exabeam

THE EXABEAM 2018 STATE OF THE SOC REPORT

CONTENTS

OVERVIEW

The Exabeam 2018 State of the SOC Report

REPORT **THE EXABEAM 2018 STATE OF THE SOC REPORT** presents the results of a survey of U.S. and U.K. security professionals who are involved in the management of Security Operations Centers (SOC) across chief information officer (CIO), chief information security officer (CISO), analyst and management roles.

The survey's purpose was to determine how the players of the SOC view key aspects of its operations, hiring and staffing, retention, SOC processes and effectiveness, technologies, training and funding.

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

GEOGRAPHY OF RESPONDENTS

UNITED STATES

UNITED KINGDOM

OVERVIEW

Key Findings on the State of the SOC

- SOCs are generally well established with 91 percent operating for three years or more.
- CIO and CISO managers are more focused on preventative measures and process improvements than frontline workers.

62%
would change their SOC

28%
of frontline workers focus on automation

91%
of SOCs are well established for three years or more

55%
of CIO/CISO and management focus on automation

OUTSOURCING

- While 40 percent of SOCs are outsourced, 95 percent only outsource parts of the SOC, versus 5 percent that outsource the whole operation.
- SOCs mostly outsource detection (47%) and monitoring (45%) and have response and expertise (68%) in-house.
- Only 5 percent of those that outsource their SOC, outsource the entire SOC.

40%

of SOCs are outsourced, but most are only pieces and not the whole operation

47%

of SOCs that outsource, outsource detection

45%

of SOCs that outsource, outsource monitoring

5%

of SOCs that are outsourced, are outsourced in their entirety

IT AND SOC TENURE

Most SOC professionals have a longer tenure in IT than in the SOC.

HIRING, STAFFING AND TRAINING

- Frontline workers are more focused on day-to-day activity (94%), while management are more heavily involved in preventive measures and process improvement.
- Most SOCs don't experience much difficulty with retention and feel that they have sufficient staffing to meet their needs.

94%

of frontline workers are more focused on day-to-day activity

OPERATIONS

- While some wouldn't change anything about the SOC (38%), many survey participants would like to see changes around technology (17%), staffing (14%) and improving processes (12%).
- Frontline workers experience more pain with reporting/documentation (53%) and technology (41%) than their managers and C-suite. This could largely be due to managers and C-suite being unaware.
- Small and medium SOCs track fewer metrics than large SOCs.

38%

wouldn't change anything about the SOC

17%

would make changes regarding technology

14%

would make changes regarding staffing

12%

would like to improve processes

EMERGING TECHNOLOGY

Machine learning is thought to be the most immediate technology to be implemented, while artificial intelligence is seen as one of the last technologies to be implemented.

INSURANCE

Only half (51%) of companies have cybersecurity insurance. There is little to no correlation between SOC size and cybersecurity insurance.

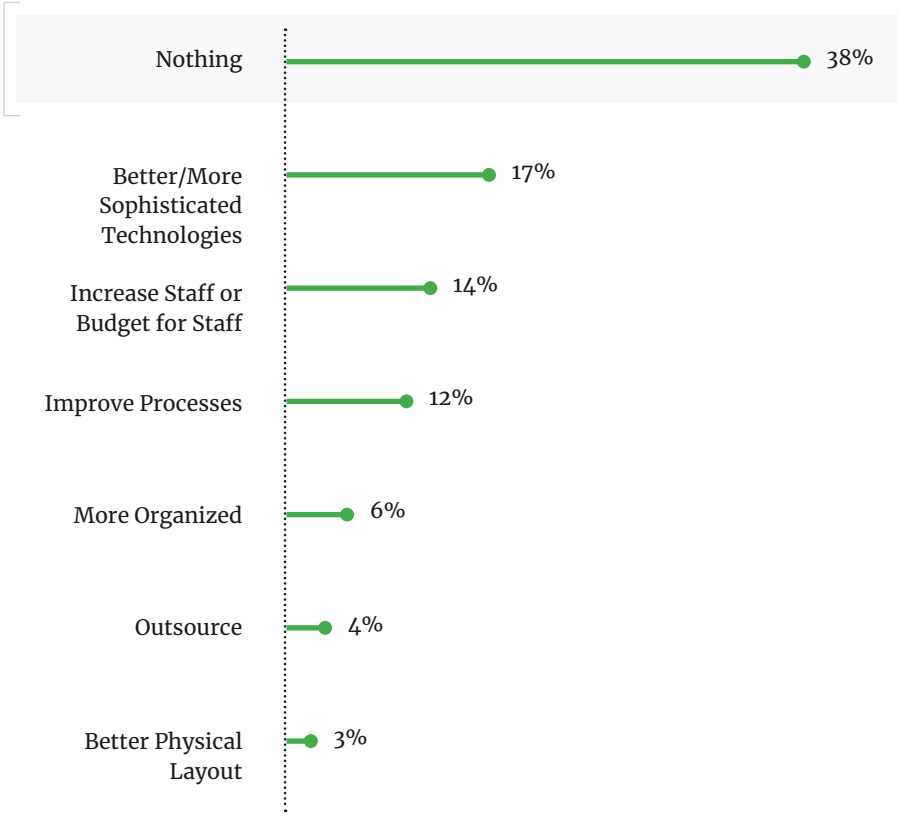
51%

of companies have cybersecurity insurance

FIXING THE SOC

Thirty-eight percent of SOC employees would change nothing if given the chance. Other areas that could be improved are technology, staffing and increased budget.

AREAS THAT SHOULD CHANGE IN THE SOC



"Focus more on employees. The tools change but good employees to run the tools can make or break overall performance."

CIO, U.S., 3-5 YRS, >$20 BILLION, OTHER MANUFACTURING

"More focus on people and less on automated tools."

CIO, U.S., 9-10 YRS, $100-299 MILLION, INFORMATION SERVICES AND DATA PROCESSING

"I would centralise the SOC budget around more, very sophisticated anti-hacking technologies rather than the current traditional method."

CIO, U.K., 6-8 YRS, $5-9.99 BILLION, FINANCE AND INSURANCE

"More automation and fewer platforms to manage"

CIO, U.K., 3-5 YRS, $5-9.99 BILLION, FINANCE AND INSURANCE

"Trash it all and start over instead of milking ancient legacy systems and hardware."

CIO, U.S., 9-10 YRS, $10-49 MILLION, RETAIL

"More future proof infrastructure"

ISO, U.K., 16-20 YRS, $5-9.99 BILLION, CONSTRUCTION

TOP OF MIND BY SECURITY ROLE

The various roles within a SOC each have different focuses, concerns and pain points.

CIO/CISO

APPEAR TO BE MORE FOCUSED ON LONG-TERM STRATEGY AND OUTCOMES THAN SHORT-TERM, DAY-TO-DAY ACTIVITIES.

- False positives or white noise
- Maintaining security monitoring tools
- Early detection and elimination of threats
- Automation
- Overall feel less pain points than managers and frontline workers

SOC MANAGERS

SIMILAR TO CIO/CISO, BUT NOT AS FOCUSED ON LONG-TERM STRATEGY AND OUTCOMES.

- Keeping up with security alerts
- Early detection and elimination of threats
- Automation
- Legacy technology

FRONTLINE ANALYSTS IN A SOC

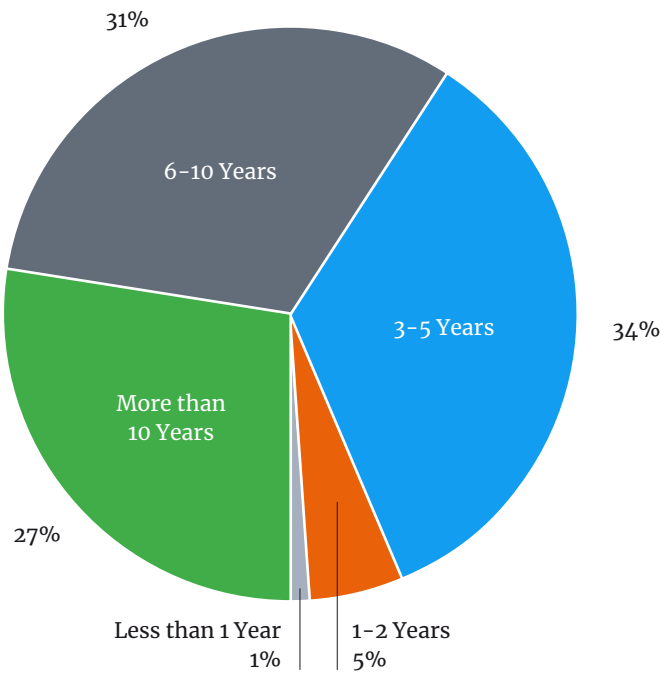
MORE LIKELY TO IDENTIFY PAIN POINTS AND GET CAUGHT UP IN DAY-TO-DAY ACTIVITIES.

- Legacy technology
- General operations and management of day-to-day tasks
- Outdated equipment
- Inexperienced colleagues
- Too much time on documentation and reporting
- Keeping up with security alerts

The majority of SOCs appear to be in large organizations whose management has three or more years of experience managing their SOC.

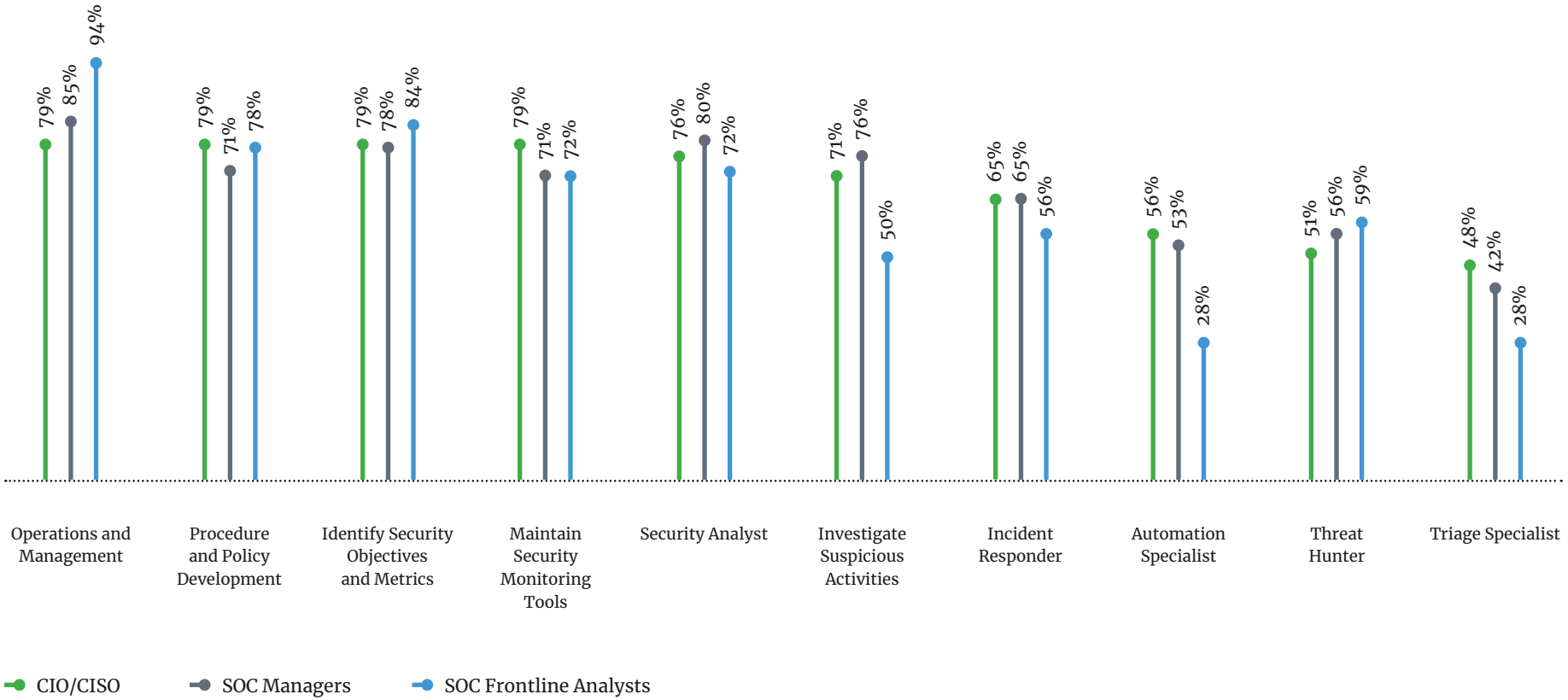
LENGTH OF TIME HAVING A SOC

Ninety-two percent of SOCs have been around for three years or more.



The responsibilities that CIOs, CISOs and SOC managers identify with are very similar, but vary more widely among frontline workers, possibly due to how the work is delegated. The fact that 56 percent of CIOs and CISOs, and 52 percent of SOC managers are focusing on automation is an indication that they need automation to keep up with threats. However, hiring automation specialists to do this work indicates they are prioritizing automation in the SOC.

