MORNING CONSULT | IBM

Global Security Operations Center Study Results

MARCH 2023

Methodology

This study was conducted between February 27 – March 18, 2023, and surveyed 1,000 SOC Team Members. The sample is comprised of 100 respondents from each of the following 10 countries: Australia, Brazil, Canada, France, Germany, India, Japan, Spain, UK, and US. To qualify for the survey, respondents currently had to be on a SOC team and also employed at an organization with more than 1,000 full-time employees. Respondents could have the following roles on their SOC Team:

- SOC manager
- Security analyst
- Security operations center engineer / architect
- Subject-matter expert (network, threat intel, compliance, malware, endpoint)
- Threat hunter
- Incident responder

The interviews were conducted online. Results from the full survey have a margin of error of +/- 3 percentage points.

Key Takeaways

1 **Globally, nearly half say that the average time to detect and respond to a security incident has increased over the past 2 years.**

More than 80% say that manual investigation of threats slows down their overall threat response times.

2 **On average, SOC Team Members spend one-third of their typical workday investigating and validating incidents that aren't a real threat.**

3 **More AI and automation in toolsets is the biggest opportunity to improve threat response time across most markets.**

SOC Team Members also say that having a defined incident response strategy is a big opportunity.

4 **A majority of threats SOC Team Members review are low priority / false positives.**

5 **SOC Team Members are only getting to half of the alerts they're supposed to review on a typical workday.**

6 **Among SOC teams that currently leverage automation, only half are currently automating threat hunting and incident enrichment.**

AGENDA

Speed / Response Times

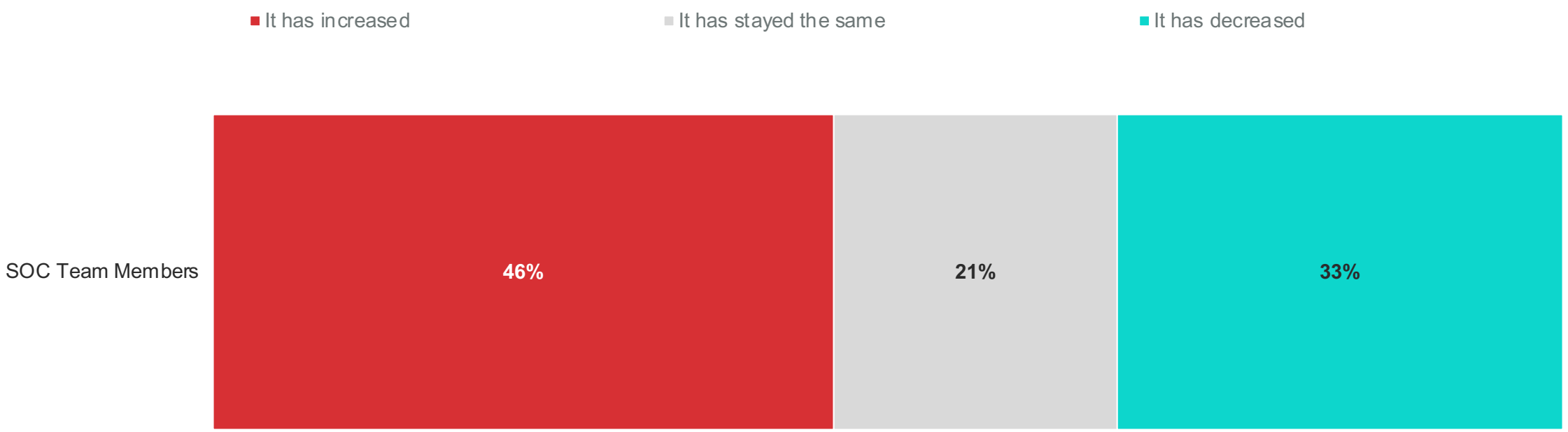
Detection

Automation

SPEED / RESPONSE TIMES

Nearly half (46%) say that the average time to detect and respond to a security incident over the past 2 years has increased.

Over the past 2 years, how would you estimate your average time to detect and respond to a security incident has changed?



SECTION TITLE

On average, SOC Team Members spend one-third of their typical workday investigating/validating incidents that are not a real threat (32%).

How often do you spend time investigating / validating incidents that are not a real threat? Please estimate the percentage of your time in a typical workday that you spend on average investigating incidents that aren't a real threat. **[Showing Average]**

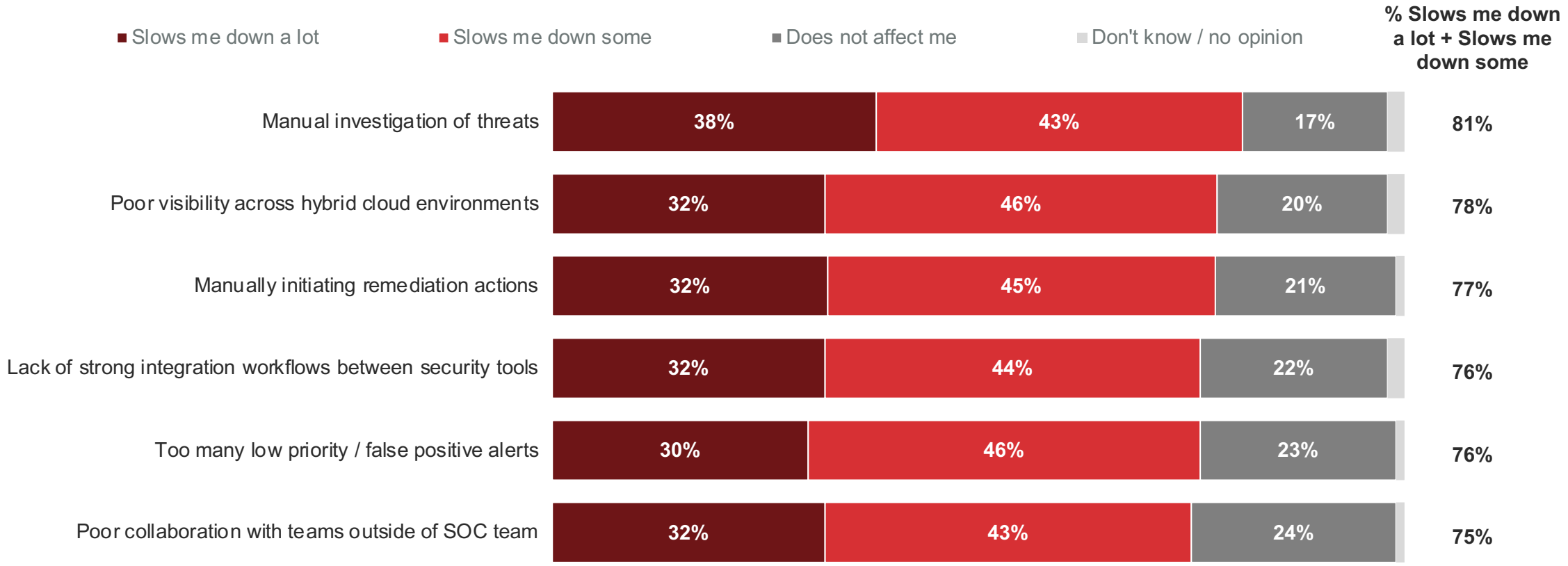
32%

Time in a typical workday global SOC Team Members spend investigating / validating incidents that are not a real threat.

