exabeam®

The Exabeam 2020 State of the SOC Report

Contents

Overview

The Exabeam 2020 State of the SOC Report

REPORT

The Exabeam 2020 State of the SOC Report presents the results of a survey of security professionals from Australia, Canada, Germany, the U.K., and the U.S. who are involved in the management of security operations centers (SOCs) across chief information officer (CIO), chief information security officer (CISO), analyst, and management roles. The survey's purpose was to determine how the players in the SOC view key aspects of its operations, hiring and staffing, retention, SOC processes and effectiveness, technologies, training, and funding. It includes notable changes in responses provided this year as compared to those in the Exabeam 2019 State of the SOC Report.

The results paint a compelling picture of the factors that contribute to a well-run, efficient, and effective SOC.

Research Objectives and Methodology

Research Objectives

In this engagement, Cicero Group agreed to pursue the following research objectives to follow up on and add to the Wave 1 and Wave 2 studies conducted in 2018 and 2019, respectively.

Objectives include:

- Purpose of SOC
- SOC demographics and basic functions including size, roles and job titles, responsibilities, and maturity
- Hiring and staffing needs including hiring difficulty, staffing levels, and desired candidate skillsets
- Processes and systems including training, logging, cloud environments, incident response, metrics (what is prioritized by leadership, management and analysts, efficacy), and pain points or areas of difficulty
- Technology including investments, upcoming trends and pain points
- Finance and budget including dollars invested in technology, staff, as well as changes in funding and cybersecurity insurance

Methodology

- Identical to the methodology used in Waves 1 and 2, a 20-minute online survey was distributed to SOC professionals in March 2020
- Wave 3 was expanded to five different geographies, i.e., U.S. (n=100), U.K. (n=50), Canada (n=50), Germany (n=45), and Australia (n=50)

100	U.S.
50	U.K.
50	Canada
45	Germany
50	Australia

UNITED STATES

UNITED KINGDOM

CANADA

GERMANY

AUSTRALIA

Survey Screening Criteria

EMPLOYMENT STATUS:

- Wave 3 solely focused on SOC employees with full-time and military status, as compared to part-time employees also included in Waves 1 and 2

EMPLOYMENT DETAILS:

- SOC employees were targeted with roles in IT, Operations, Management, and Security
- **Specific roles were targeted and segmented as follows:**
    1. CIO/CISO
    2. SOC Managers (Information Security Officer, Security Engineer/Manager)
    3. Frontline Employees (Security Engineer/Analyst, Threat Researcher, Security Architect)

INDUSTRIES:

- Cicero Group used quotas to ensure a similar distribution of industries to Waves 1 and 2

YEAR-OVER-YEAR SOC TRENDS

To determine year-over-year SOC trends, the Wave 3 study made two adjustments to the data to control for this year's changes in methodology.

1. Removed Germany, Australia, and Canada from the 2020 data (as 2018/2019 was only the U.S. and U.K.)
2. Removed contractor responses from the 2018/2019 data, as these individuals were not included in 2020

Since this action led to an already low sample for 2018 and 2019, the Wave 3 study combined 2018/2019 data into a weighted response average to compare 2020 U.S./U.K. responses to a weighted average of 2018/2019 U.S./U.K. responses (minus contractors).

Key Findings of the Exabeam 2020 State of the SOC Report

How Effective is Your SOC?

Your SOC represents a major investment in the security of your IT assets and intellectual property. So much is riding on the answer to the question, “How Effective is Your SOC?” Are you getting the results you hoped for? What are the metrics for determining a successful ROI on your security investment?

Now you can compare the effectiveness of your company’s security operations center to peer responses in the “Exabeam 2020 State of the SOC Report.” This is our third annual comprehensive survey of cybersecurity professionals who manage and operate SOCs. The data comes from a geographically dispersed set of respondents, including the U.S., U.K., Canada, Germany, and Australia.

Exabeam’s May 2020 survey includes input from CISO, CIO, frontline security analyst, and management roles.

Exabeam's May 2020 survey includes input from CISO, CIO, frontline security analyst, and management roles.

We asked respondents like you about:

- Basic SOC Operations
- Hiring and Staffing
- Operational Processes
- Technology
- Finance and Budget

Based on the data we received, the survey algorithmically determined if a SOC was Highly Effective (35%), Effective (40%), or Less Effective (25%) in its approach to safeguarding enterprise security. Please refer to the appendix, page 77 for criteria on how SOC effectiveness was determined.

On the following pages, we present some of the key findings from our report.

SOC BASICS

- Monitoring/analytics, access management, and logging are now high priorities for all SOC roles.
- While SOC outsourcing in the U.S. has relatively declined (36% to 28%), it has become more common in Europe, with the U.K. seeing a 9-percentage point year-over-year increase (36% to 47%), and Germany reporting 47% outsourcing — threat intel services being the most outsourced function.

HIRING AND STAFFING

SOC staffing remains an issue with nearly 40% of the organizations who feel their SOC is understaffed, often by fewer than ten employees. However, less effective SOCs, in specific, reported feeling more overstaffed and lacking necessary investment in technology, training, and staffing.

- While hard skills remain critical, SOCs place increased emphasis on soft skills with the ability to work in teams taking precedence over formerly reported social ability.

Although the U.S. and U.K. SOCs show year-over-year improvements in identifying candidates with the right expertise and recruiting costs, organizations today continue struggling with the former, citing it as one of the top challenges experienced in SOC hiring.

- Workplace benefits, high wages, and a positive culture are reported to be the top drivers this year of continued high employee retention for nearly 60% of SOCs.

PROCESS

While U.S. and U.K. SOCs reported significant year-over-year declines in their ability to do threat modeling and budget/resource allocation, concerning overall processes, German SOCs appeared more effective. In contrast, Australian SOCs appeared less effective than their global counterparts in nearly all categories.

- In terms of size, smaller sized SOCs (less than 25 team members) reported a higher ability to respond to common issues.
- Too much time spent on reporting and documentation, as well as out-of-date systems, continues to be a common pain point.

Effective SOCs continue to trend toward monthly/quarterly training and are more likely to have structured training.

- Training quality remains adequate. Potential improvements now include increased updates and budget spends.

Much like past years, small SOCs are more concerned with downtime or business outage as an operational metric than SOCs with 25+ team members.

TECHNOLOGY

- Monitoring/analytics, access management, and logging are now high priorities for all SOC roles.
- Most SOCs now expect to see biometrics authentication, and SOAR (security orchestration, automation and response) tools will take precedence over other technologies in the coming years.
- Keeping up with security alerts and coordinating information between cybersecurity and IT remain pain points across all SOC roles, particularly frontline employees.

FINANCE AND BUDGET

- In a carryover from the Wave 2 study, where respondents stated improved funding in technology and facilities, the Wave 3 study observed nearly 40% shifting to staffing as now being most underfunded and would like to see continued investment in technology, training, and staffing.
- Concerning risk insurance, Europe takes precedence over their global counterparts in more often possessing first-party risk insurance, focused on risk compliance.

SOC Basics

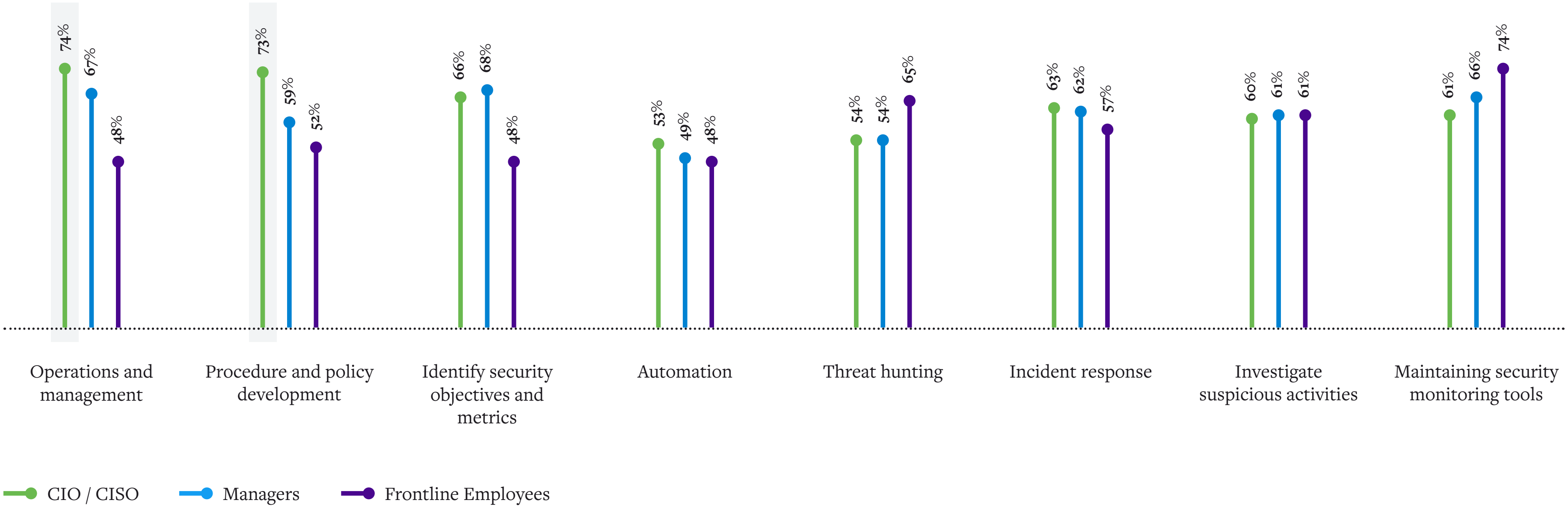
You'll find the following topics covered in this section:

1. SOC RESPONSIBILITIES
2. AUTOMATION
3. SOC OUTSOURCING
4. SOCIAL ENGINEERING ATTACKS

SOC managers drive metrics specifically in ops/management and procedure/policy development.

RESPONSIBILITY BY ROLES

TOP 1 – THIS FALLS UNDER MY ROLE



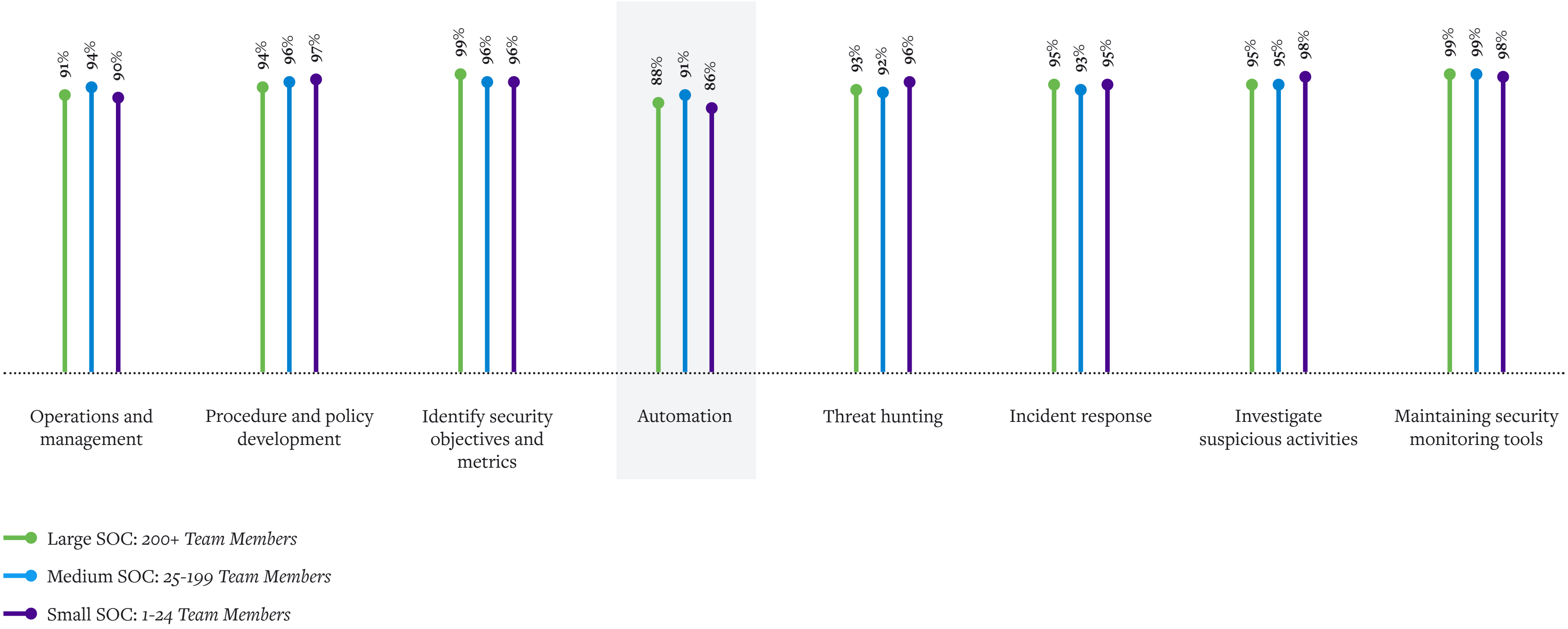
When comparing SOC responsibilities across geographies, SOCs in Europe also placed increased importance in **identifying security objectives and measures** as a primary part of their role.

In addition, the more than 5% point YoY decline can be observed in the top two responses on SOC responsibilities around **incident response and automation** in U.K. SOCs.

Automation is the least common function within the SOC and shows the greatest differentiation between Medium-sized SOCs and Small/Large ones.

SOC RESPONSIBILITY BY SIZE

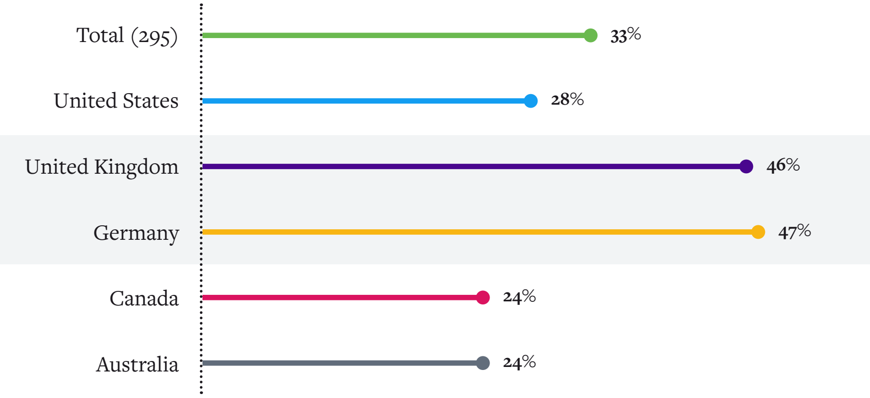
THIS FALLS UNDER MY ROLE, AND THIS DOES NOT FALL UNDER MY ROLE BUT IS PART OF THE SOC'S RESPONSIBILITIES



While SOC outsourcing in the U.S. has relatively declined, it has become more common in Europe, where threat intel services are the most outsourced function.

USE OF OUTSOURCING

YES, MY ORGANIZATION DOES OUTSOURCE SOC ACTIVITIES

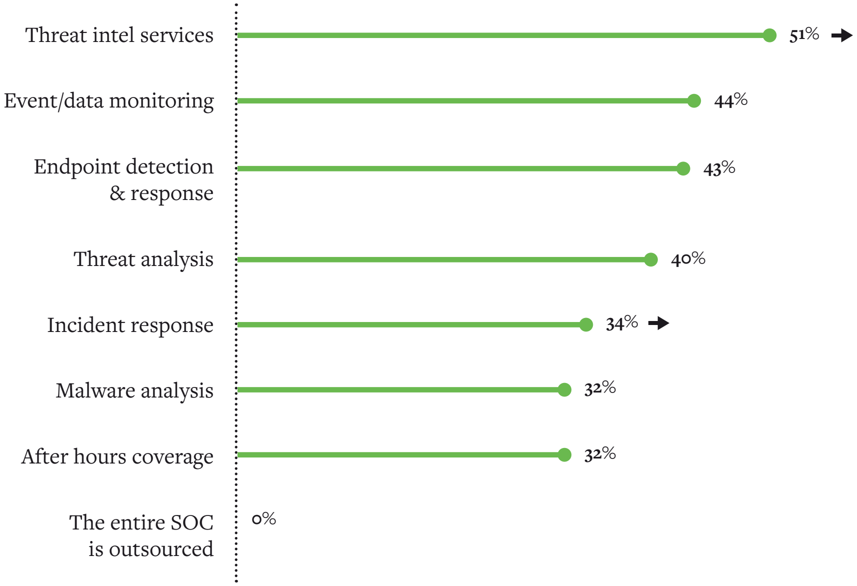


In 2018/2019 (which only included the U.S. and U.K.), the outsourcing average was 42% compared to the 34% U.S. and U.K. average in 2020. **The U.S. is less outsourced while the U.K. is more.**

→ *Indicates more than a 15% point YoY increase/decrease between 2018/2019 and 2020 U.S., U.K. aggregated data.*

OUTSOURCED FUNCTIONS

N=96

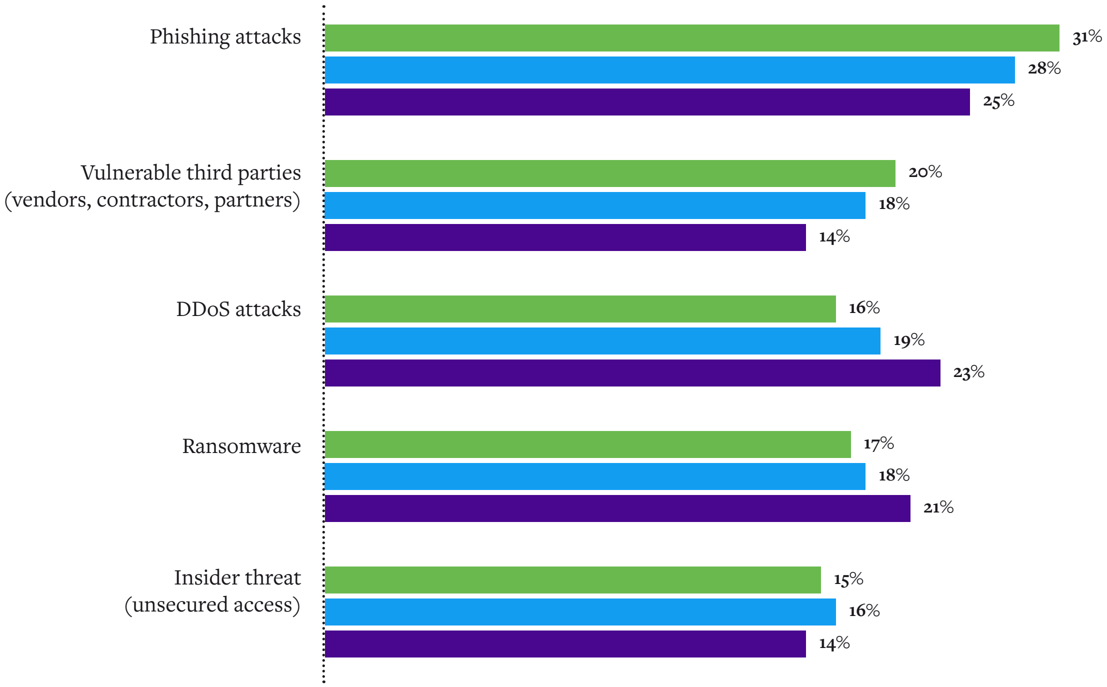


Much like its counterparts, but in increased capacity, the **U.K. tends to exceed outsourcing threat intel services.**

SOC leaders and frontline analysts do not agree on the most common threats facing the organization. SOC leaders believe that phishing and supply chain vulnerabilities are more important issues, while analysts see DDoS attacks and ransomware as greater threats.

COMMON SECURITY THREATS

N=295



🟩 CIO / CISO

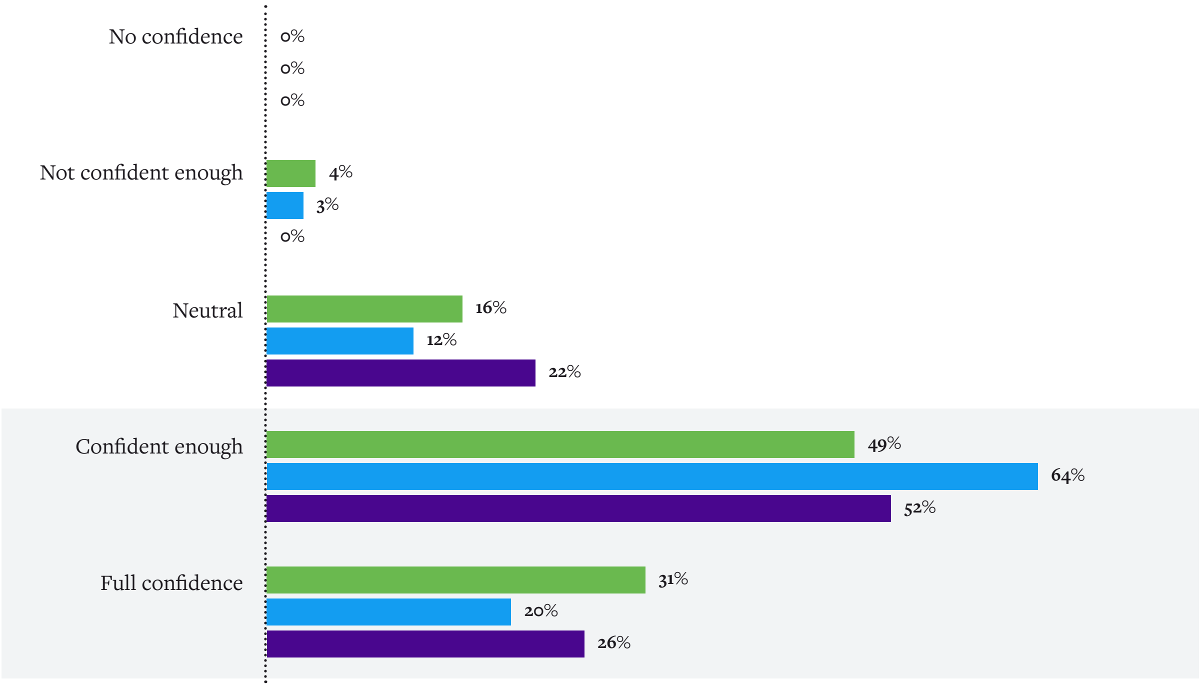
🟦 SOC Managers

🟪 Frontline

82% of SOC professionals are confident in their ability to detect threats.

CONFIDENCE IN ABILITY TO DETECT THREATS

N=295



🟩 CIO / CISO

🟦 SOC Managers

🟪 Frontline

Hiring and Staffing

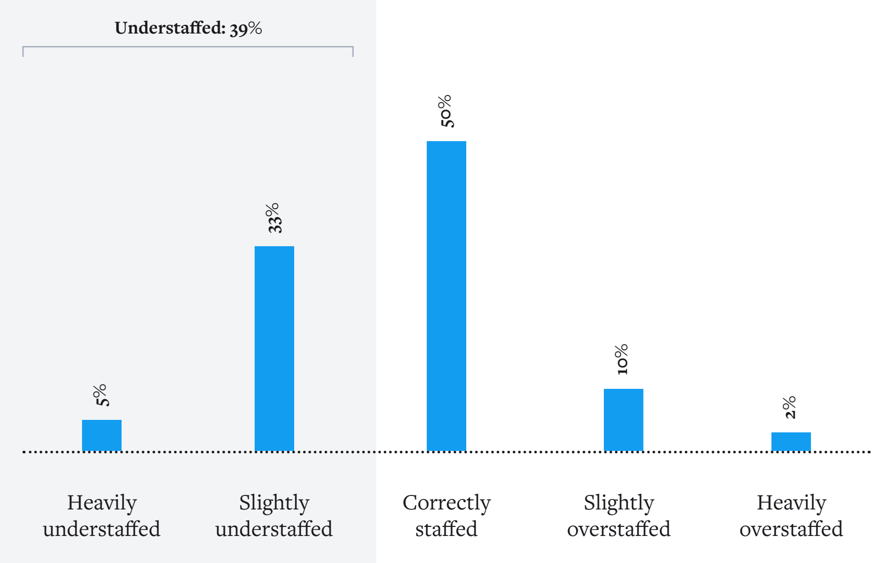
You'll find the following topics covered in this section:

1. **SOC STAFFING**
2. **LESS EFFECTIVE SOCS AND STAFFING**
3. **HARD SKILLS/SOFT SKILLS**
4. **COMMUNICATION**
5. **THREAT HUNTING**
6. **IDENTIFYING CANDIDATES**
7. **EMPLOYEE RETENTION**
8. **WORKERS AGREE/DISAGREE ABOUT RETENTION**

SOC staffing remains an issue with nearly 40% of the organizations who feel their SOC is understaffed, often by fewer than ten employees.

PERCEPTION OF CURRENT STAFFING LEVELS

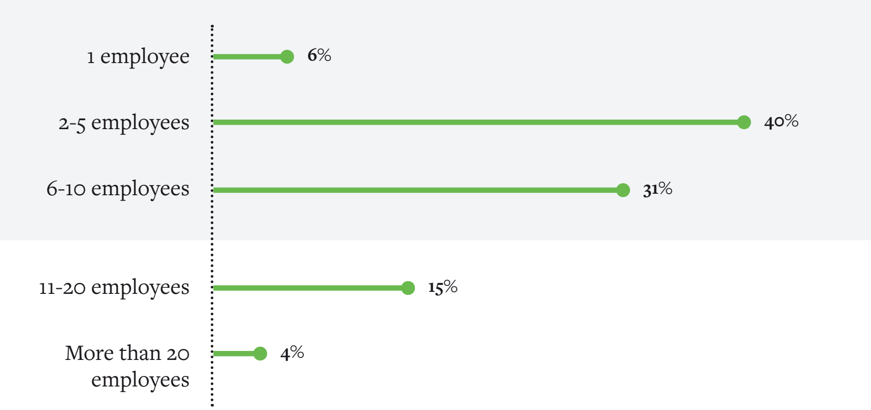
N=295



U.S. SOCs are slightly less correctly staffed now as compared to 2018/2019 (53% to 51%) whereas **U.K. SOCs now report improvements in correct staffing** (43% to 48%).

NUMBER OF EMPLOYEES UNDERSTAFFED

N=131

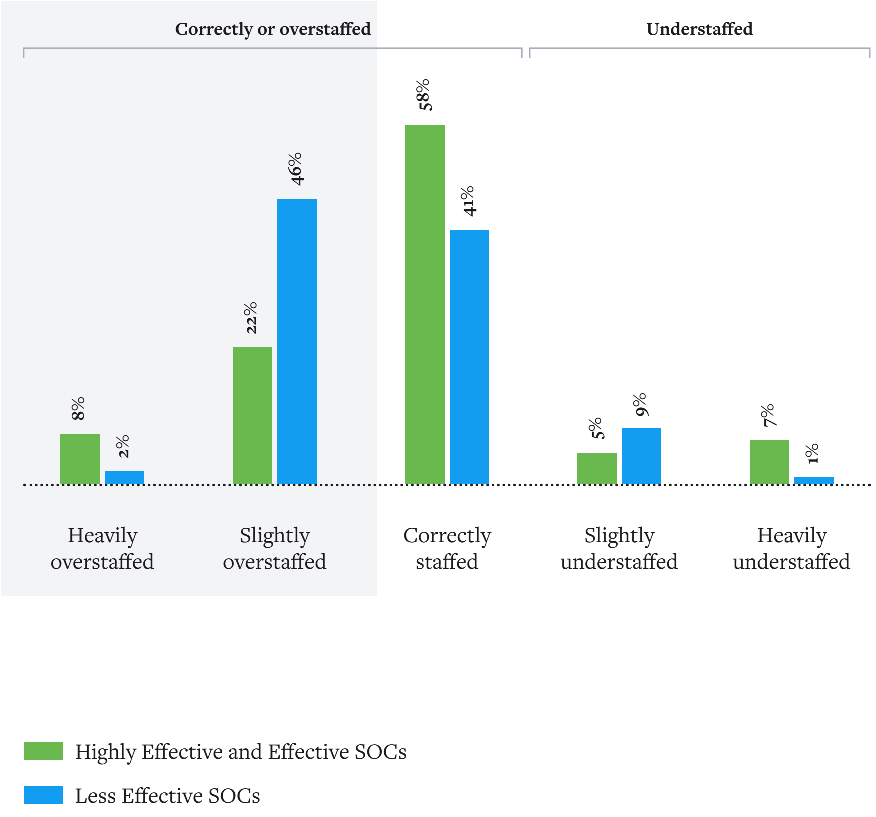


When comparing the number of employees by which SOCs feel understaffed, **23% of SOC personnel across the U.S. and 35% across Canada** report being understaffed by more than 10 employees.

However, almost half of less effective SOCs, specifically, feel overstaffed, even while a quarter of less effective SOCs reported lacking necessary investment in technology, training, and staffing.