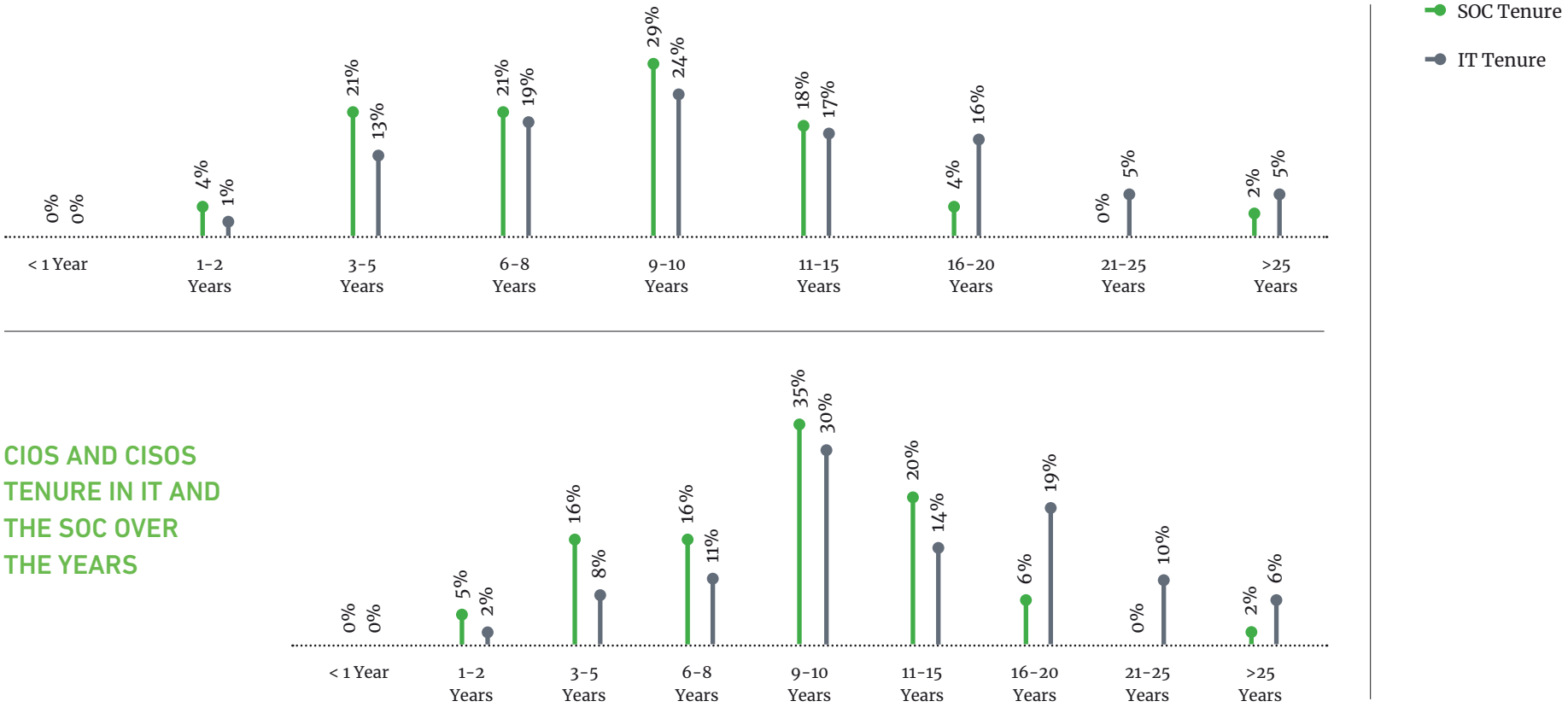
RESPONSIBILITIES WITH SOCS



IT AND SOC TENURE

CIOs and CISOs tend to have more tenure in both IT and the SOC. In general, IT professionals have been in their positions longer than people who work in or manage a SOC. This statistic is likely due to the relative youth of the security field compared to the overall IT field. A possible explanation is that many SOC workers want to move out of operations roles after a limited amount of time, while many SOC managers are pulled into other leadership roles.

CIOS AND CISOS TENURE IN IT AND THE SOC OVER THE YEARS



STAFFING LEVELS

Key Findings on the Hiring, Staffing and Training of the SOC

The majority of SOC professionals think their SOC is correctly staffed (55%). Forty-five percent believe that the SOC is understaffed. Of those 45 percent, 63 percent think they could use anywhere from two and 10 additional employees.

55%

of SOC professionals think their SOC is correctly staffed

45%

believe that the SOC is understaffed

63%

think they could use anywhere from two and 10 additional employees

MOST IMPORTANT SKILLS

The most important skills were identified as:

1. Data loss prevention
2. Ability to work in teams
3. Malware analysis skills
4. Network and system administration

GAPS IN CURRENT SKILLS

Gaps in current skills were identified as:

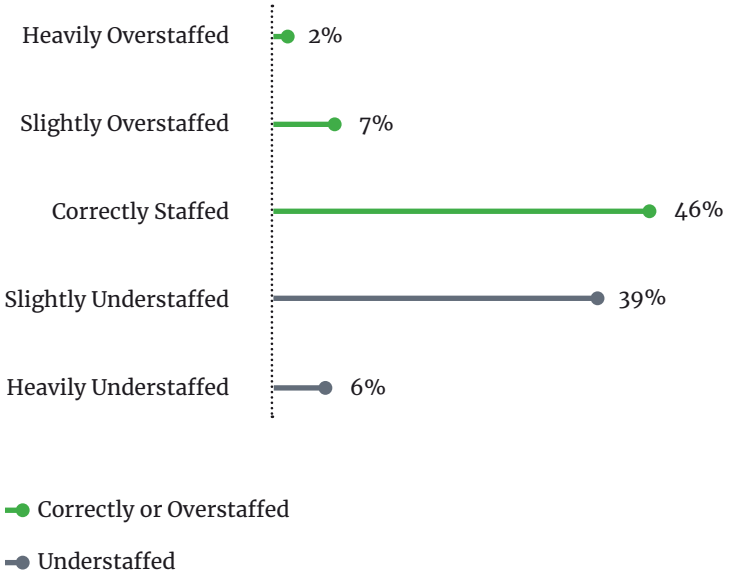
- Digital forensics
- Communication

EMPLOYEE RETENTION IN THE SOC

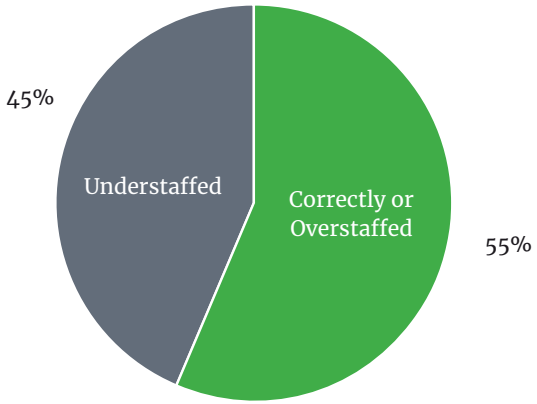
- High wages, a challenging work environment and workplace benefits are all top reasons for retention.
- Heavy competition for security employees is seen as the biggest challenge in retention (60%).

STAFFING IN THE SOC

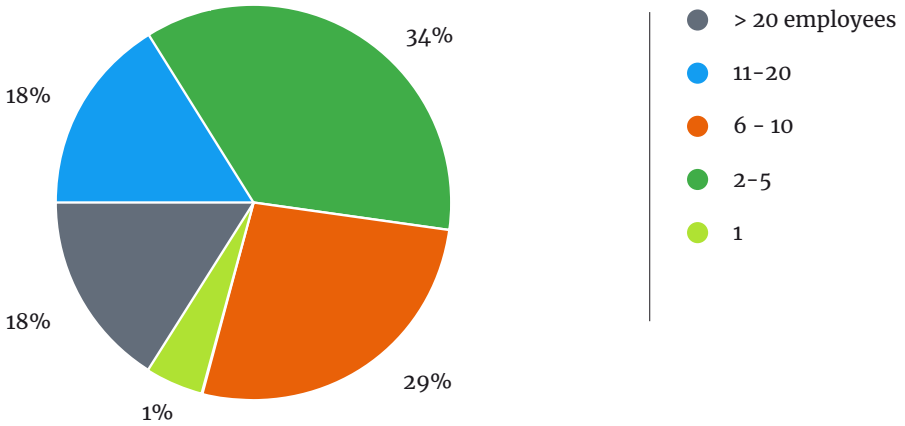
Forty-five percent of the respondents report that SOCs are understaffed, while 55 percent report they are correctly or over staffed. The 36 percent who felt the SOC was understaffed said they needed to add more than 10 employees to be correctly staffed. The need to add that many people to the SOC is a significant investment for most organizations.



STAFFING LEVELS



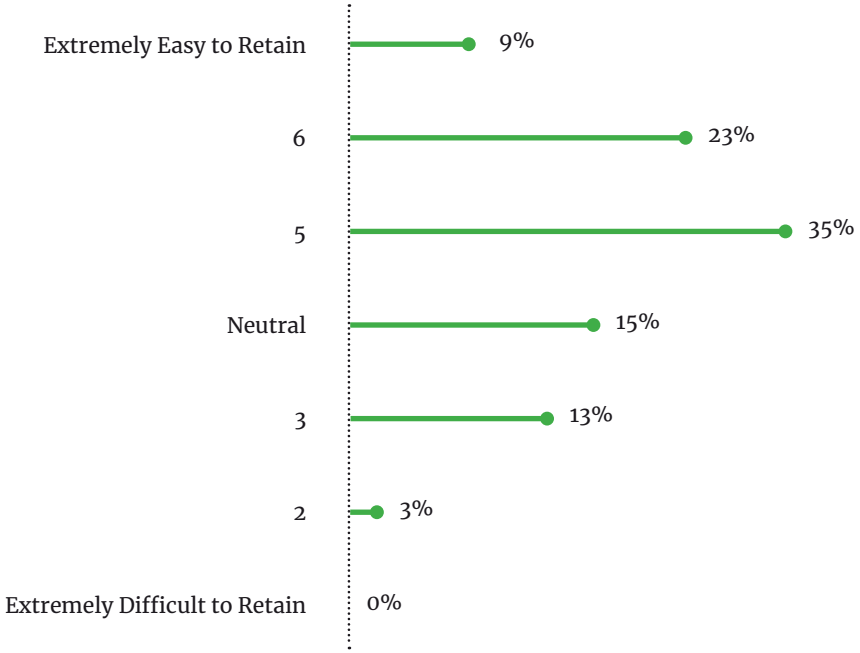
NUMBER OF EMPLOYEES IN UNDERSTAFFED SOCS



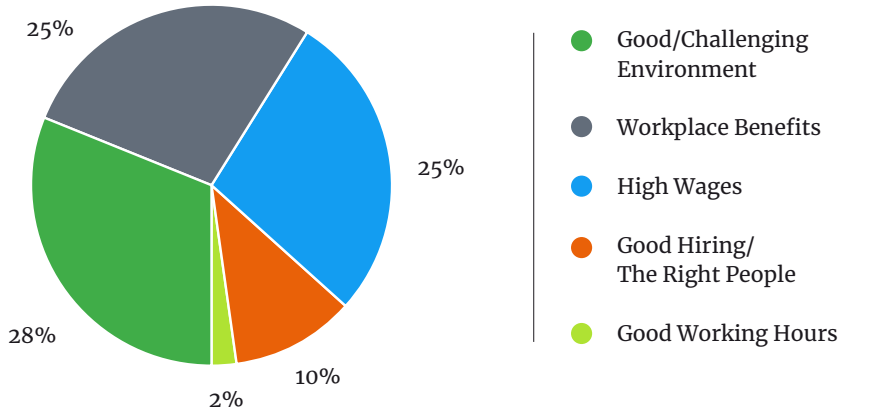
EMPLOYEE RETENTION

Contributing factors to retention are a challenging work environment, workplace benefits and high wages.

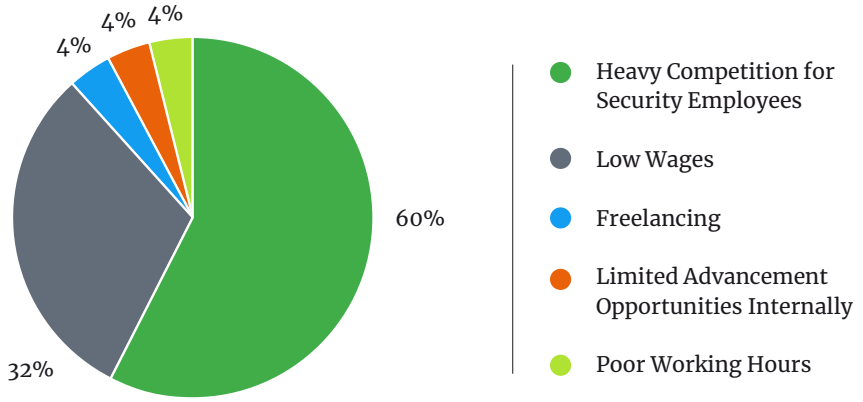
DIFFICULTY OF RETAINING EMPLOYEES



REASONS EMPLOYEES ARE EASY TO RETAIN



REASONS EMPLOYEES ARE DIFFICULT TO RETAIN



WHY EMPLOYEE RETENTION IS EASY

Employees are retained through challenging, high-paying environments. Competition for available talent is a challenge in retention.

"We have a great team with very good pay, incentives and benefits."

ISO, U.S., 6-8 YRS, $300-499 MILLION, SCIENTIFIC AND TECHNICAL SERVICES

"We offer a good workplace, a lot of autonomy and good wages."

CISO, U.K., 9-10 YRS, $500-799 MILLION, TRANSPORTATION AND WAREHOUSING

"I think we are compensated well, and it is a challenging and rewarding environment."

CIO, U.K., 9-10 YRS, >$20 BILLION, CONSTRUCTION

"We have a good benefits program and an exceptional working environment."

ISO, U.S., 6-8 YRS, $1-4.99 BILLION, FINANCE AND INSURANCE

"We offer good benefits, pay a fair salary, and make sure our employees are supported in their jobs."

ISO, U.K., 6-8 YRS, $500-799 MILLION, RETAIL

WHY EMPLOYEE RETENTION IS DIFFICULT

"Plenty of job openings in this field"

SECURITY ENGINEER / MANAGER / ANALYST, U.S., 11-15 YRS, $1-4.99 BILLION, OTHER MANUFACTURING

"Always pressure with wage demands and competing organisations"

RISK / COMPLIANCE OFFICER, U.K., 3-5 YRS, $100-299 MILLION, WHOLESALE

"Significant opportunities within the industry as a whole"

ISO, U.K., 11-15 YRS, $800-999 MILLION, INFORMATION SERVICES AND DATA PROCESSING

"Many big firms are hunting for experienced resources."

