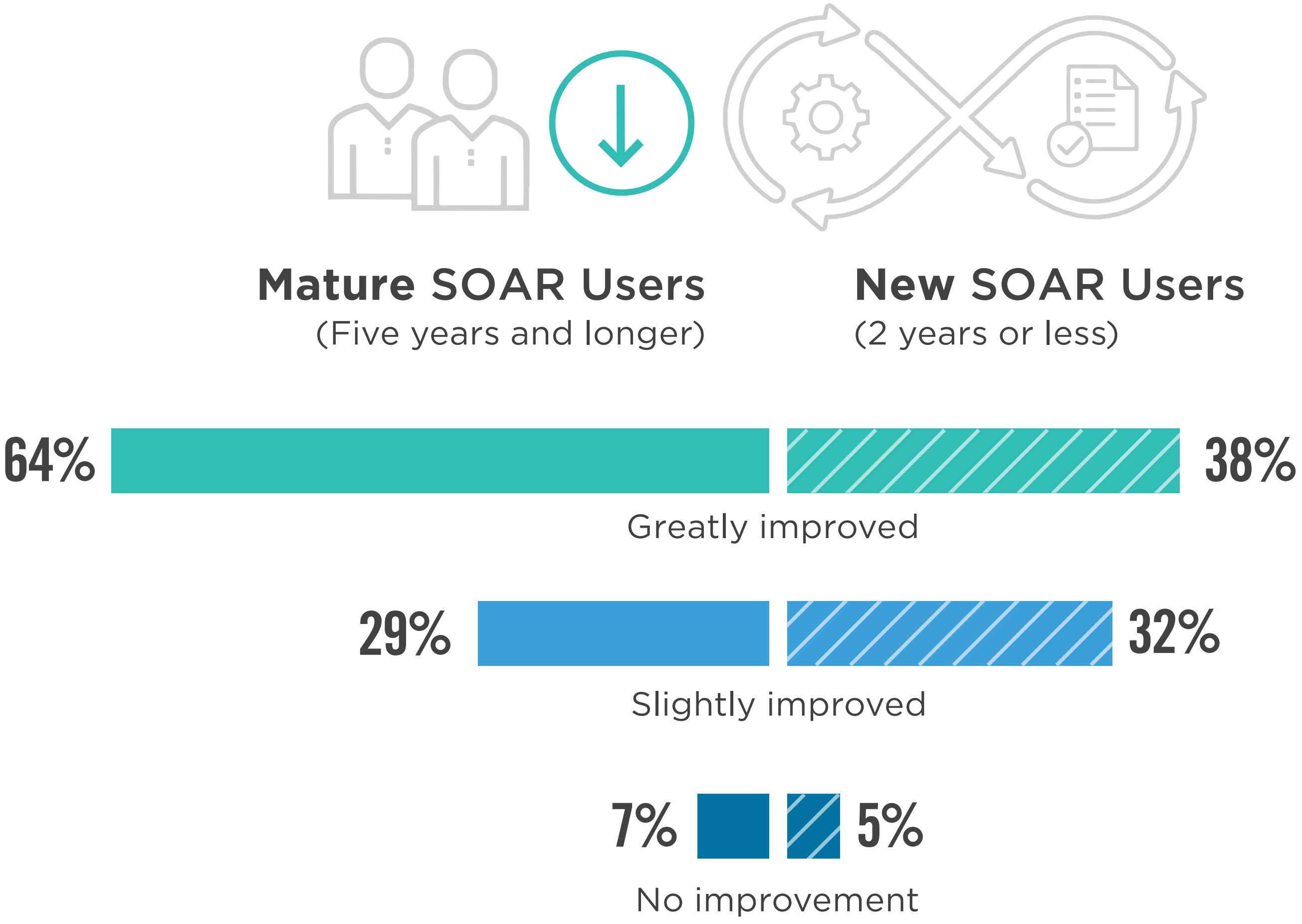


Mature SOAR users not sure 7% | New SOAR users not sure 27%

REDUCTION OF ROUTINE WORK

A majority of long-term SOAR users (64%) report that the solution has greatly reduced mundane and repetitive routine work for security teams. That's in comparison to 38% among overall SOAR user organizations.

How has using a SOAR solution reduced mundane or repetitive routine work for security teams in your organization?



Mature SOAR users not sure 7% | New SOAR users not sure 27%

KEY USE CASES

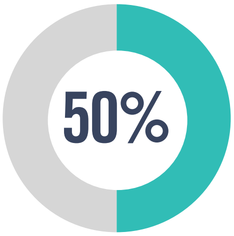
Organizations use SOAR for a variety of reasons and use cases, depending on priorities and existing security tools. The most popular use cases include threat intelligence (57%), followed by remediating phishing attacks (56%) and SIEM triage (54%).