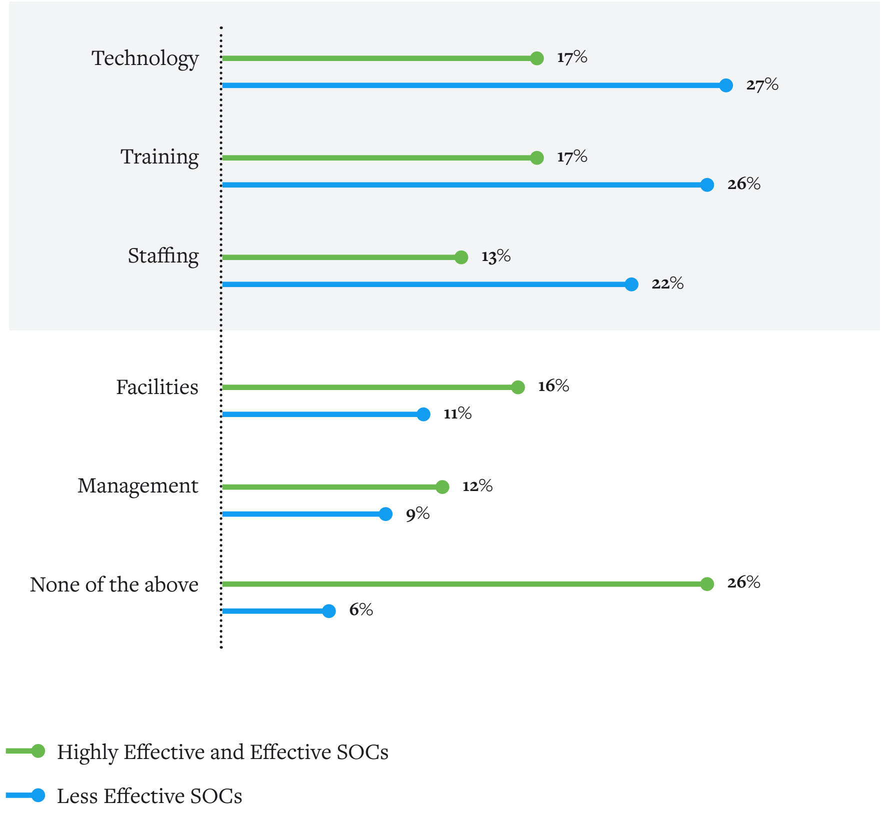
PERCEPTION OF CURRENT STAFFING LEVELS

N=295



AREAS OF INSUFFICIENT FUNDING

N=295



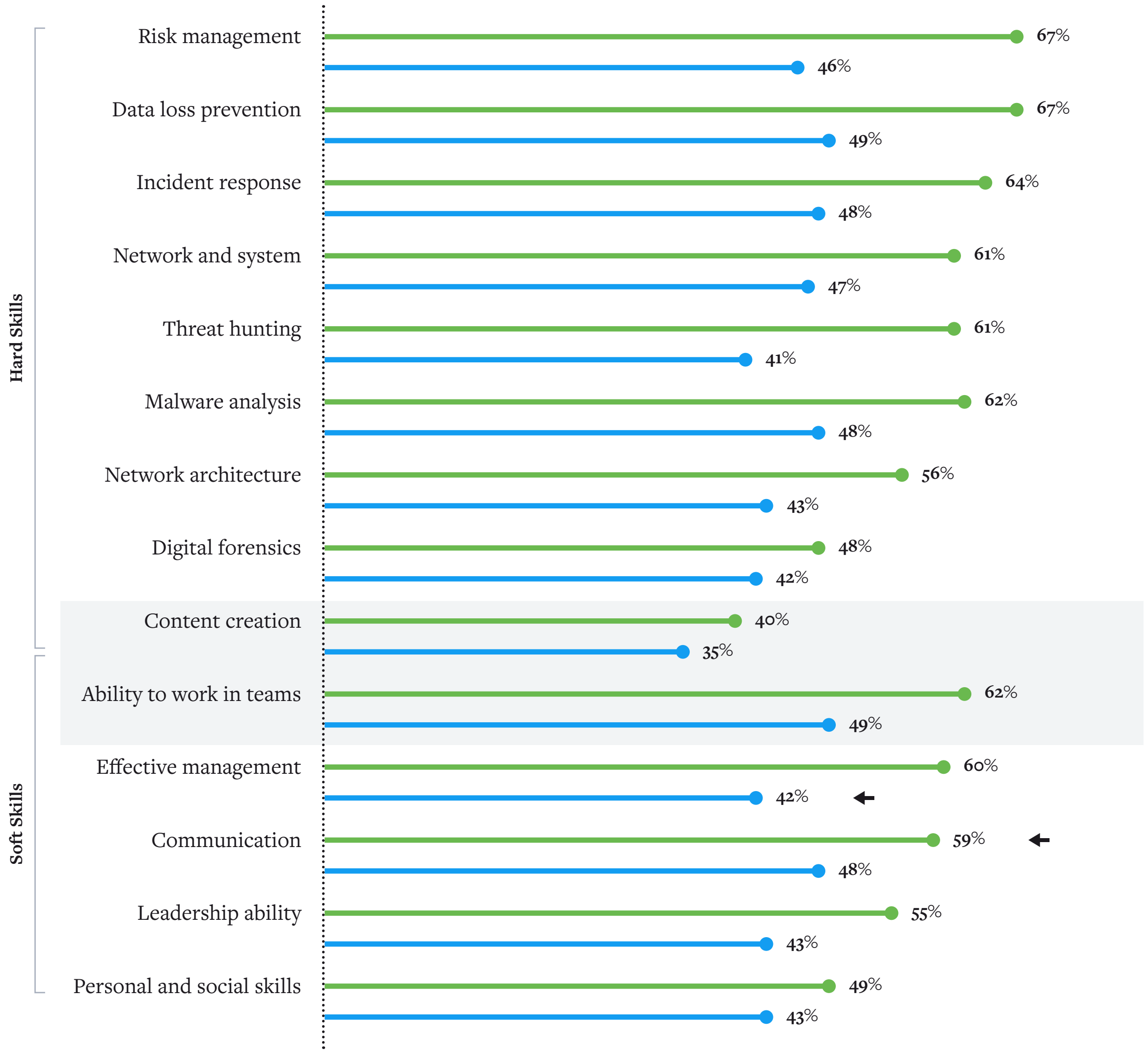
While hard skills remain critical, SOCs place emphasis on soft skills with the ability to work in teams taking precedence over formerly reported social ability.

SOCs are, based on their own rating, least able to create content. Creating content is the skill around the creation of detection logic, validation, tuning, and reporting.

The importance of skills has maintained nearly the same for the U.S. but dropped for the U.K. in nearly all categories, with a significant drop in communication, malware analysis, and social ability.

SKILLS - IMPORTANCE AND ABILITY

7-POINT SCALE, TOP 2, N=295



🟩 Skills importance

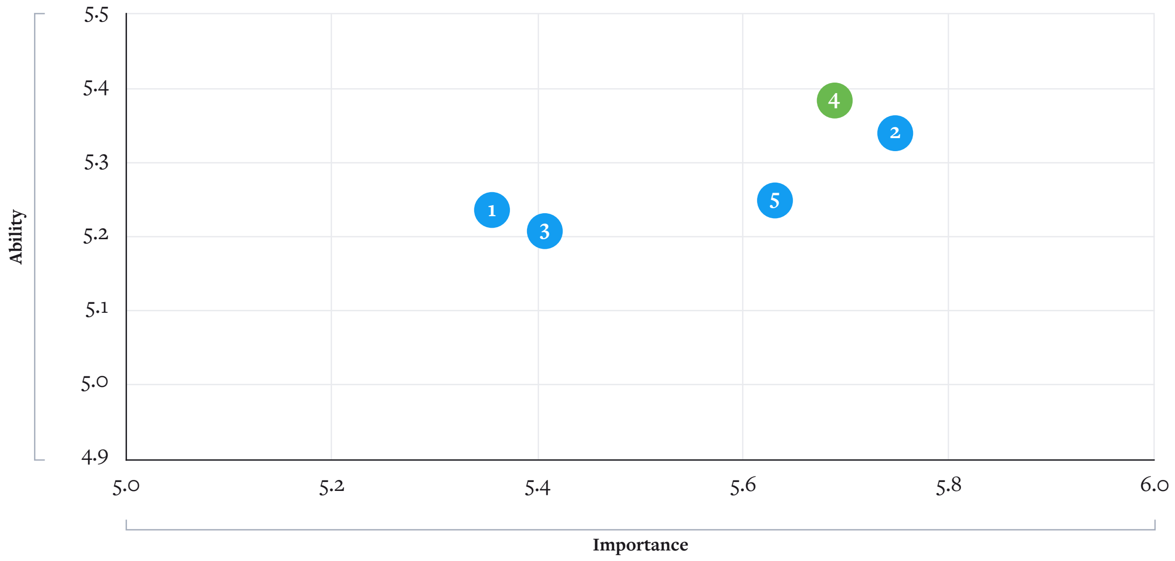
🟦 Skills ability

→ *Indicates more than a 15% point YoY increase/decrease between 2018/2019 and 2020 U.S., U.K. aggregated data.*

Despite lowering in YoY importance, Communication remains a soft skill that SOC personnel state is important to have and feel confident about.

SOFT SKILLS - IMPORTANCE AND ABILITY

7-POINT SCALE, MEAN, N=295



SOFT SKILLS

1 Personal/Social Skills

2 Ability to work in teams

3 Leadership ability

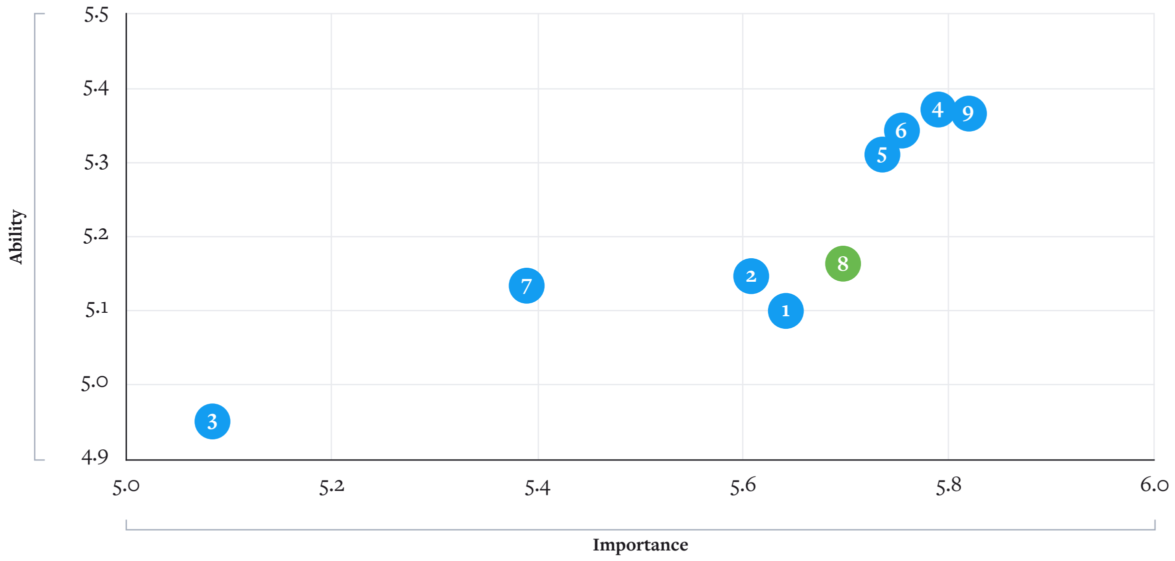
4 Communication

5 Effective management

Threat hunting stands out as a hard skill that is highly important but that SOC personnel feel they lack the ability to resolve.

HARD SKILLS - IMPORTANCE AND ABILITY

7-POINT SCALE, MEAN, N=295



HARD SKILLS

1 Network and system administration

2 Network architecture

3 Content creation

4 Data loss prevention

5 Malware analysis

6 Risk management

7 Digital forensics

8 Threat hunting

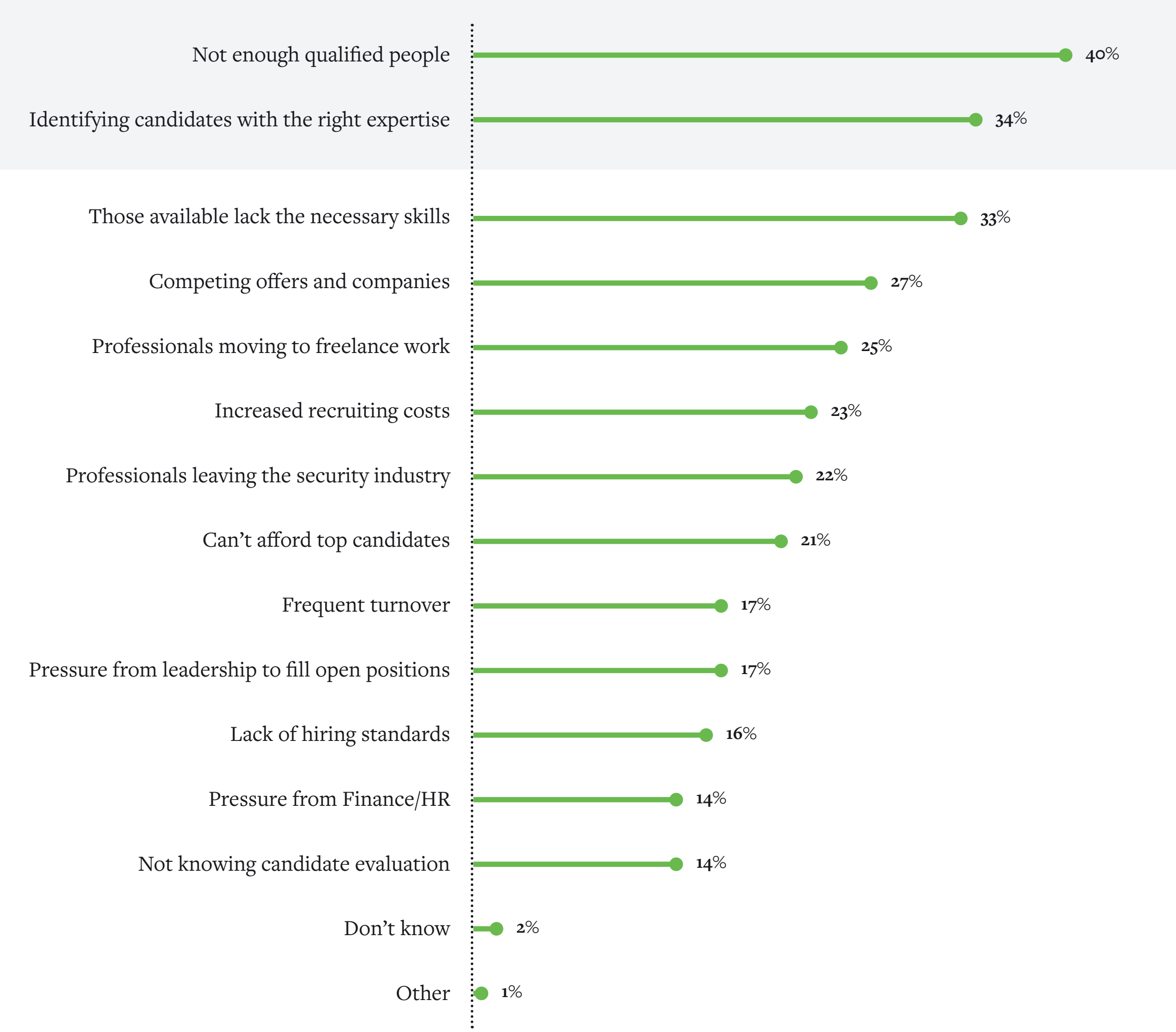
9 Incident response

Although the U.S. and U.K. SOCs show YoY improvements in identifying candidates and lowering recruiting costs, SOCs still struggle with the former.

Although still a challenge, SOCs across the U.S. and U.K. stated significant improvements in being able to **identify candidates with the right expertise and recruiting costs.**

COMMON HIRING CHALLENGES

N=295

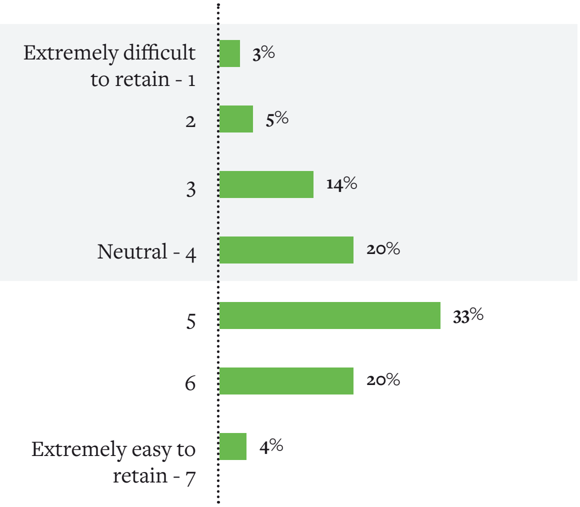


60%

Workplace benefits, high wages, and a positive culture continue to be drivers of high employee retention for nearly 60% of SOCs.

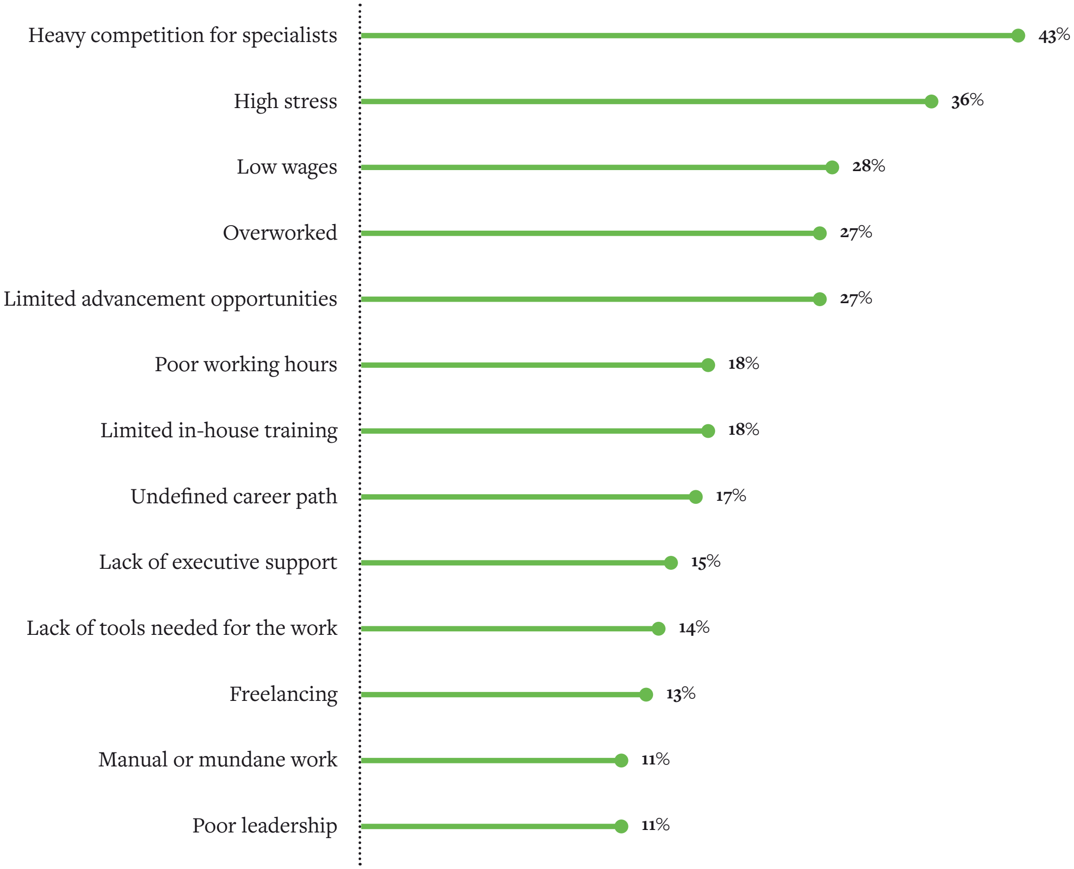
DIFFICULTY OF RETAINING EMPLOYEES

N=295



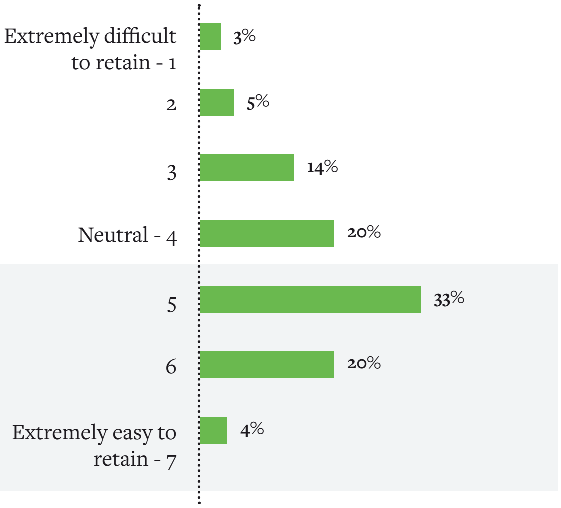
REASONS EMPLOYEES ARE DIFFICULT TO RETAIN

N=132



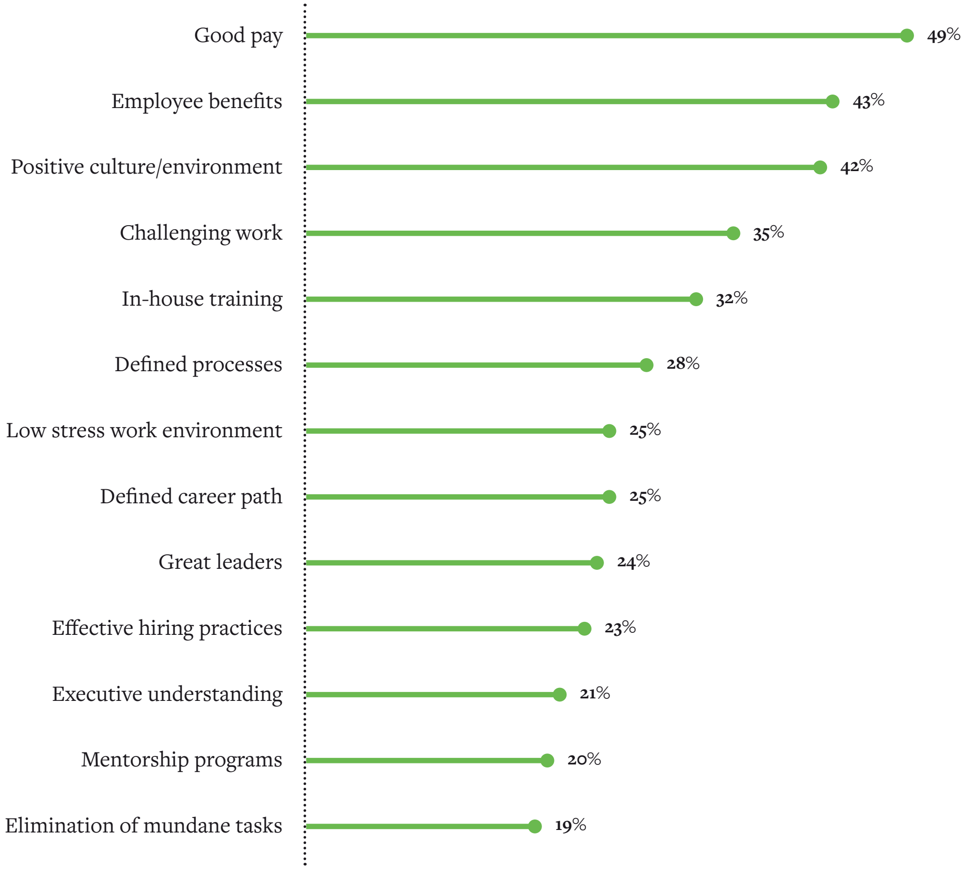
DIFFICULTY OF RETAINING EMPLOYEES

N=295



REASONS EMPLOYEES ARE EASY TO RETAIN

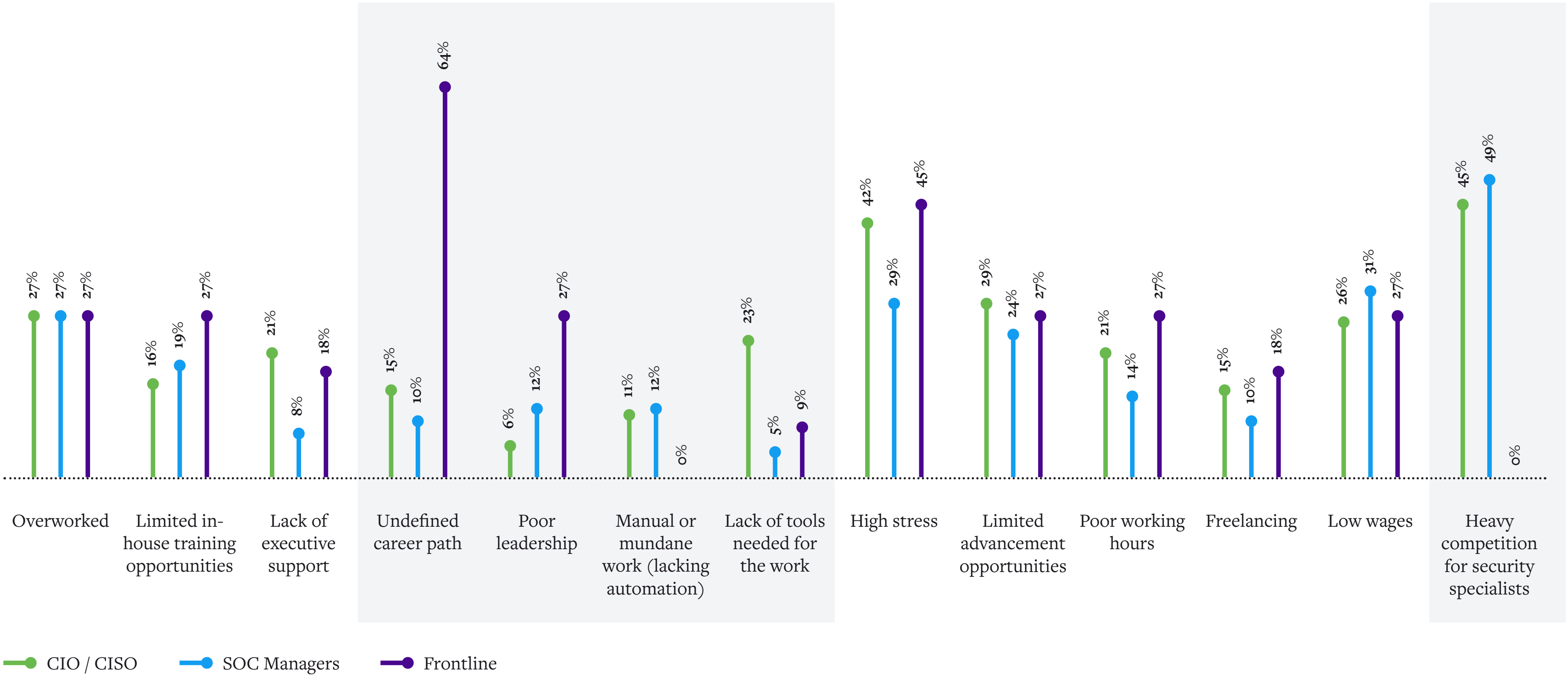
N=228



Breaking this out by role, workers agree on why employees are easy to retain but have some stark differences about why they leave, especially when it comes to an undefined career path.