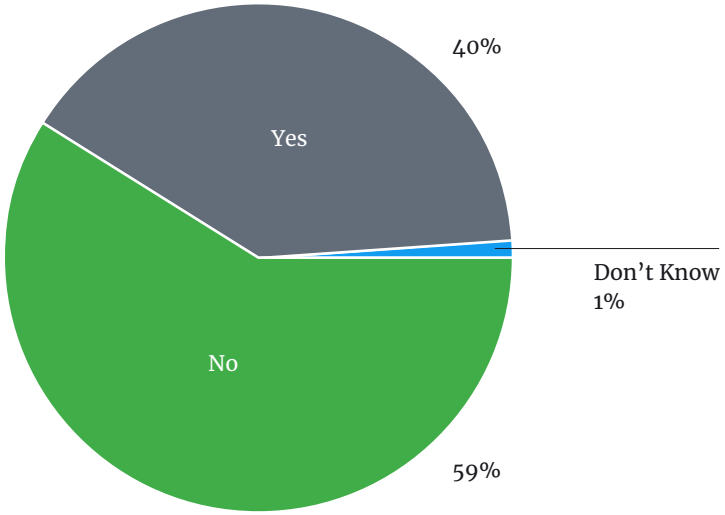
CIO, U.S., 9-10 YRS, $5-9.99 BILLION, FINANCE AND INSURANCE

OUTSOURCING OF THE SOC

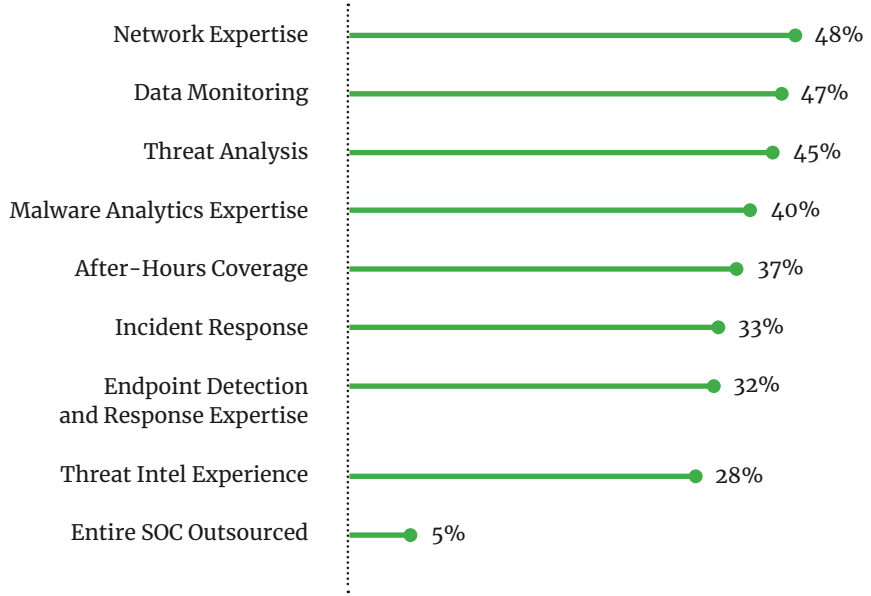
It is common for organizations to outsource some SOC functions such as after-hours coverage.

While there is the trend of bringing the responsibility for security in-house, it is also interesting to note that fully a third of respondents need outside help with incident response, after-hours coverage and endpoint detection and response.

DO YOU OUTSOURCE OR CONTRACT OUT ANY PART OF THE YOUR ORGANIZATION'S SOC?



OUTSOURCED FUNCTIONS OF THE SOC

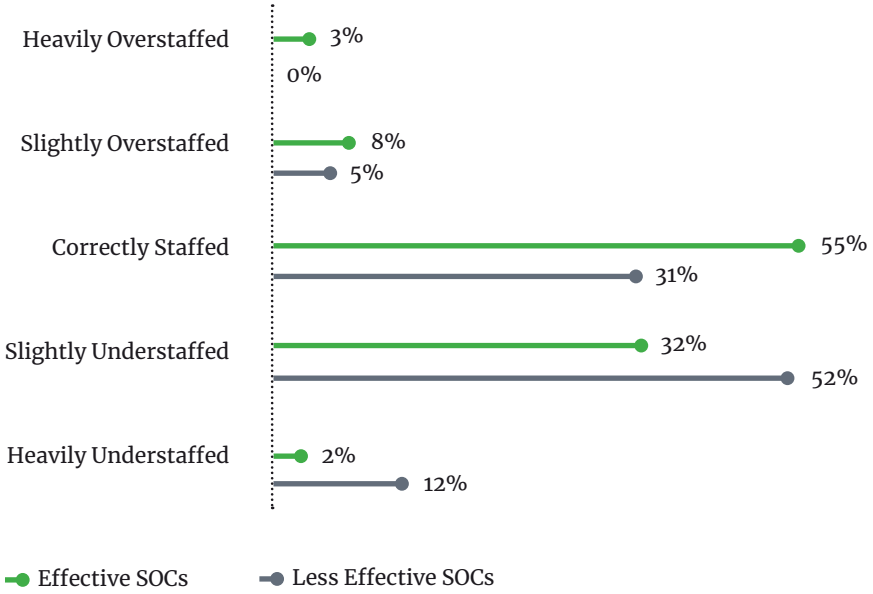


STAFFING LEVELS

Less effective SOCs provide less funding for staffing and technology and more funding for facilities and management than efficiently run SOCs.

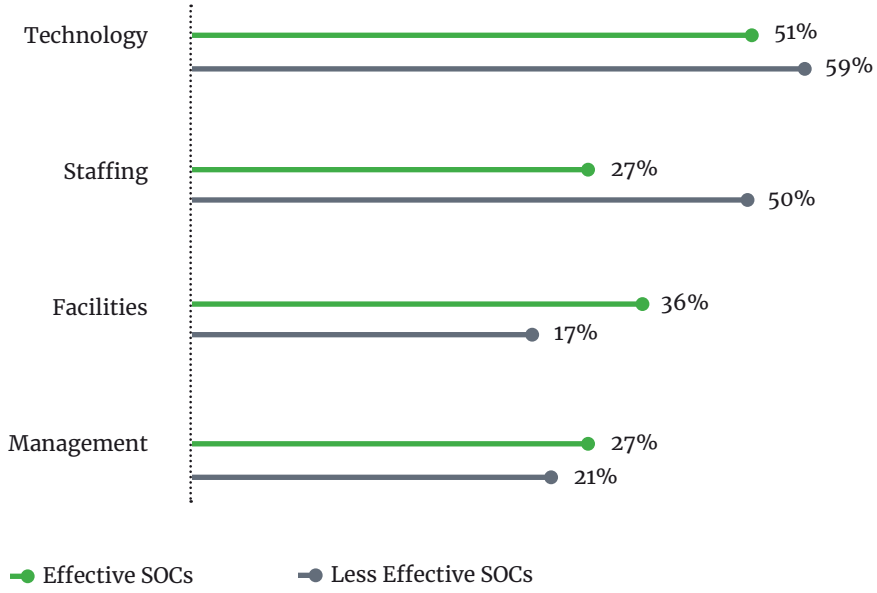
It is not a surprise that less effective SOCs believe they are understaffed. Adequate staffing and good leadership allow the SOC to look beyond the daily alerts and consider thematic measures of efficiency and maturity.

COMPARING THE STAFFING LEVELS AND TECHNOLOGY FUNDING OF EFFECTIVE AND LESS EFFECTIVE SOCS



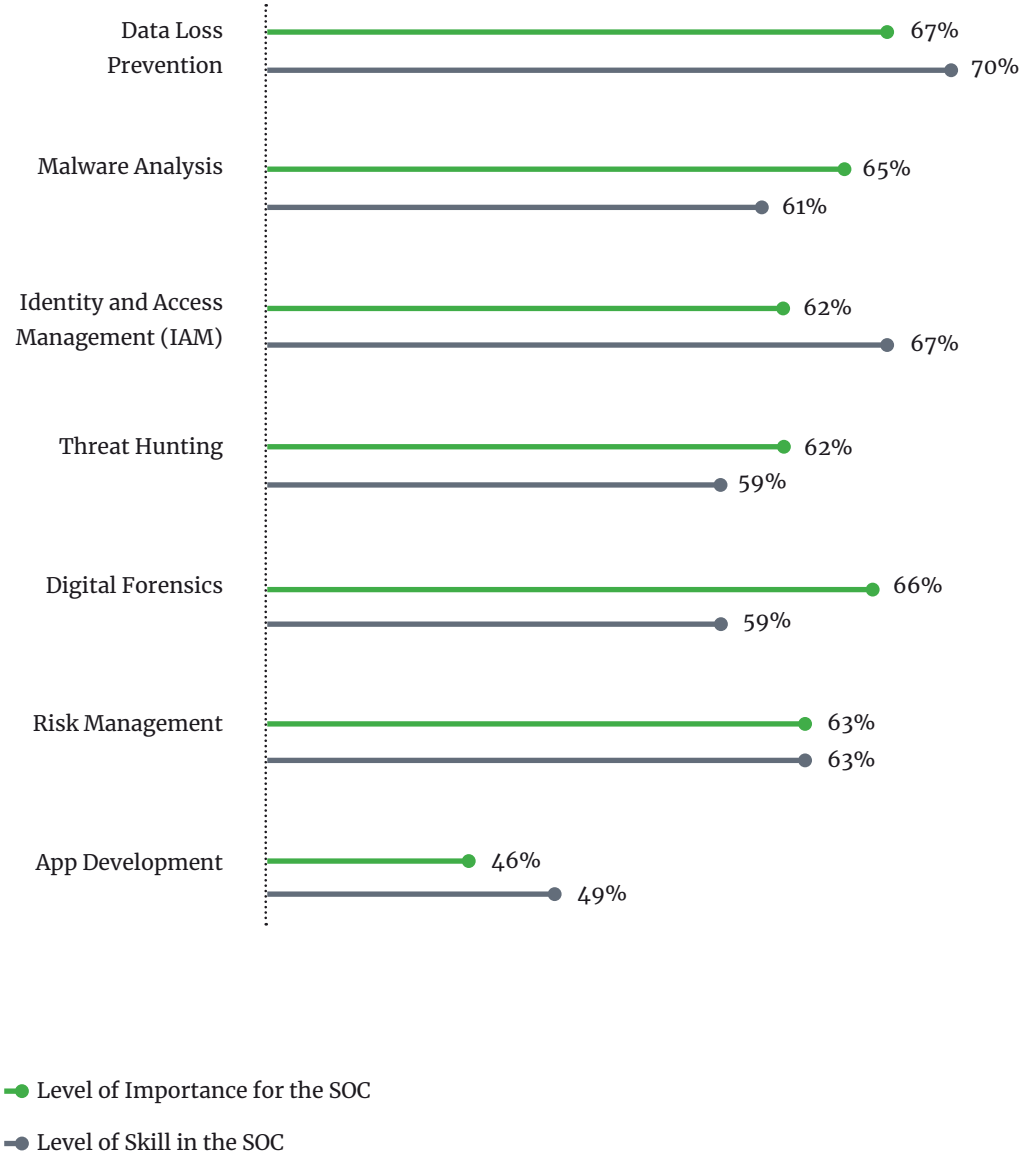
AREAS OF TECHNOLOGY FUNDING: SOCS THAT ARE RATED EFFICIENT OR INEFFICIENT AND THE AREAS WHERE THEY ARE UNDERFUNDED

COMPARING THE STAFFING LEVELS AND TECHNOLOGY FUNDING OF EFFECTIVE AND LESS EFFECTIVE SOCS



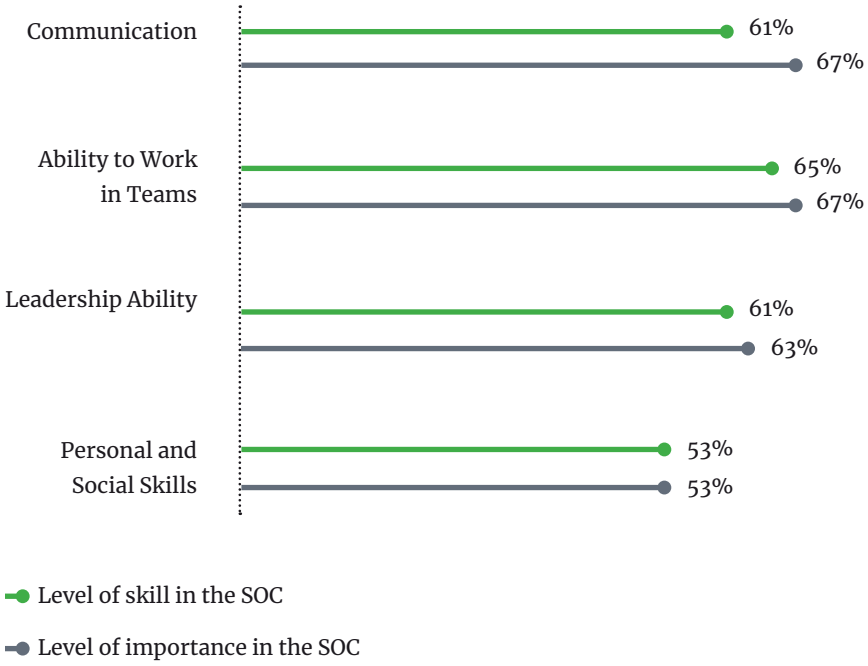
TOP ACTIVITIES AND TECHNOLOGIES USED FOR THE OPERATIONS OF THE SOC AND THEIR LEVEL OF IMPORTANCE

Malware analysis, threat hunting and digital forensics are considered more important than the current level of skill in the SOC, while identity and access management (IAM) and app development is considered less important than the level of skill in the SOC.