SPEED / RESPONSE TIMES

More than eight-in-ten say that manual investigation of threats slows down their overall threat response times (81%).

To what extent do each of the following slow down your overall threat response time?



SPEED / RESPONSE TIMES

Poor collaboration with teams outside of the SOC team (20%) and a lack of strong integration workflows between security tools (19%) slow down overall threat response the most.

Which of the following would you say slows down your overall threat response time the **most**?

MORNING CONSULT

Among respondents that said more than one item slows down their threat response time

SPEED / RESPONSE TIMES

SOC Team Members across the globe say the use of AI, automated capabilities, and real-time notifications would help improve threat response time. Having a defined incident response strategy and properly trained teams are also opportunities to improve response time.

What do you think is the **biggest** opportunity to improve your threat response time?

The biggest opportunity to improve threat response time is to ensure that all staff are properly trained and knowledgeable in the latest security protocols and best practices. Additionally, investing in the latest security technologies and tools can help to detect and respond to threats more quickly. Finally, having a well-defined incident response. – **SOC Manager, Canada**

Real time threat notifications can help our teams and security staff better understand the threats they face, allowing them to make better choices every day and helping us better understand how to shorten the time to respond to threats. – **Security Analyst, France**

Firewalls and interruption identification frameworks (IDS) can be utilized to recognize and keep malicious traffic from entering the organization data center. They can also detect malicious movement and caution the security group of any dubious action. – **Security Operations Center Engineer / Architect, Germany**

Threat reaction time can be sped up by having a defined incident response strategy in place that includes steps for detection, analysis, containment, eradication, and recovery as well as giving all of our workers the tools they need. – **Threat Hunter, Australia**

I think that the ability to utilize AI when responding to multiple incidents that are occurring at one time would be of real benefit within the SOC role. These could then weed out any erroneous claims and mean a major saving in wasted time. – **SOC Manager, UK**

With the use of generative AI applications, we are able to reduce response times by having a system that can take action if a threat is detected, as well as alert our team if the threat is detected. – **Security Analyst, Australia**

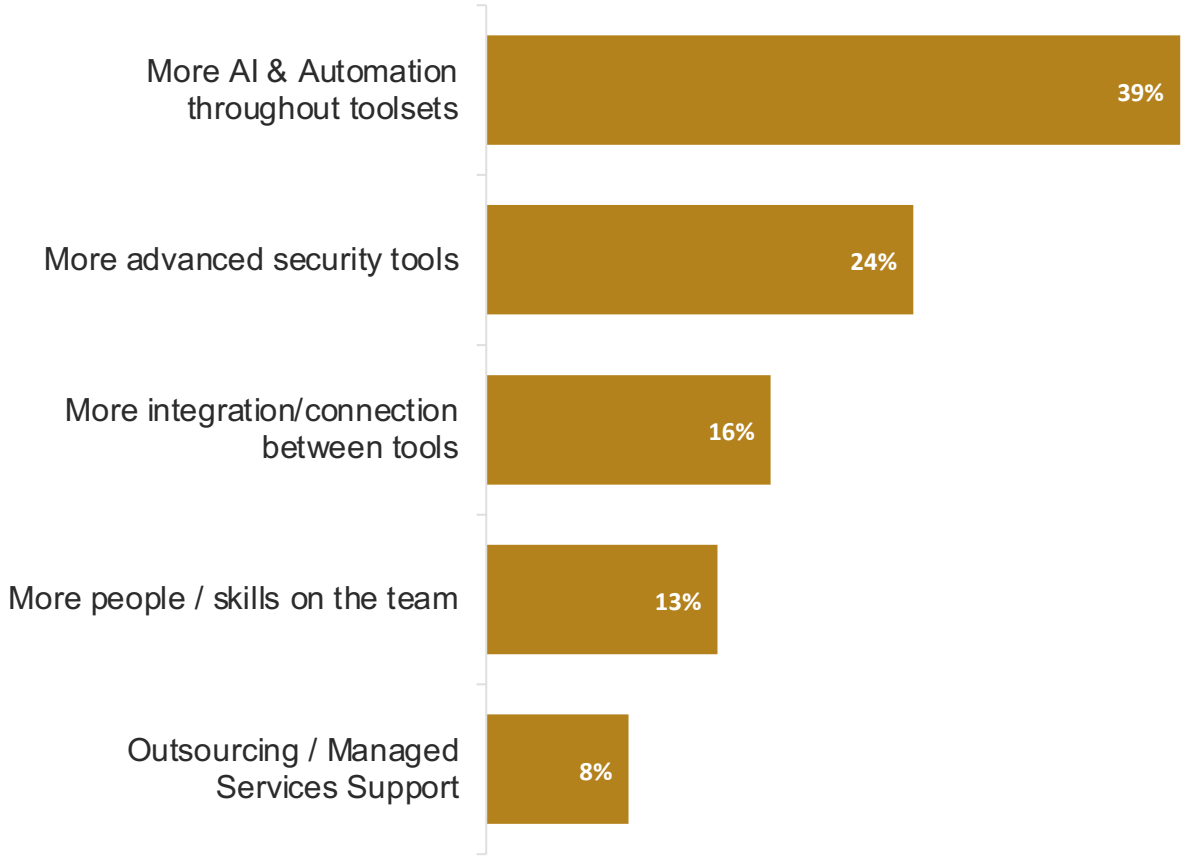
Integrate teams to be able to respond with the greatest possible speed and efficiency in the face of this type of challenges. – **Security Operations Center Engineer / Architect, Spain**

Spending money on threat intelligence platforms and utilizing their offers like automated threat response capabilities that can warn the security team about threats in real time and give them the knowledge they need to act swiftly. – **Security Analyst, Canada**

SPEED / RESPONSE TIMES

More AI and automation throughout toolsets is viewed as a potential solution to poor collaboration across teams, lack of strong integration between tools, and too many low priority / false positive alerts.