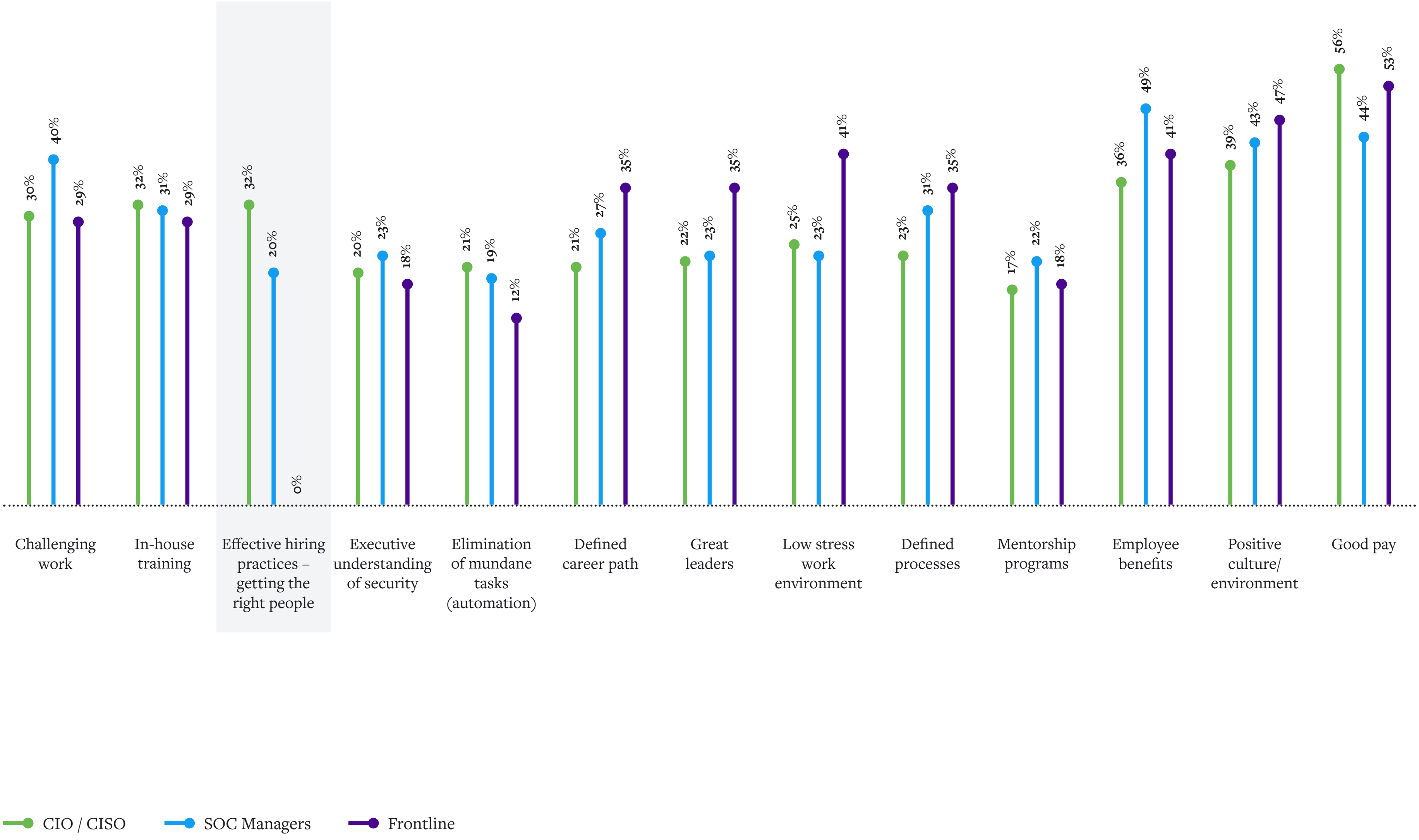
REASONS EMPLOYEES ARE DIFFICULT TO RETAIN BY ROLE

N=132



TOP REASONS EMPLOYEES ARE EASY TO RETAIN BY ROLE

N=228



Process

You’ll find the following topics covered in this section:

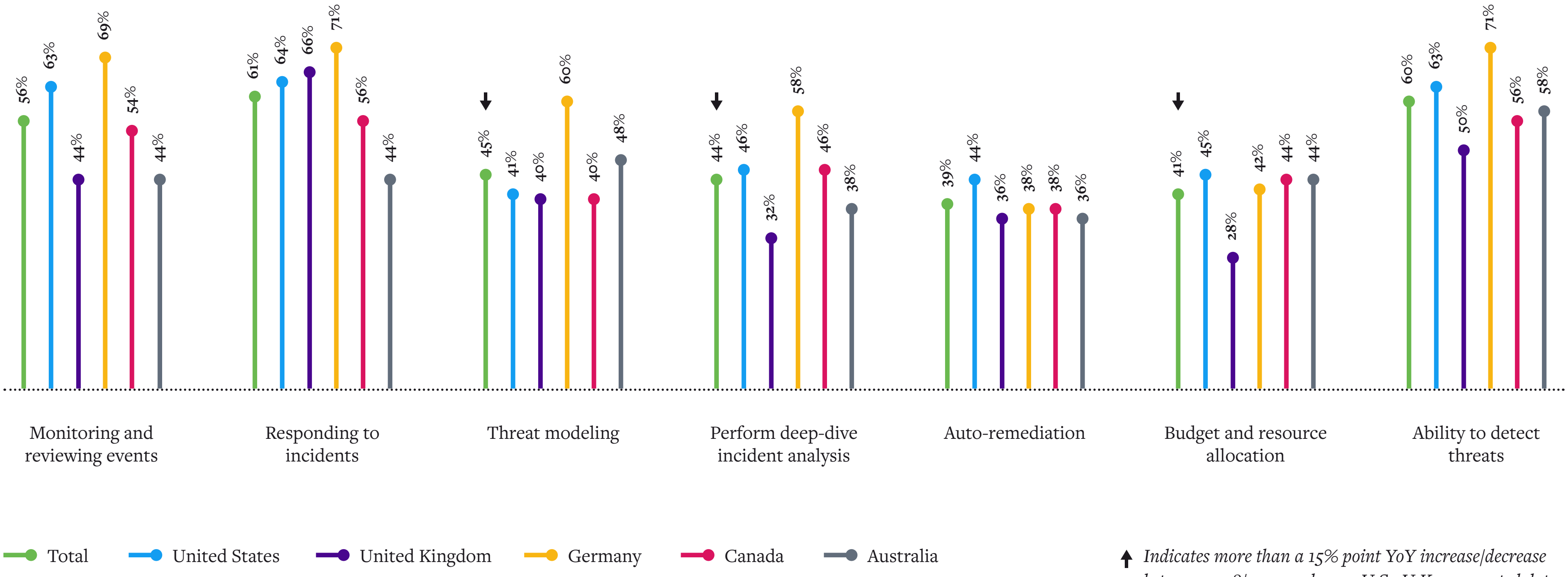
1. PROCESS SELF-ASSESSMENT
2. EFFECTIVENESS BY ROLE
3. SOC SIZE VS. RESPONSIVENESS
4. COMMON PAIN POINTS FOR ALL SOCS
5. PAIN POINTS FOR SOCS IN GERMANY
6. COMMON PAIN POINTS FOR MANAGERS AND FRONTLINE STAFF
7. EXTENT OF LOGGING
8. SOC TRAINING FREQUENCY
9. EFFECTIVE SOCS AND TRAINING
10. FOCUS ON IN-HOUSE TRAINING
11. TRAINING QUALITY
12. DOWNTIME OR BUSINESS OUTAGE BY SOC SIZE
13. DOWNTIME OR BUSINESS OUTAGE BY SOC ROLE
14. SOC COLLABORATION WITH OTHER FUNCTIONAL AREAS

Concerning processes, German SOCs assess themselves as more effective, while Australian SOCs appear less effective in nearly all categories.

U.S. and U.K. SOCs reported declines in their ability to do threat modeling and budget and resource allocation in YoY change.

EFFECTIVENESS OF SOC TEAM

ABILITY TO RESPOND TO COMMON ISSUES ON A 7-POINT SCALE, TOP 2, N=295

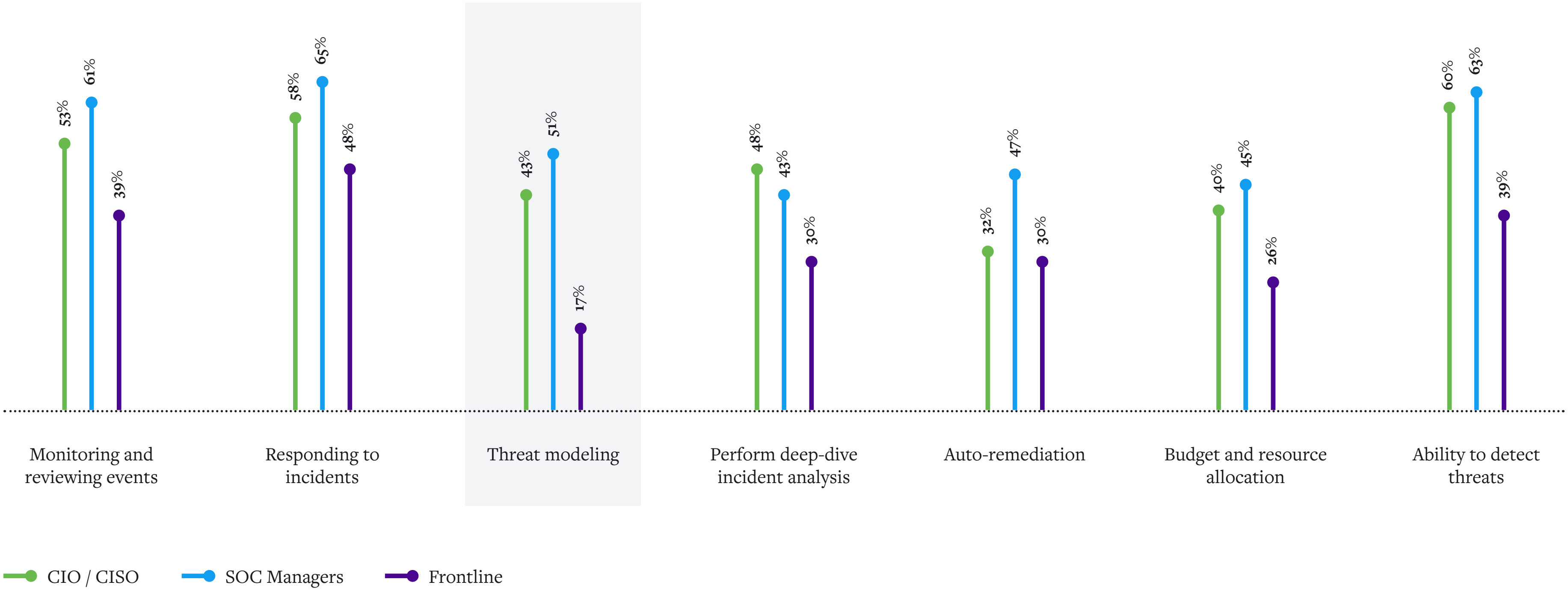


↑ *Indicates more than a 15% point YoY increase/decrease between 2018/2019 and 2020 U.S., U.K. aggregated data.*

Considering effectiveness by role in the company, we see that frontline employees are less confident for each ability, with the greatest difference in threat modeling.

EFFECTIVENESS OF SOC TEAM

ABILITY TO RESPOND TO COMMON ISSUES ON A 7-POINT SCALE, TOP 2, N=295

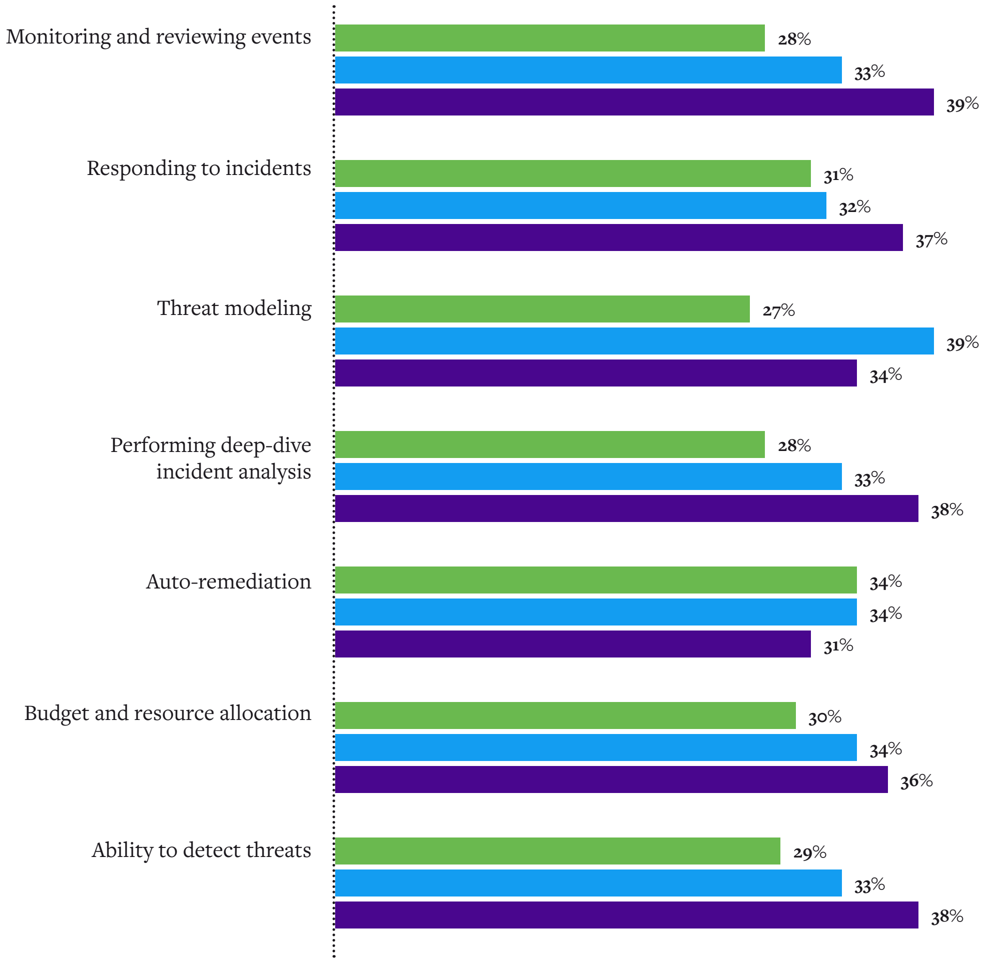


<25

In terms of size, smaller sized SOCs (less than 25 team members) reported a higher ability to respond to common issues in nearly all categories.

EFFECTIVENESS OF SOC TEAM BY SOC SIZE

ABILITY TO RESPOND TO COMMON ISSUES ON A 7-POINT SCALE, TOP 2, N=295



🟩 Large SOC: *200+ Team Members*

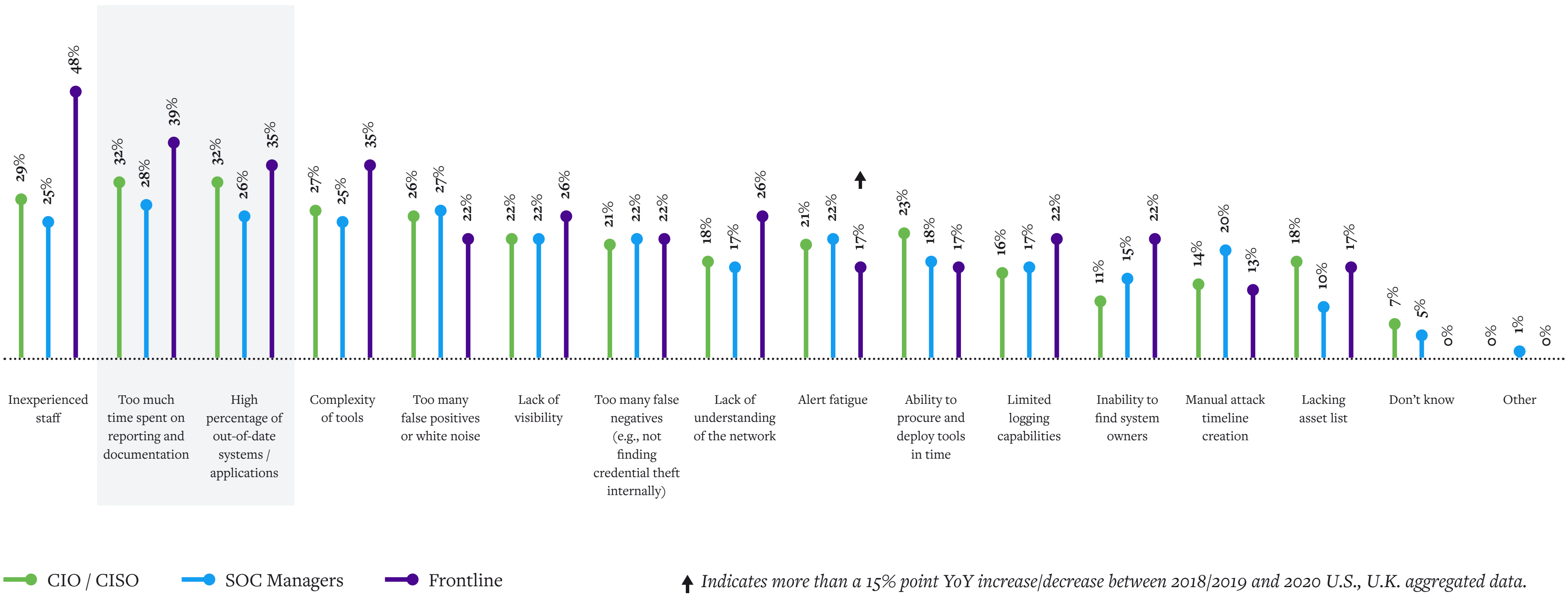
🟦 Medium SOC: *25-199 Team Members*

🟪 Small SOC: *1-24 Team Members*

Inexperienced staff and too much time spent on reporting and documentation continue to be a common pain point for SOCs in 2020.

PAIN POINTS

COMMON PAIN POINTS EXPERIENCED OVERALL, N=295



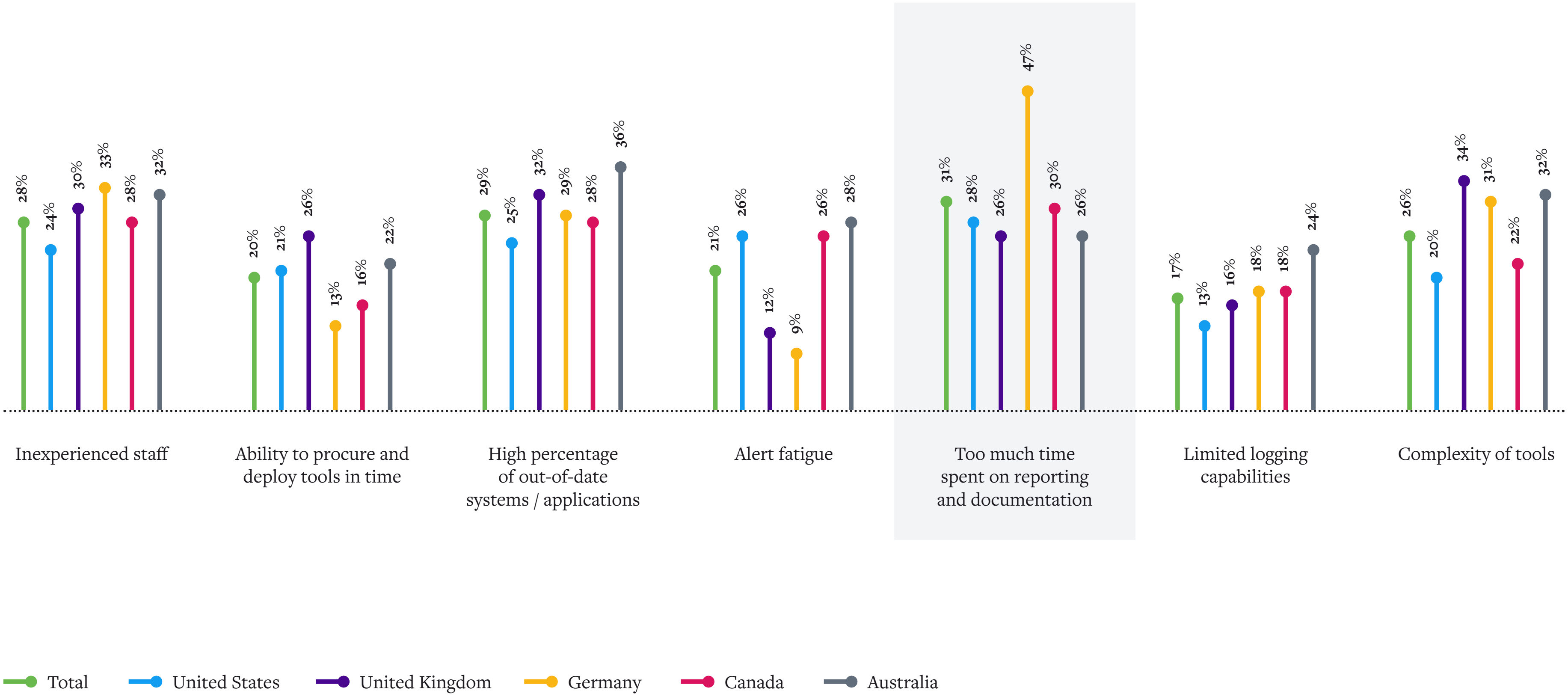
↑ *Indicates more than a 15% point YoY increase/decrease between 2018/2019 and 2020 U.S., U.K. aggregated data.*

This may be one of the reasons why large SOCs have a lower ability to address common issues effectively.

SOCs in Germany experience higher pain points in documentation time, but relatively lower levels of pain in many other areas. Section continued on the following page.

PAIN POINTS FOR TOTAL AND UNITED STATES

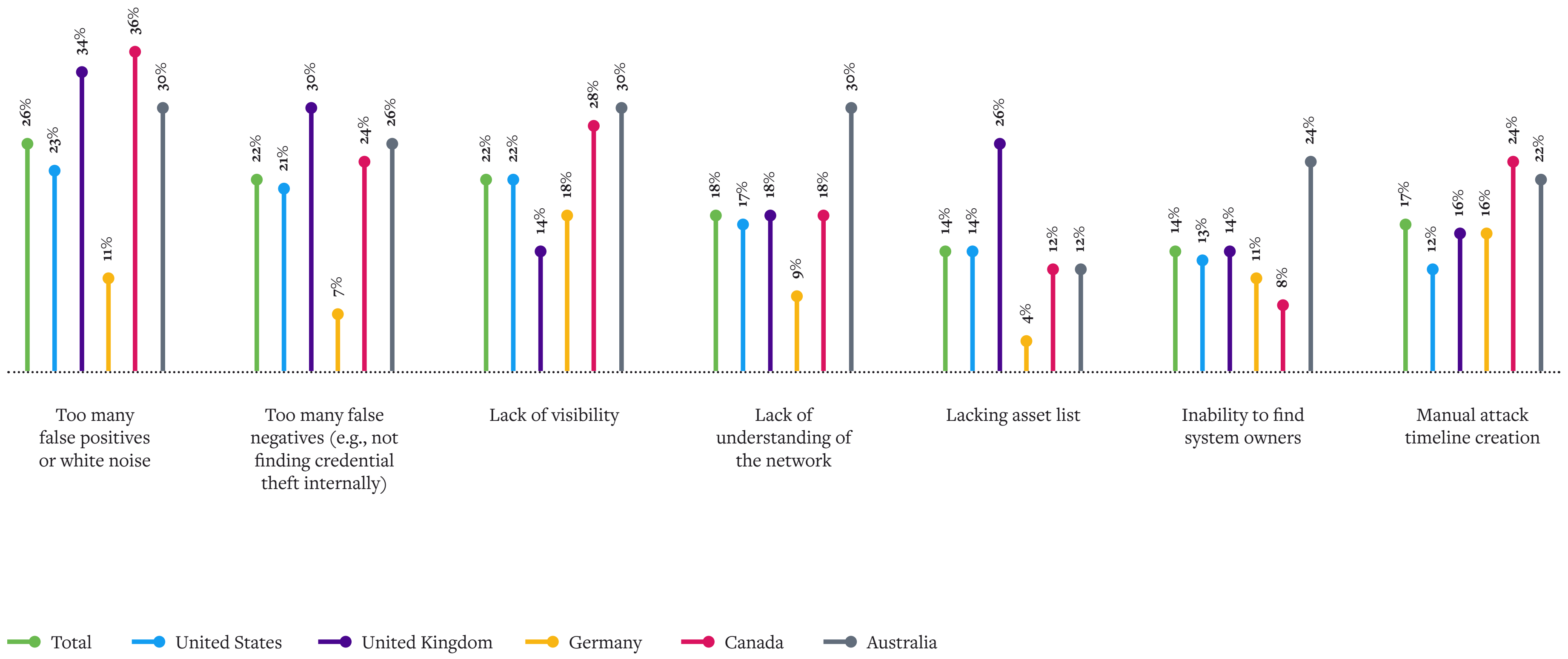
COMMON PAIN POINTS EXPERIENCED OVERALL



Inexperienced staff is a growing challenge, especially for U.K. SOCs in 2020, when compared to 2018/2019, and this may be one of the reasons why U.K. SOCs are generally rating themselves lower in their skills importance and ability.

PAIN POINTS FOR TOTAL AND UNITED STATES

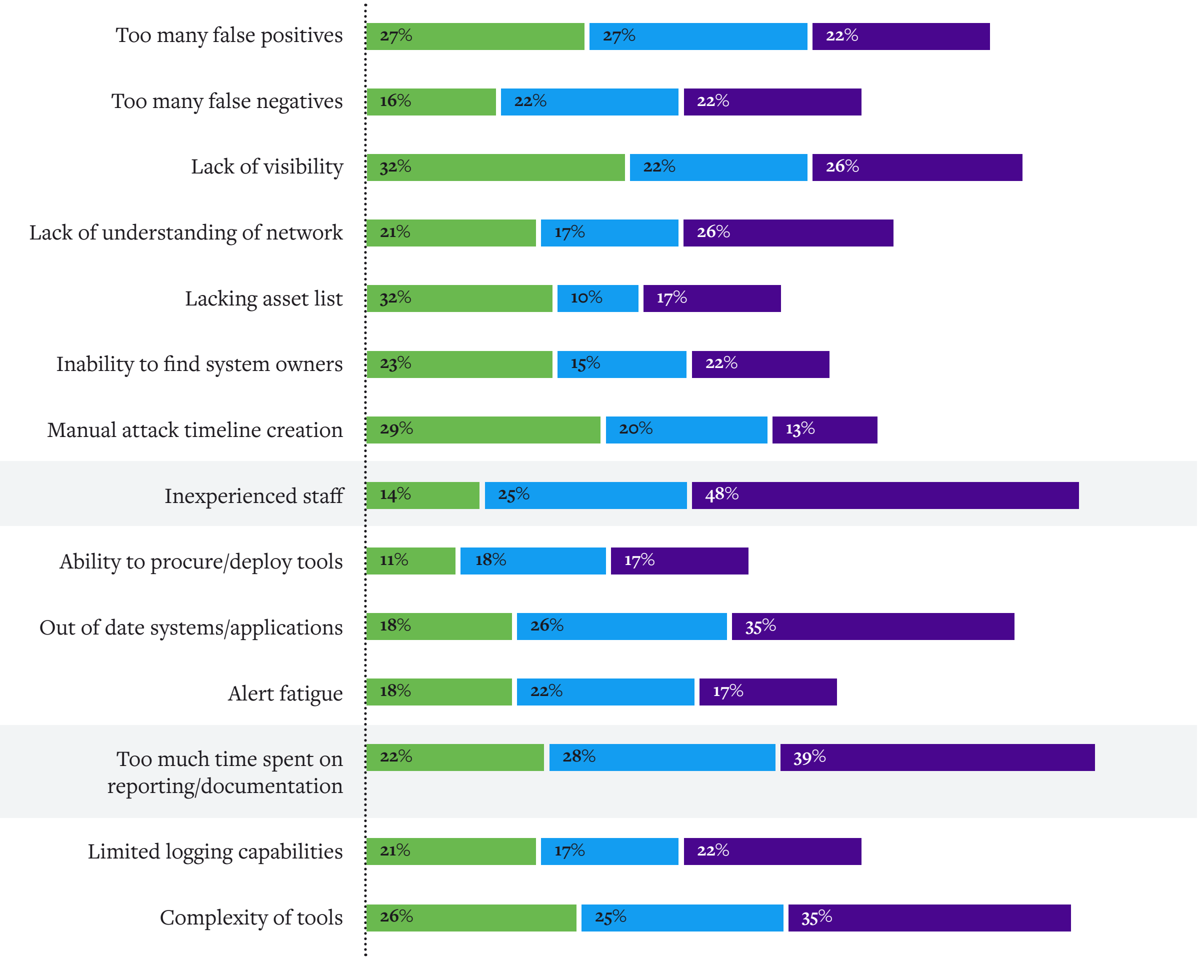
COMMON PAIN POINTS EXPERIENCED OVERALL



Inexperienced staff and time spent on reporting/documentation also remain a common pain point for Managers and Frontline employees that is not being noticed by Executives.

PAIN POINTS BY ROLE

COMMON PAIN POINTS EXPERIENCED OVERALL



🟩 CIO / CISO

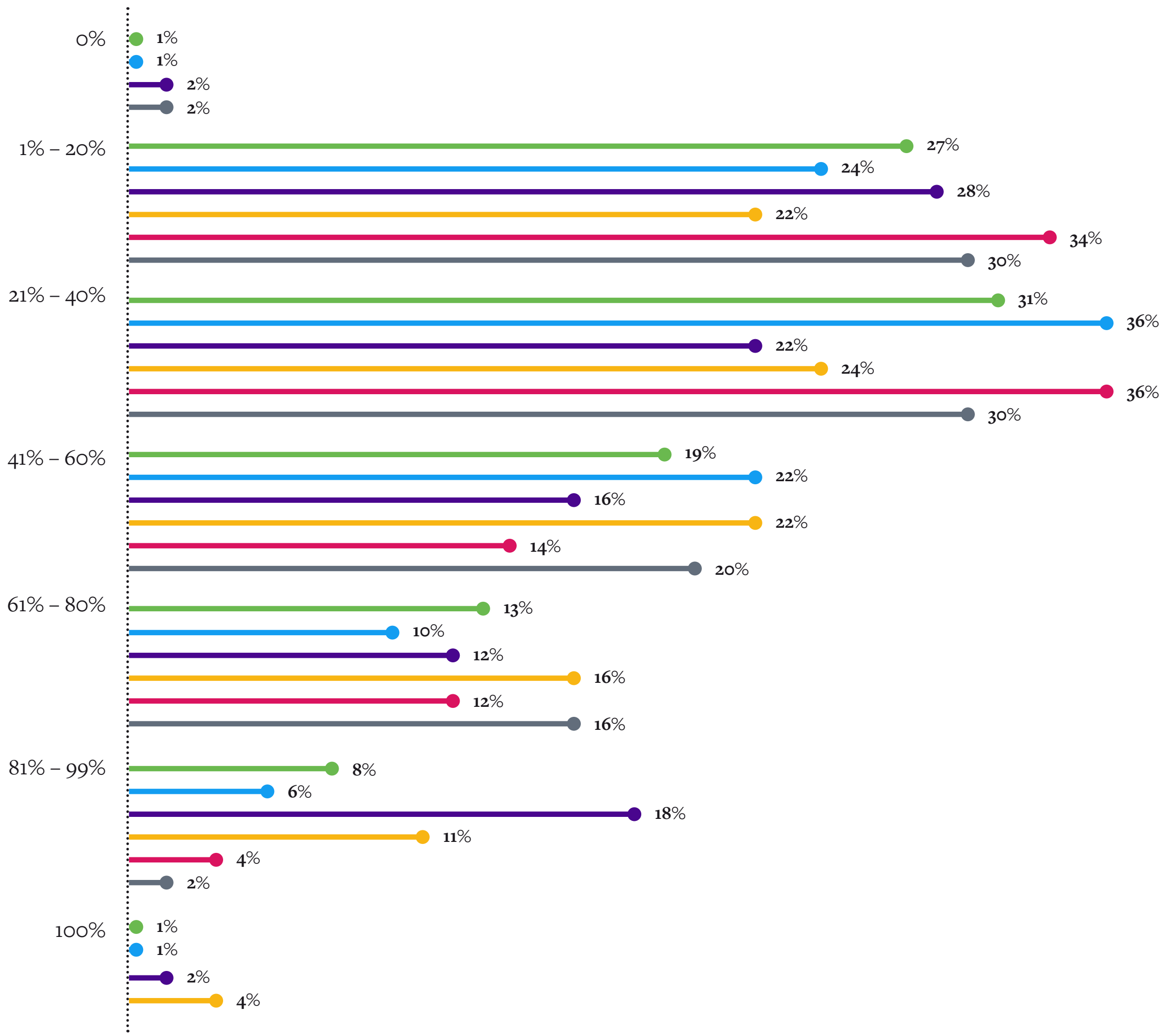
🟦 SOC Managers

🟪 Frontline Employees

40%

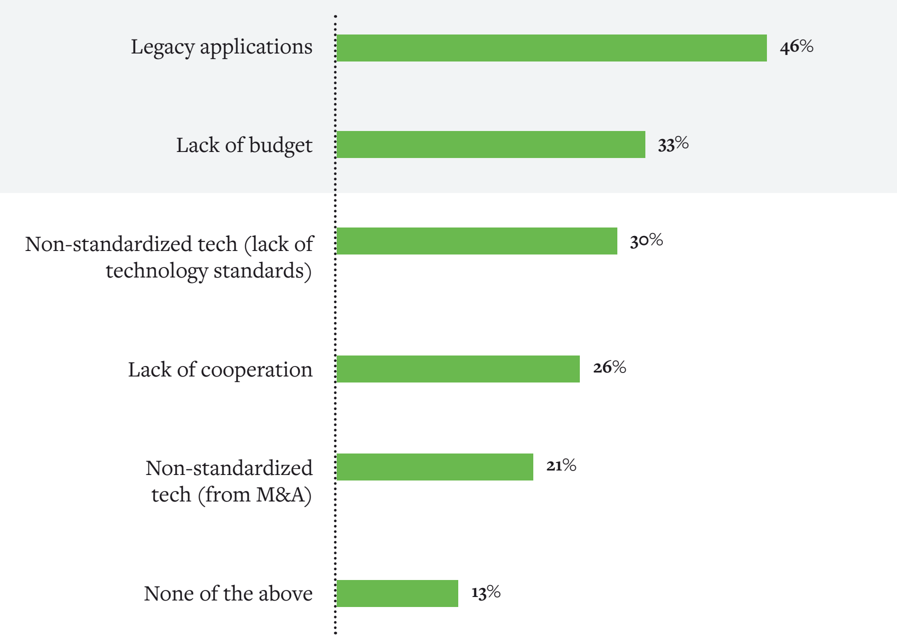
More than half of SOCs log at least 40% of events in their SIEM, with the United Kingdom performing the most logging compared to their counterparts.