THE IMPORTANT SOFT SKILLS FOR THE OPERATIONS OF A SOC AND THEIR LEVEL OF IMPORTANCE

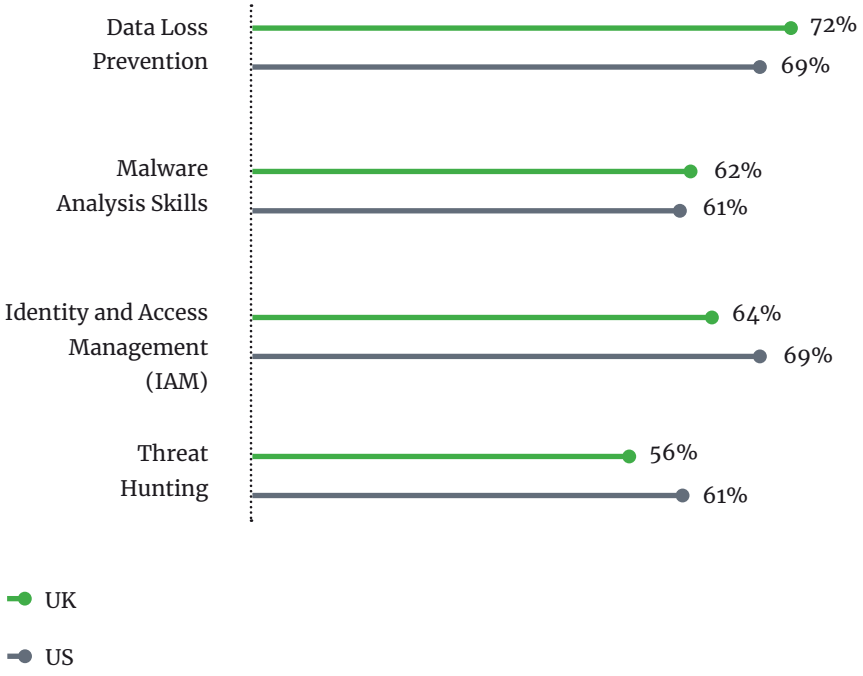
There are no major gaps, but it is interesting how personal and social skills rank the lowest. Emotional intelligence (EQ) is often the bedrock of a healthy and productive team, especially during a crisis or when onboarding and training new staff.



COMPARING US AND UK SOCS: THEIR MOST IMPORTANT ACTIVITIES AND THEIR LEVEL OF SKILL

There are no significant gaps in the skillsets of SOCs in the U.S. versus the U.K. The U.S. SOCs lead slightly in identity and access management (IAM) and threat hunting, while the U.K. leads slightly in data loss prevention and malware analysis.

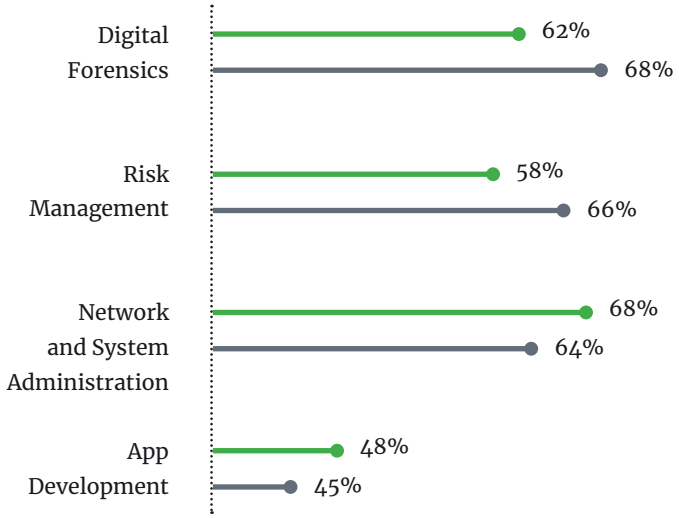
CURRENT SKILLSETS IN THE SOC



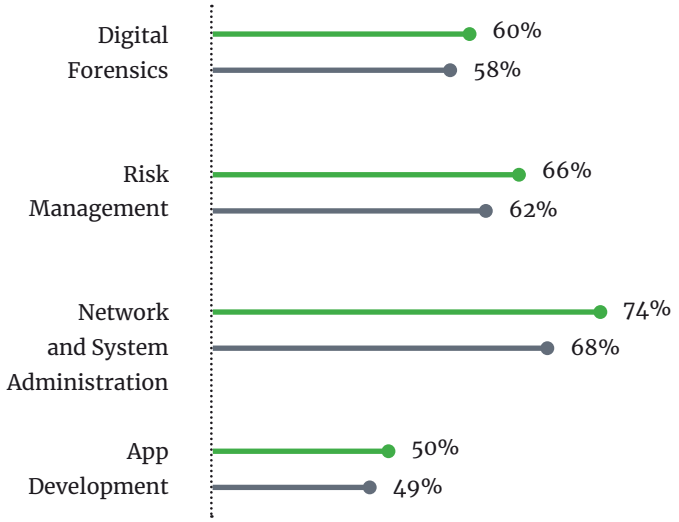
COMPARING SOCS IN THE US AND UK: CYBERSECURITY ACTIVITIES AND THEIR LEVEL OF IMPORTANCE

Risk management is not seen as important in the U.K., but a more developed skill set than in the U.S.

LEVEL OF IMPORTANCE

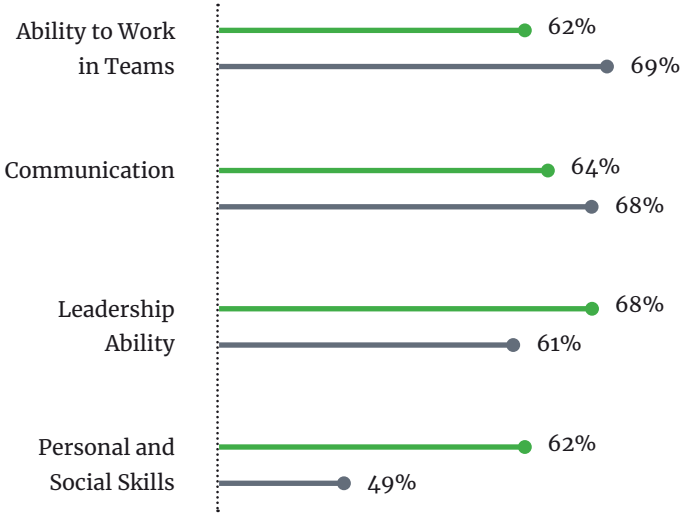


CURRENT SKILLSETS IN THE SOC

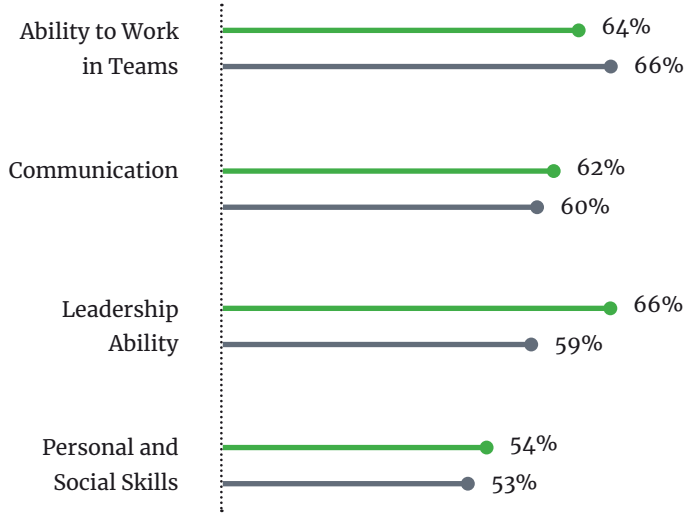


COMPARING SOCS IN THE US AND UK: THE IMPORTANCE OF SOFT SKILLS AND THEIR LEVEL OF DEVELOPMENT

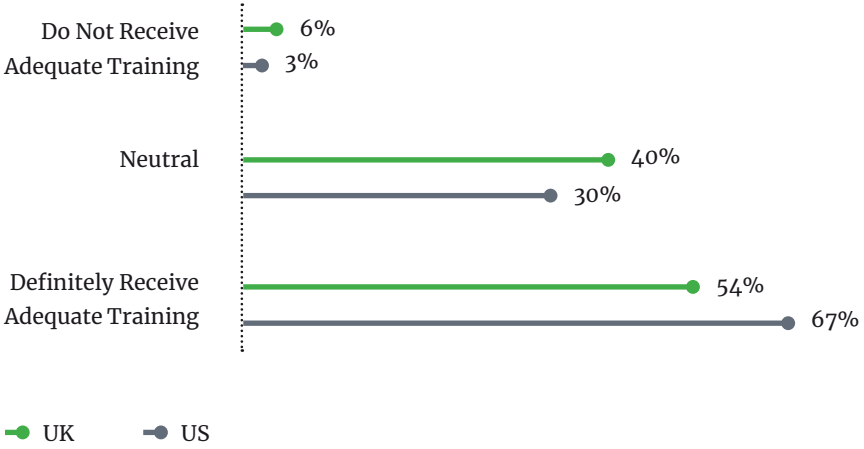
LEVEL OF IMPORTANCE



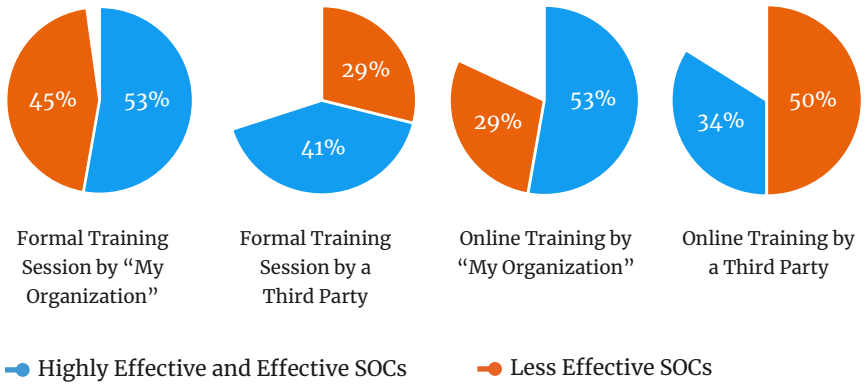
CURRENT SKILLSETS IN THE SOC



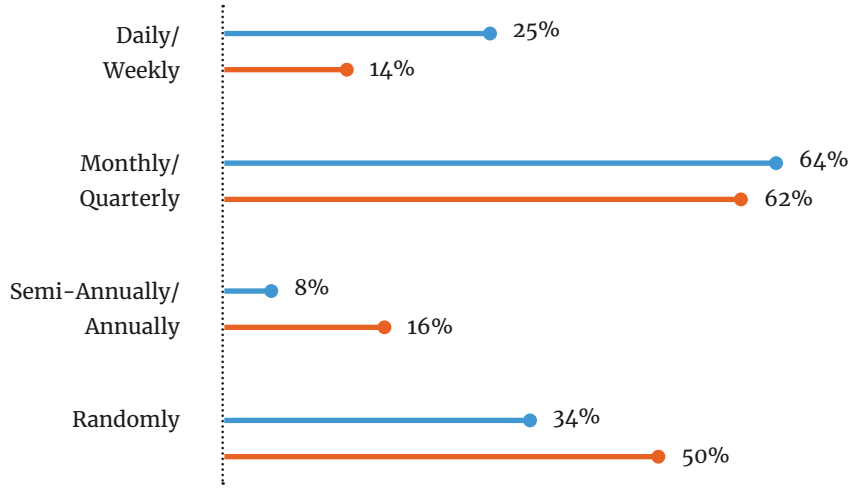
SOCS IN THE US RECEIVE MORE ADEQUATE TRAINING THAN THOSE IN THE UK



TYPE OF TRAINING RECEIVED

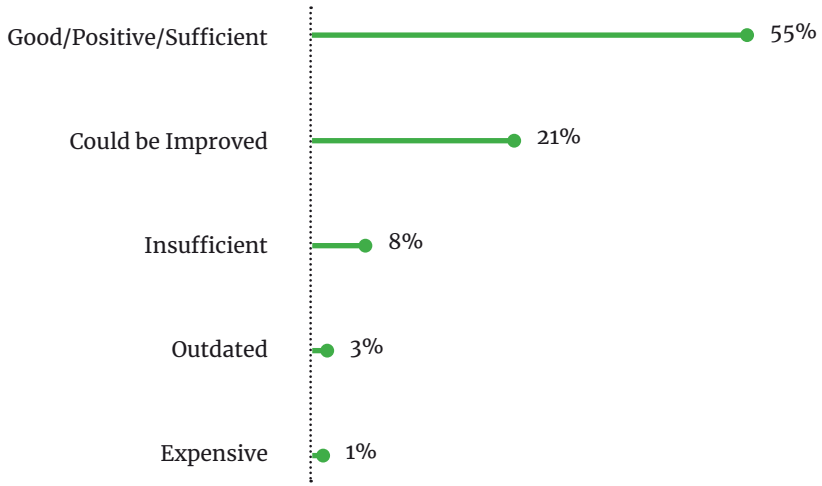


Effective SOCs have more frequent training consisting of online trainings provided by their organization and third parties providing the formal training.



MORE THAN HALF OF SOCS SEE THEIR TRAINING PROGRAMS AS POSITIVE

THOUGHTS ON TRAINING



"I would prefer more training. I find most of the training we receive to be valuable, but the company and our employees would benefit from more frequent opportunities to learn or improve our skills."

ISO, U.S., 3-5 YRS, $300-499 MILLION, INFORMATION TECHNOLOGY

"It is never enough and threats change frequently so you have to keep on drill training."

RISK / COMPLIANCE OFFICER, U.S., 9-10 YRS, $1-4.99 BILLION, INFORMATION SERVICES AND DATA PROCESSING

"Most is too generic to be of any real value."

RISK / COMPLIANCE OFFICER, U.S., 9-10 YRS, $1-4.99 BILLION, INFORMATION SERVICES AND DATA PROCESSING

"It is extremely important to keep abreast of developments."

ISO, U.K., 11-15 YRS, $800-999 MILLION, INFORMATION SERVICES AND DATA PROCESSING

"It's excellent; the initial and remedial training are the best in our field."

ISO, U.S., 11-15 YRS, $1-4.99 BILLION, TRANSPORTATION AND WAREHOUSING

"It's great, but few have time to take advantage of it."