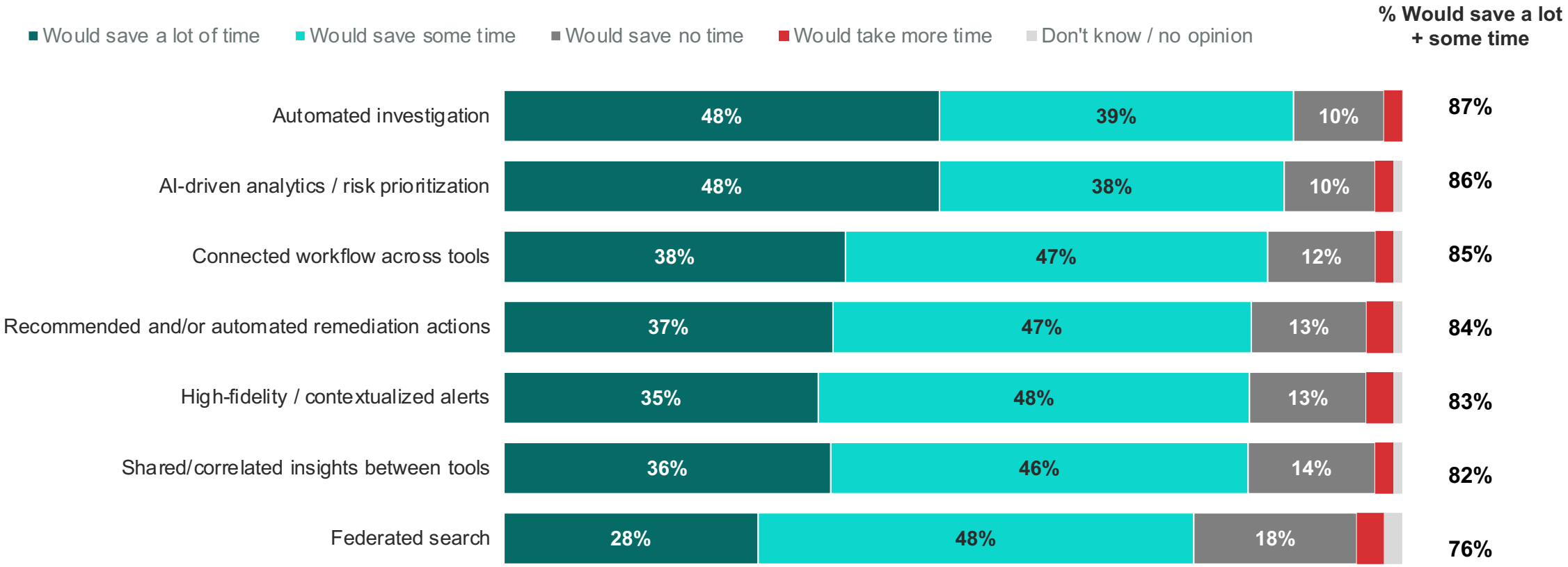
Which of the following do you think is the **biggest** opportunity to improve your threat response time?



SPEED / RESPONSE TIMES

AI-driven analytics / risk prioritization, automated investigation, and recommended and/or automated remediation actions are the top features that SOC Team Members say would save them a lot of time during their threat response.

How much time do you think the following features would save you during your threat response?



AGENDA

Speed / Response Times

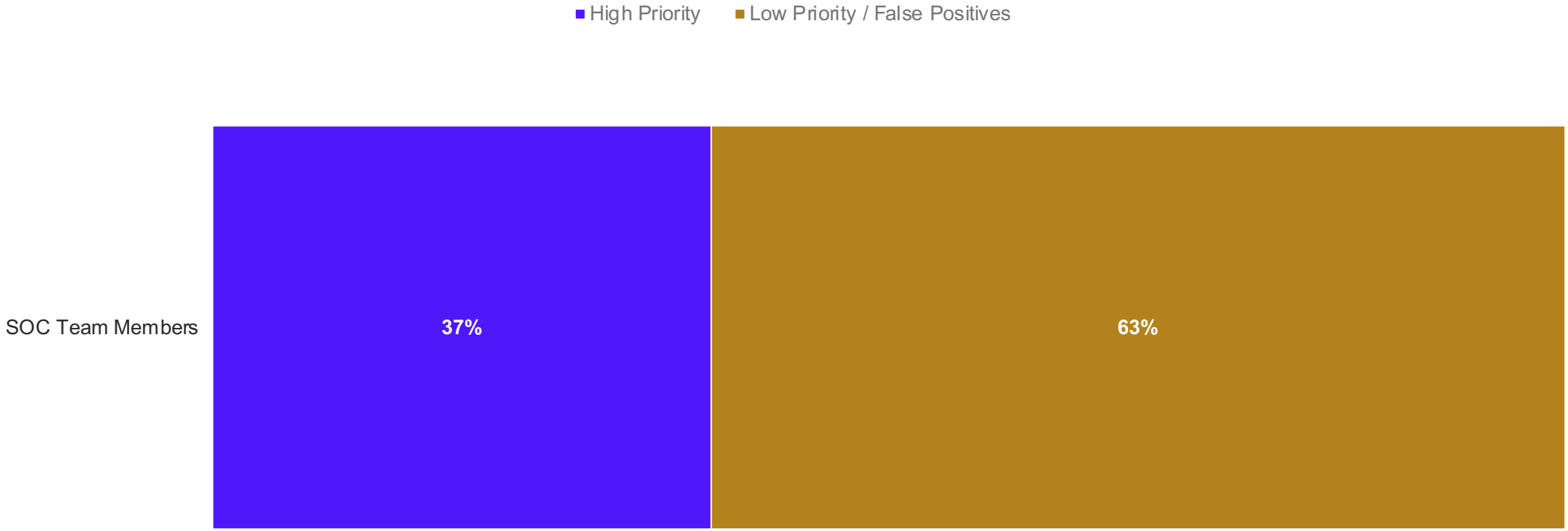
Detection

Automation

DETECTION

Globally, a majority of threats SOC Team Members manually review in a typical workday are low priority / false positives.

Thinking about all the threats you manually review during a typical workday, what percentage of threats fall into high priority and what percentage of threats fall into low priority/false positives? **[Showing Averages]**



DETECTION

SOC Team Members are only getting to half of the alerts that they're supposed to review within a typical workday (49%).

On average, what percentage of alerts that you're supposed to review do you get to within a typical workday? **[Showing Averages]**

49%

Percentage of alerts Global SOC Team Members are supposed to review that they get to within a typical workday.