PERCENTAGE OF EVENTS SEEN IN SIEM



REASON FOR NOT LOGGING MORE EVENTS IN SIEM

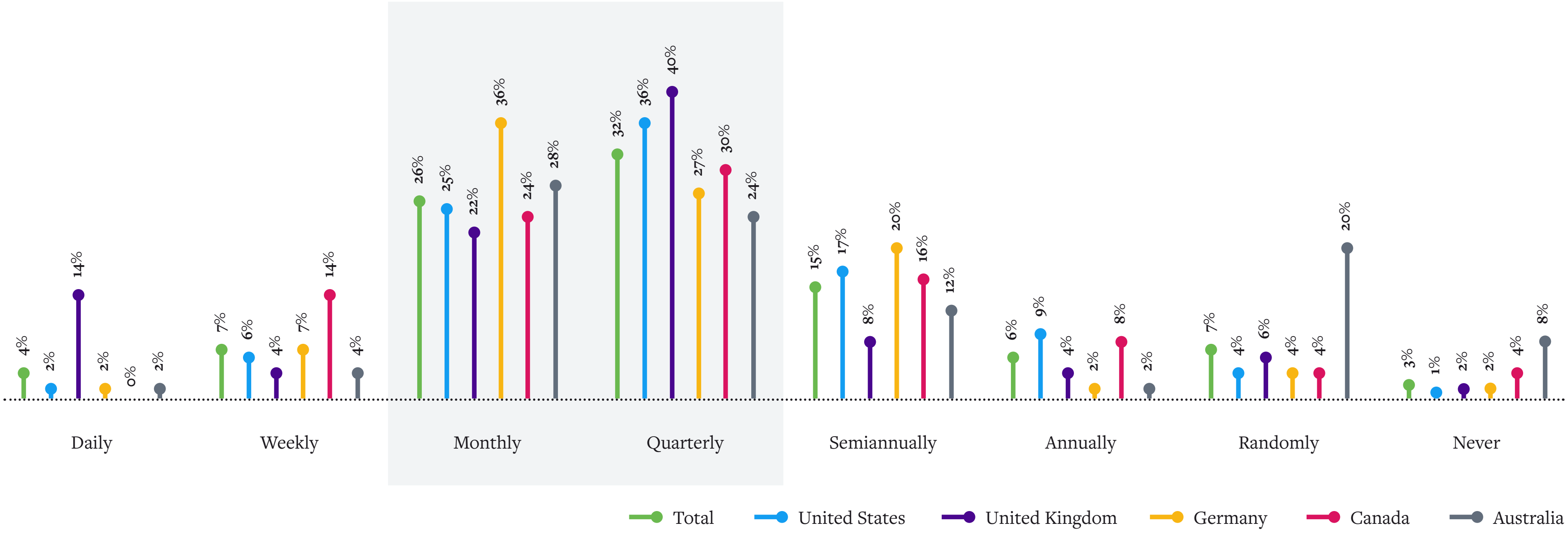
N=282



In terms of training, the majority of SOC training occurs monthly or quarterly, and almost all SOCs outside of Australia have a regular training schedule or plan.

FREQUENCY OF TRAINING

SOC PERSONNEL TRAINING CADENCE, N=295

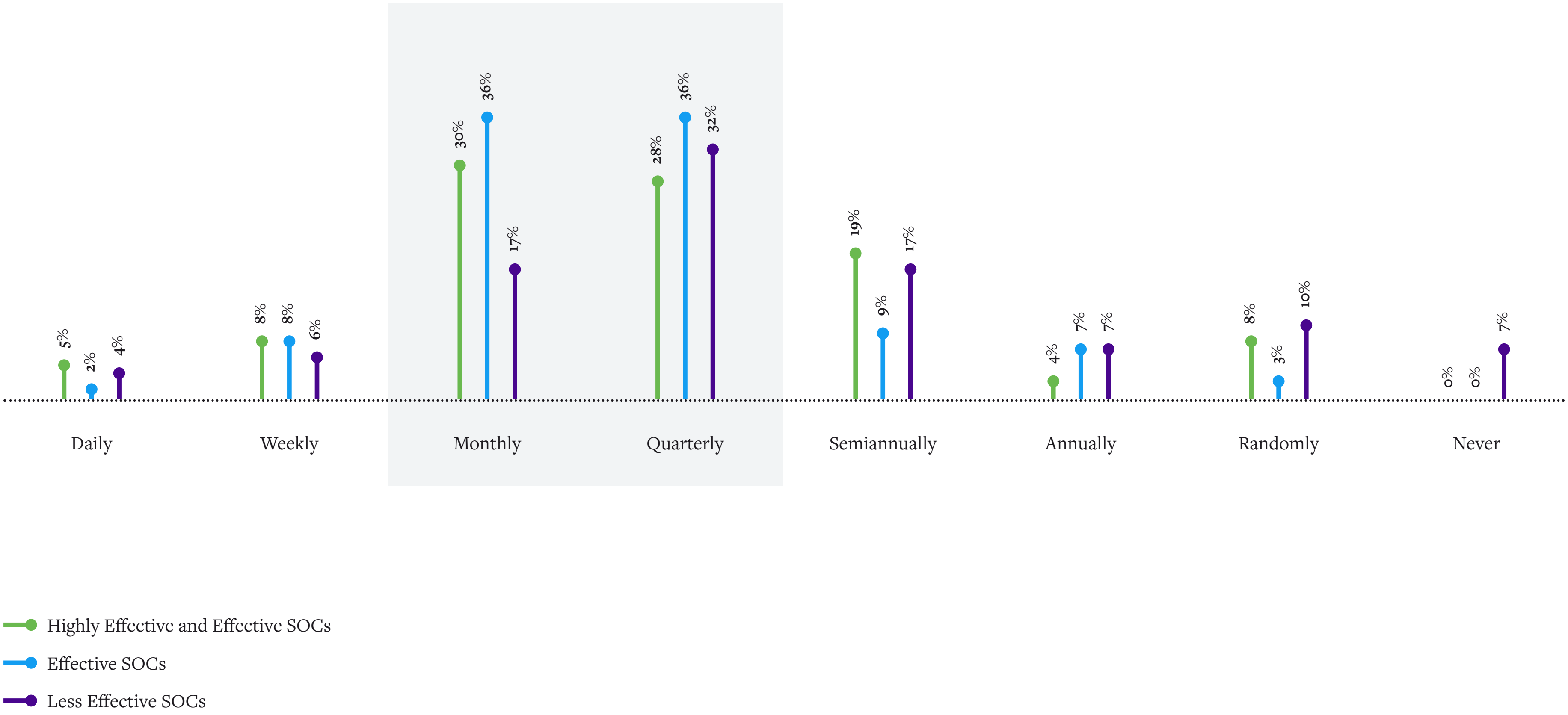


U.S. and U.K. SOCs reported similar YoY trends in training occurring either monthly or quarterly.

Effective SOCs continue to trend toward monthly/quarterly training and are more likely to have structured training.

TRAINING FREQUENCY BY EFFECTIVENESS

SOC PERSONNEL TRAINING CADENCE, N=295

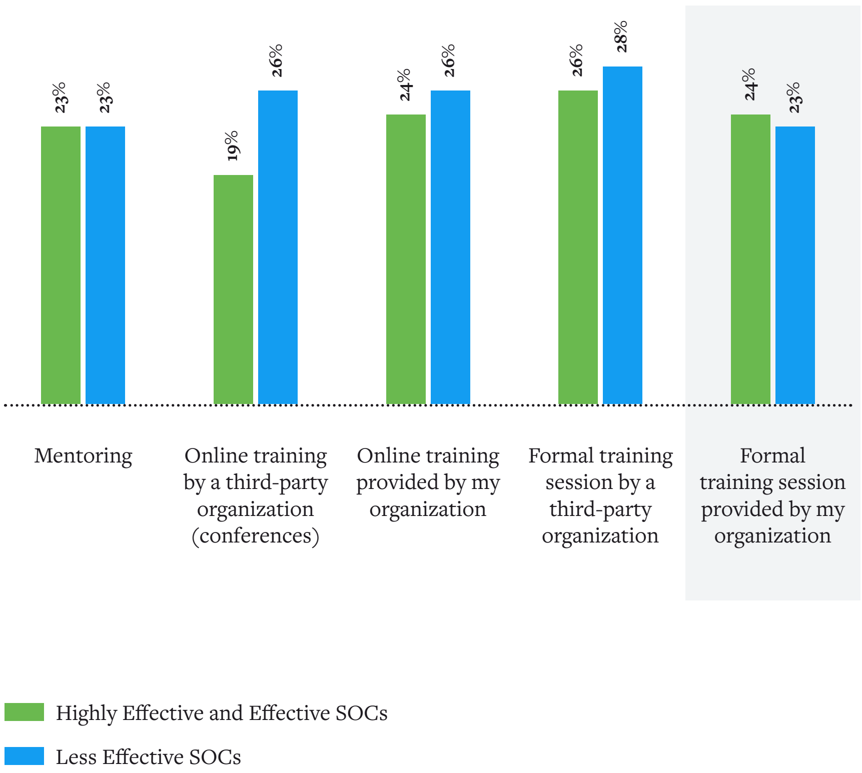


Highly effective and less effective SOCs appear to employ similar training, but the former seems slightly more focused on in-house training.

U.S. and U.K. SOCs have increased YoY training efforts across most categories, with the U.K. specifically increasing the use of online training.

TYPES OF TRAINING

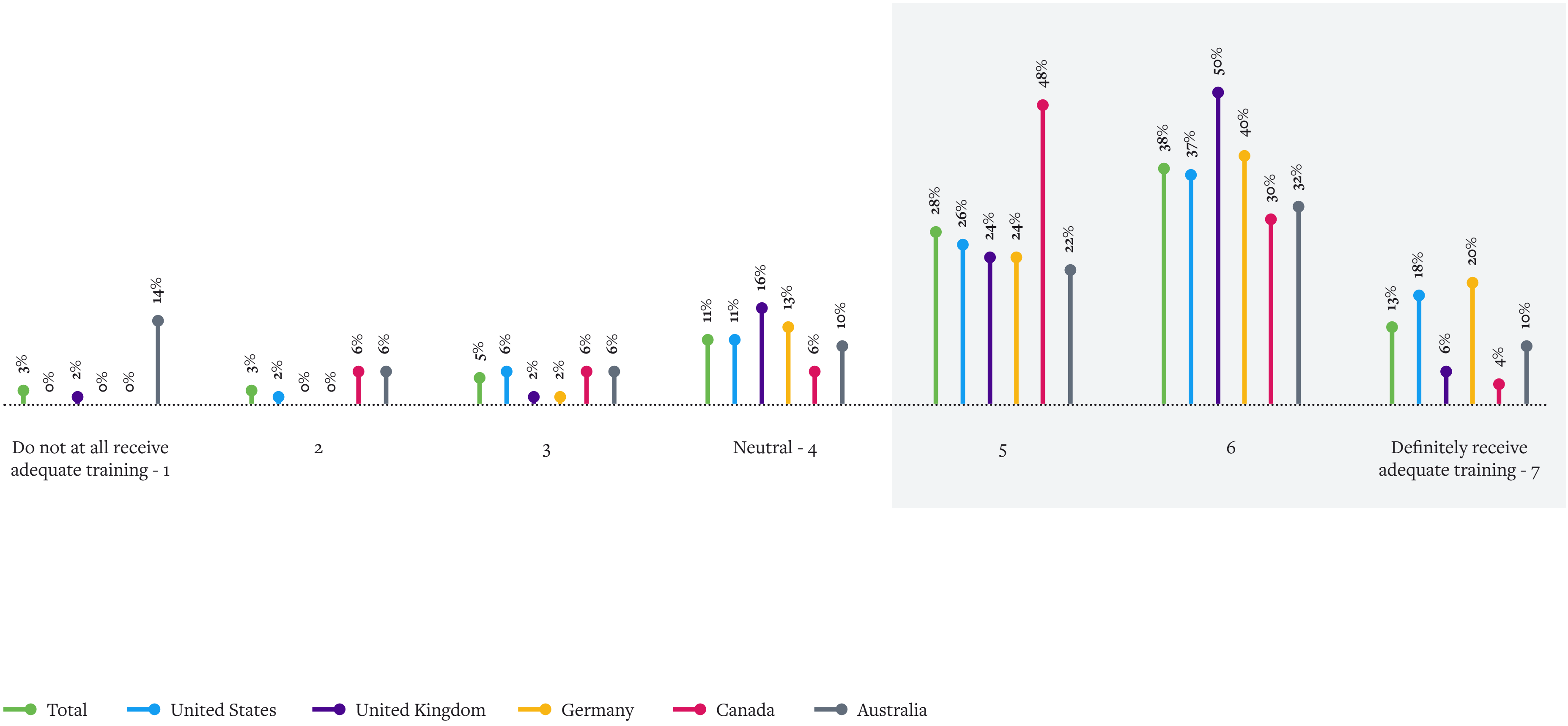
SOC PERSONNEL TRAINING TYPES, N=286



Training quality remains adequate. Potential improvements now include increased updates and budget spends.

QUALITY OF TRAINING

TRAINING ADEQUACY 7-POINT SCALE, N=295



THOUGHTS ON TRAINING

“

I love the fact that we create and ensure our staff is trained with the latest methodology. I would love an increase in training budget to contract out for an outside, latest perspective to our methodology, process, and skill set.”

UNITED STATES

“

Our organization is running tailor-made training to both existing and new entrants. Introduction to general IT environment and risk management is compulsory for new entrants.”

UNITED KINGDOM

“

The training is intense, but it doesn’t inform our technicians when a new virus is found and how to quickly patch the network in time to reduce an infection.”

CANADA

“

Well organized, interesting, with many case studies and latest IT development.”

GERMANY

“

Thorough – Identifies most scenarios possible to eventuate and addresses these all individually.”

AUSTRALIA

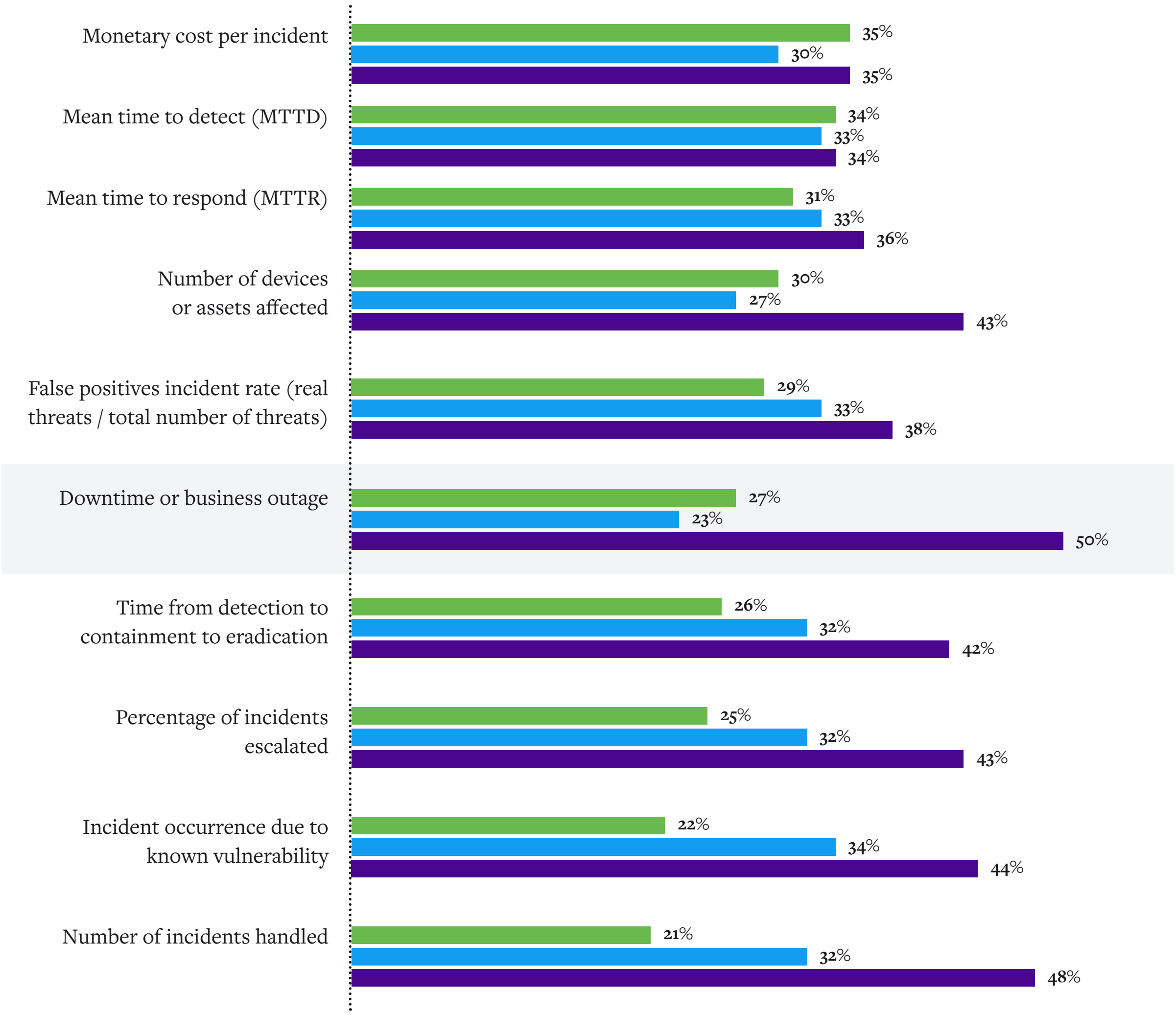
Much like past years, small SOCs are more concerned with downtime or business outage as an operational metric than SOCs with 25+ team members.

21%

U.S. remains fairly aligned in nearly all categories; however, U.K. SOCs reported a 21% point YoY increase in tracking **the number of incidents handled.**

METRICS TRACKED BY SOC SIZE

TOP METRICS COMMONLY TRACKED BY THE SOC, N=295



🟩 Large SOC: *200+ Team Members*

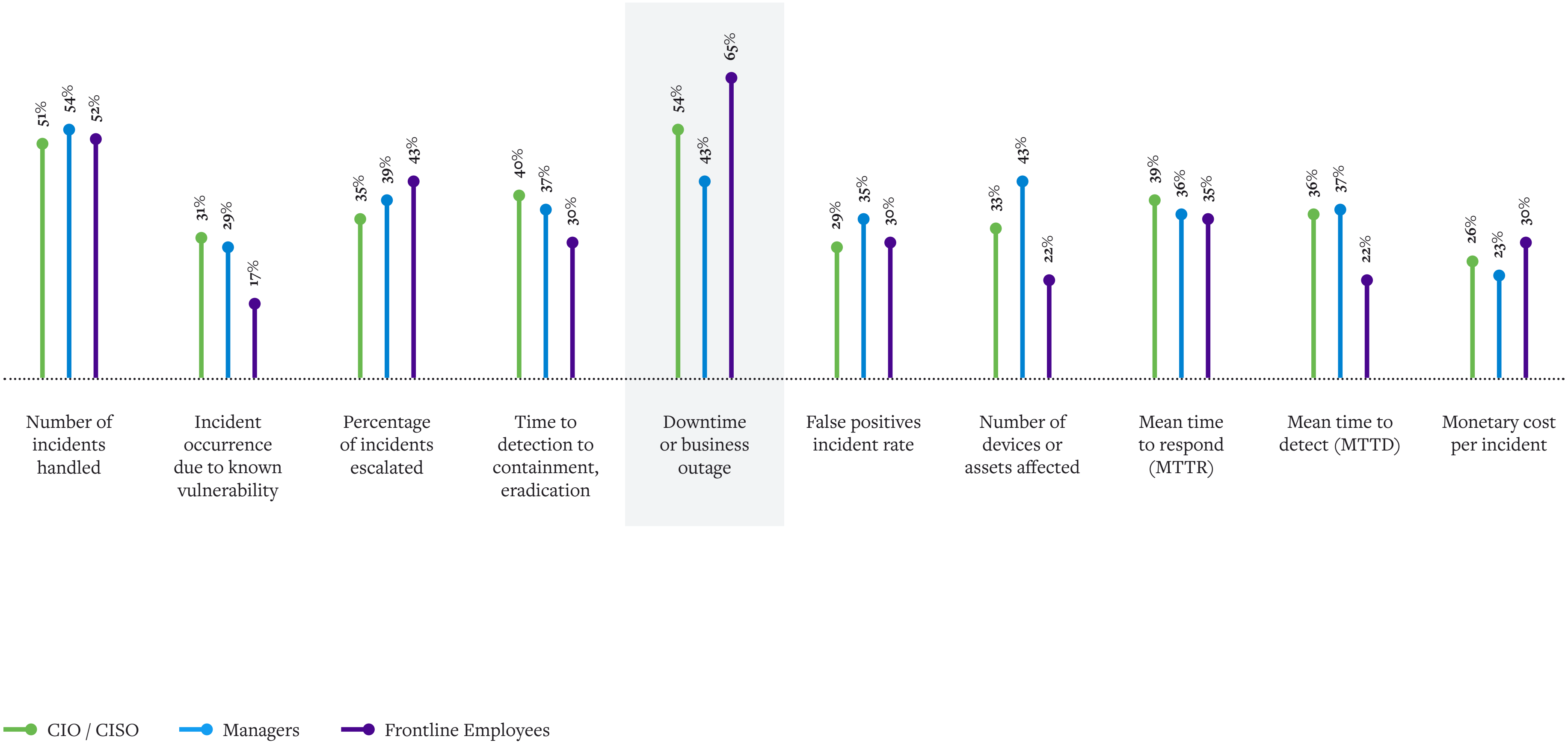
🟦 Medium SOC: *25-199 Team Members*

🟪 Small SOC: *1-24 Team Members*

By role, we see that downtime or business outage is a concern of all employees, and especially those on the frontlines.

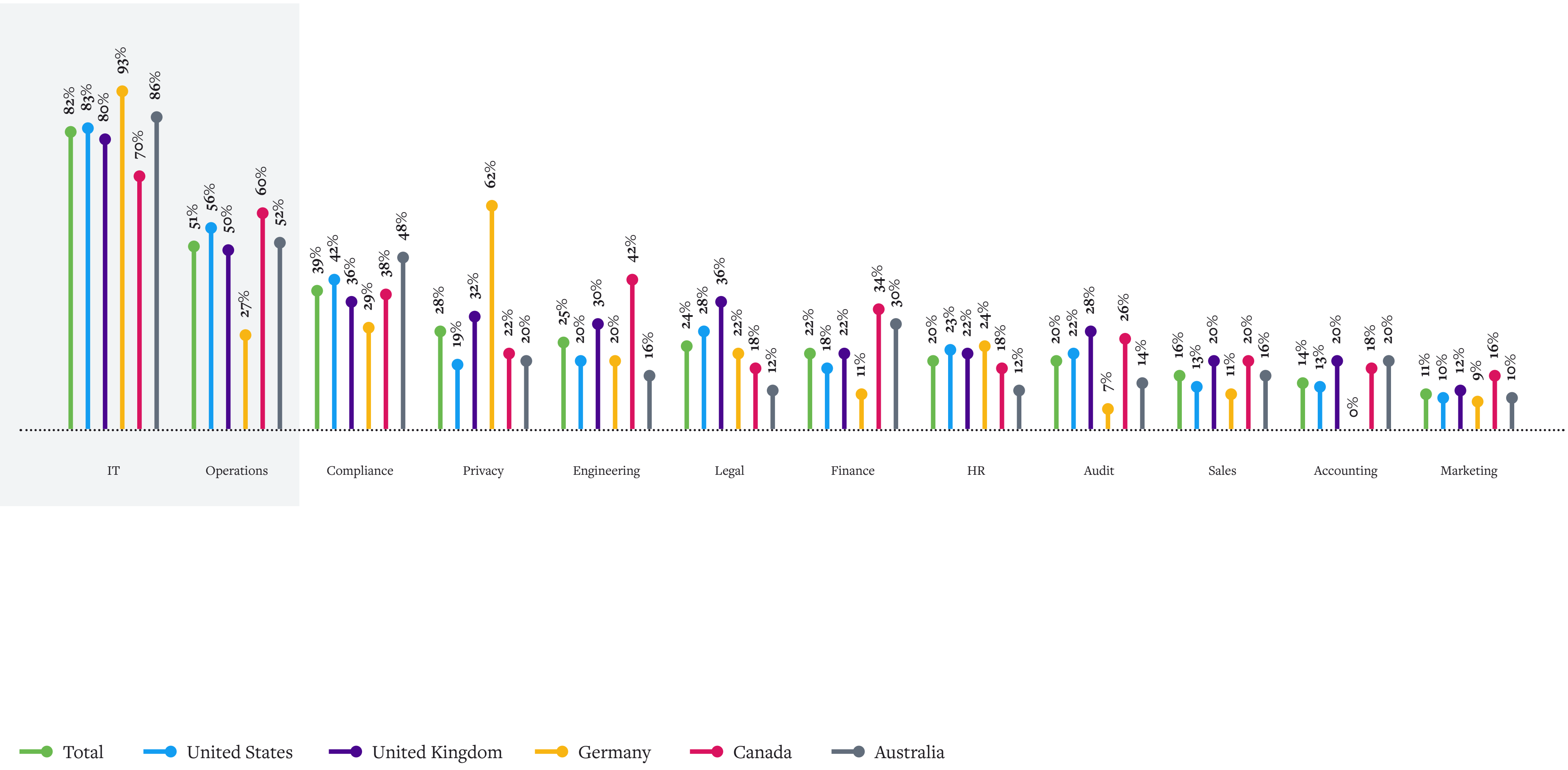
METRICS TRACKED BY ROLE

TOP METRICS COMMONLY TRACKED BY THE SOC, N=295

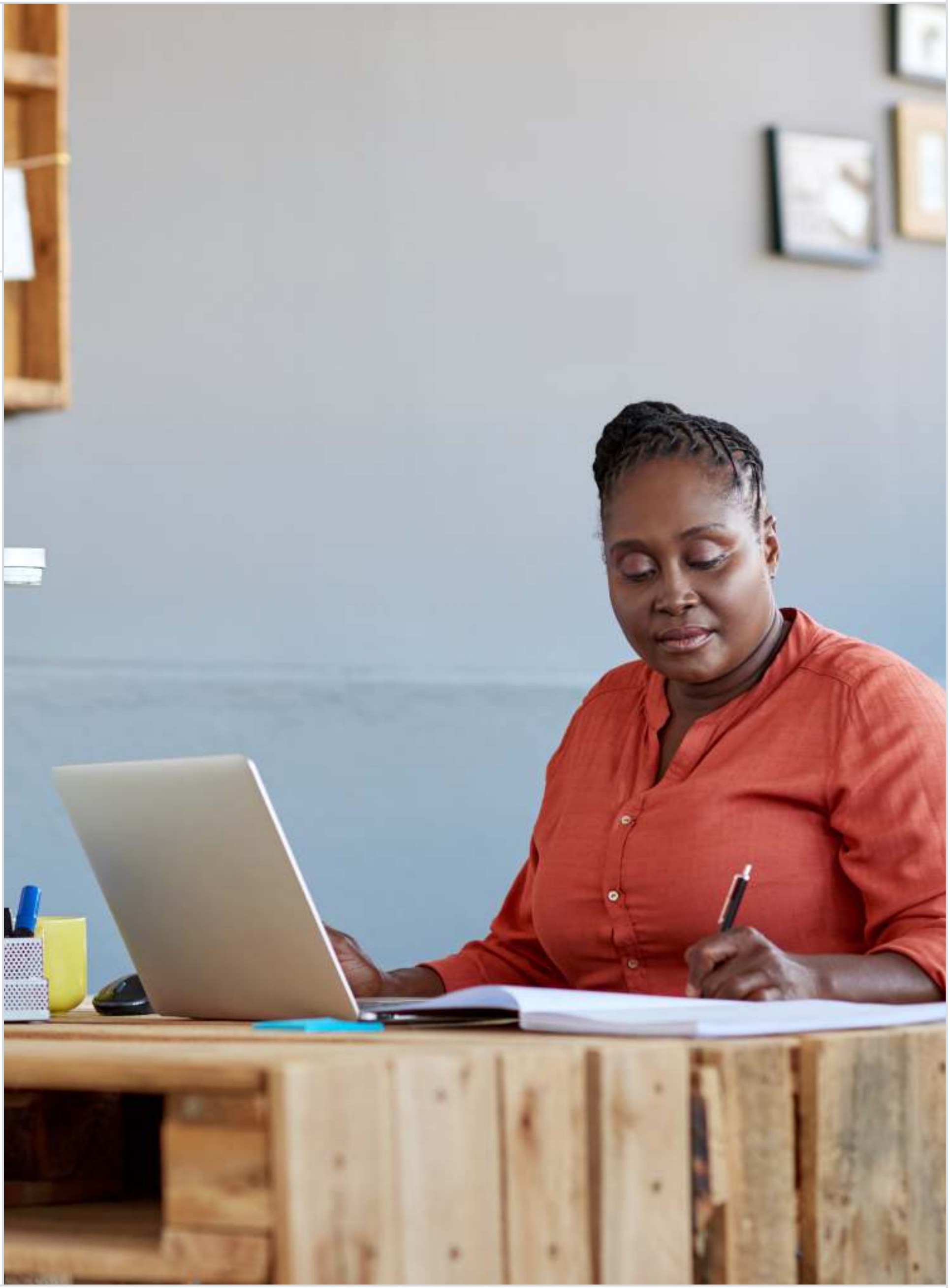


Unsurprisingly, most SOCs continue to collaborate with IT and Operations, and German SOCs, specifically, also have a high interaction with Privacy.