CIO, U.S., 11-15 YRS, $1-4.99 BILLION, FINANCE AND INSURANCE

KEY FINDINGS

Key Findings on the Operations of the SOC

EFFECTIVENESS OF THE SOC

Large SOCs are the most confident in their ability to respond to incidents and business challenges.

PAIN POINTS

- Frontline workers spend a disproportionate amount of time on reporting and documentation in comparison to managers and the C-suite.
- Managers and frontline workers see technology (42%) as a much bigger problem than does the C-suite (27%). This may indicate a lack of awareness on technology needs from the C-suite.
- Frontline workers see inexperienced staff (38%) as a much larger pain point than do managers or the C-suite (23%).

42%

of managers and frontline workers see technology as a problem

27%

of C-suite members see technology as a problem

38%

of frontline workers see inexperienced staff as a pain point

23%

of C-suite members see inexperienced staff as a pain point

TRAINING

- Majority (63%) of organizations have monthly and quarterly training.
- Employees feel that the adequacy of training decreases as the frequency of training decreases.
- More than 50 percent are satisfied with their current training.

63%

of organizations have monthly and quarterly training

50%

of employees are satisfied with their current training

METRICS

- Small SOCs tend to track fewer metrics than large SOCs.
- Exceptions to this are incident occurrence due to known vulnerabilities and the monetary cost per incident.

DEPARTMENTS INVOLVED WITH THE SOC

- The SOC overwhelmingly interfaces mainly with the IT department 90 percent of the time.
- The operations department is the next closest at 59 percent of the time.

90%

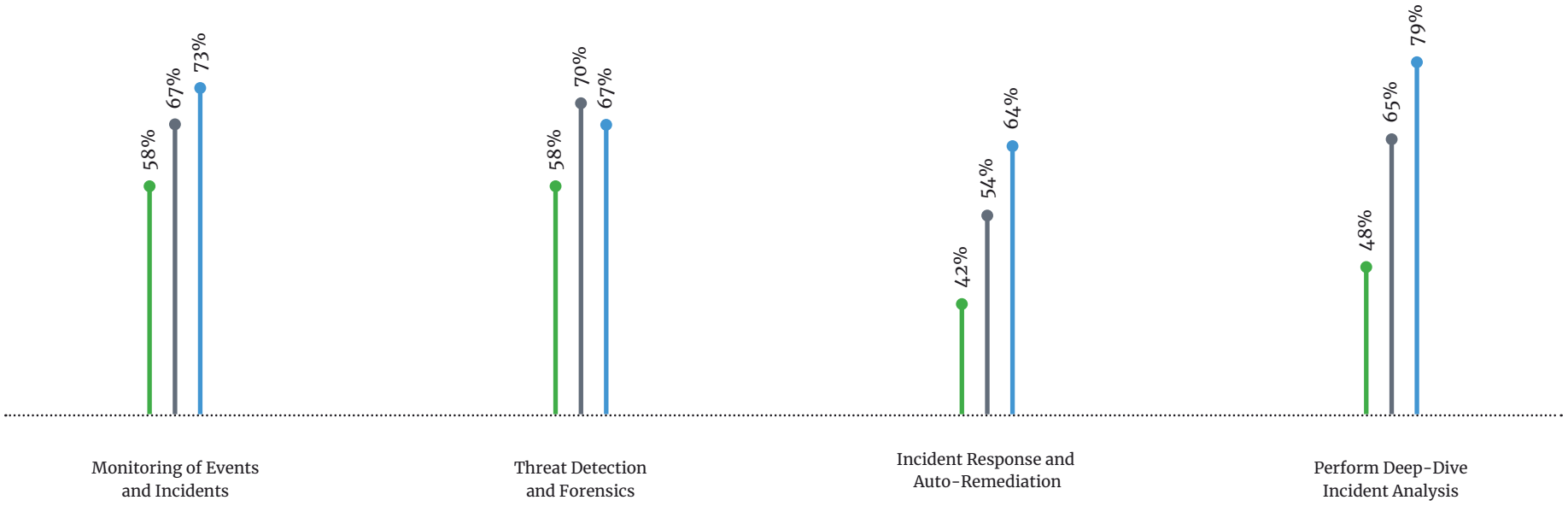
is the rate of time that the SOC interfaces with the IT department

59%

is the rate of time that the SOC interfaces with the operations department

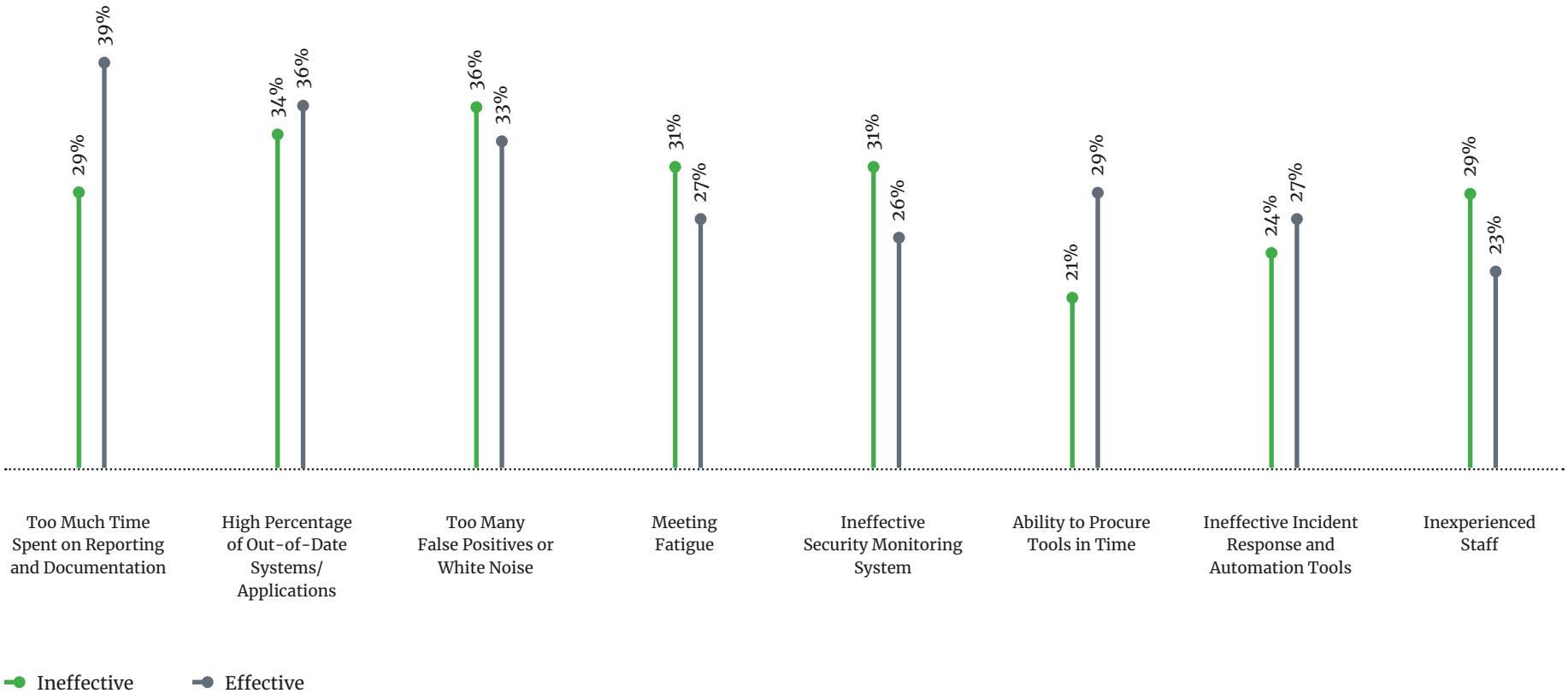
Confidence in the ability to respond to incidents or business demands is highest in large SOCs. Medium-sized organizations have greater confidence in their threat detection than larger companies. Smaller companies have the least confidence in their incident response.

EFFECTIVENESS OF THE SOC TEAM AND ITS ABILITY TO RESPOND TO COMMON ISSUES ACCORDING TO THE SIZE OF THE COMPANY



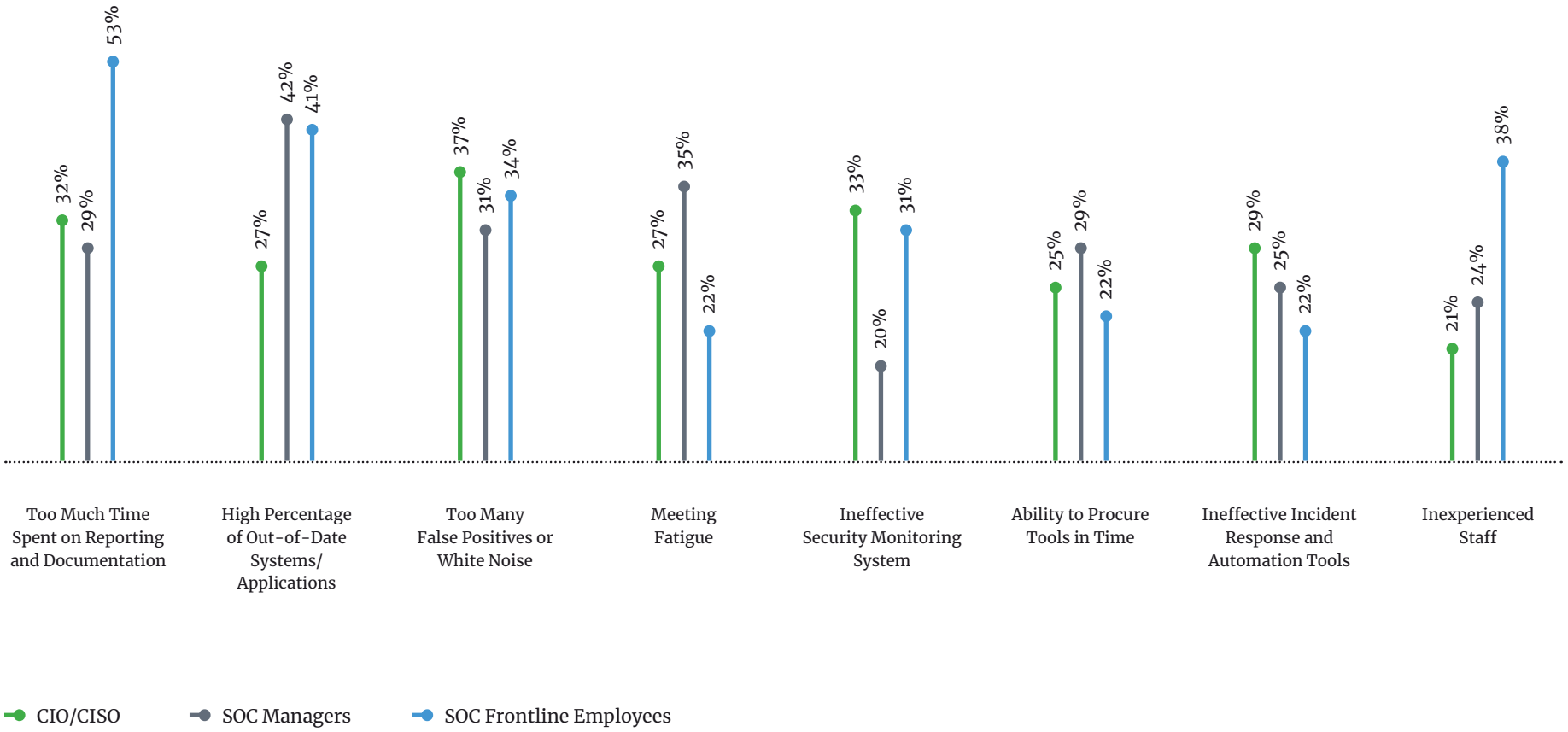
While both the ineffective and the effective SOCs must manage and interact with out-of-date technology, highly efficient SOCs are working on limiting the time spent on reporting and documentation. Automating investigations and responses through playbooks, and creating reusable reports for internal organizations, address this concern over time.

COMMON PAIN POINTS EXPERIENCED IN THE SOC

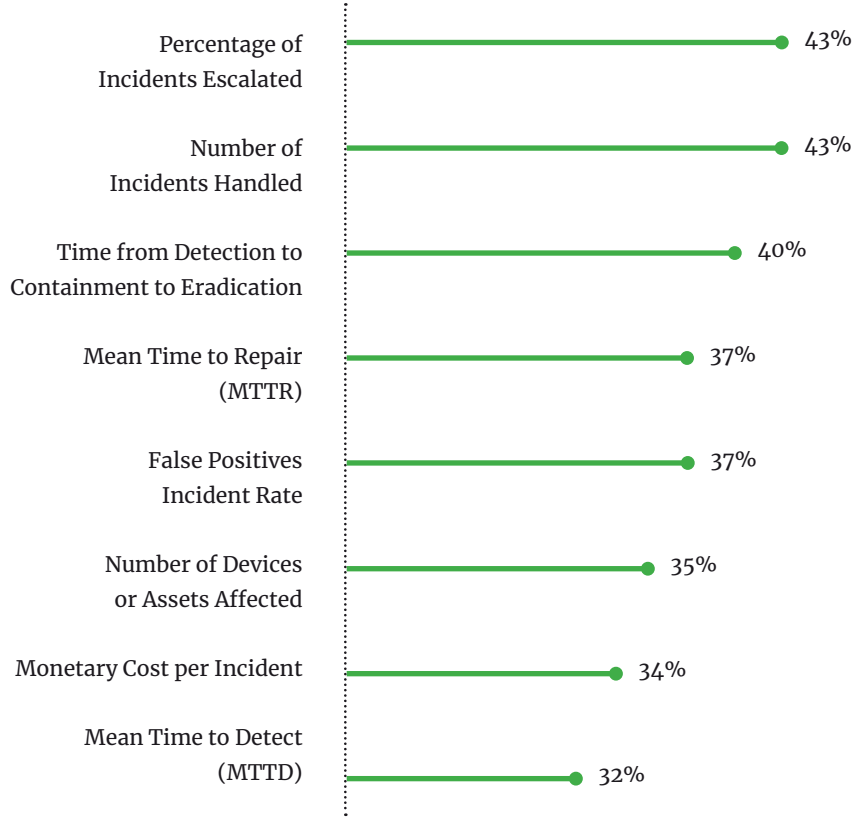


The top pain points for CIOs and CISOs are false positives and white noise. For managers, it is the high percentage of out-of-date systems and applications. Frontline workers experience the greatest pain points with documentation and reporting and out-of-date systems.