AGENDA

Speed / Response Times

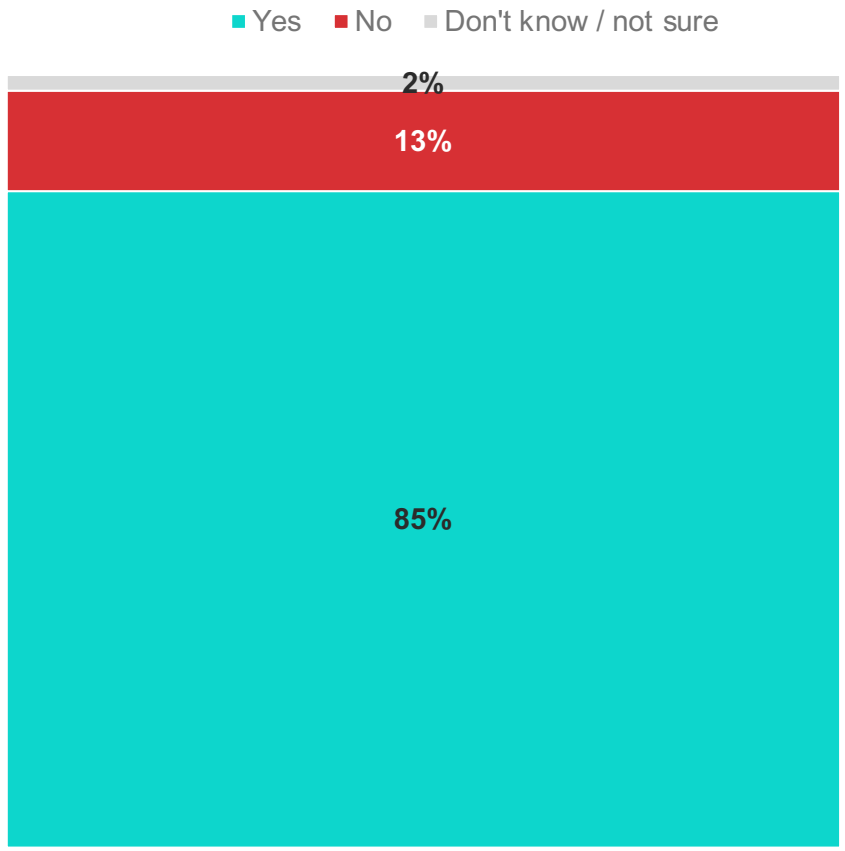
Detection

Automation

AUTOMATION

A majority of surveyed SOC Team Members say there are individuals within their team with skillsets to build automated incident response workflows.

Within your SOC team, are there individuals with skillsets to build automated incident response workflows?



AUTOMATION

Among SOC teams that currently leverage automation, only half are currently automating threat hunting (55%) and incident enrichment (53%).

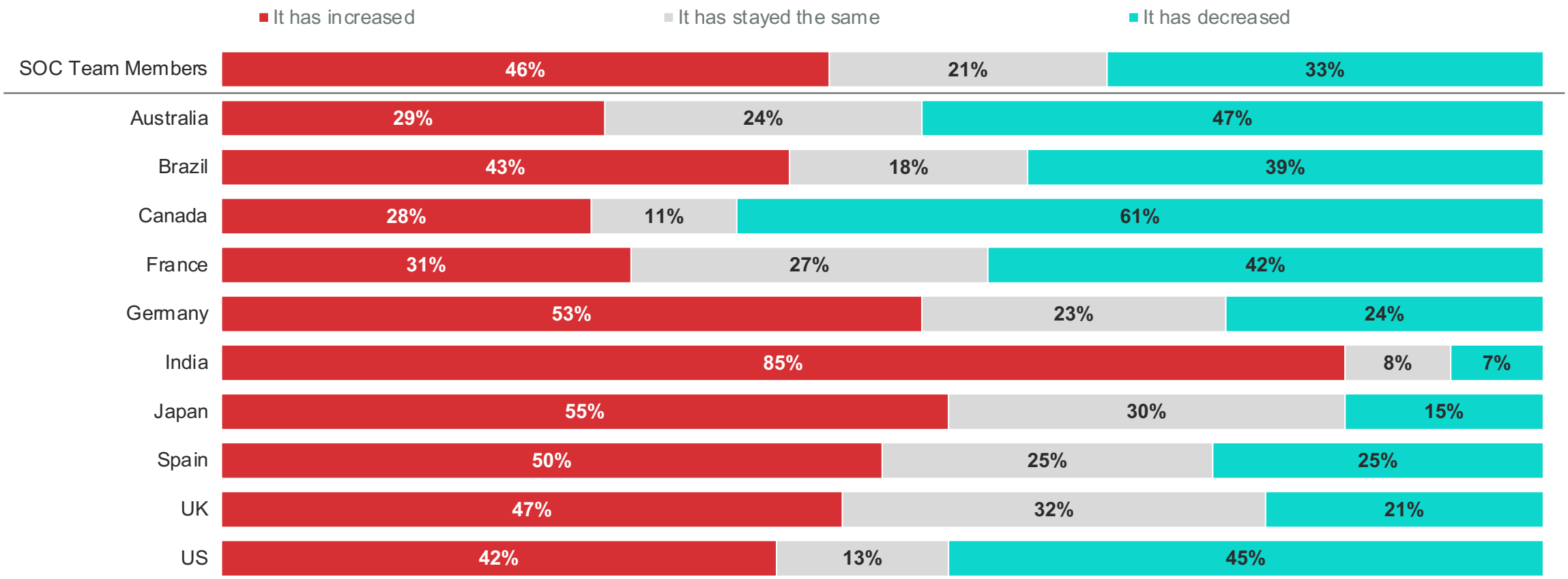
What tasks does your team currently leverage automation for? Please select all that apply.

MORNING CONSULT® Among respondents that say there are individuals on their SOC team with skillsets to build automated incident response workflows

Appendix

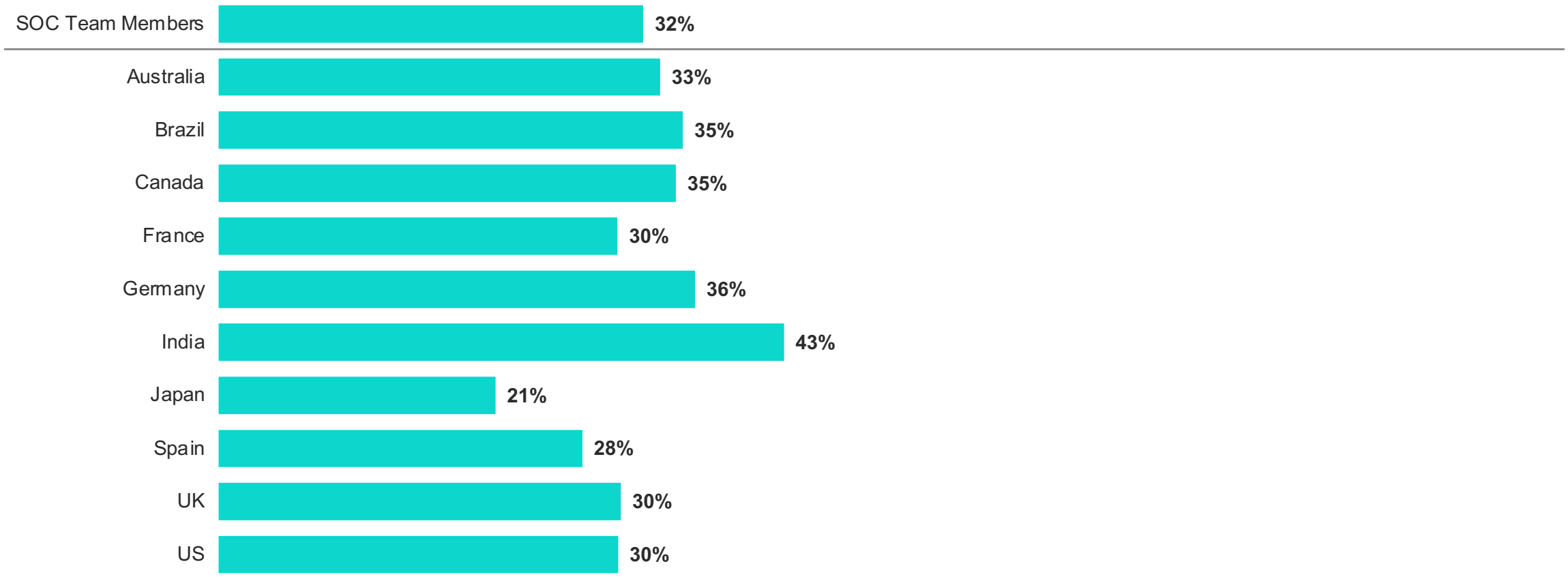
APPENDIX

Over the past 2 years, how would you estimate your average time to detect and respond to a security incident has changed?