DEPARTMENTS OF COLLABORATION



Technology

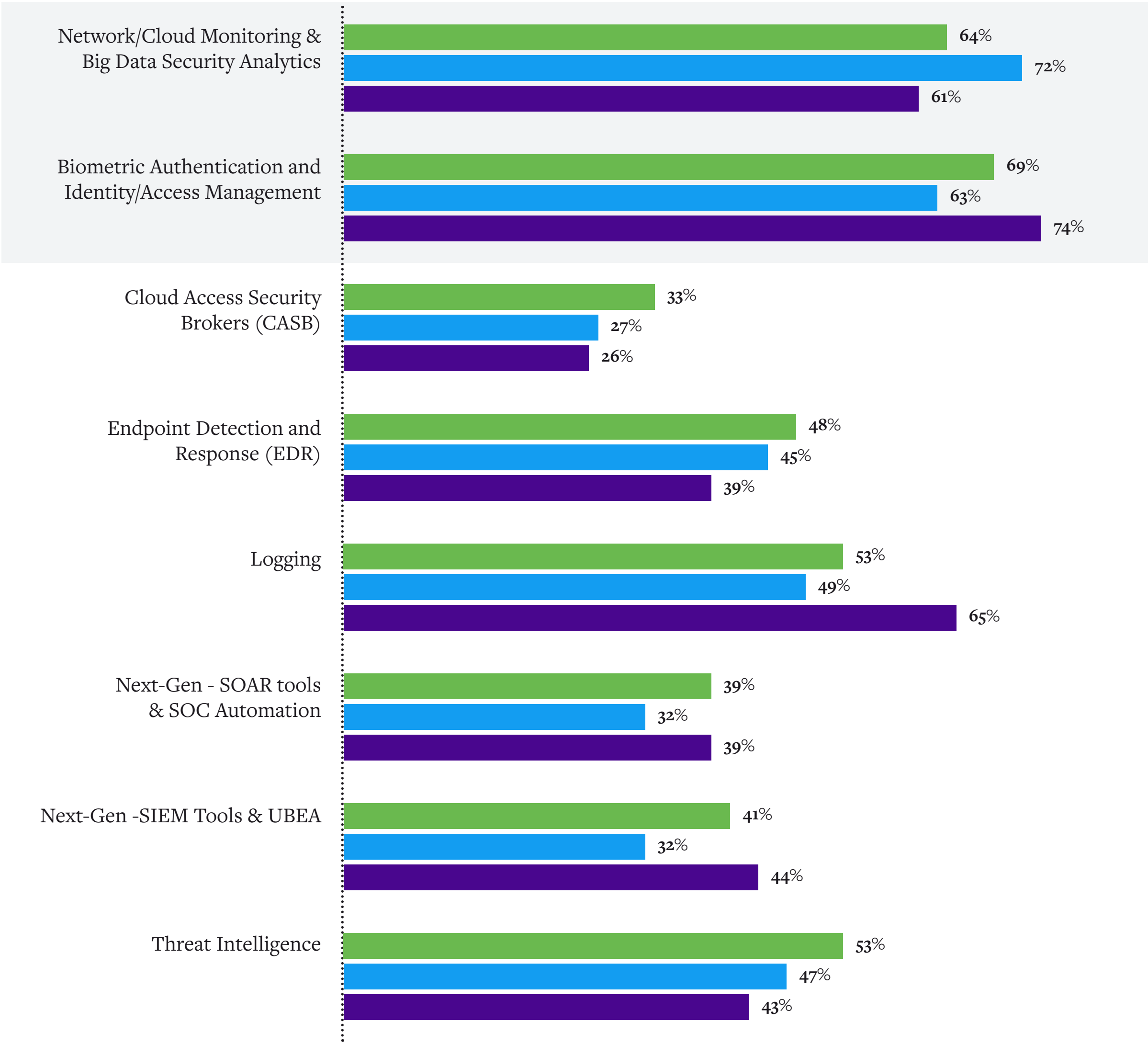


You'll find the following topics covered in this section:

1. SOC PRIORITIES
2. UPTAKE OF NEXT-GEN TOOLS
3. SECURITY ALERTS AND COORDINATION WITH IT AN SOC PAIN POINT…
4. …ACROSS ALL SOC ROLES, PARTICULARLY FRONTLINE EMPLOYEES

Monitoring/analytics, access management, and logging are now high priorities for all SOC roles.

CURRENT TECHNOLOGY USAGE BY ROLE



🟩 CIO / CISO

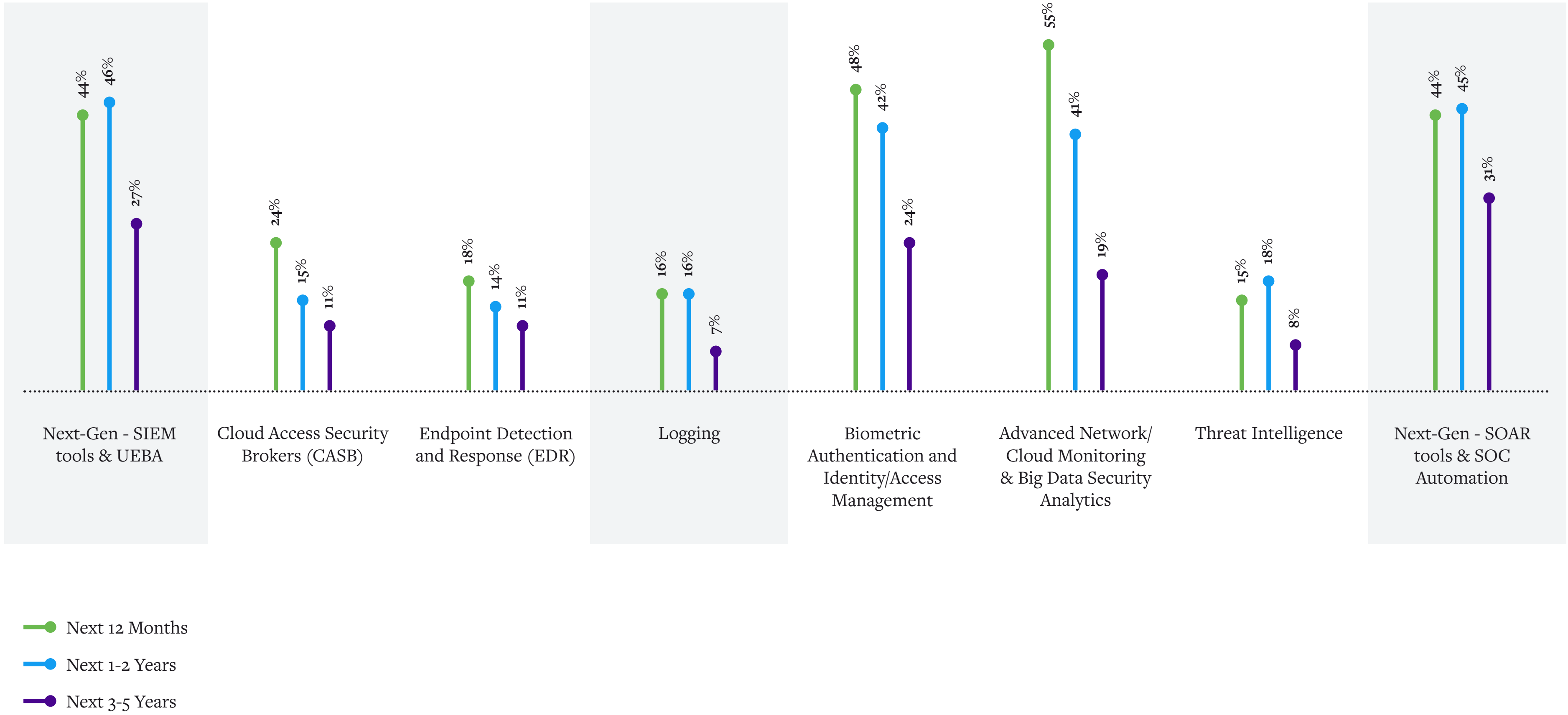
🟦 Managers

🟪 Frontline Employees

Most SOCs now expect Next-Gen SIEM tools/UEBA and Next-Gen SOAR tools & SOC Automation will take precedence in the coming years.

FUTURE TECHNOLOGY USAGE

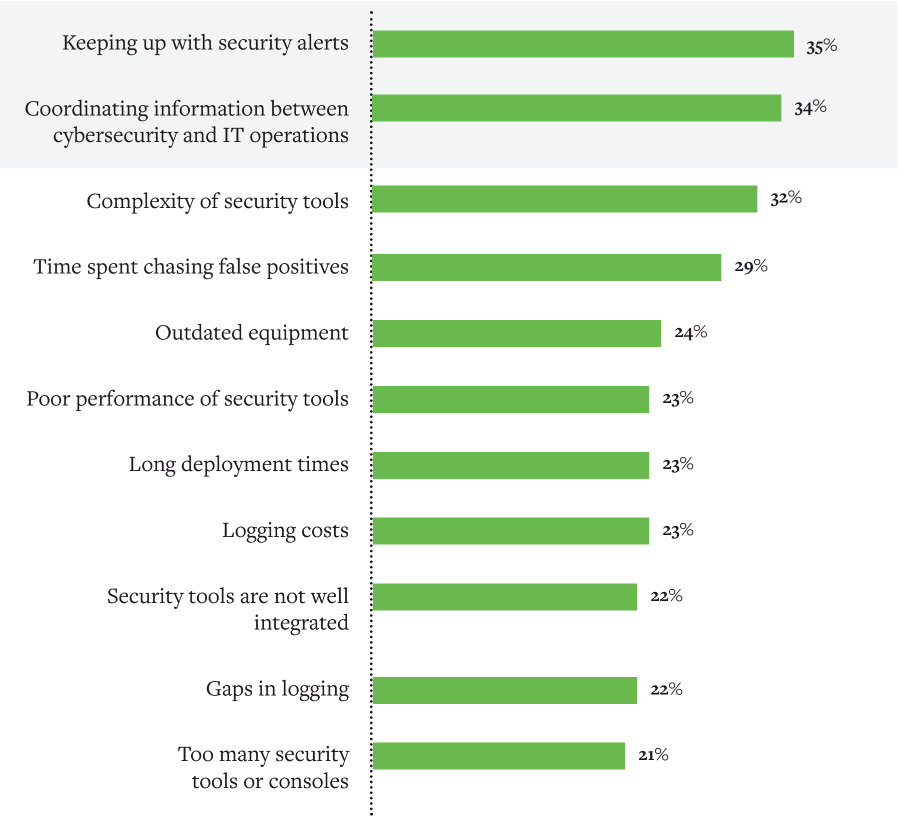
N=295



Keeping up with security alerts and coordinating information between cybersecurity and IT remains a common pain point across all SOCs...

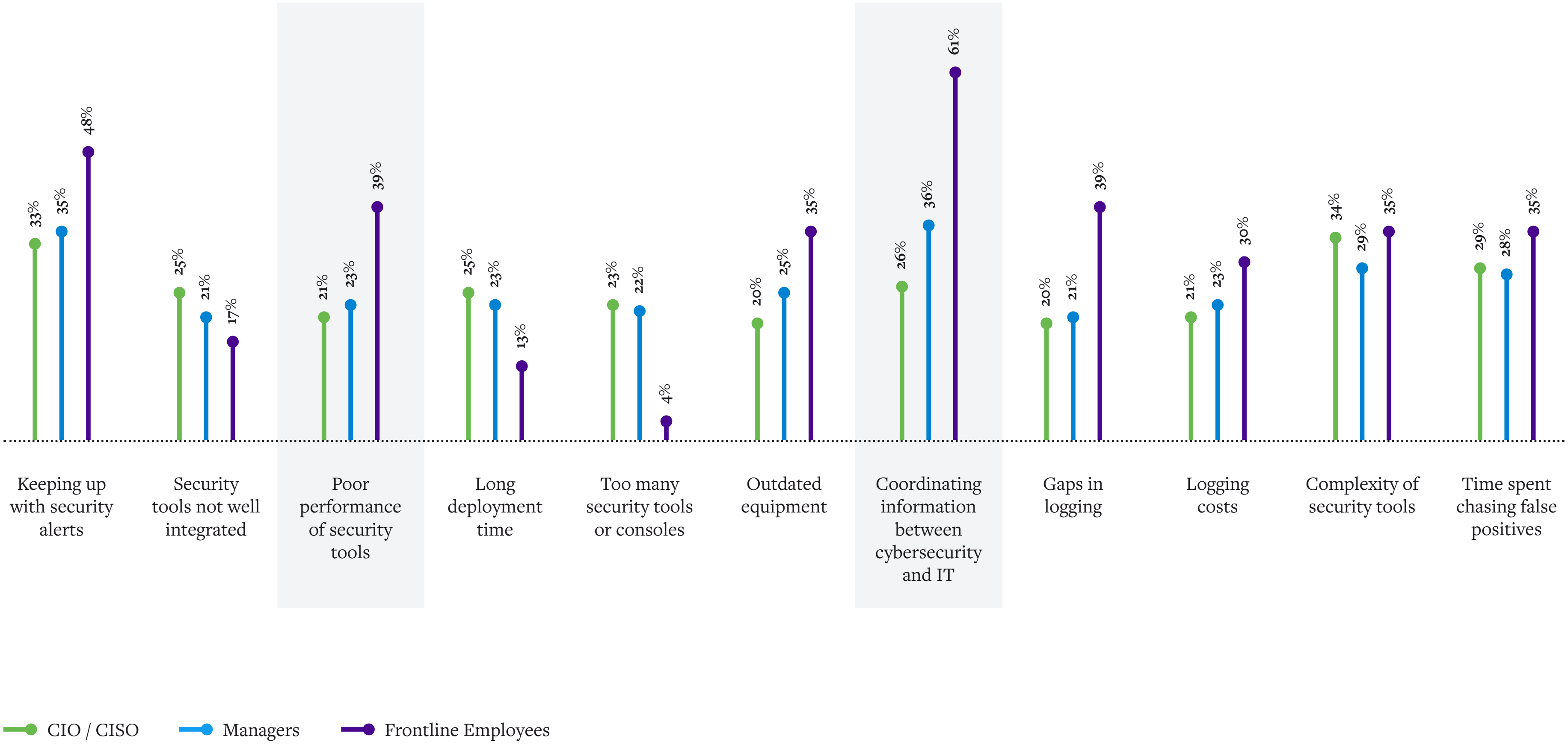
PAIN POINTS IN TECHNOLOGY

COMMON PAIN POINTS EXPERIENCED IN THE SOC FOR TECHNOLOGY, N=295



...and across all SOC roles, particularly frontline employees, with poor performance of tools also finding extra emphasis in the frontline.

PAIN POINTS IN TECHNOLOGY BY ROLE



Finance and Budget

You'll find the following topics covered in this section:

1. STAFFING
2. TASK AUTOMATION
3. FUNDING FOR TECHNOLOGY
4. ADDITIONAL STAFFING
5. FURTHER INVESTMENTS
6. RISK INSURANCE

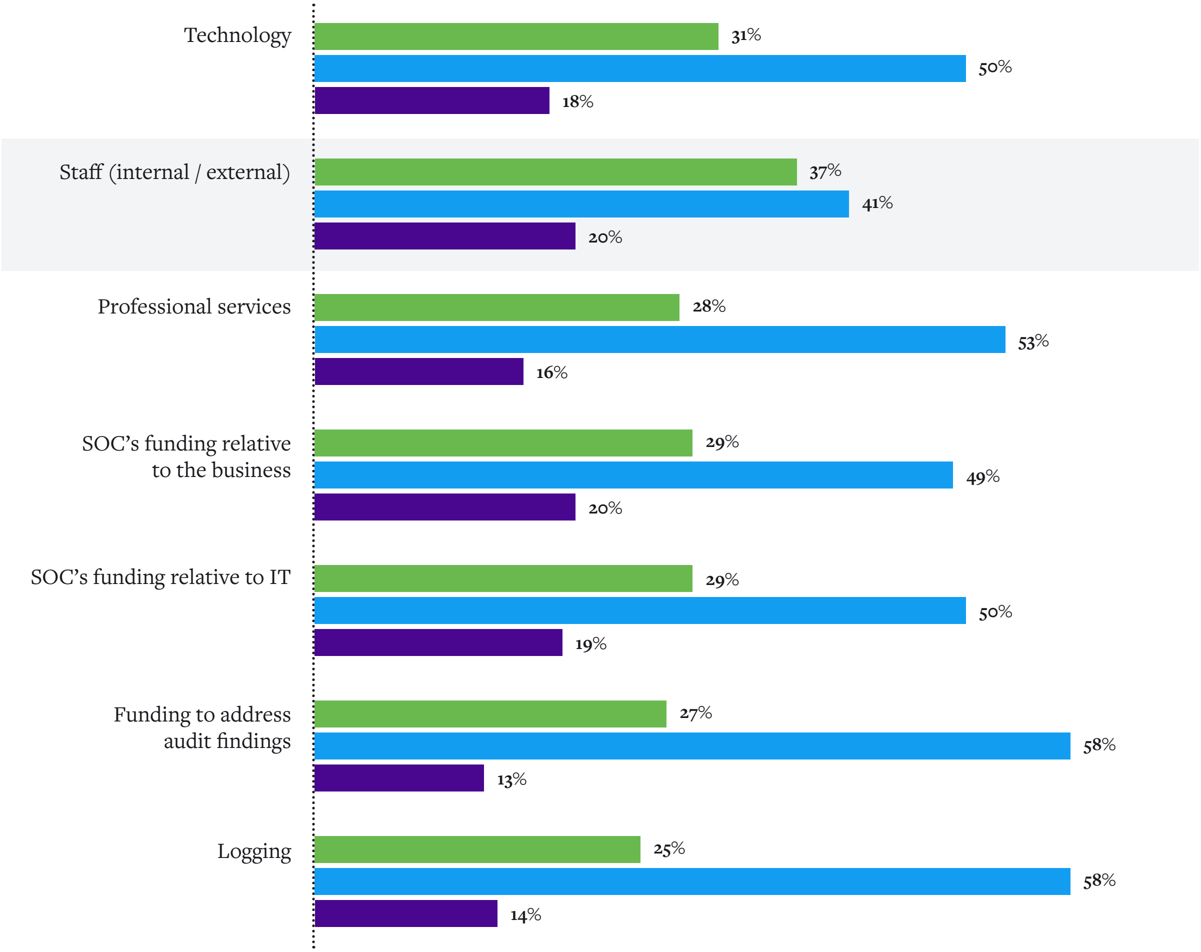
40%

Wave 3 observed nearly 40% of SOCs shifting to Staffing as now being most underfunded.

In the U.K., **underfunding for technology doubles** while U.S. funding remains fairly constant YoY.

FUNDING DISTRIBUTION BY AREA

SOC AREAS AND THEIR FUNDING LEVEL, N=295



🟩 Underfunded

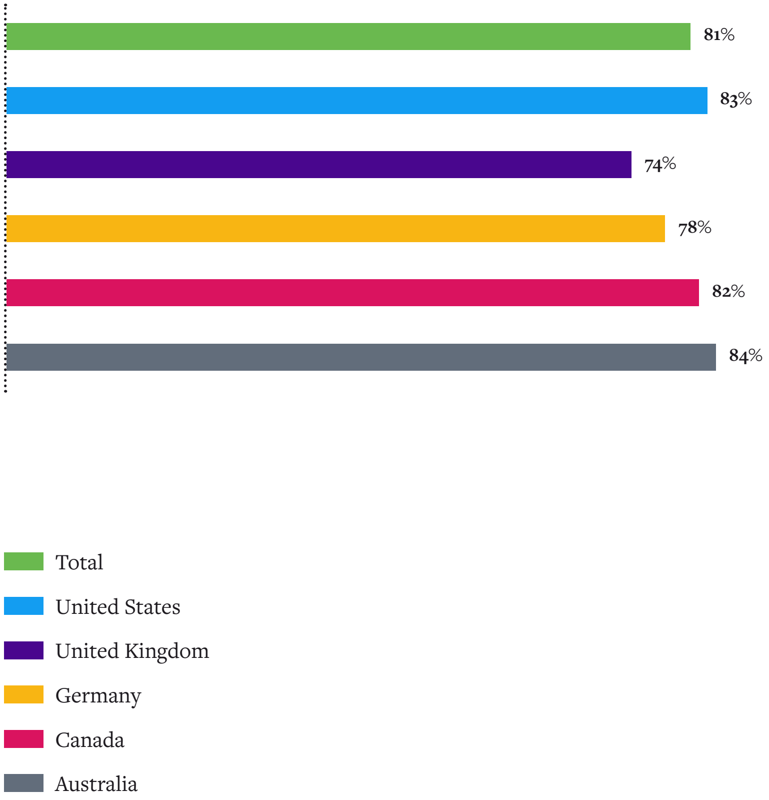
🟦 Correctly funded

🟪 Overfunded

SOCs across all geographies feel that Task Automation is important to their work.

IMPORTANCE OF TASK AUTOMATION IN SOC

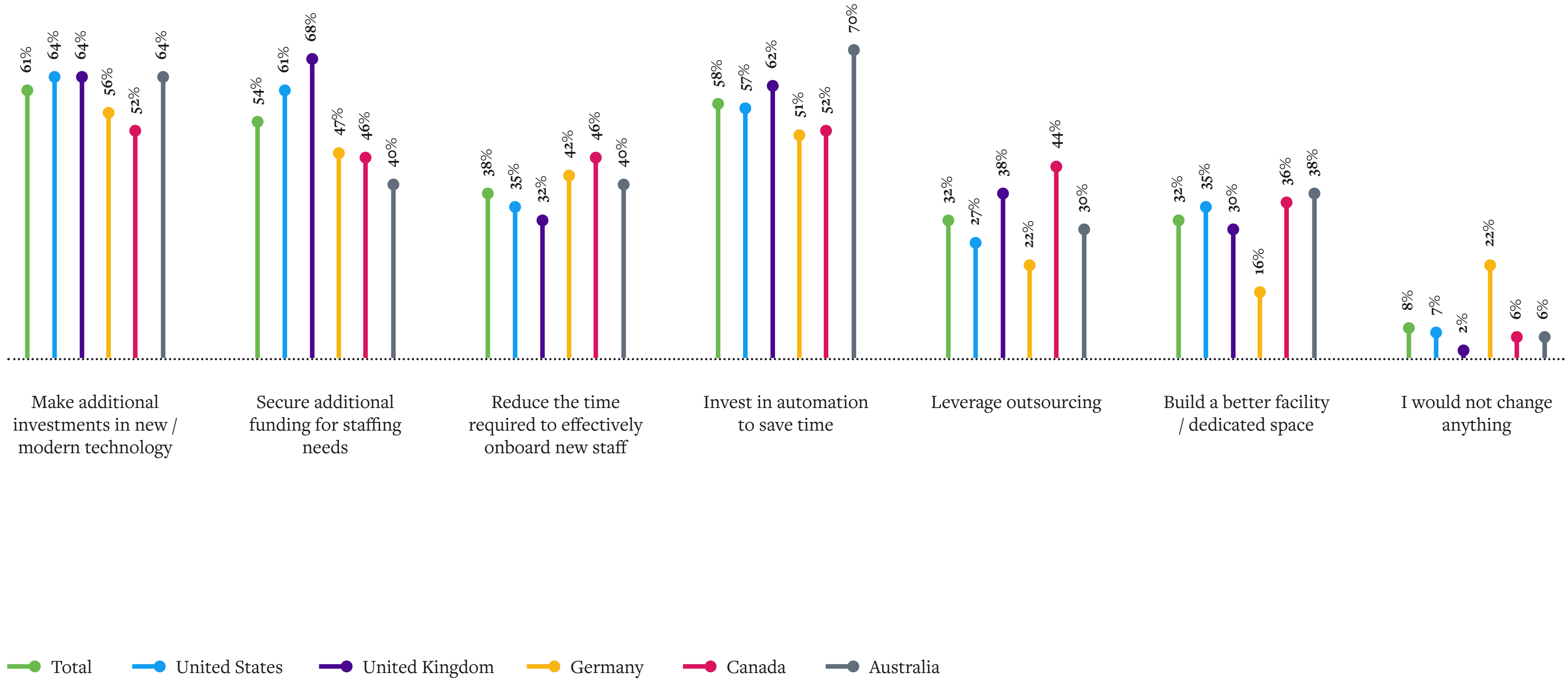
TOP 2, N=295



Despite a continued rise in funding for technology, SOC personnel recommend continued investment in new/modern technologies and automation.

CHOSEN METHODS TO IMPROVE SOC

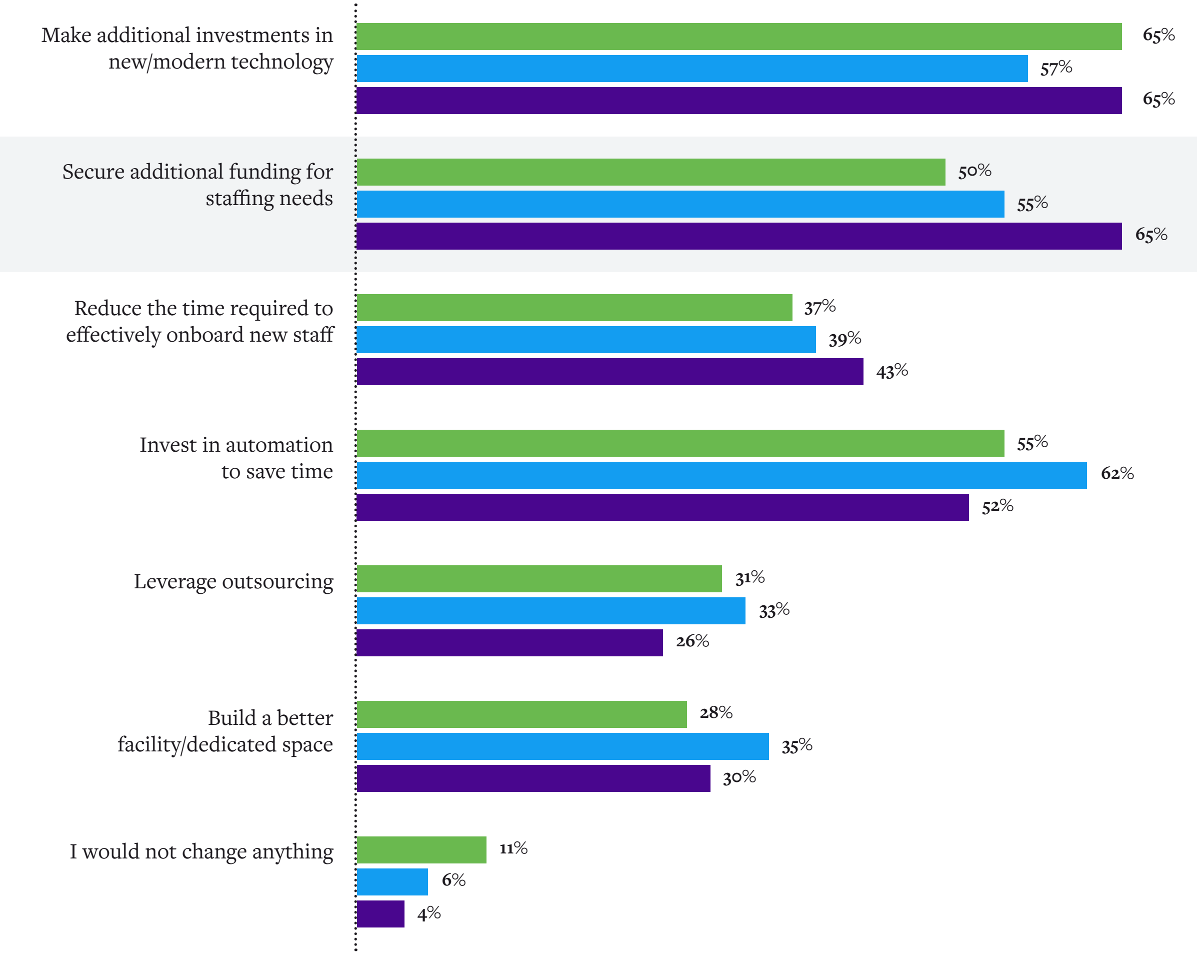
WHAT SURVEY RESPONDENTS WOULD CHANGE ABOUT THEIR SOC, N=295



Frontline employees suggest additional staffing funding significantly more than their superiors, although all roles tend to agree on SOC changes...