COMMON PAIN POINTS EXPERIENCED IN THE SOC ACCORDING TO ROLE



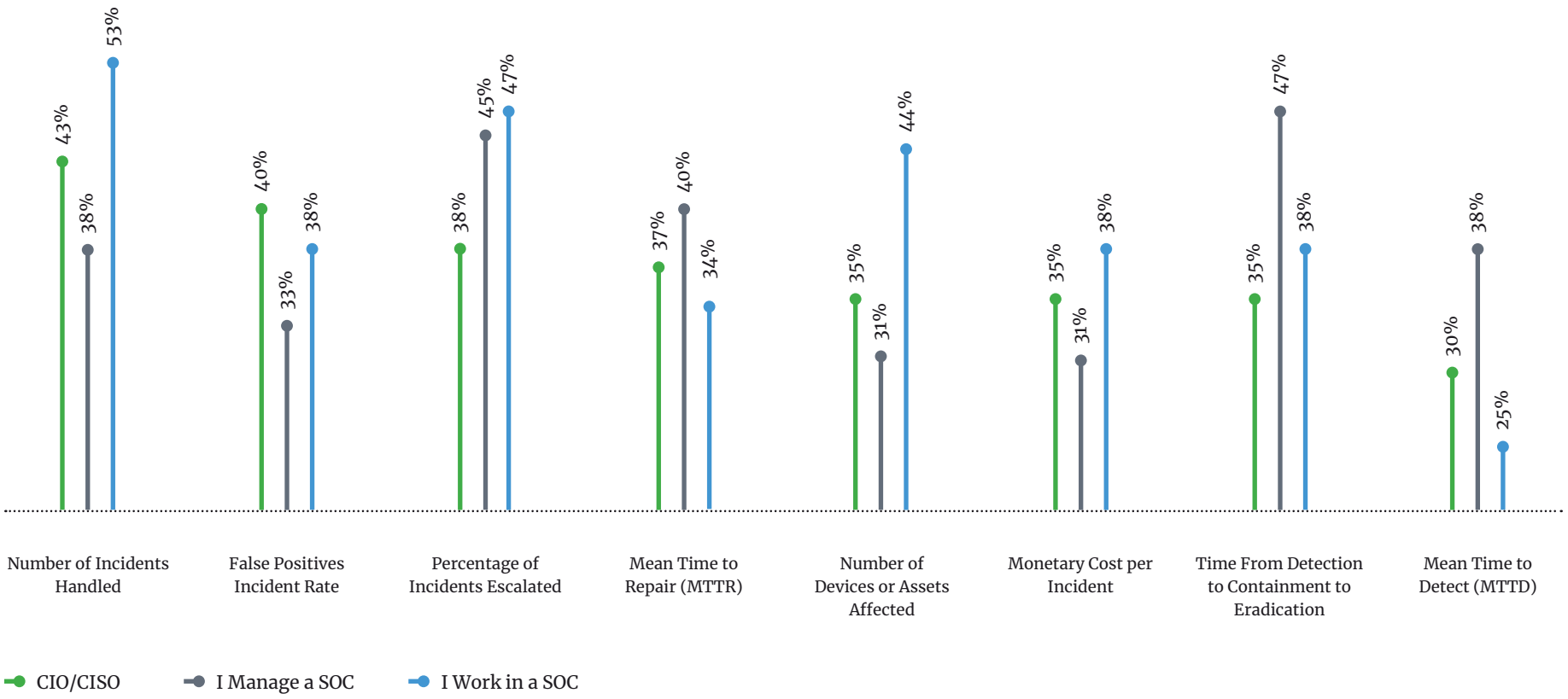
TOP METRICS AND STATS COMMONLY TRACKED BY THE SOC



It is impressive to see at least a third of organizations are tracking effort-based metrics tied to response and environmental repair.

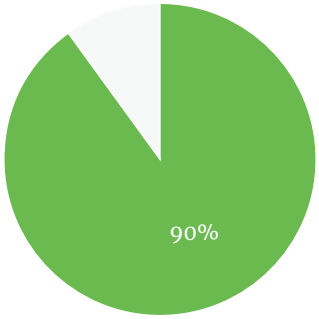
Executives are more interested in the raw number of incidents and false positives, while SOC management is focused more on eradication times. Interestingly, SOC analysts are the least interested in mean time to detect (MTTD) and repair times (MTTR), which could be due to many factors, including emphasis on other measures or simply investigative fatigue.

TOP METRICS COMMONLY TRACKED BY THE SOC

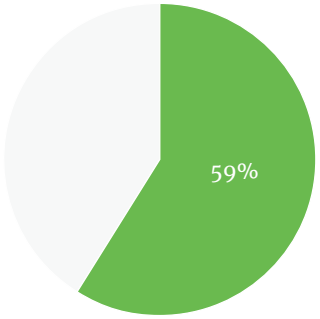


While SOCs must cover the entire organization, it is interesting to see that so many are collaborating with Sales (18%) and Marketing (21%). It is a path to organizational relevance when a SOC can add value to the departments that help earn revenue for the company.

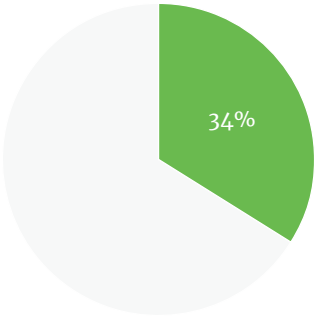
DEPARTMENTS MOST INVOLVED WITH THE SOC



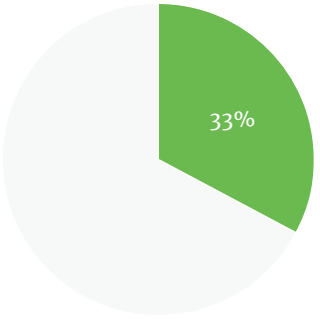
IT



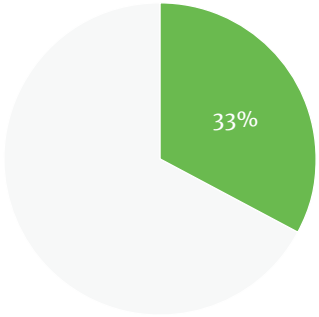
Operations



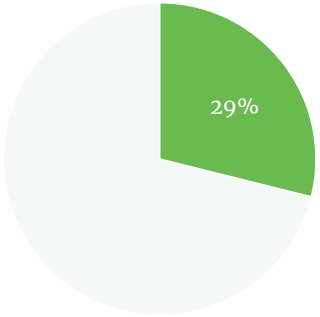
Finance



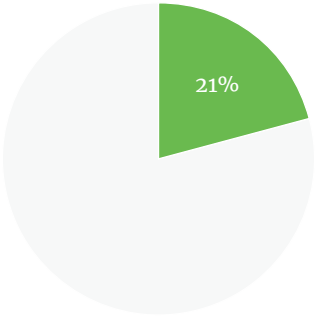
Engineering



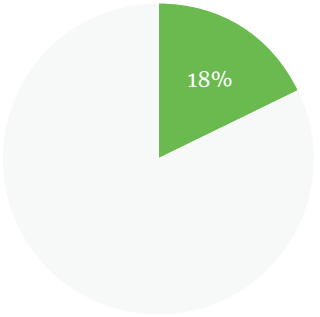
HR



Accounting



Marketing



Sales

KEY FINDINGS

Key Findings on Technologies Employed in the SOC

UPCOMING TECHNOLOGIES

- Machine learning technologies are perceived as some of the soonest to impact the security space.
- Artificial intelligence is a technology that will take the longest before it is ready to impact the security industry.

PAIN POINTS IN TECHNOLOGY

- Frontline workers and managers are more concerned with keeping up with security alerts (47%) than the C-suite (35%).
- Technology is two times more of a pain point for frontline workers (50%) than for the C-suite (22%). This could be due to the C-suite not being informed about the technologies being utilized.

47%

of frontline workers and managers are concerned with keeping up with security alerts

35%

of C-suite members are concerned with keeping up with security alerts

50%

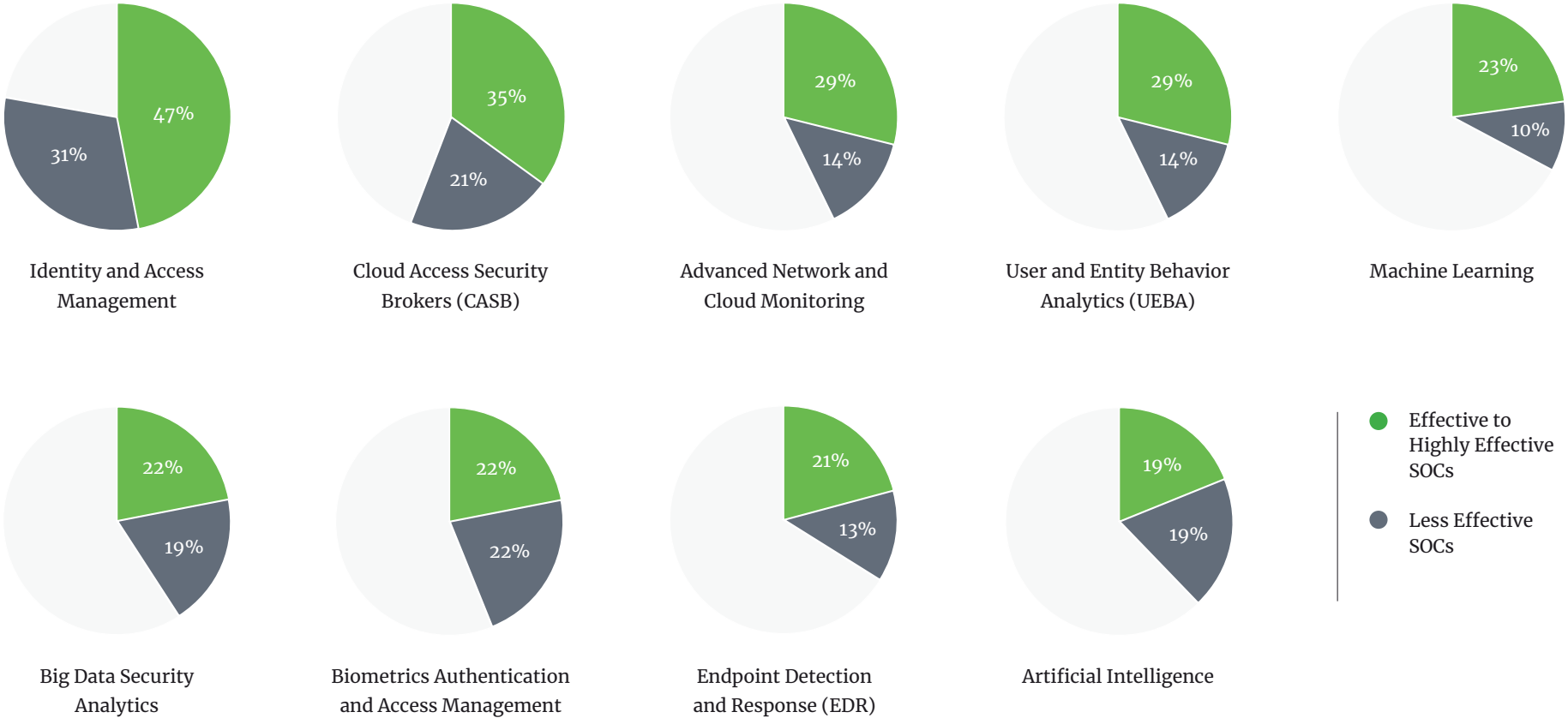
of frontline workers find technology to be a pain point

22%

of C-suite members find technology to be a pain point

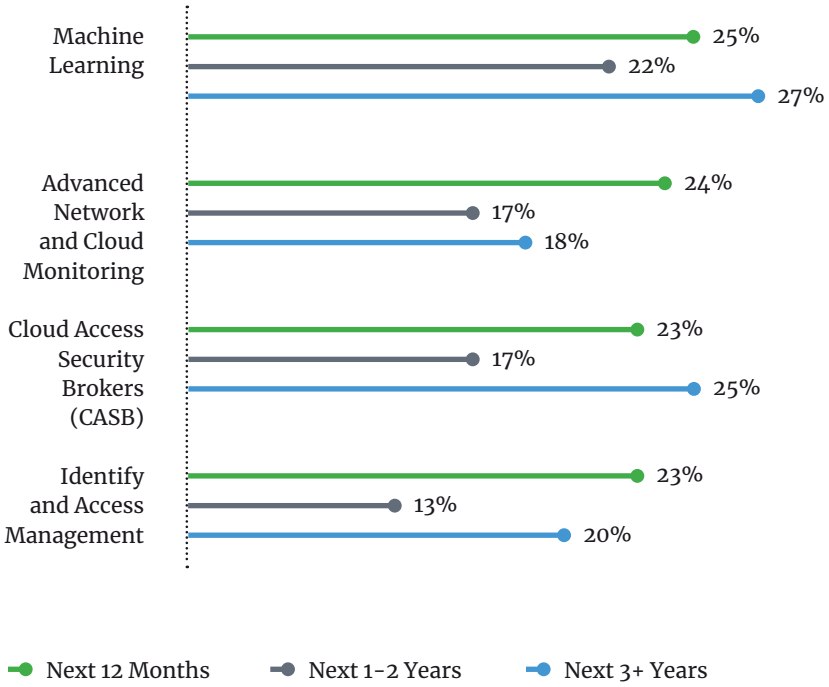
On the surface, SOCs that rate themselves as highly effective have adopted technology at a higher rate than those that rate themselves as less effective. Based on recent data, this could be tied to a lack of talent or funding.