APPENDIX

How often do you spend time investigating / validating incidents that are not a real threat? Please estimate the percentage of your time in a typical workday that you spend on average investigating incidents that aren't a real threat.



MORNING CONSULT® Showing Averages

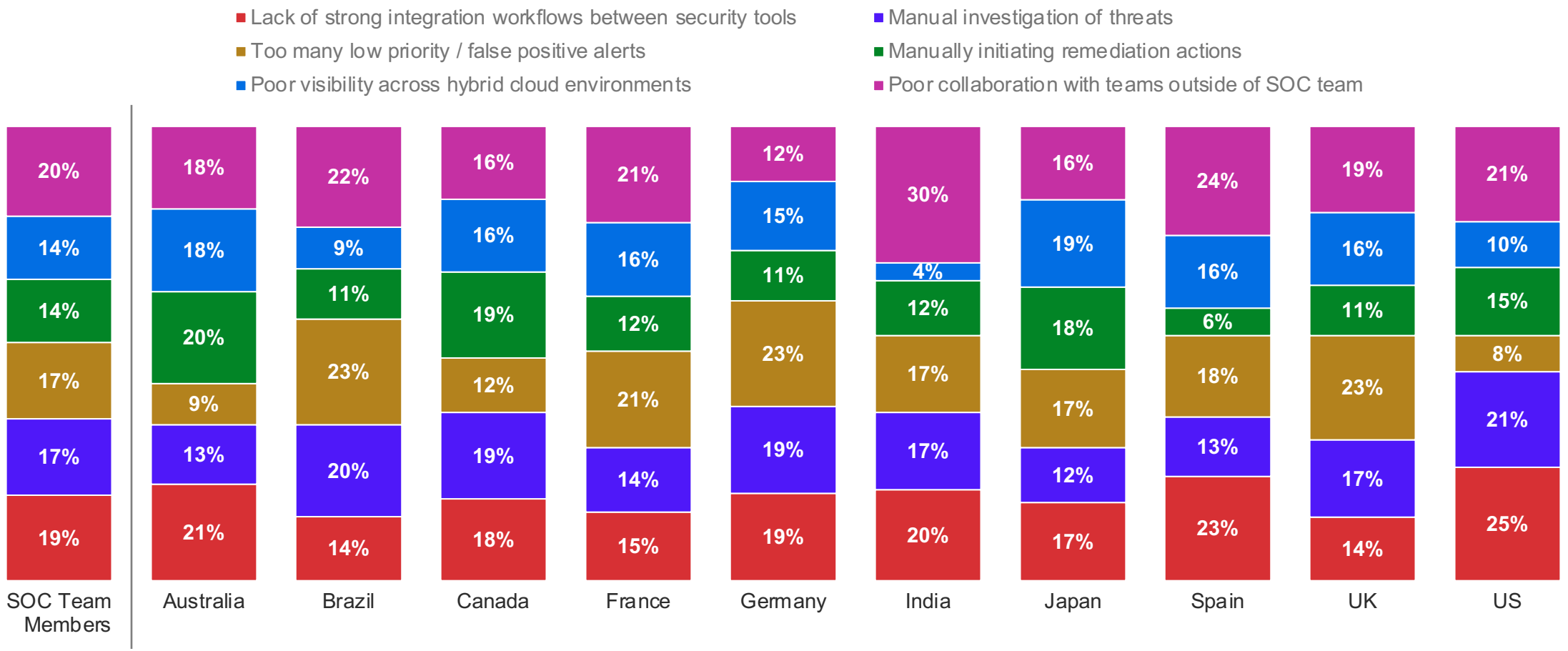
APPENDIX

To what extent do each of the following slow down your overall threat response time?

Market	Manual investigation of threats (81%)	Poor visibility across hybrid cloud environments (78%)	Manually initiating remediation actions (77%)	Lack of strong integration workflows between security tools (76%)	Too many low priority / false positive alerts (76%)	Poor collaboration with teams outside of SOC team (75%)
Australia	91%	91%	87%	78%	74%	84%
Brazil	81%	76%	77%	82%	72%	81%
Canada	89%	88%	82%	75%	70%	72%
France	74%	72%	73%	68%	75%	70%
Germany	85%	76%	76%	70%	80%	69%
India	75%	78%	71%	85%	73%	80%
Japan	71%	68%	67%	64%	65%	69%
Spain	87%	76%	91%	89%	89%	77%
UK	81%	73%	73%	76%	85%	75%
US	77%	82%	79%	73%	74%	72%

APPENDIX

Which of the following would you say slows down your overall threat response time the most?



APPENDIX

Which of the following do you think is the biggest opportunity to improve your threat response time?

	SOC Team Members	Australia	Brazil	Canada	France	Germany	India	Japan	Spain	UK	US
Outsourcing / managed services support	8	11	5	13	13	7	3	7	3	9	10
More advanced security tools	24	18	32	21	15	16	41	33	20	20	24
More integration / connection between tools	16	18	13	17	18	16	9	12	17	22	16
More AI and automation throughout toolsets	39	37	36	38	37	49	37	33	46	32	42
More people / skills on the team	13	16	14	11	16	12	10	15	14	16	8