CHOSEN METHODS TO IMPROVE SOC

WHAT SURVEY RESPONDENTS WOULD CHANGE ABOUT THEIR SOC, N=295



🟩 CIO / CISO

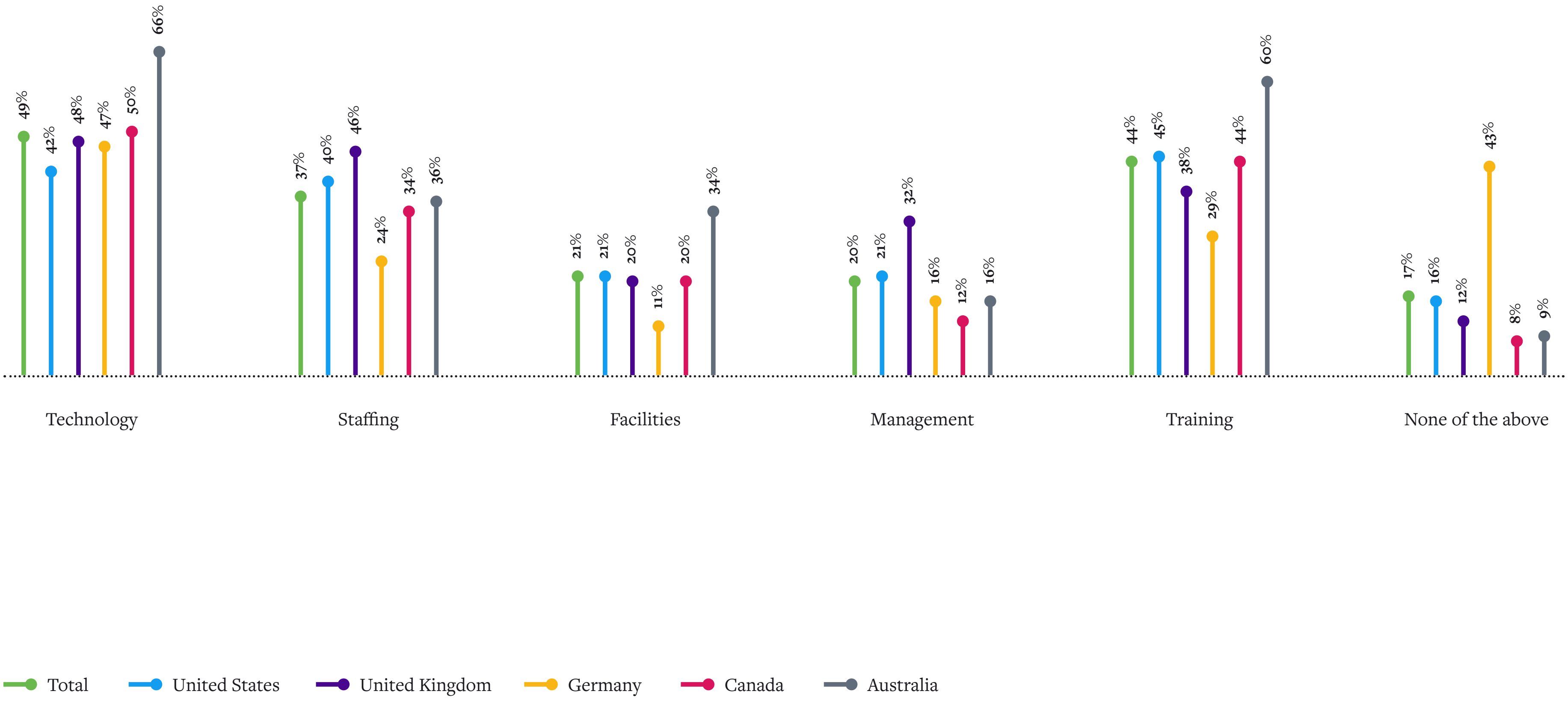
🟦 Managers

🟪 Frontline Employees

...and would like to see further investments in technology, training, and staffing.

FUNDING DISTRIBUTIONS

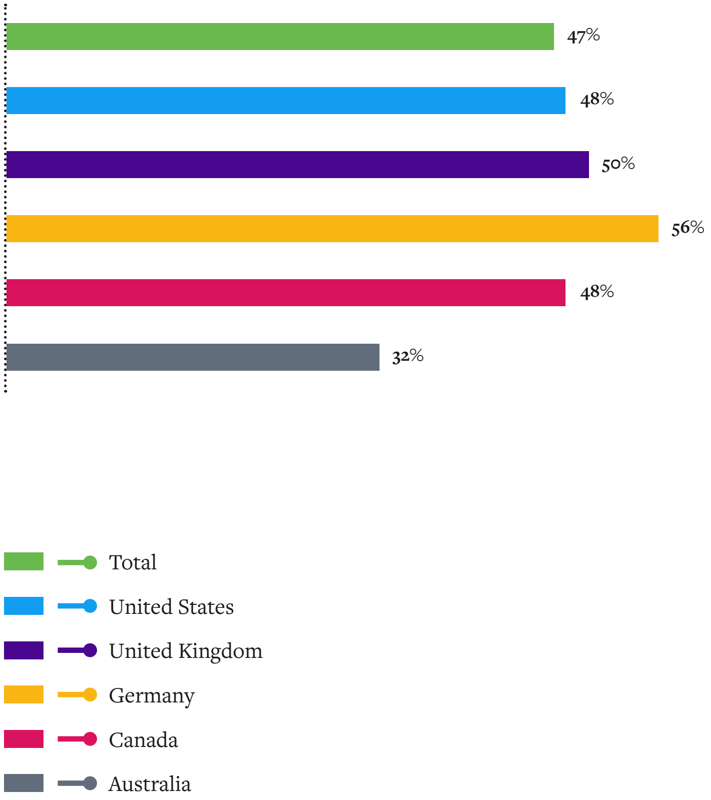
SOC AREAS THAT ARE BELIEVED TO BE UNDERFUNDED; N=295



Concerning risk insurance, Europe takes precedence over its global counterparts in possessing first-party risk insurance, focused on compliance.

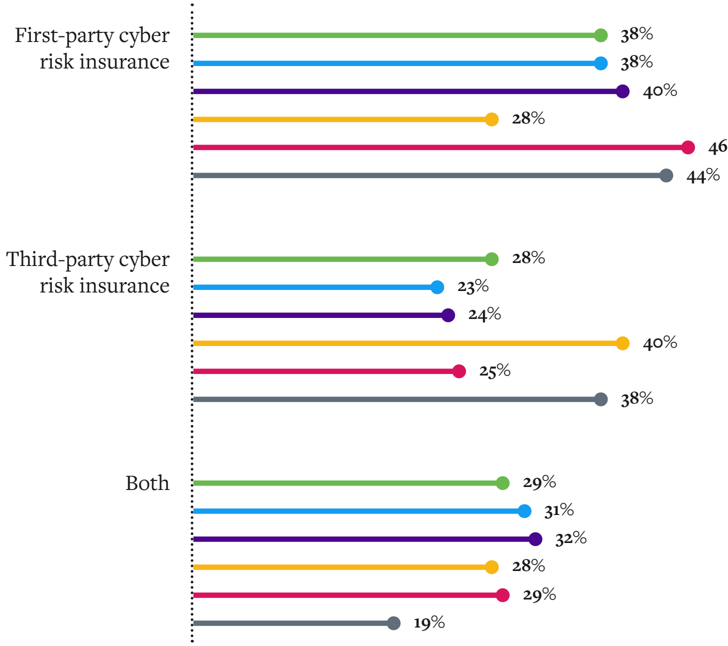
POSSESSION OF CYBERSECURITY INSURANCE

YES, N=295



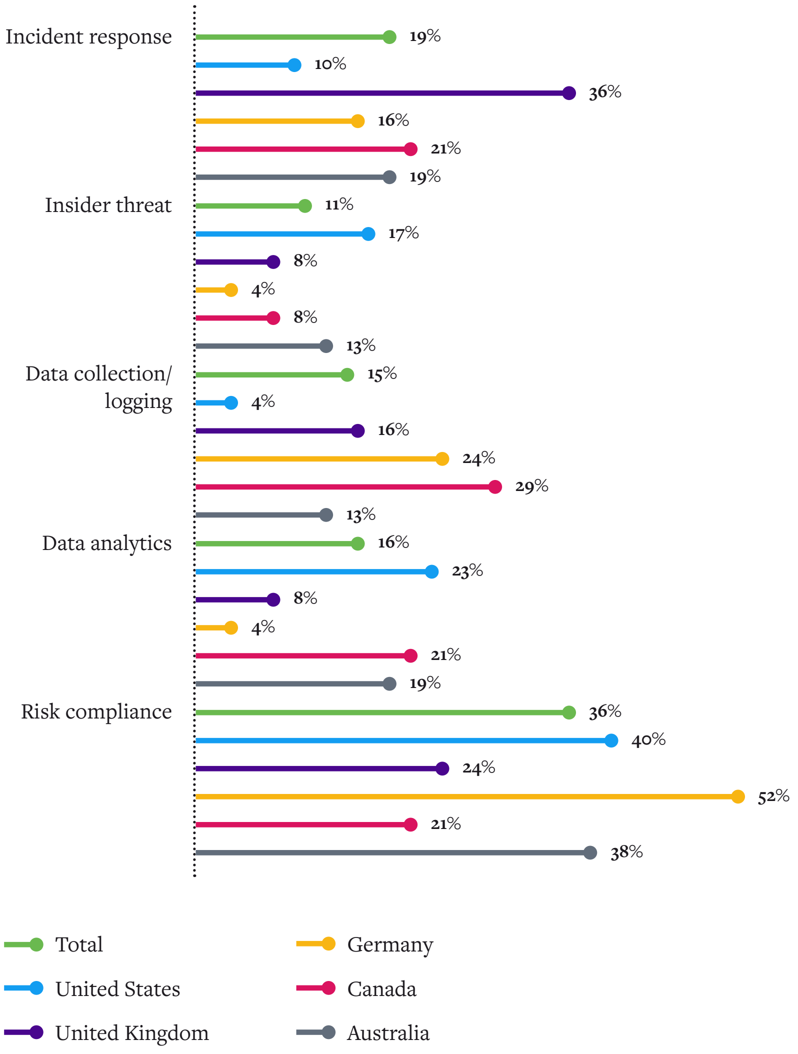
TYPE OF INSURANCE COVERAGE

N=138



UNDERWRITER ATTENTION TO TOPICS

N=138



Appendix 1: Trends

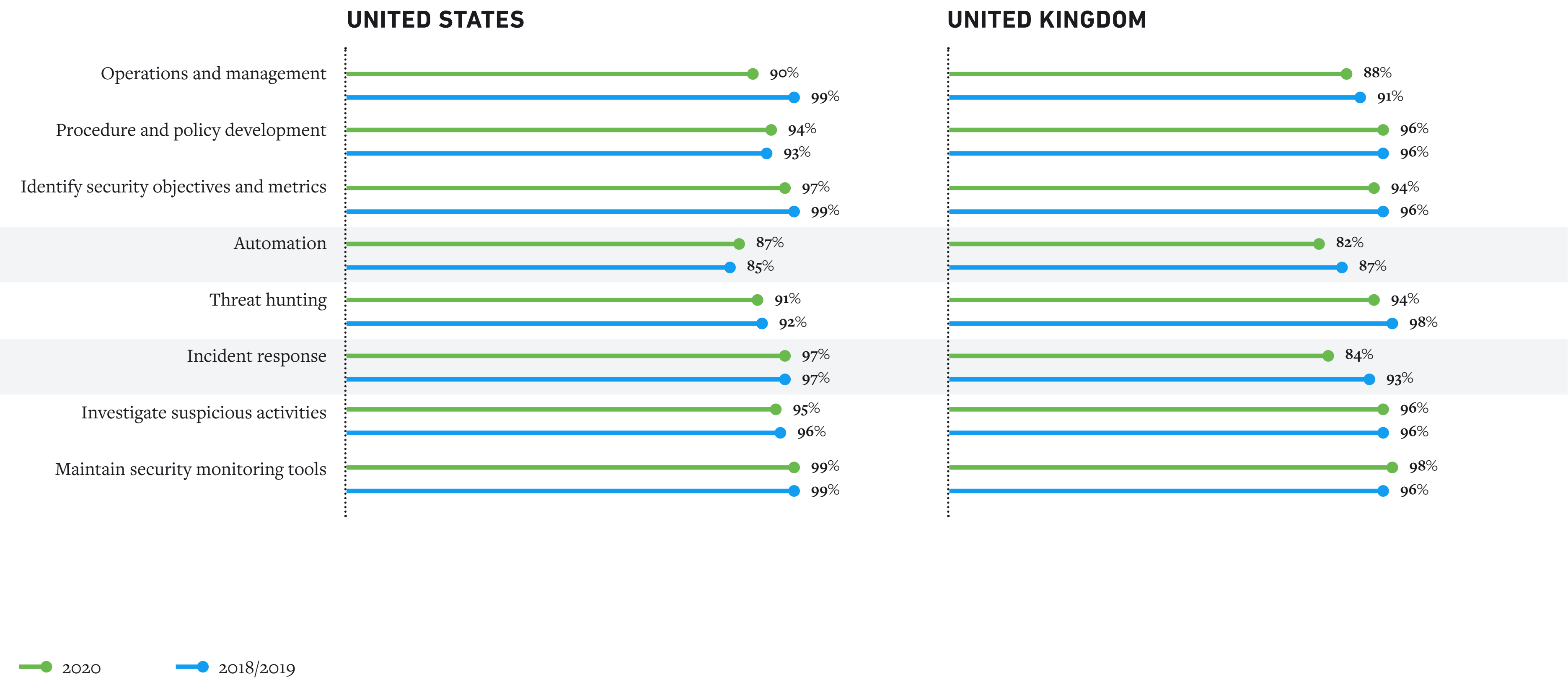
You'll find the following topics covered in this section:

1. INCIDENT RESPONSE AND AUTOMATION
2. OUTSOURCING
3. CORRECT STAFFING
4. IMPORTANCE OF SKILLS IN U.K. SOCS
5. SOFT SKILL ABILITIES BY REGION
6. HARD SKILL ABILITIES BY REGION
7. IDENTIFYING CANDIDATES
8. DECLINES IN THREAT MODELING, ETC. IN U.S. AND U.K. SOCS
9. CHALLENGE OF INEXPERIENCED STAFF
10. MONTHLY, QUARTERLY TRAINING
11. INCREASED TRAINING BY U.S. AND U.K. SOCS
12. INCIDENT TRACKING BY U.S. AND U.K. SOCS
13. TECHNOLOGY FUNDING BY U.S. AND U.K. SOCS

More than a 5% point YoY decline can be observed in the top two responses on SOC responsibilities around incident response and automation in U.K. SOCs.

SOC RESPONSIBILITIES

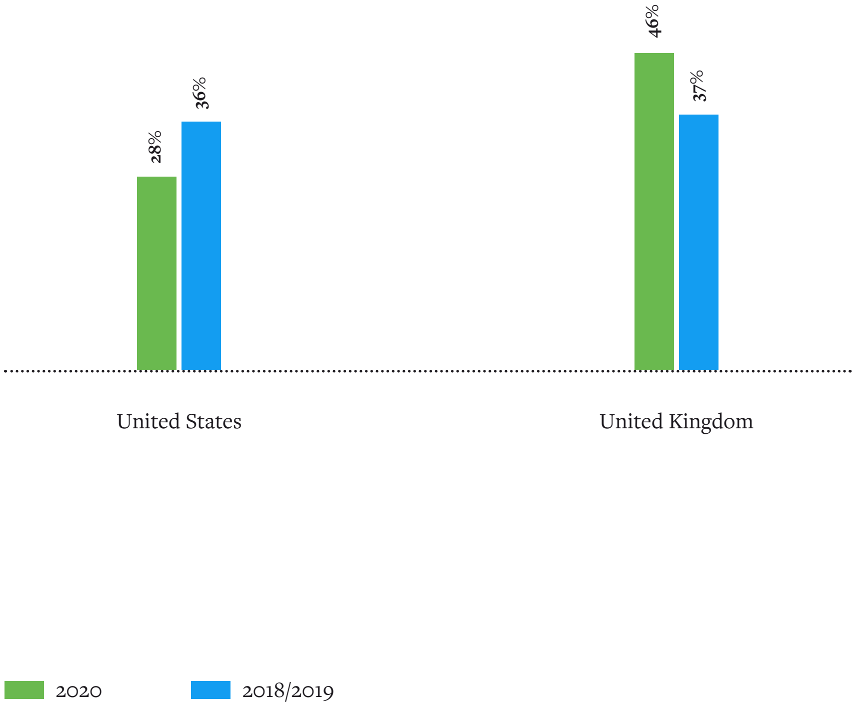
2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, TOP 2, MY ROLE AND RESPONSIBILITIES THAT FALL UNDER THE SOC; N=339



U.S. SOCs are less outsourced now as compared to 2018/2019 (36% to 28%), whereas U.K. SOCs are now being outsourced more (37% to 46%).

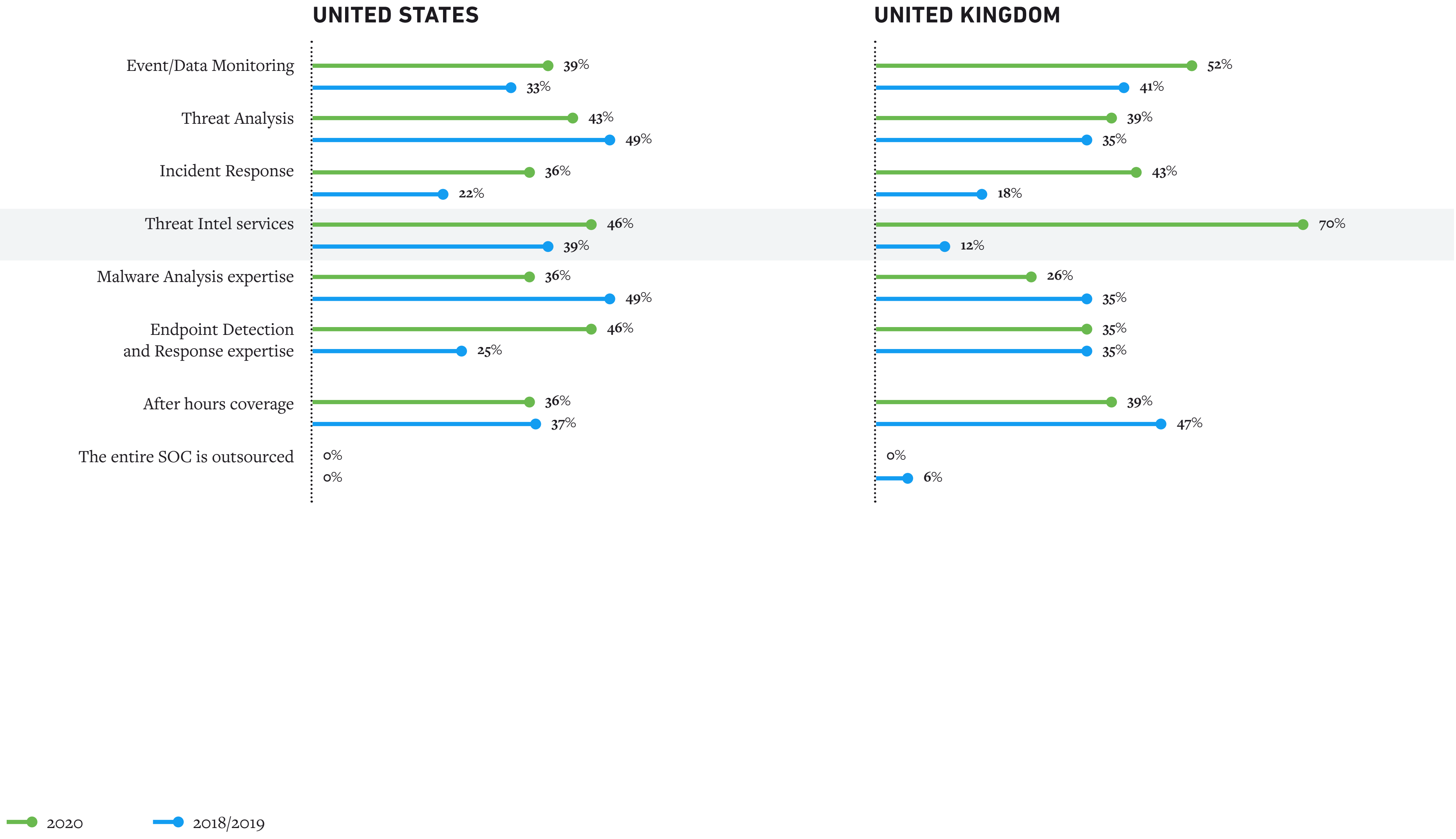
OUTSOURCING

2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, USE OF OUTSOURCING OR CONTRACTING, N=339



OUTSOURCED FUNCTIONS

2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, FUNCTIONS OUTSOURCED OR CONTRACTED OUT, N=339

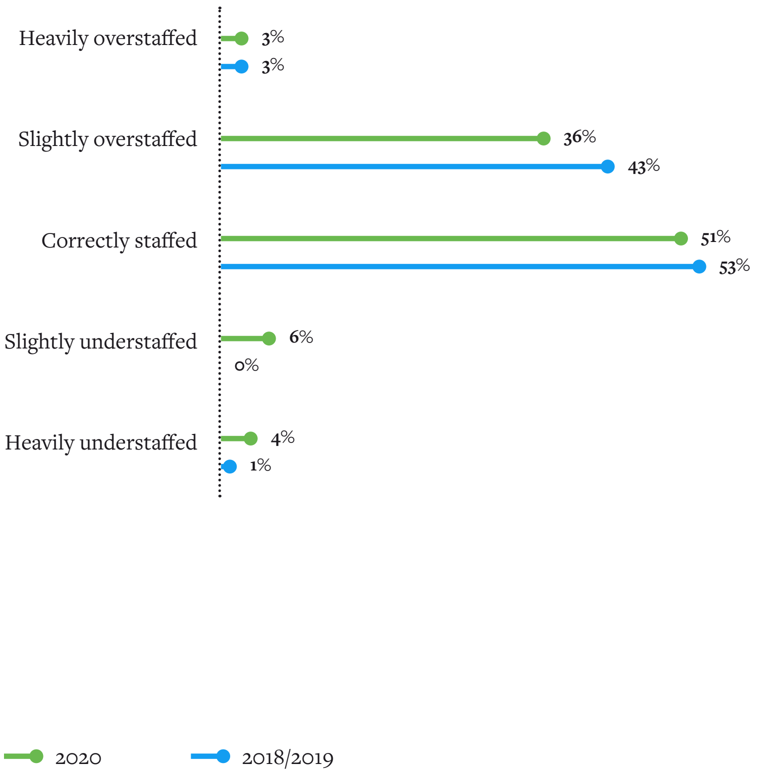


U.S. SOCs are slightly less correctly staffed now as compared to 2018/2019.

CURRENT STAFFING LEVELS

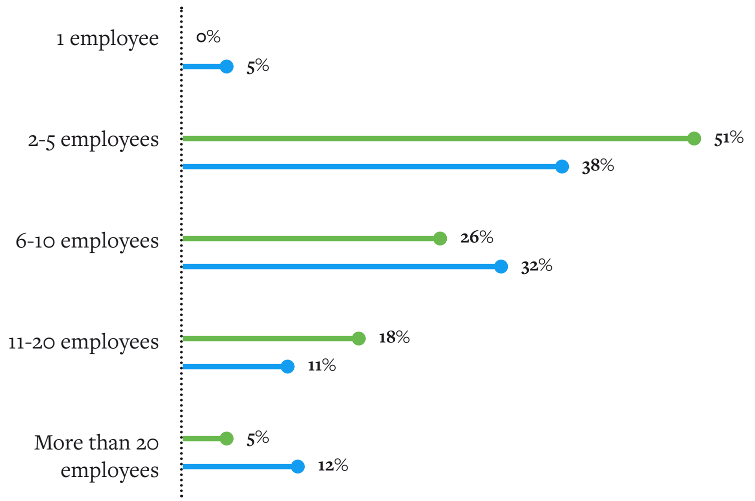
2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, IMPRESSION OF CURRENT STAFFING LEVEL

UNITED STATES



UNDERSTAFFED EMPLOYEES

2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, NUMBER OF UNDERSTAFFED EMPLOYEES, N=339

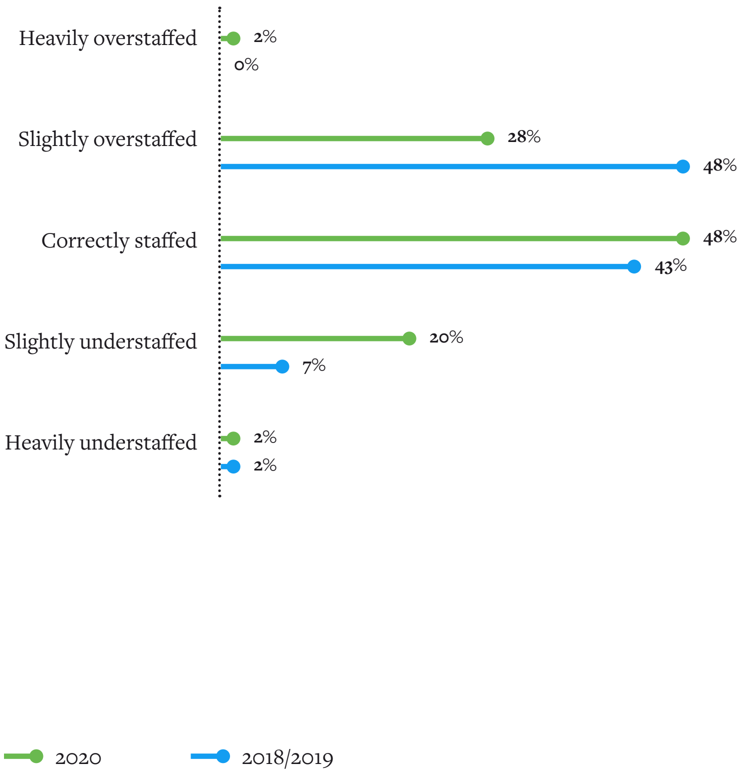


U.K. SOCs now report improvements in correct staffing.

CURRENT STAFFING LEVELS

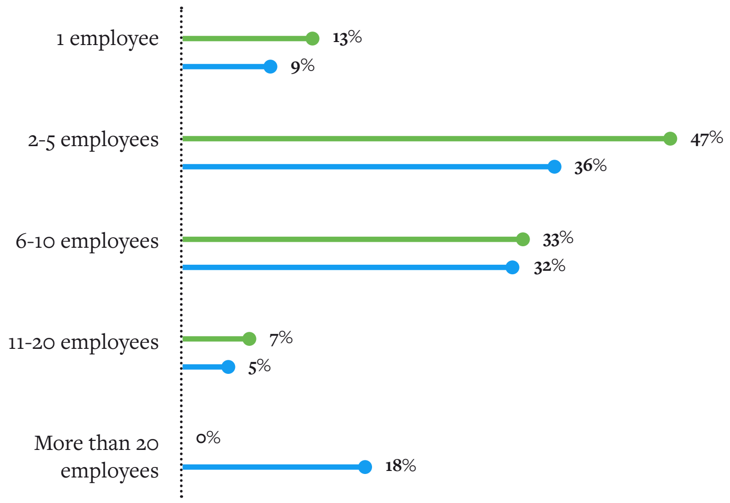
**2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA,
IMPRESSION OF CURRENT STAFFING LEVEL**

UNITED KINGDOM



UNDERSTAFFED EMPLOYEES

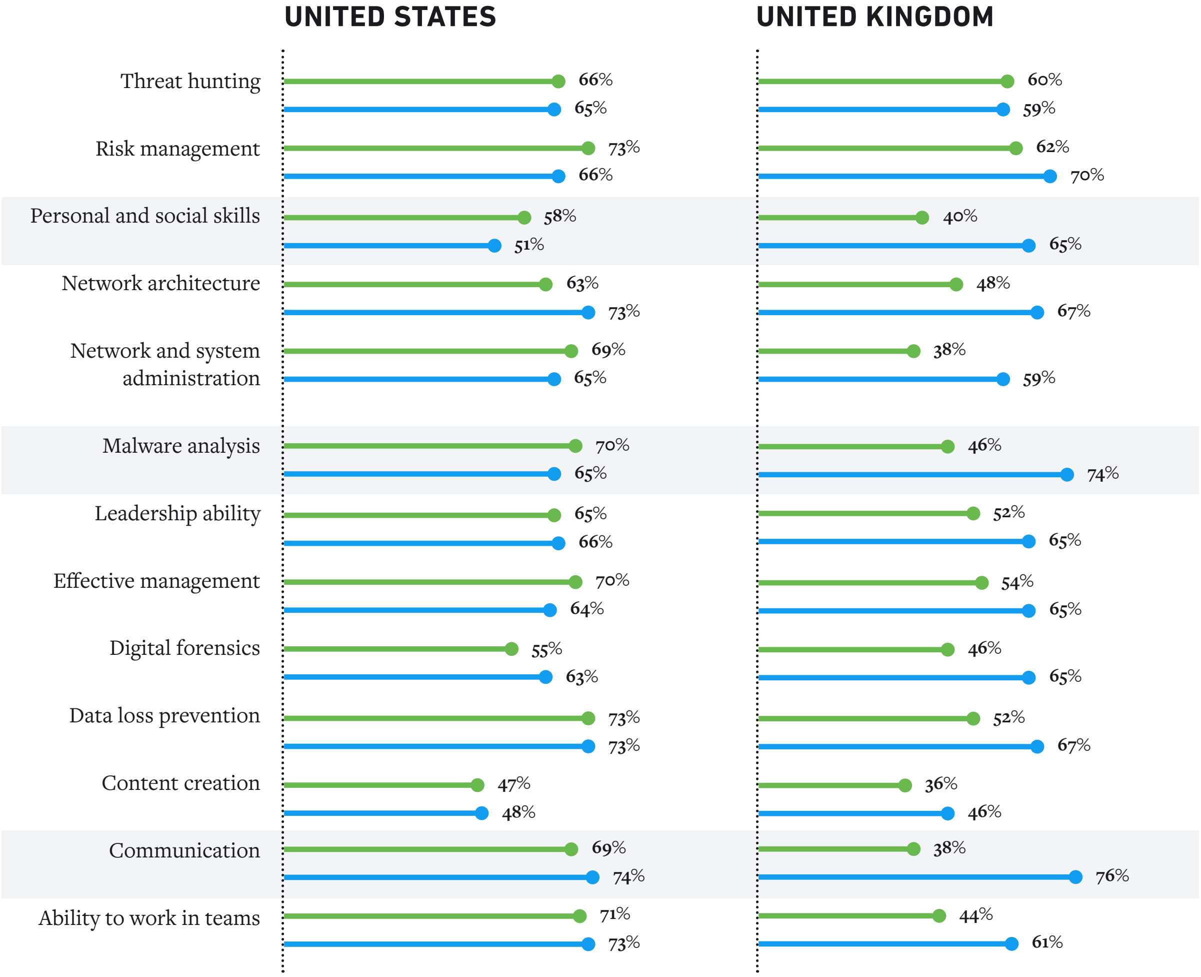
**2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA,
NUMBER OF UNDERSTAFFED EMPLOYEES, N=339**



The importance of skills has dropped for the U.K. in nearly all categories, with a significant drop in communication, malware analysis, and social ability.