TECHNOLOGY CURRENTLY ADOPTED BY SOCS

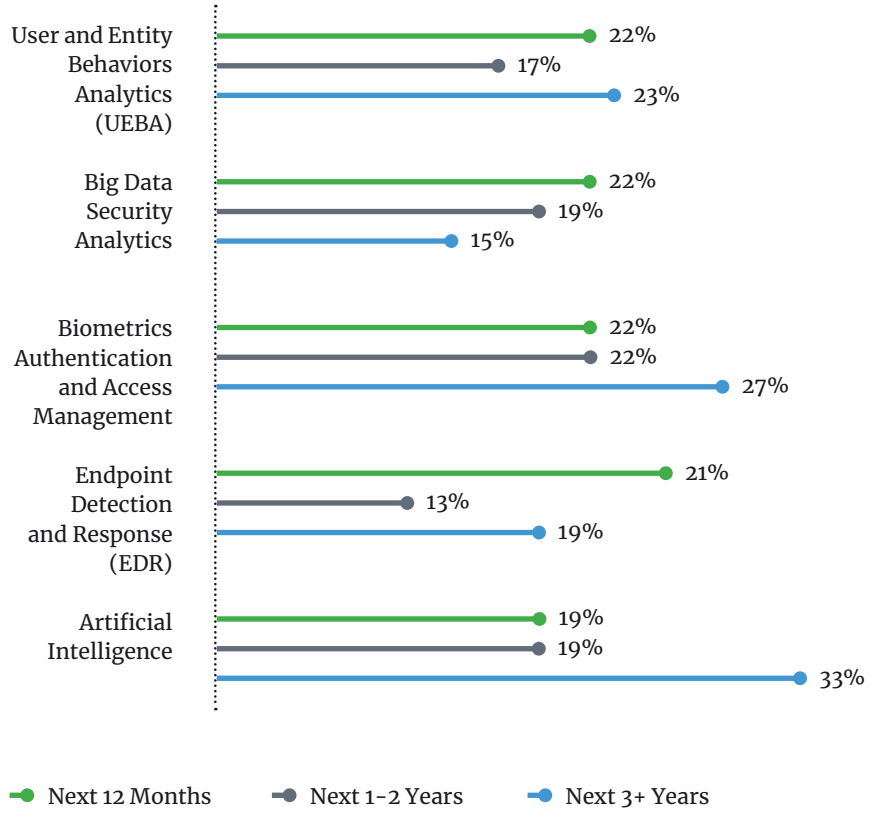


TOP TECHNOLOGIES THAT WILL IMPACT THE SOC IN THE FUTURE

Across the board, machine learning was predicted to be the next technology to purchase and deploy, followed by cloud visibility solutions. Why? When it comes to the cloud, you can't protect what you're not able to see. And without the advantages of machine learning, teams won't be able to fully respond to what they can't completely investigate.

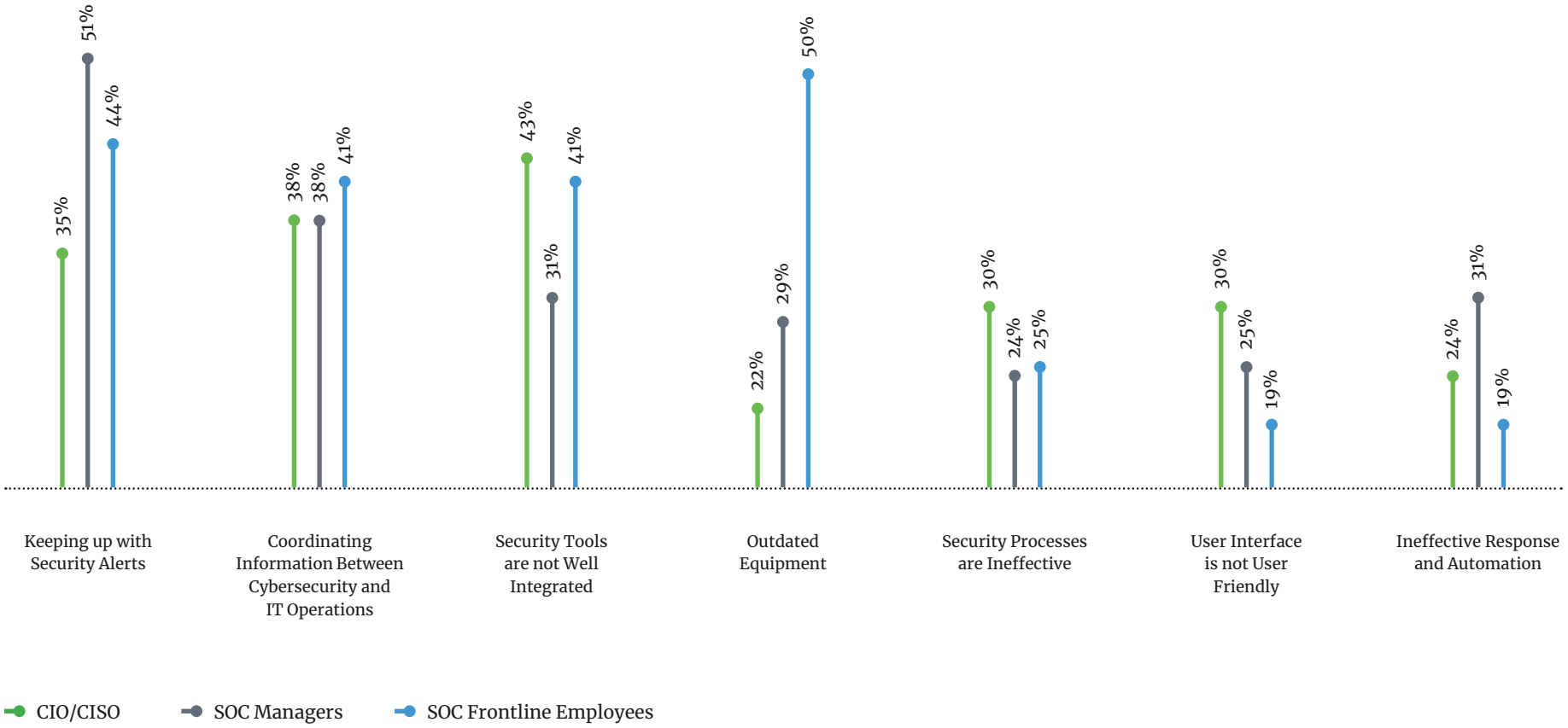


The long-tail prediction of artificial intelligence adoption will become better understood with time, with 33 percent predicting its adoption occurring in the next three or more years. As Exabeam's chief data scientist Derik Lin has said, "Today, AI is often little more than a catchy marketing label, liberally applied to any system that performs tasks having some semblance of automated decision-making."



Information security professionals are often the first to find pain points. SOC analysts are most interested in old technology and the high number of alerts, because it has a negative effect on the quality of their work. However, managers and executives do not see the same effects.

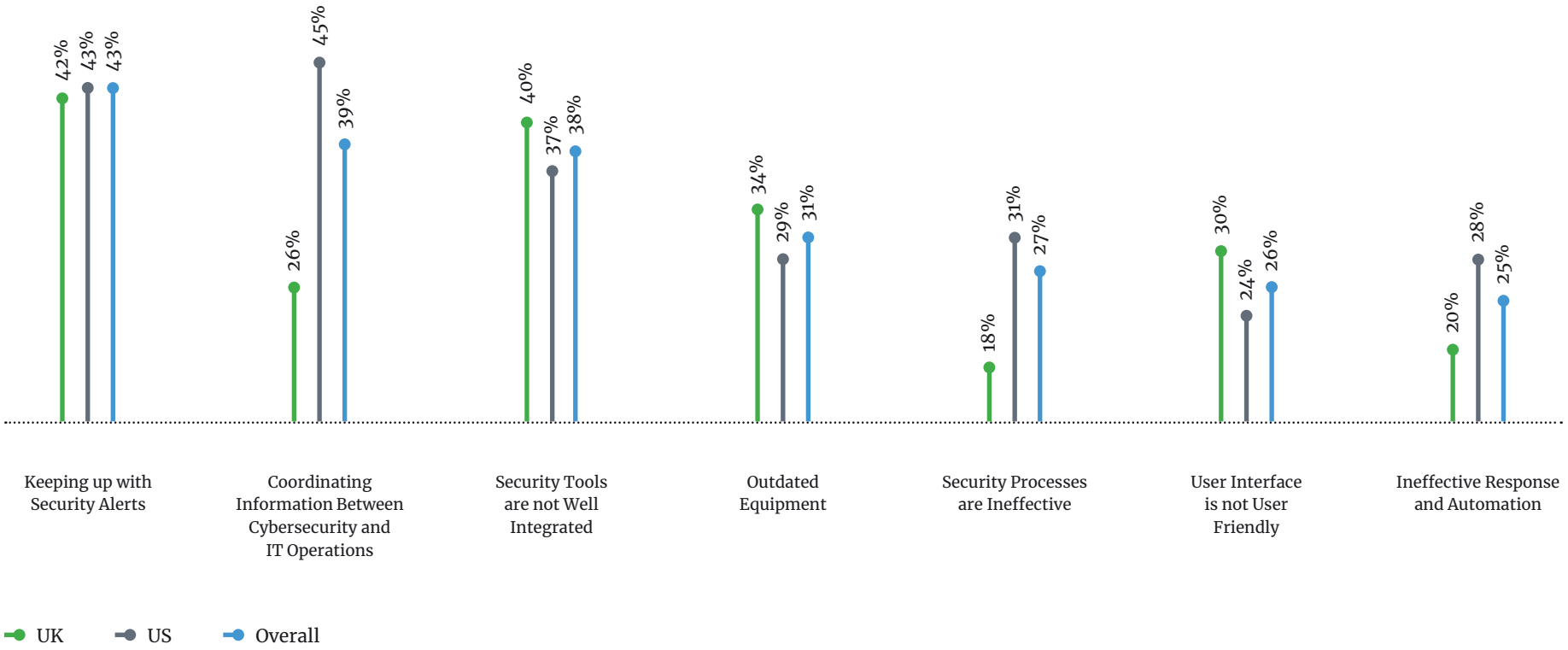
COMMON TECHNOLOGY PAIN POINTS EXPERIENCED IN THE SOC BY ROLE



US-BASED SOCS HAVE A MORE DIFFICULT TIME CREATING EFFICIENT PROCESSES, WHILE THOSE IN THE UK STRUGGLE MORE WITH HAVING OUTDATED TECHNOLOGY

Comparing the U.S. versus the U.K., all SOCs struggle with too many alerts, which create poor analytic and response cultures. In the U.S., there is almost double the pain associated with IT coordination, and there are significant issues with ineffective security processes.

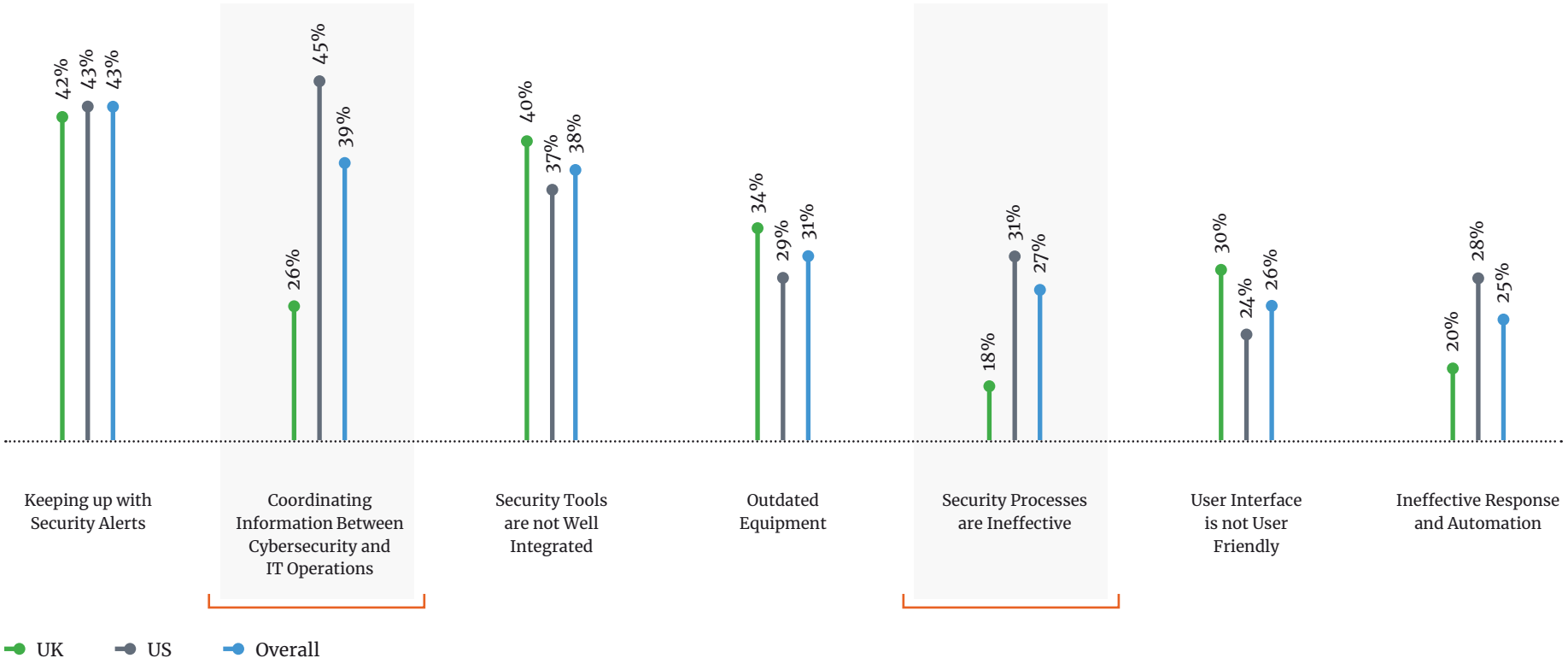
COMMON PAIN POINTS EXPERIENCED IN THE SOC FOR TECHNOLOGY



SECURITY PROCESSES AND COORDINATION ARE SEEN AS MORE OF A PROBLEM IN THE US THAN THE UK

To continue comparisons of the U.S. and the U.K. SOCs, the biggest need according to the U.S. respondents is for improved processes, while the U.K. respondents overwhelmingly said technology sophistication was their greatest need. This could have something to do with the age of the technologies and the inception date differences of SOCs in the U.S. versus the U.K.