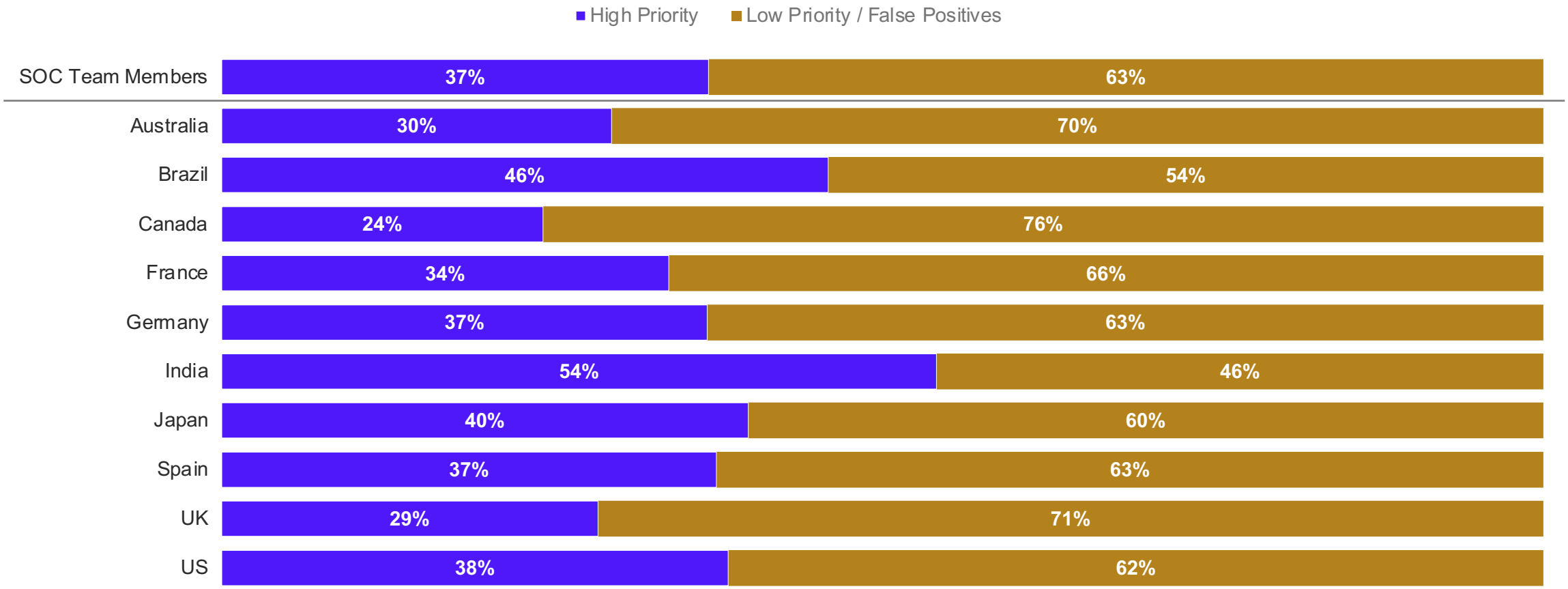
APPENDIX

How much time do you think the following features would save you during your threat response?

Market	High-fidelity / contextualized alerts	AI-driven analytics / risk prioritization	Federated search	Automated investigation	Recommended and/or automated remediation actions	Connected workflow across tools	Shared/correlated insights between tools
SOC Team Members	35%	48%	28%	48%	37%	38%	36%
Australia	37%	45%	37%	49%	40%	34%	39%
Brazil	46%	57%	20%	64%	58%	44%	47%
Canada	42%	46%	37%	48%	40%	39%	40%
France	30%	46%	29%	50%	40%	40%	38%
Germany	37%	56%	15	47%	34%	36%	28%
India	42%	55%	32%	58%	30%	49%	46%
Japan	25%	34%	25%	26%	31%	31%	27%
Spain	30%	50%	33%	46%	36%	32%	34%
UK	23%	39%	20%	46%	18%	31%	27%
US	39%	47%	33%	51%	39%	40%	34%

APPENDIX

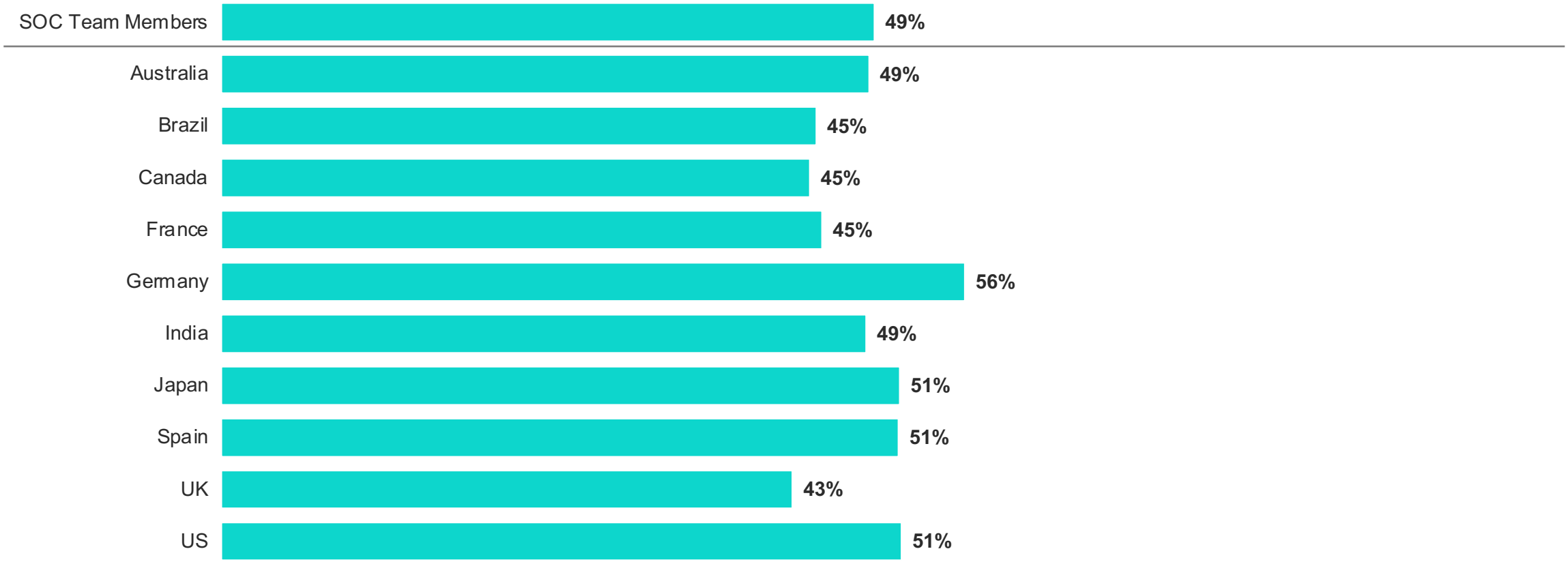
Thinking about all the threats you manually review during a typical workday, what percentage of threats fall into high priority and what percentage of threats fall into low priority/false positives?