SKILL IMPORTANCE

2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, THE NECESSITY OF THE SKILL IN SOC



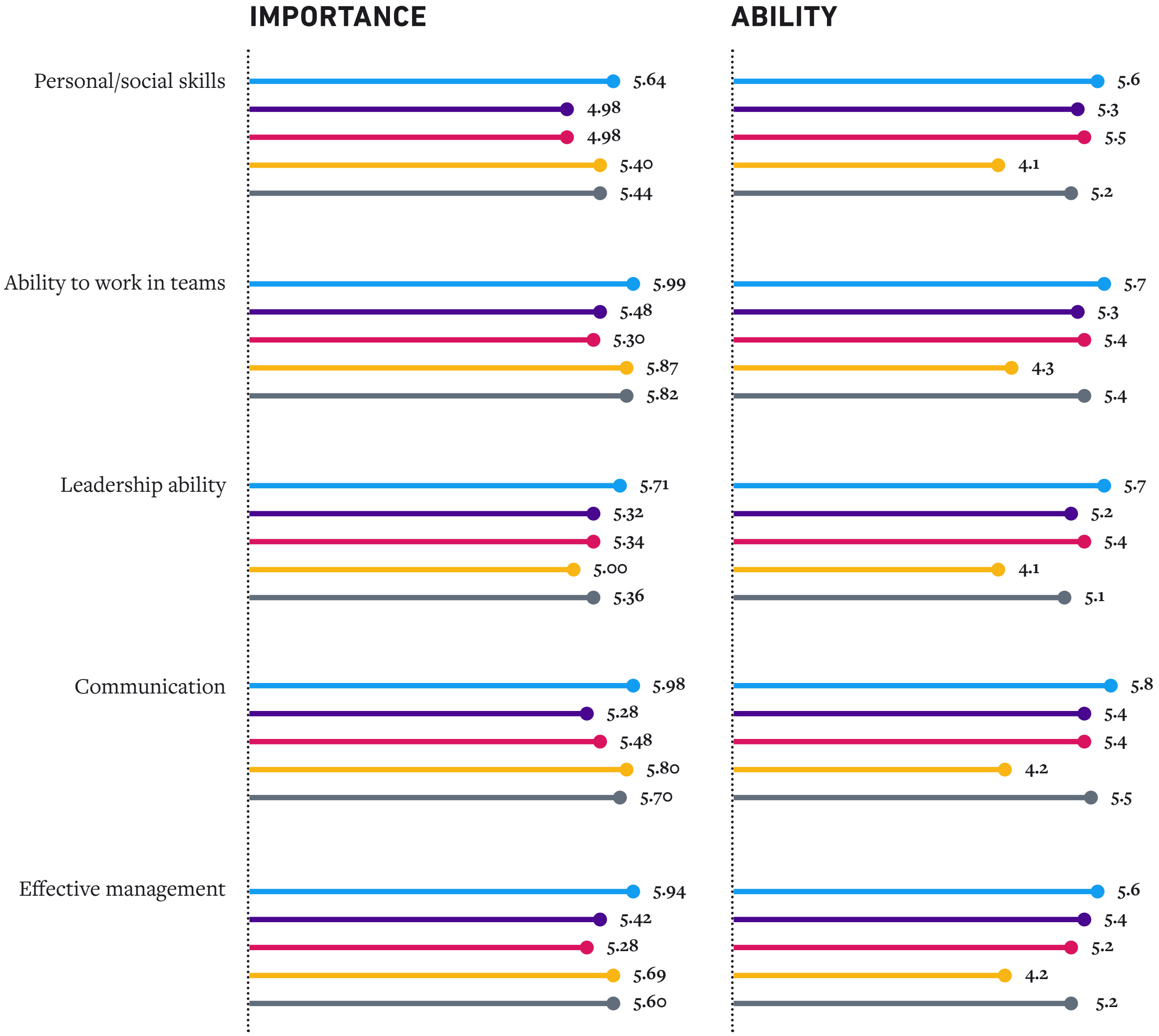
🟩 2020 🟦 2018/2019

When broken down by region, there is little variation in how SOCs in each country rank their soft skill abilities.

Differences in self-assessments are common by country. Because Germany rated themselves lower in both soft and hard skills (next page), it is more likely cultural than empirical.

SOFT SKILLS - IMPORTANCE AND ABILITY - 2020

7-POINT SCALE, MEAN, N=295

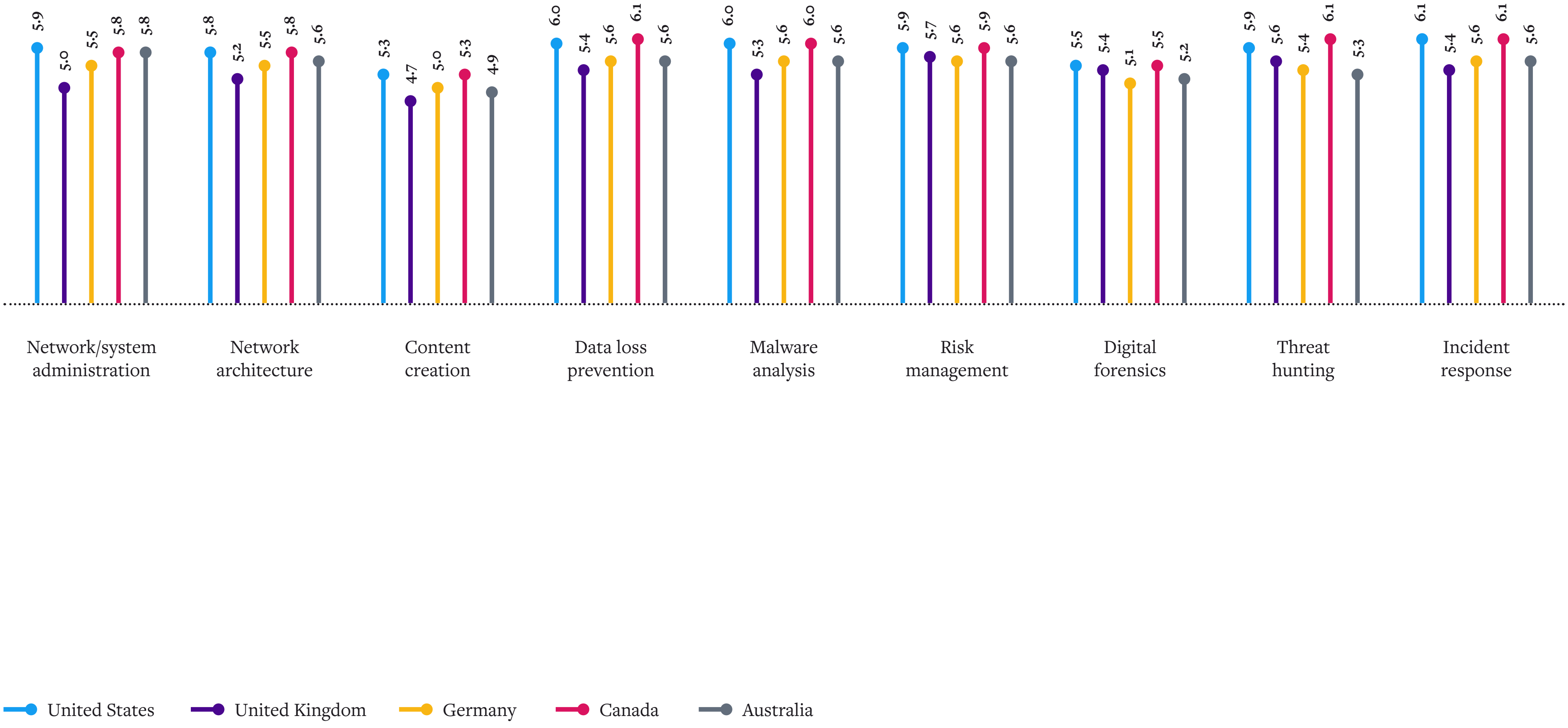


- ● United States
- ● United Kingdom
- ● Germany
- ● Canada
- ● Australia

Hard skill importance and proficiencies are similar across regions.

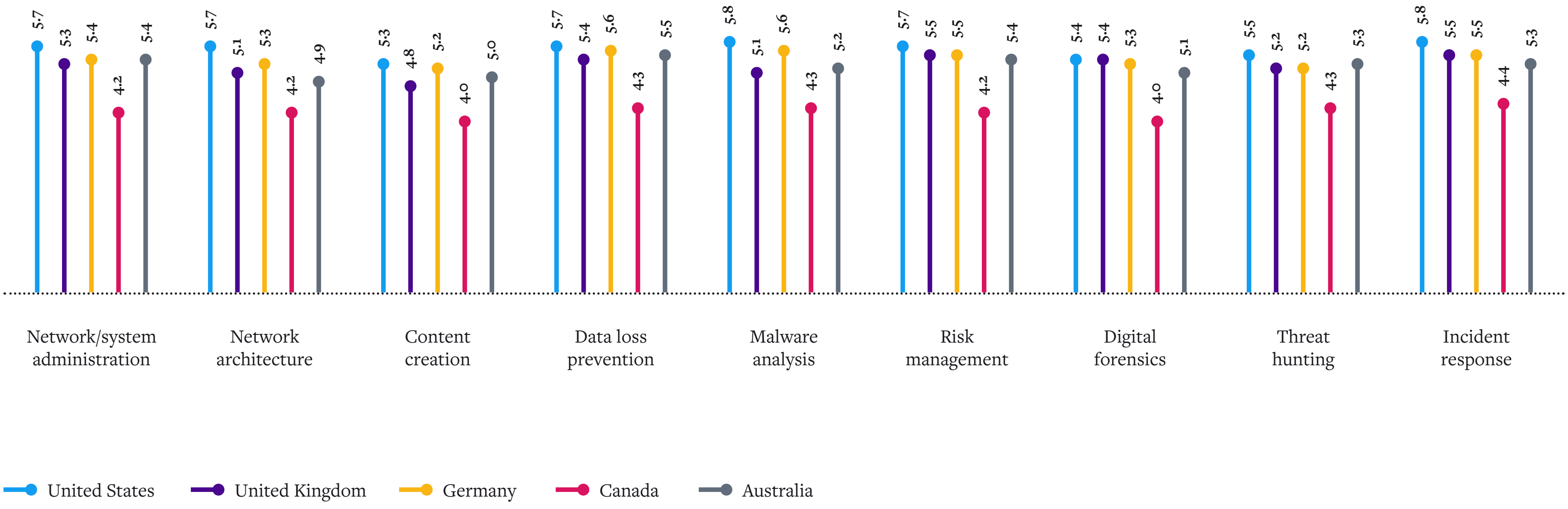
HARD SKILLS - IMPORTANCE - 2020

7-POINT SCALE, MEAN, N=295



HARD SKILLS - ABILITY - 2020

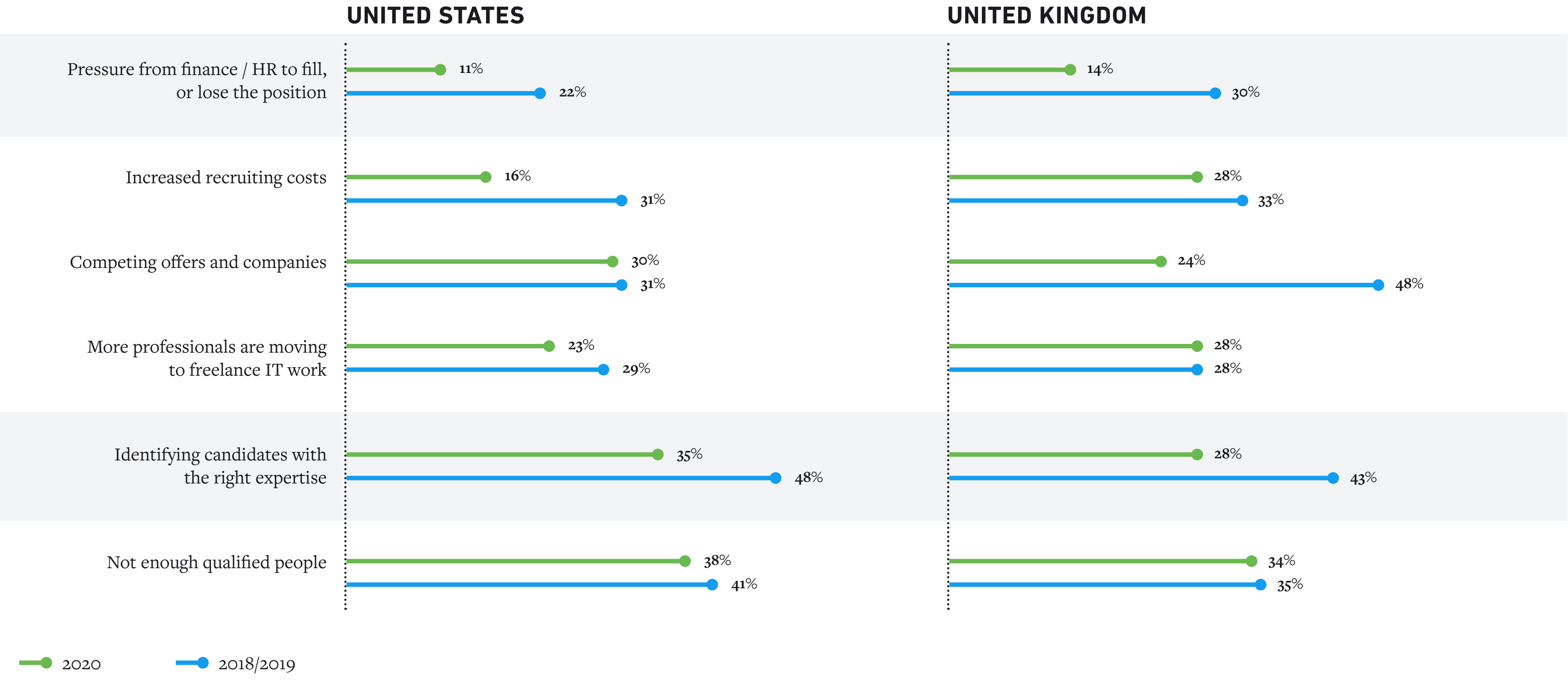
7-POINT SCALE, MEAN, N=295



Although still a challenge, SOCs across the U.S. and U.K. stated significant improvements in being able to identify candidates and hiring pressure from corporate finance or HR.

HIRING CHALLENGES

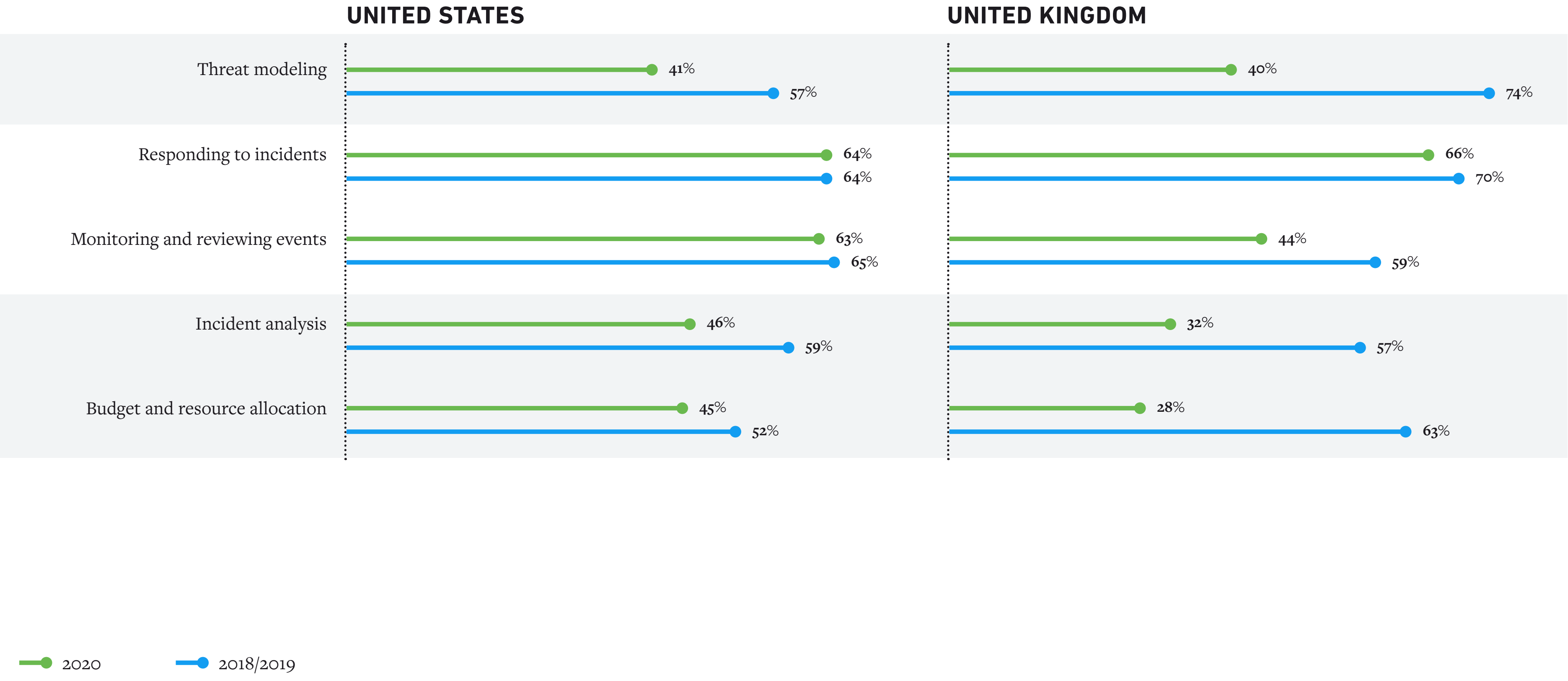
2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, MOST FREQUENT CHALLENGES IN HIRING



U.S. and U.K. SOCs reported significant declines in their ability to do threat modeling, incident analysis, and budget/resource allocation in YoY change.

EFFECTIVENESS OF SOC TEAM

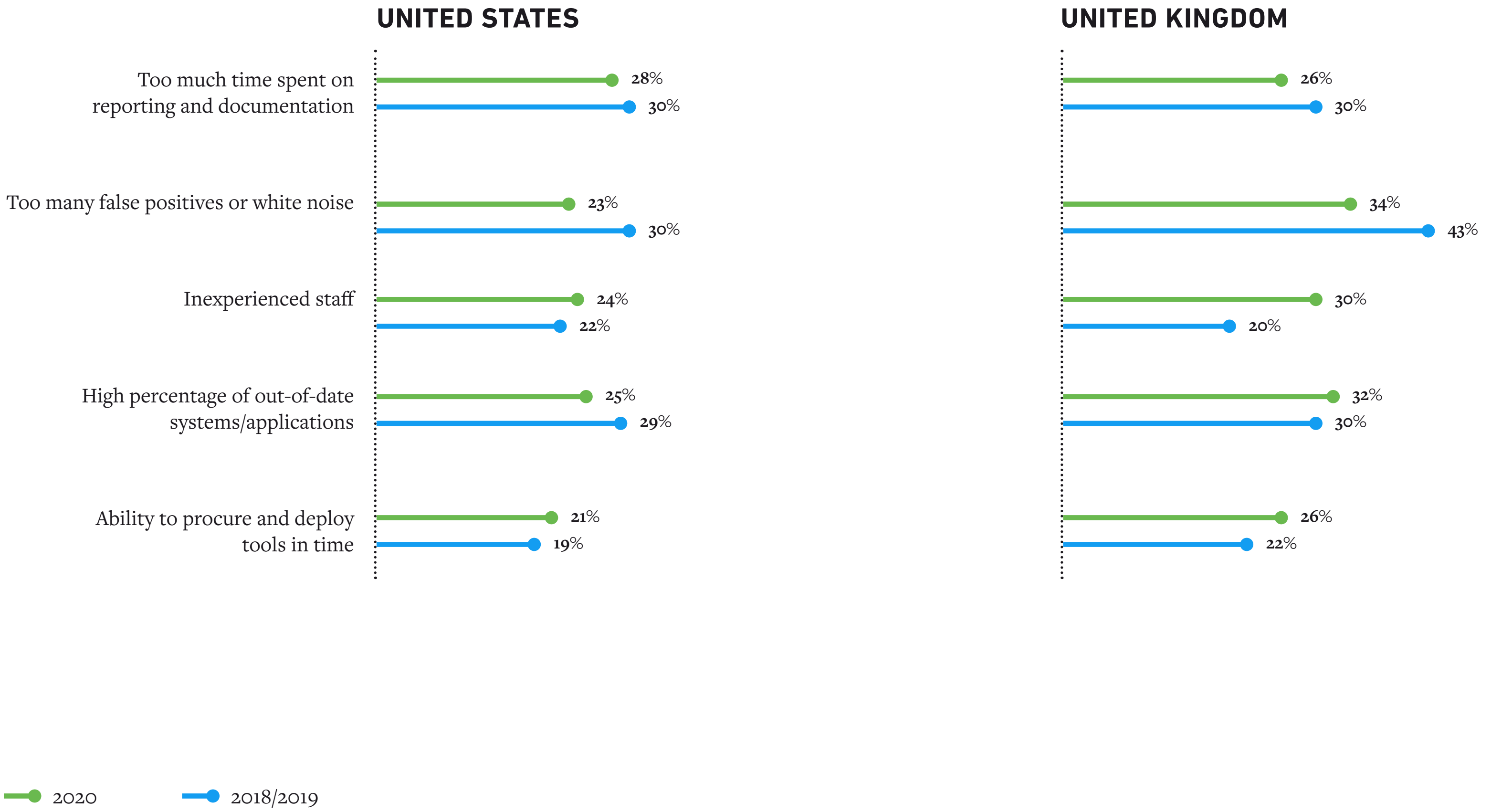
2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, ABILITY TO RESPOND TO COMMON ISSUES ON 7-POINT SCALE, TOP 2



Inexperienced staff is a growing challenge, especially for U.K. SOCs in 2020.

PAIN POINTS

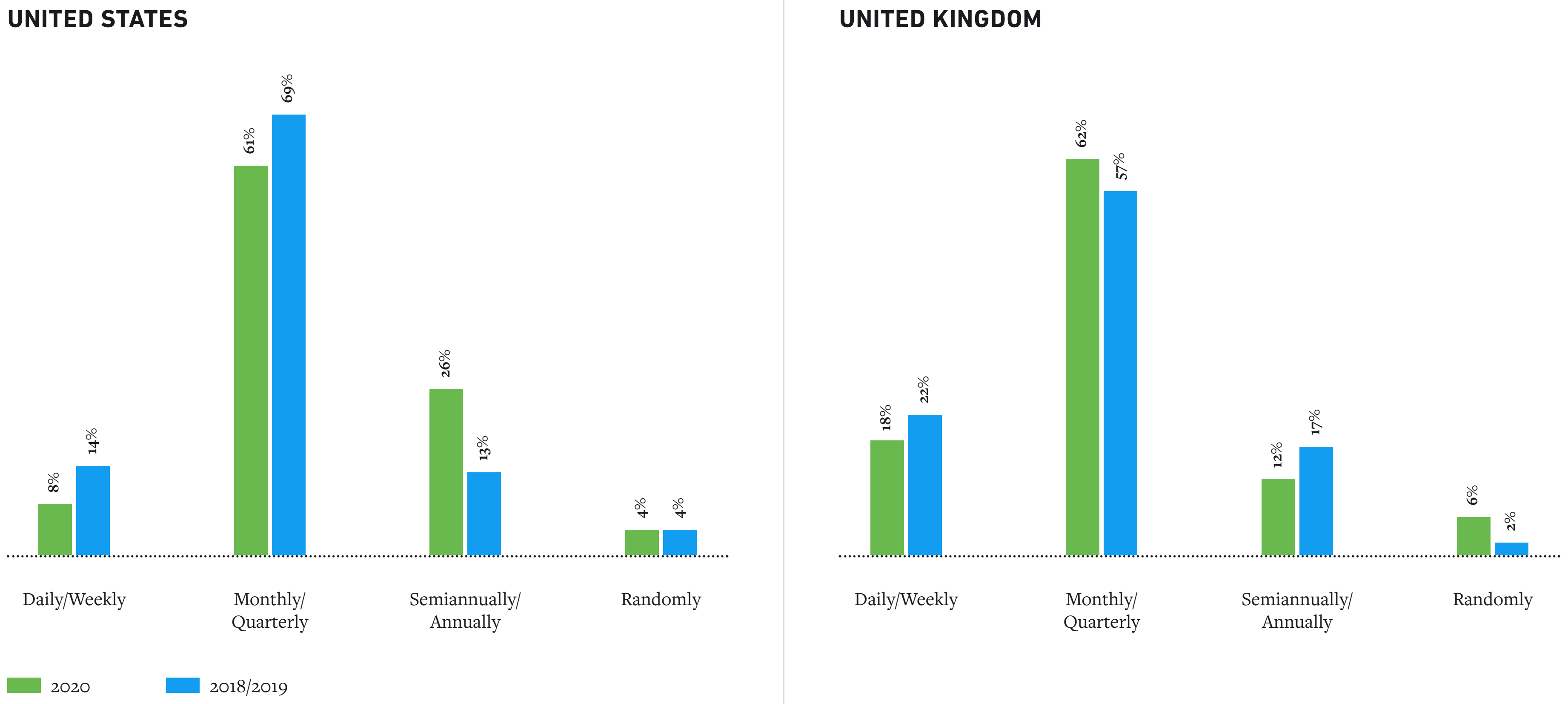
2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, COMMON PAIN POINTS EXPERIENCED OVERALL



U.S. and U.K. SOCs reported similar YoY trends in training occurring either monthly or quarterly.

FREQUENCY OF TRAINING

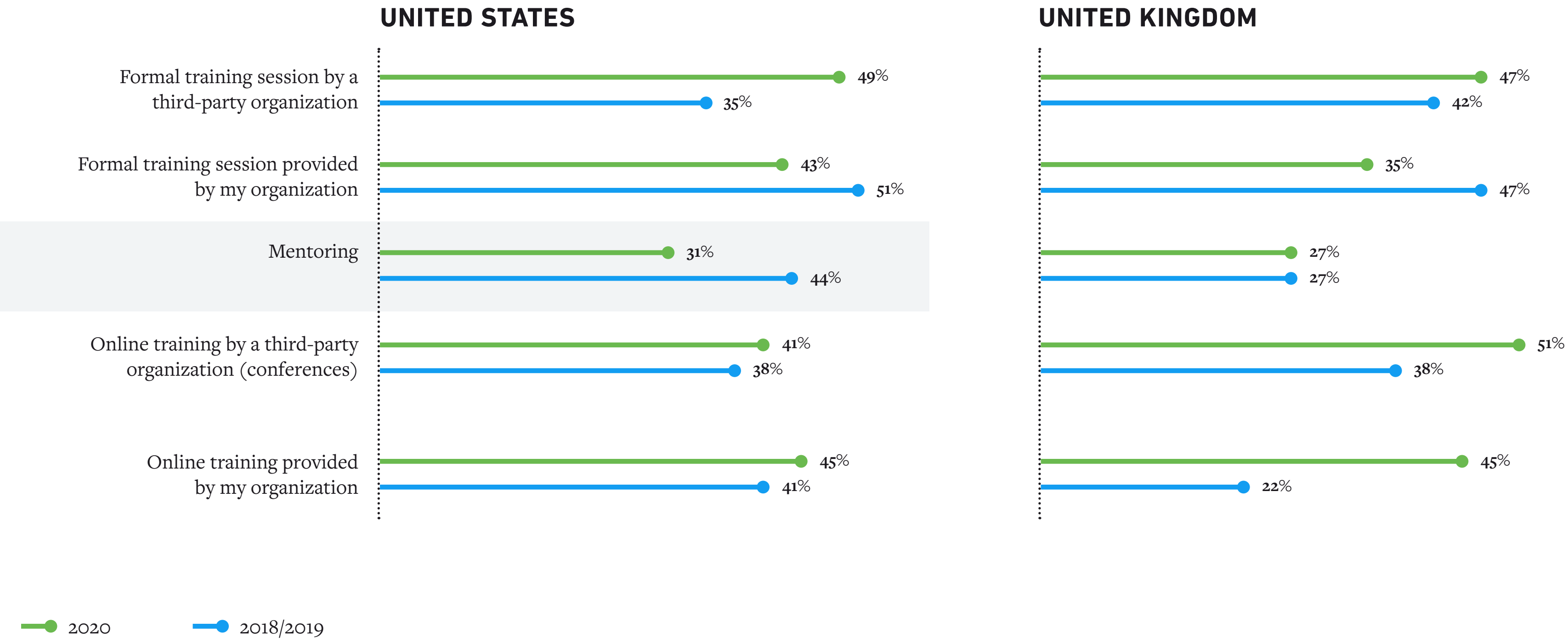
2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, SOC PERSONNEL TRAINING CADENCE, N=339



U.S. and U.K. SOCs have increased YoY training efforts across most categories, with the U.K. specifically increasing the use of online training.