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

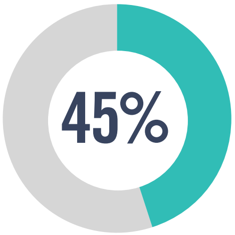
57%
Threat intelligence

56%
Phishing attacks

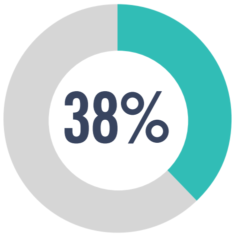
54%
SIEM triage



Threat hunting



Endpoint protection



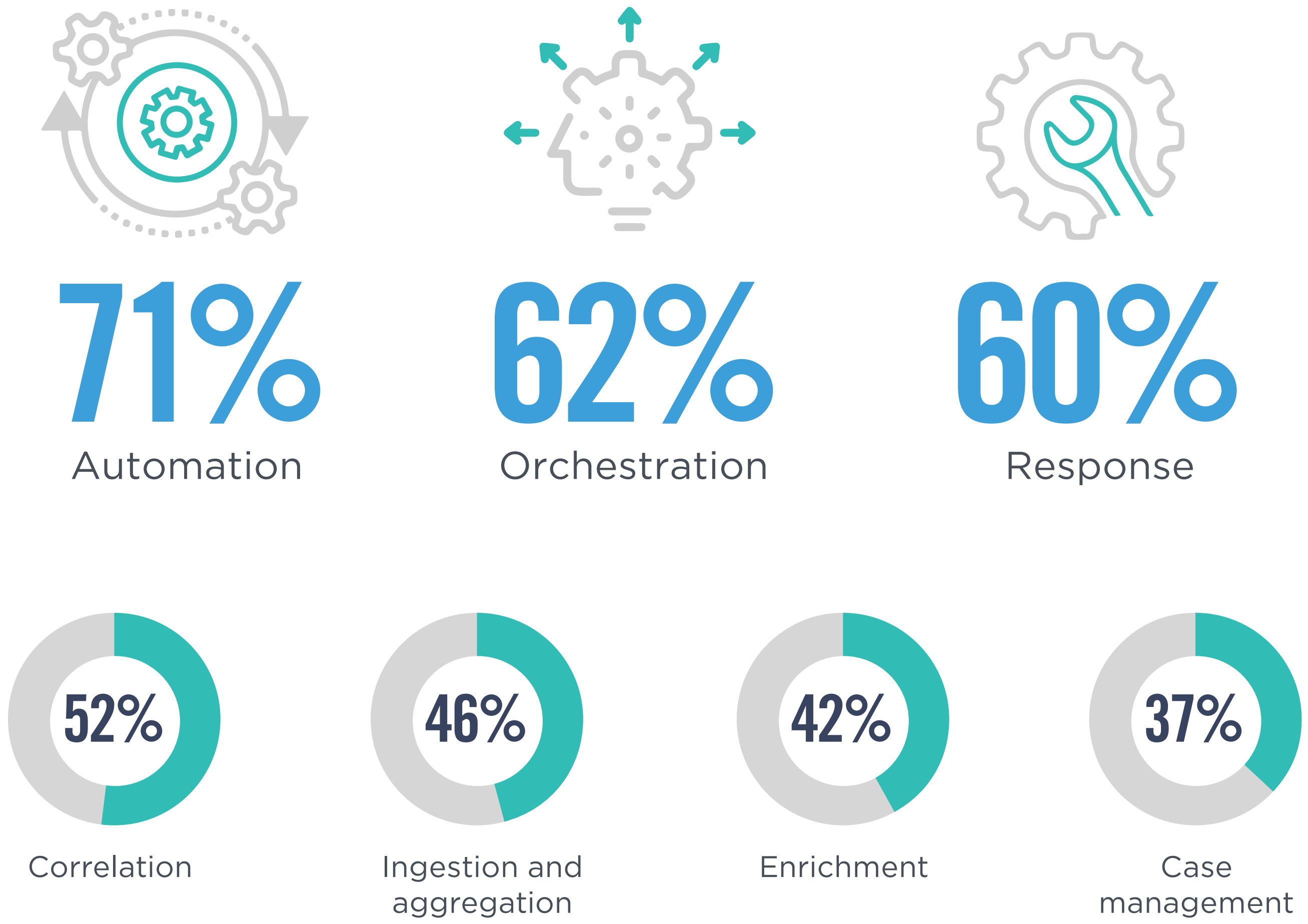
Vulnerability management

Malware analysis 34% | Insider threat detection 33% | Forensic investigation 30% | Identity verification/enforcement 29% | Other 9%

SOAR CAPABILITIES

The most valuable SOAR capability is automation of manual tasks (71%). Especially long-term SOAR users prioritize automation capabilities (92%). This is followed by orchestration of multiple security tools and tasks (62%), and response capabilities (60%).

▶ **What general SOAR capabilities are most valuable to your organization?**



SOAR INTEGRATION

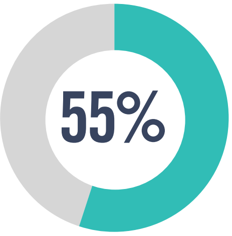
The types of tools organizations integrate with their SOAR platforms depend greatly on the use cases they prioritize. While virtually any tool can be integrated with SOAR, organizations in our survey prioritize endpoint security (63%) and SIEM and log management (63%), followed by threat intelligence (60%).

What tools are you integrating with your SOAR solution?