MORNING CONSULT® Showing Averages

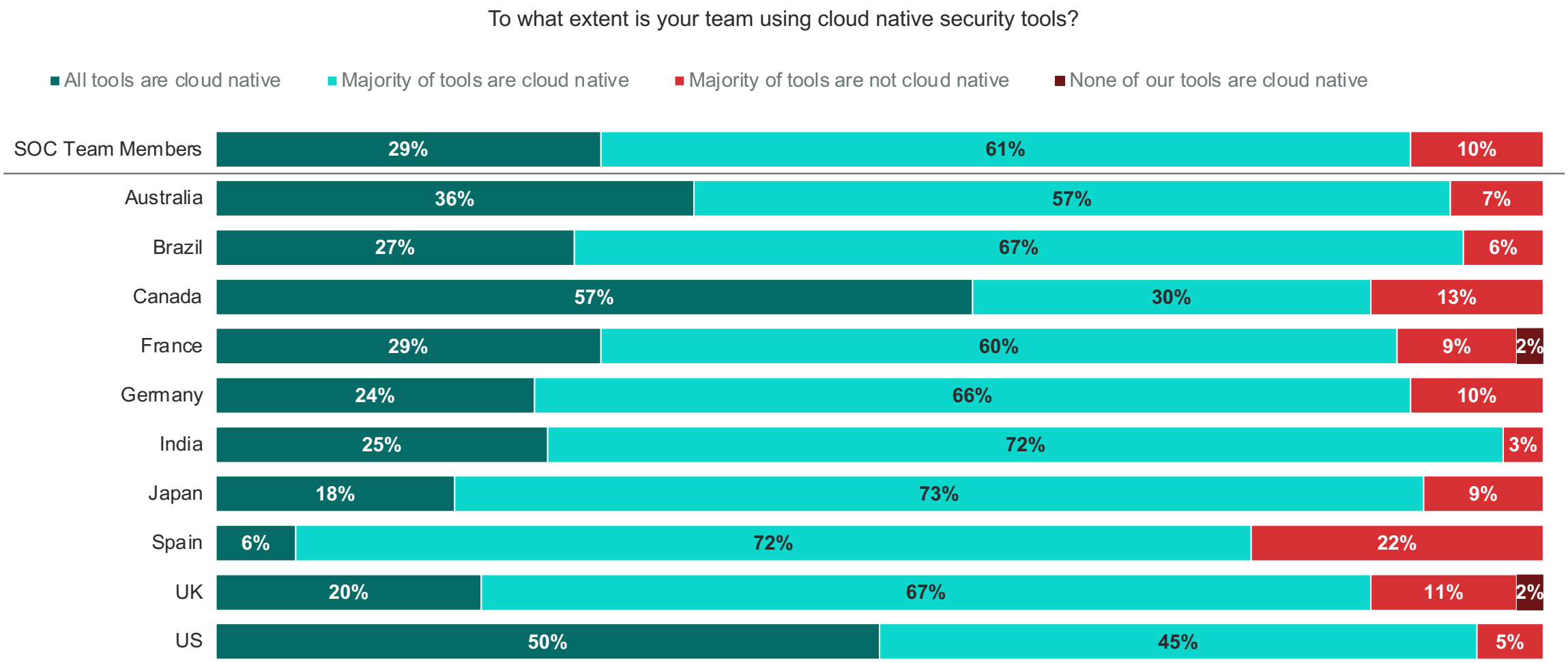
APPENDIX

On average, what percentage of alerts that you're supposed to review do you get to within a typical workday?



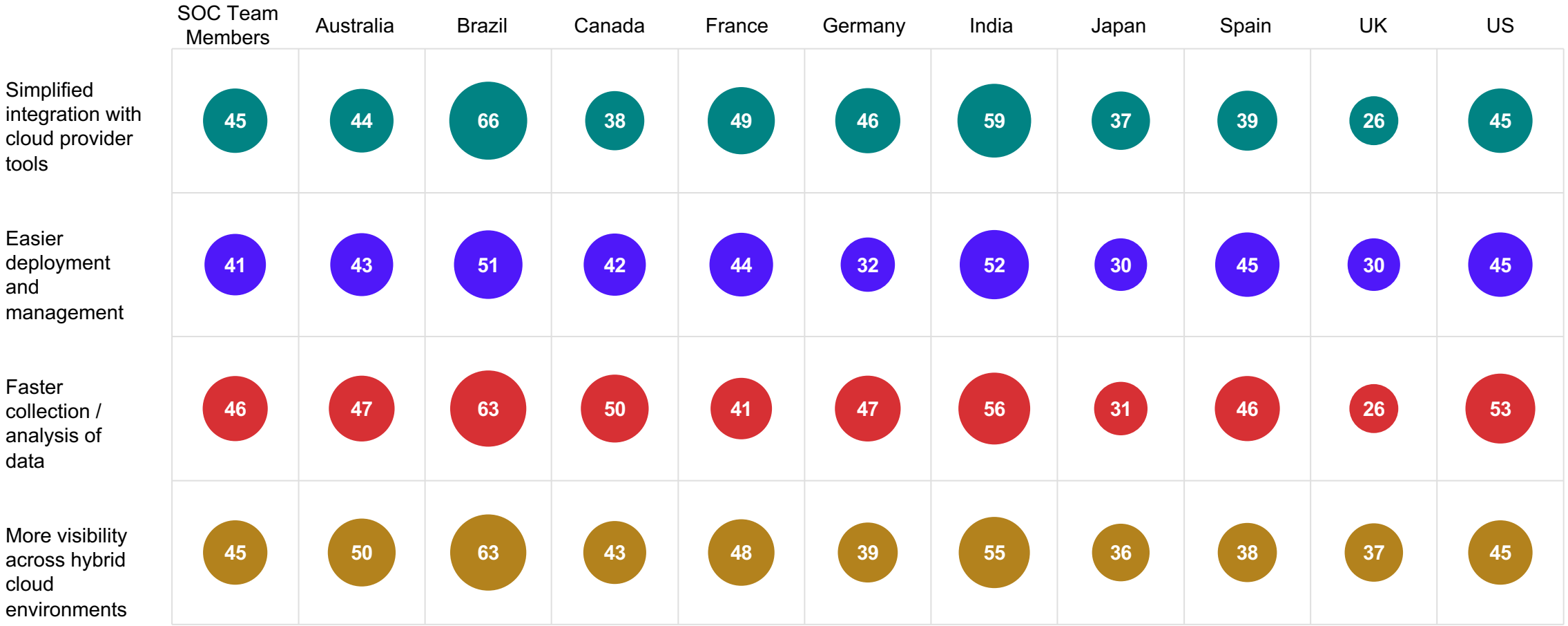
APPENDIX

To what extent is your team using cloud native security tools?