TYPES OF TRAINING

2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, SOC PERSONNEL TRAINING TYPES; N=339



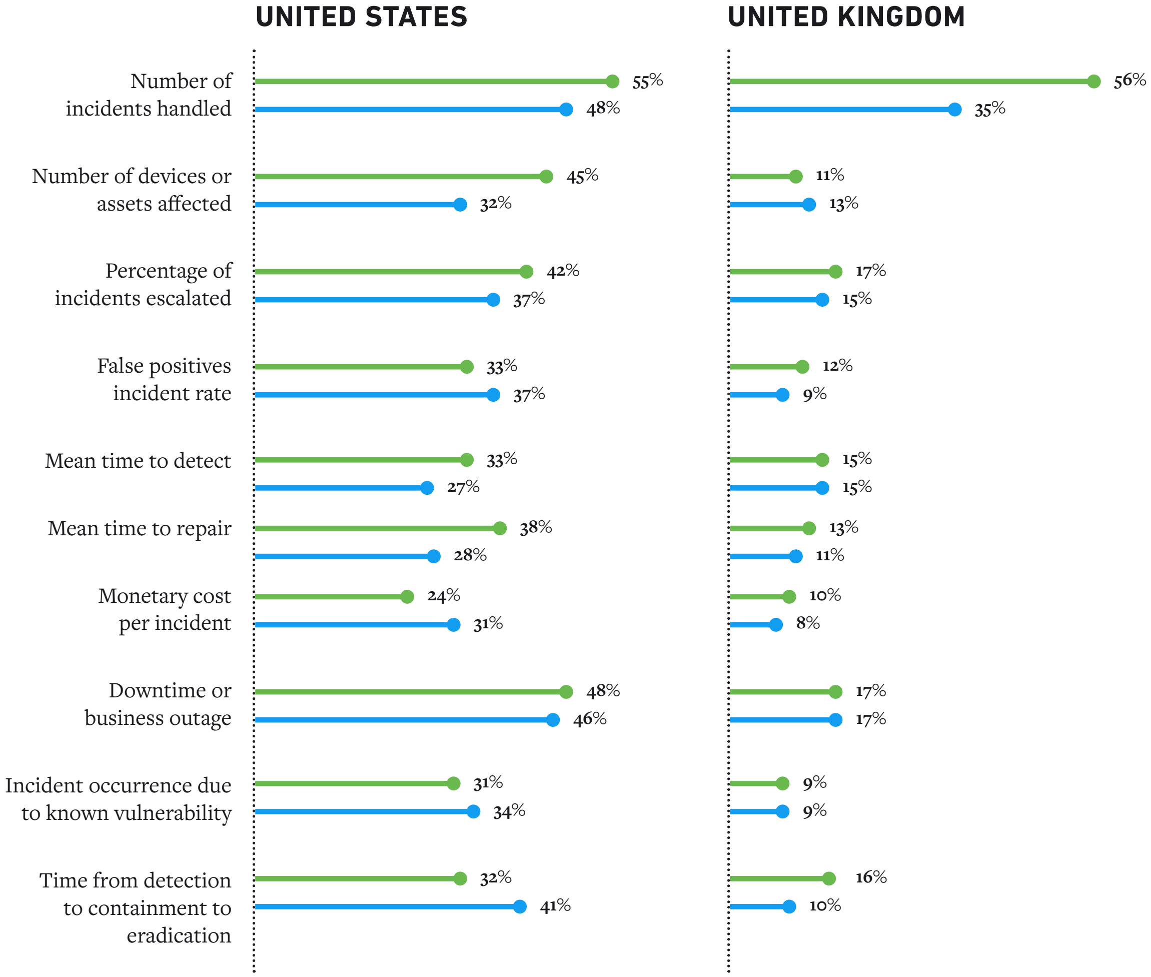
Drop in mentoring may be due to an increase in third-party training.

21%

U.S. remains fairly aligned in nearly all categories, but U.K. SOCs reported a 21% point YoY increase in tracking the number of incidents handled.

METRICS TRACKED

2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, TOP METRICS COMMONLY TRACKED BY THE SOC

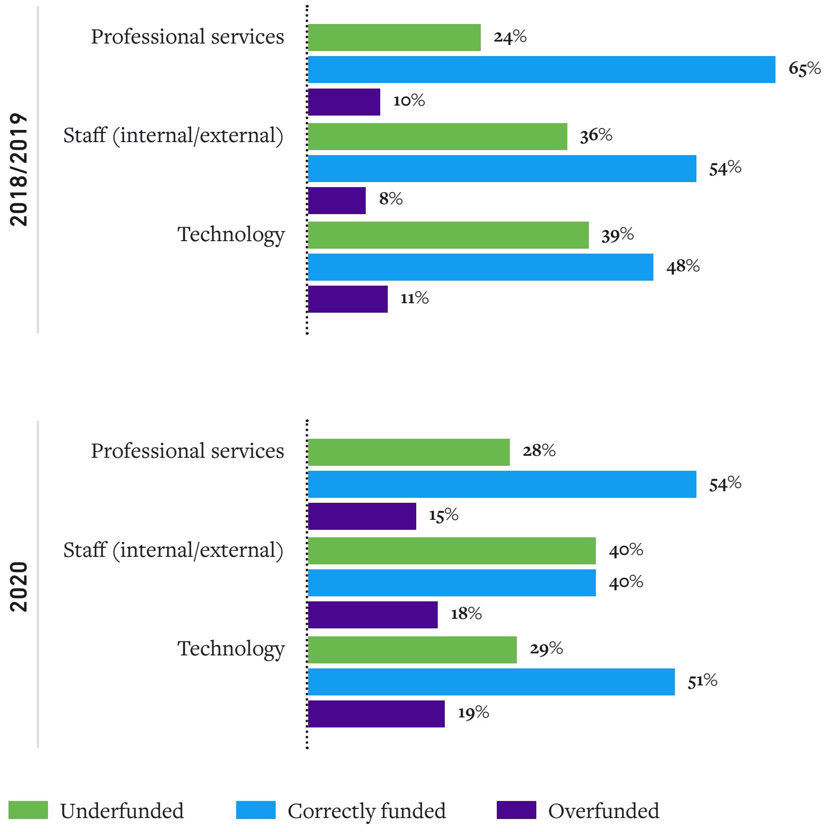


🟩 2020 🟦 2018/2019

While only slight funding changes are observed in the U.S., technology has become twice as underfunded in the U.K.

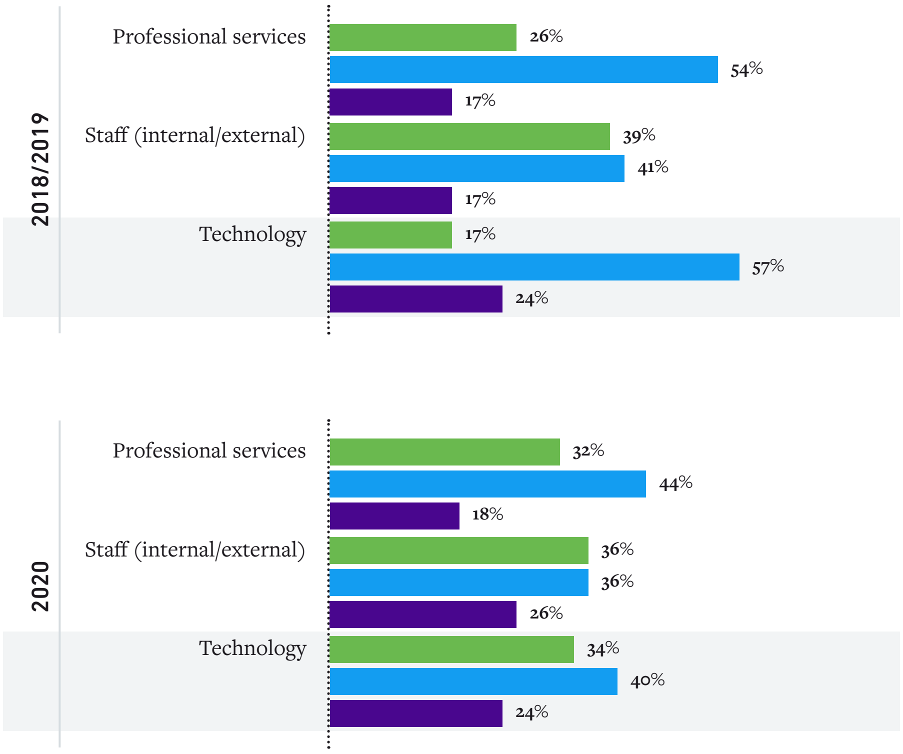
UNITED STATES FUNDING DISTRIBUTION BY AREA

2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, SOC AREAS, AND THEIR FUNDING LEVEL

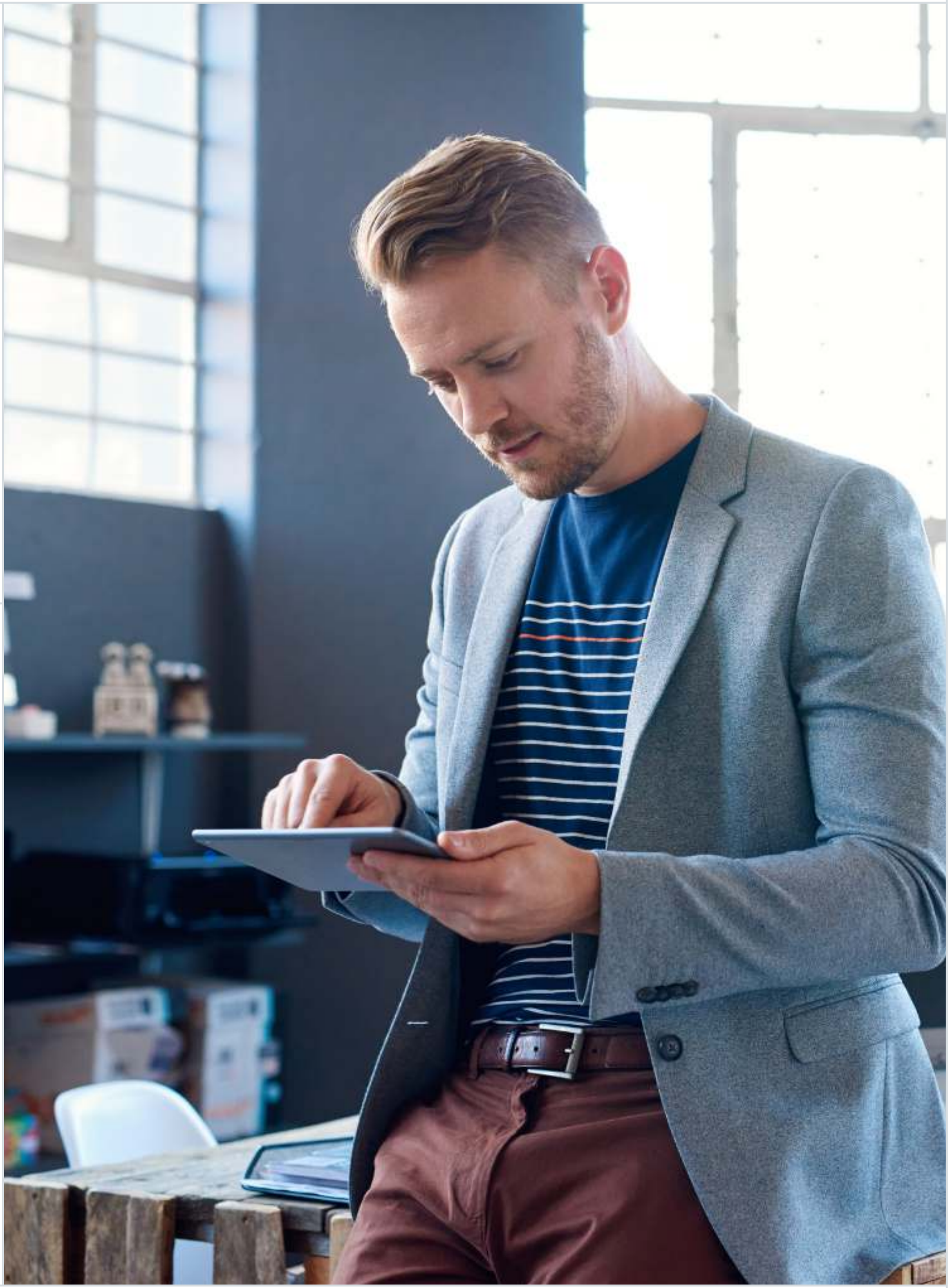


UNITED KINGDOM FUNDING DISTRIBUTION BY AREA

2018/2019 U.S., U.K. VS. 2020 U.S., U.K. DATA, SOC AREAS, AND THEIR FUNDING LEVEL

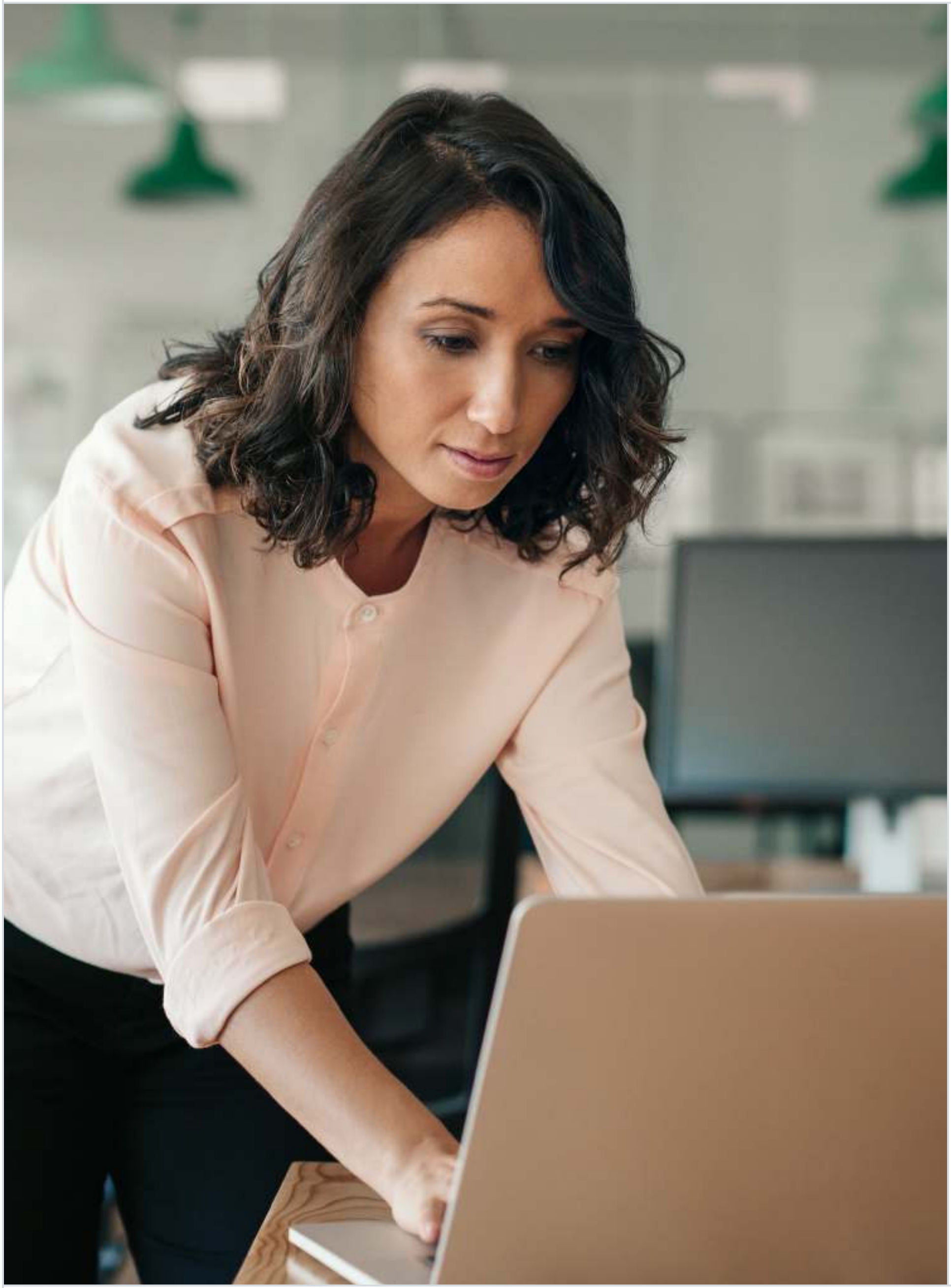


Appendix 2: Effectiveness Calculation and Demographics



You'll find the following topics covered in this section:

1. EFFECTIVENESS METHODOLOGY
2. GENERAL DEMOGRAPHICS OF 2020 SURVEY RESPONDENTS
3. PARTICIPANT DESCRIPTIVE DEMOGRAPHICS
4. COMPANY SIZE



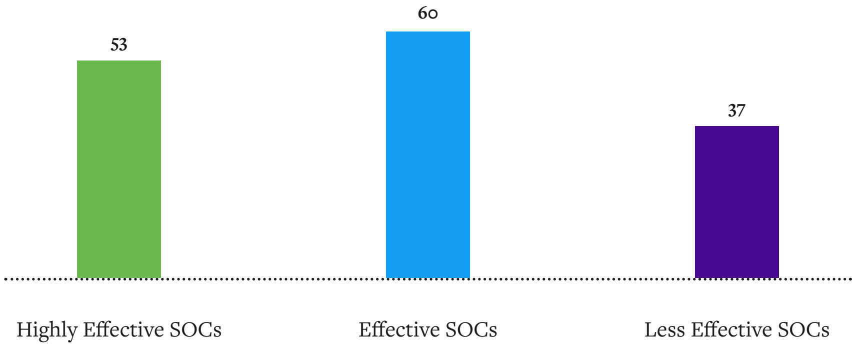
Effectiveness Methodology

Total effectiveness scores were determined by averaging respondent selections of the ratings of 6 distinct abilities:

- Monitoring and reviewing events
- Responding to incidents
- Threat modeling
- Performing deep-dive incident analysis
- Auto-remediation
- Budget and resource allocation

AGGREGATE EFFECTIVENESS SCORING

ABILITY TO RESPOND TO COMMON ISSUES ON A 7-POINT SCALE; N=150



General Demographics of 2020 Survey Respondents

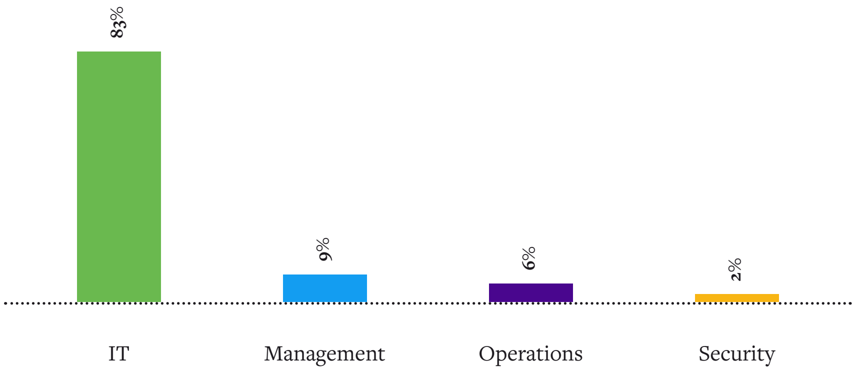
PARTICIPANT GEOGRAPHY

N=295

34%	17%	15%	17%	17%
U.S.	U.K.	GERMANY	CANADA	AUSTRALIA

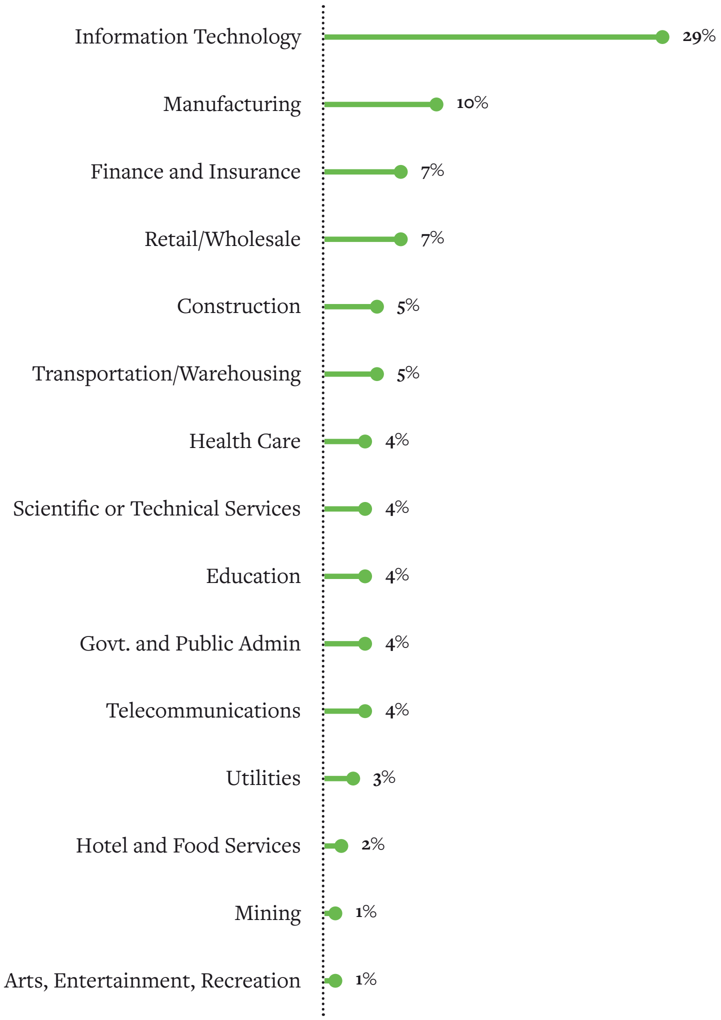
AREA OF WORK

N=295



PARTICIPANT INDUSTRY

N=295



Participant Descriptive Demographics

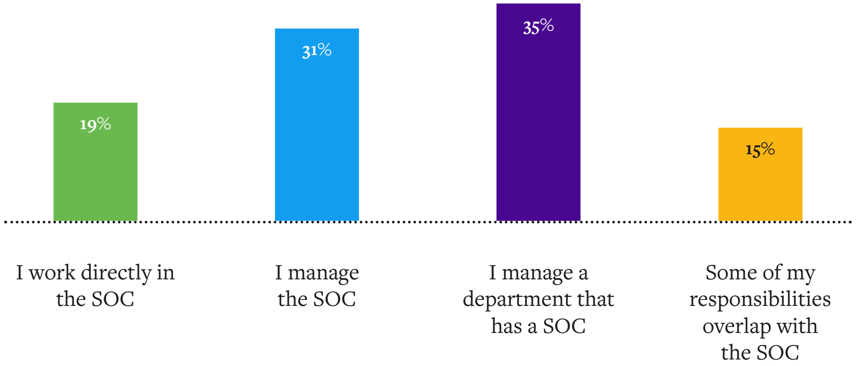
JOB TITLE

N=295

38%	CIO
4%	CISO
35%	INFORMATION SECURITY OFFICER (ANALYST, MANAGER, VP OF SECURITY, DIRECTOR)
16%	SECURITY ENGINEER/MANAGER
6%	SECURITY ENGINEER/ANALYST
2%	SECURITY ARCHITECT

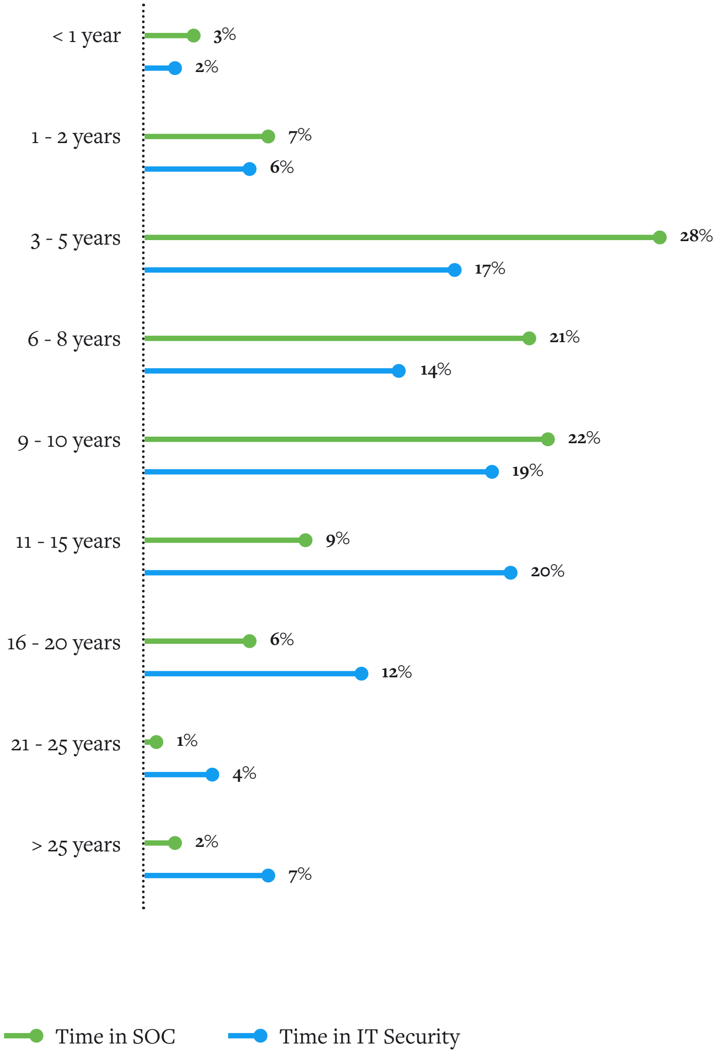
RELATIONSHIP WITH SOC

N=295



TIME IN SOC AND IT SECURITY

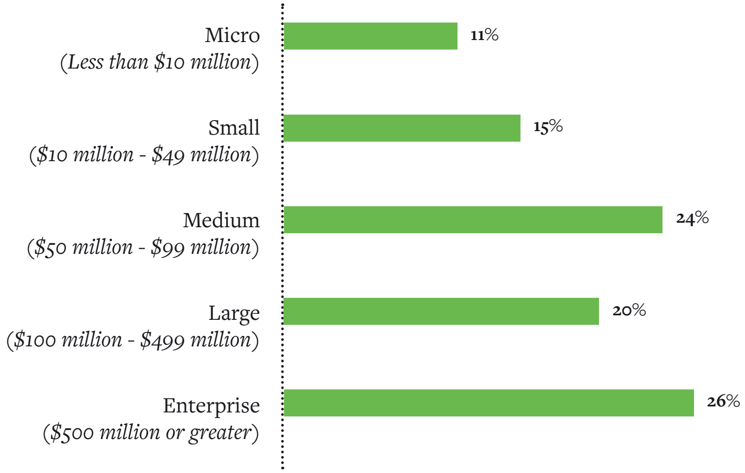
N=295



Company Size

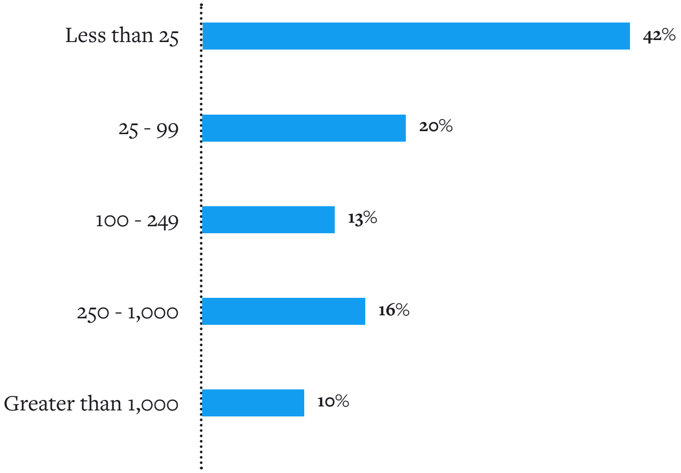
ESTIMATED COMPANY REVENUE

N=295



ESTIMATED NUMBER OF EMPLOYEES

N=295



exabeam®

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures. For more information, visit **www.exabeam.com**.

1051 E. Hillsdale Blvd., 4th Floor,
Foster City, CA 94404

1.844.EXABEAM
or 1.844.392.2326
info@exabeam.com