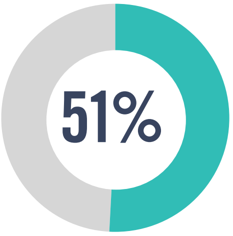
63% Endpoint security

63% SIEM & log management

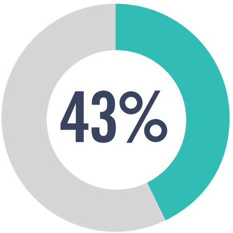
60% Threat intelligence



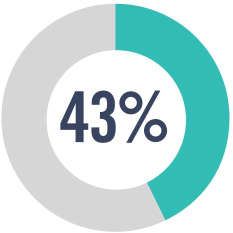
Firewall



Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)



Ticketing



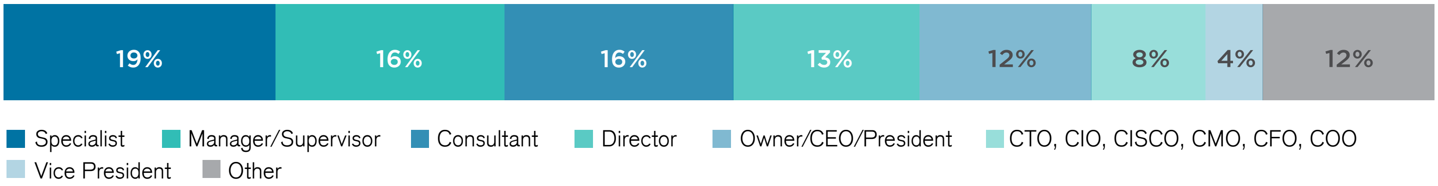
Vulnerability and risk management

Identity and Access Management (AIM) 38% | Forensics and malware analysis 35% | Other 8%

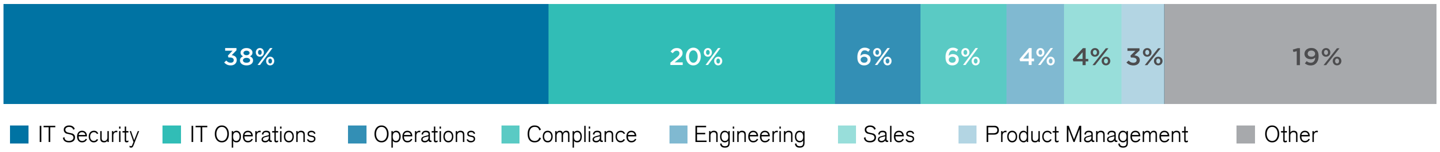
METHODOLOGY & DEMOGRAPHICS

The 2021 SOAR Report is based on the results of a comprehensive online survey of xxx cybersecurity professionals, conducted in April 2021 to gain deep insight into the latest trends, key challenges and solutions for security orchestration, automation and response. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

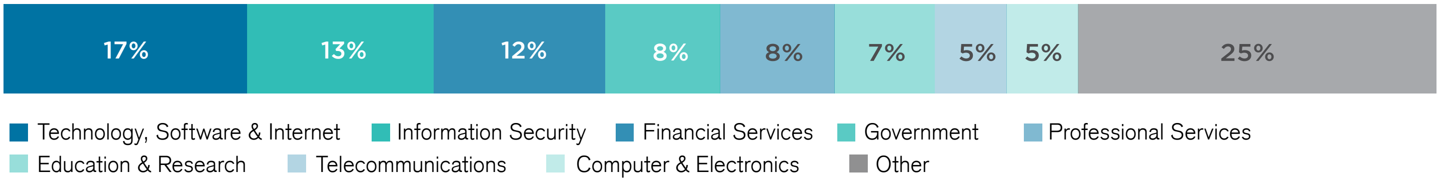
CAREER LEVEL



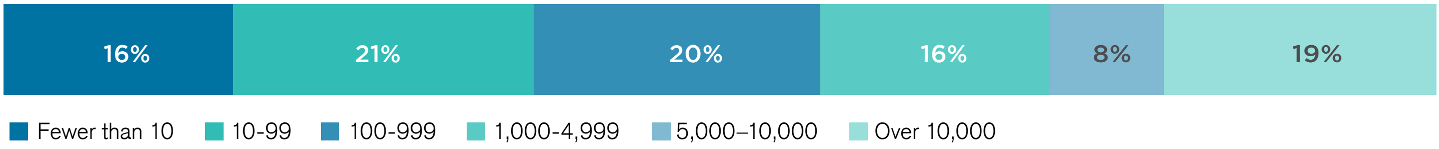
DEPARTMENT



INDUSTRY



COMPANY SIZE



SWIMLANE

Swimlane is at the forefront of the growing market of security orchestration, automation and response (SOAR) solutions and was founded to deliver scalable and flexible security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages. Swimlane's solution helps organizations address all security operations needs, including prioritizing alerts, orchestrating tools and automating the remediation of threats—improving performance across the entire organization. Swimlane is headquartered in Denver, Colo. with operations throughout North America, Central America, Europe, the Middle East and Australia.

For more information, visit

www.Swimlane.com