APPENDIX

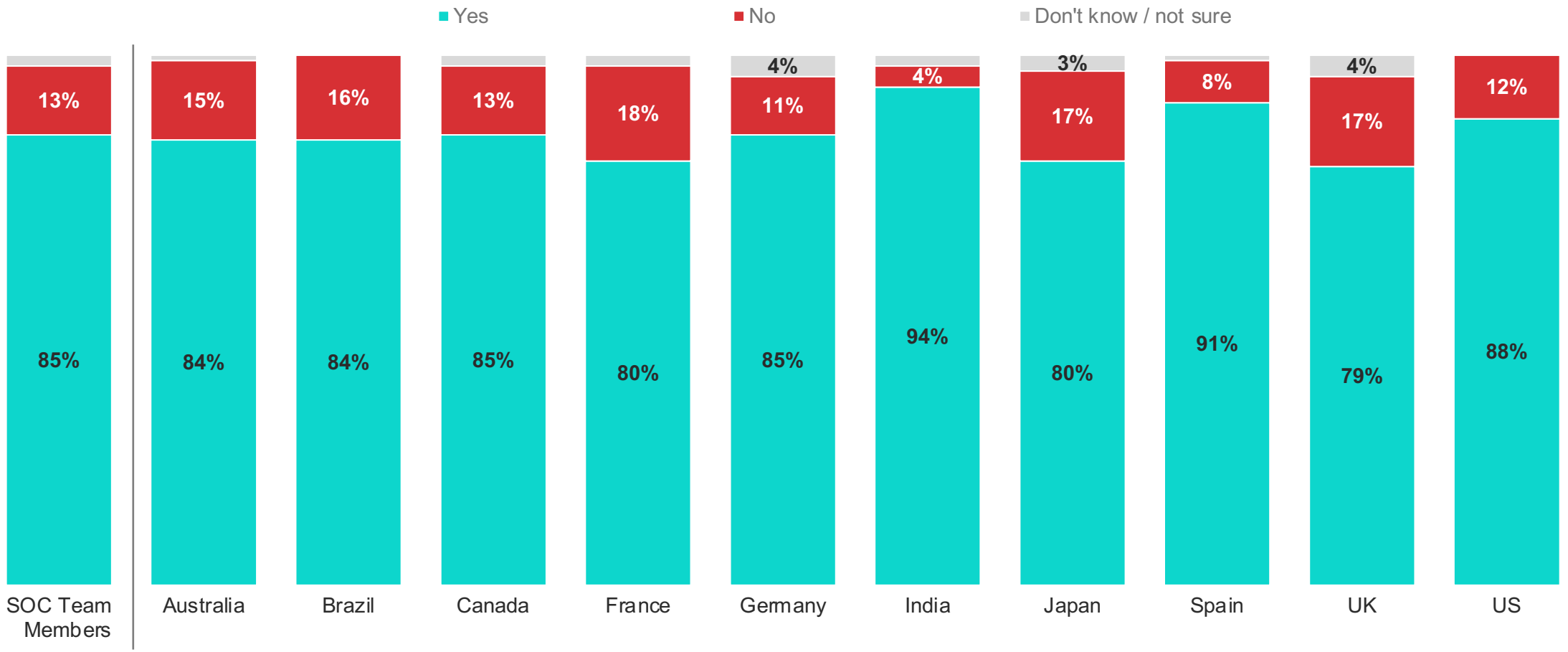
From your experience using cloud-native security tools, to what extent do you agree or disagree that the following are benefits of cloud-native security tools?



MORNING CONSULT® Showing % Strongly Agree

APPENDIX

Within your SOC team, are there individuals with skillsets to build automated incident response workflows?



APPENDIX

What tasks does your team currently leverage automation for? Please select all that apply.

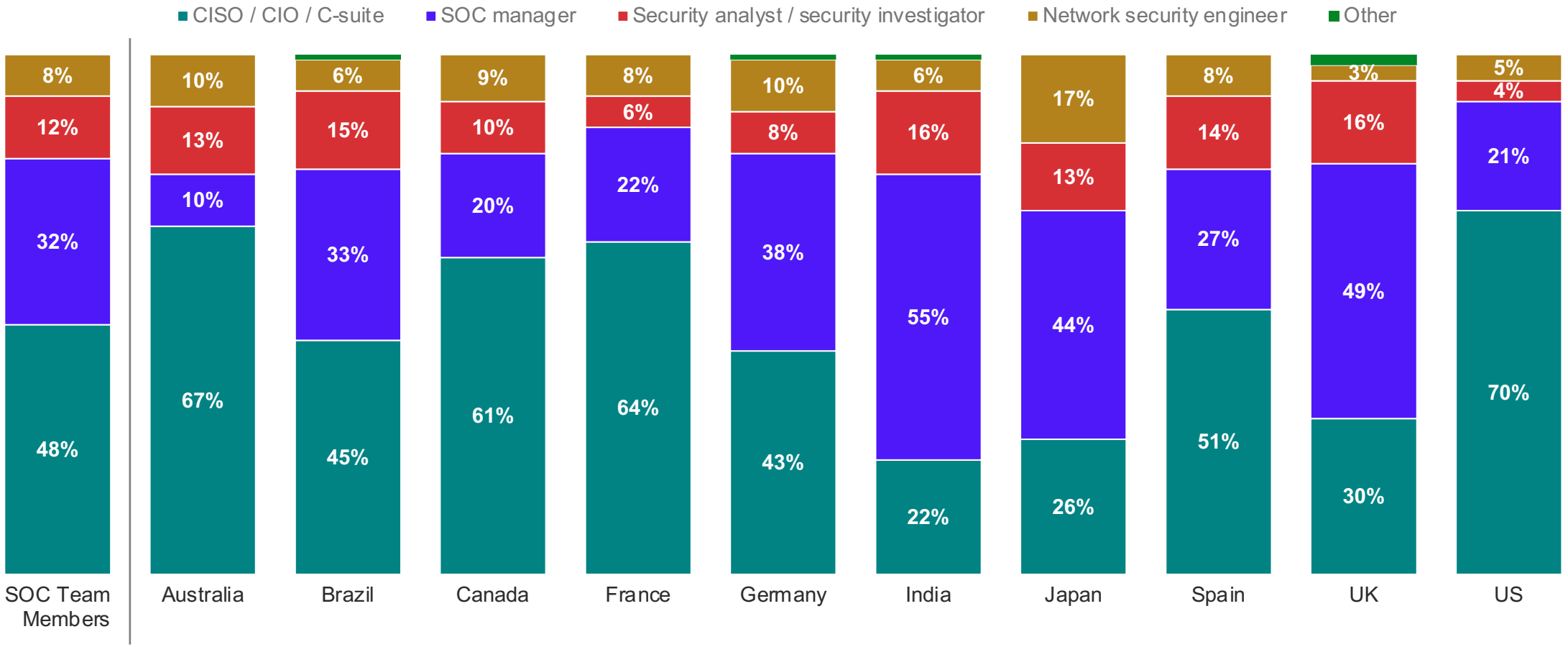
Market	Threat detection	Incident enrichment (adding additional context & logic to alerts)	Threat hunting	Incident response actions
SOC Team Members	77%	53%	55%	65%
Australia	86%	51%	63%	63%
Brazil	88%	67%	46%	73%
Canada	67%	56%	58%	55%
France	68%	55%	52%	68%
Germany	84%	41%	54%	59%
India	81%	59%	57%	74%
Japan	71%	50%	48%	60%
Spain	76%	54%	69%	73%
UK	73%	30%	46%	65%
US	77%	62%	55%	60%

MORNING CONSULT

Among respondents that say there are individuals on their SOC team with skillsets to build automated incident response workflows

APPENDIX

What role/title within your organization is primarily responsible for influencing and/or making decisions on SOC technology / investment?



APPENDIX

How many distinct incident playbooks does your team use on a regular basis?