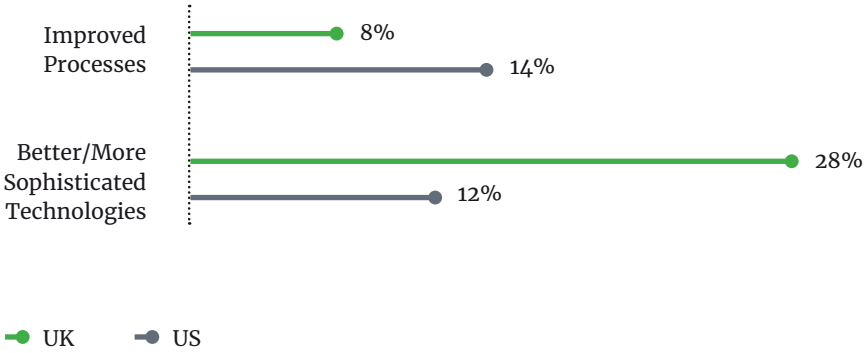
COMMON PAIN POINTS EXPERIENCED IN THE SOC FOR TECHNOLOGY



GREATEST NEED IN THE SOC IN THE US AND UK

The U.S. sees the biggest need for improved processes for the SOC, while the U.K. would like more sophisticated technologies.

GREATEST NEEDS OF THE SOC



KEY FINDINGS

Key Findings on the Financing and Budgeting of the SOC

FUNDING ALLOCATION

- According to many of the respondents, funding is sufficiently allocated (51%), but many expressed that they would like to have a larger budget (81%).

51%

of employees feel that funding for their SOC is sufficiently allocated

81%

of employees felt that they would like to see a larger budget

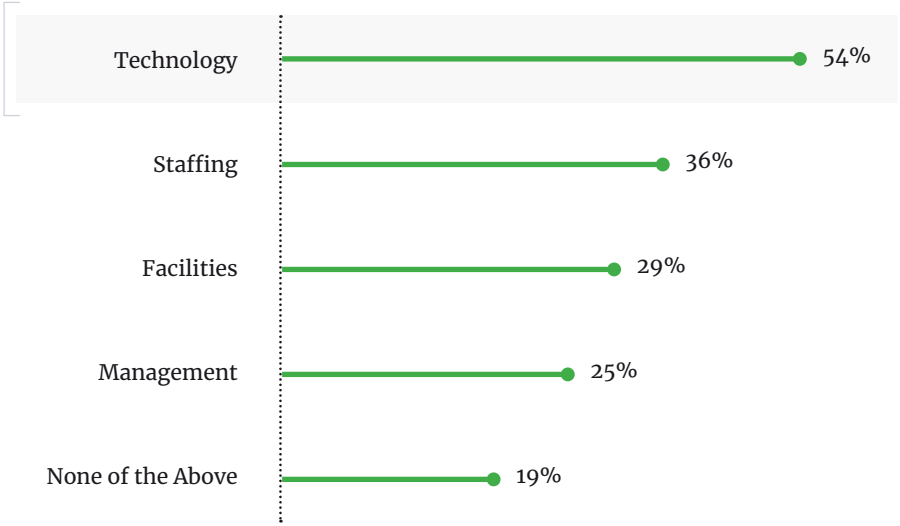
CYBERSECURITY INSURANCE

- Only half of companies have cybersecurity insurance. There is little to no correlation between SOC size and cybersecurity insurance.
- Many of the respondents who have chosen not to have cybersecurity insurance feel that it is unnecessary or too expensive (45%).

45%

of SOCs who have chosen not to have cybersecurity insurance feel that it is unnecessary or too expensive

FIFTY-FOUR PERCENT RESPONDED THAT THEY ARE UNDERFUNDED WHEN IT COMES TO TECHNOLOGY



"At the moment yes, however, this needs to be reviewed on a regular basis."

ISO, U.K., 11-15 YRS, $800-999 MILLION, INFORMATION SERVICES AND DATA PROCESSING

"I think we have too much spent on monitoring systems when what we need are more trained staff to help incident prevention."

CIO, U.S., 11-15 YRS, $1-4.99 BILLION, FINANCE AND INSURANCE

"Not allocated efficiently as we need more technical and less administrative."

SECURITY ENGINEER / MANAGER / ANALYST, U.S., 11-15 YRS, $1-4.99 BILLION, OTHER MANUFACTURING

"Additional resources should be allocated to staffing."

CYBERSECURITY ANALYST, U.S., 3-5 YRS, $1-4.99 BILLION, FINANCE AND INSURANCE

"The budget is allocated correctly, but I don't think the budget is big enough to begin with, which explains the underfunding."

ISO, U.S., 3-5 YRS, $300-499 MILLION, INFORMATION TECHNOLOGY

"I think it could be better aligned in regards to AI and multicomputer-based cyber hackers."

CIO, U.K., 6-8 YRS, $5-9.99 BILLION, FINANCE AND INSURANCE

"It's allocated perfectly as planned."

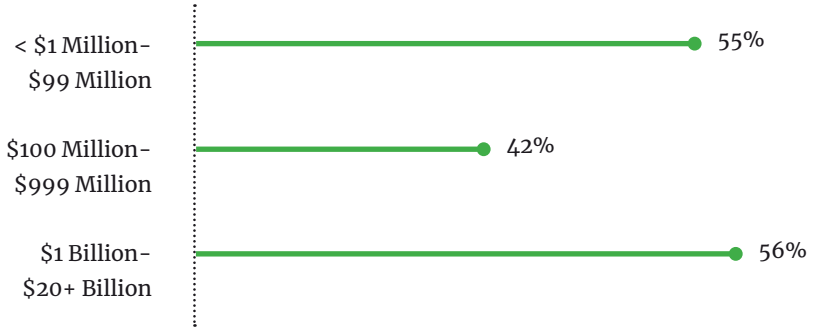
CIO, U.S., 9-10 YRS, $500-799 MILLION, HEALTHCARE AND SOCIAL ASSISTANCE

"Management needs to fund more so that the security events can be handled more efficiently. Better be prepared than sorry."

CIO, U.S., 9-10 YRS, $5-9.99 BILLION, FINANCE AND INSURANCE

COMPANY SIZE IN RELATION TO CYBERSECURITY INSURANCE

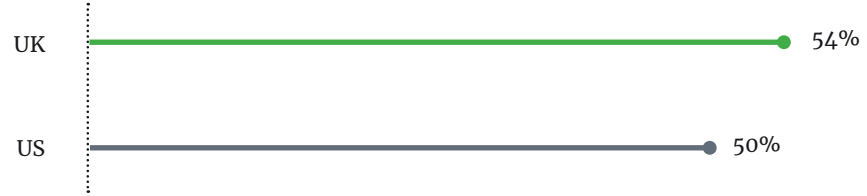
Only half of companies with the SOC have cybersecurity insurance. Of those that do, it appears the size of the company is not a driver for having insurance.



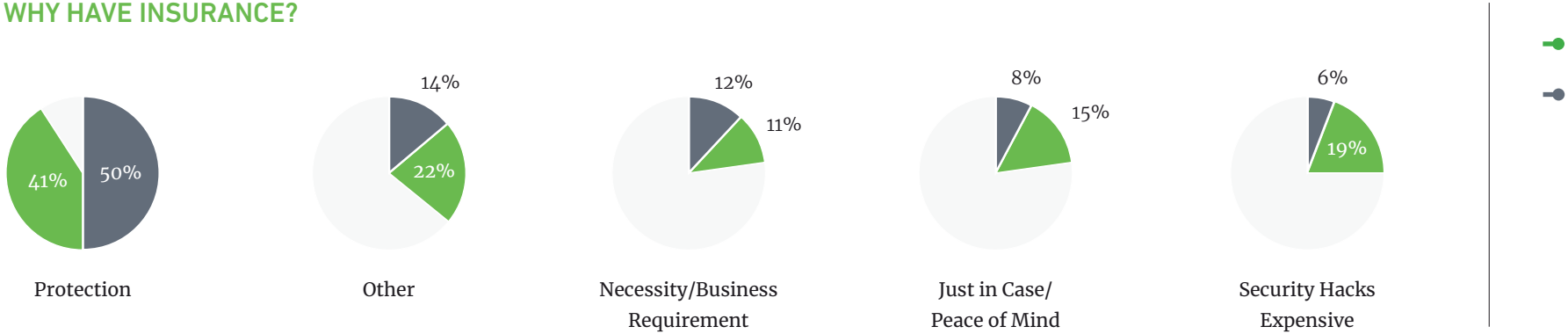
CYBERSECURITY INSURANCE

While both the U.S. and the U.K. are likely to have insurance, SOCs in the U.K. believe that the reason why is because security hacks are more expensive.

SOCS WITH INSURANCE



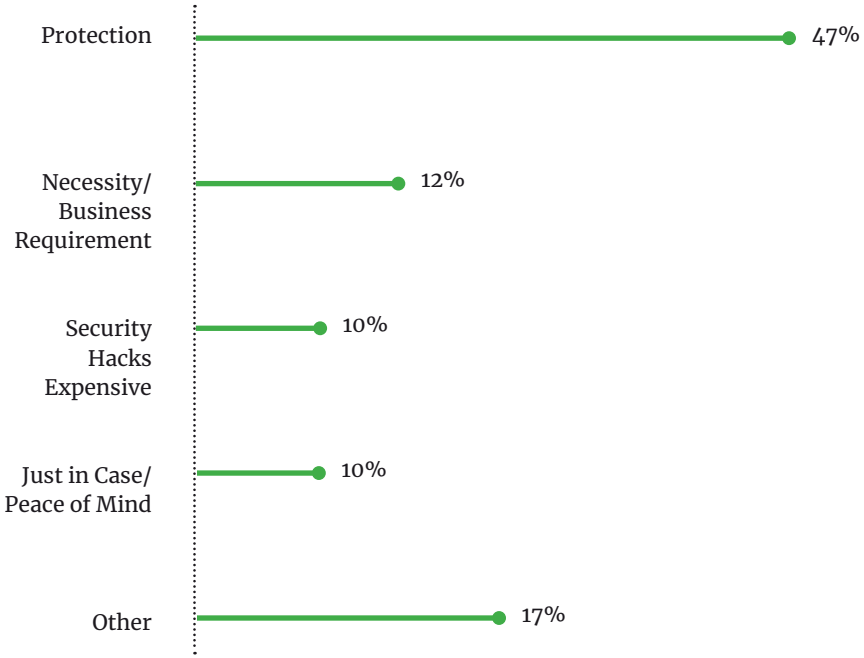
WHY HAVE INSURANCE?



CYBERSECURITY INSURANCE

Protection of data and the organization is the biggest driver for cybersecurity insurance. Those that do not have insurance feel that it is unnecessary or too expensive.

REASONS ORGANIZATIONS DO HAVE CYBERSECURITY INSURANCE



"For coverage and peace of mind, so that we can be assured that we have back up if anything were going wrong."

CIO, U.K., 6-8 YRS, $800-999 MILLION, RETAIL

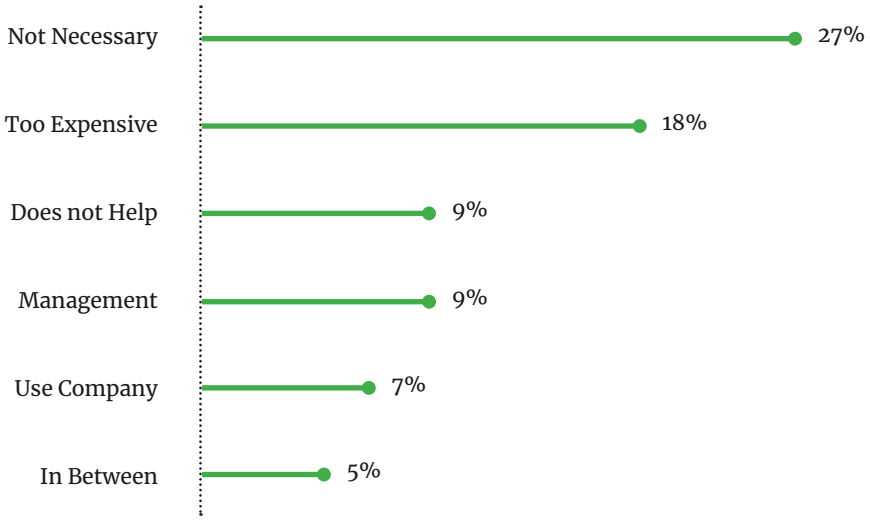
"Because we need to make sure that we are properly protected."

ISO, U.K., 11-15 YRS, $300-499 MILLION, PRIMARY/SECONDARY (K-12) EDUCATION

"It was determined that the benefits outweigh the costs."

ISO, U.S., 3-5 YRS, $100-299 MILLION, OTHER MANUFACTURING

REASONS ORGANIZATIONS DO NOT HAVE CYBERSECURITY INSURANCE



"The risk does not outweigh the cost and internal management is sufficiently contained."

SECURITY ENGINEER / MANAGER / ANALYST, U.K., 11-15 YRS, >$20 BILLION, FINANCE AND INSURANCE

"Because we have so much cash flow we are self insured."

ISO, U.S., 6-8 YRS, $1-4.99 BILLION, WHOLESALE

"This doesn't fit into my company's budget at the present time."

ISO, U.S., 3-5 YRS, $50-99 MILLION, INFORMATION SERVICES AND DATA PROCESSING

DEMOGRAPHICS

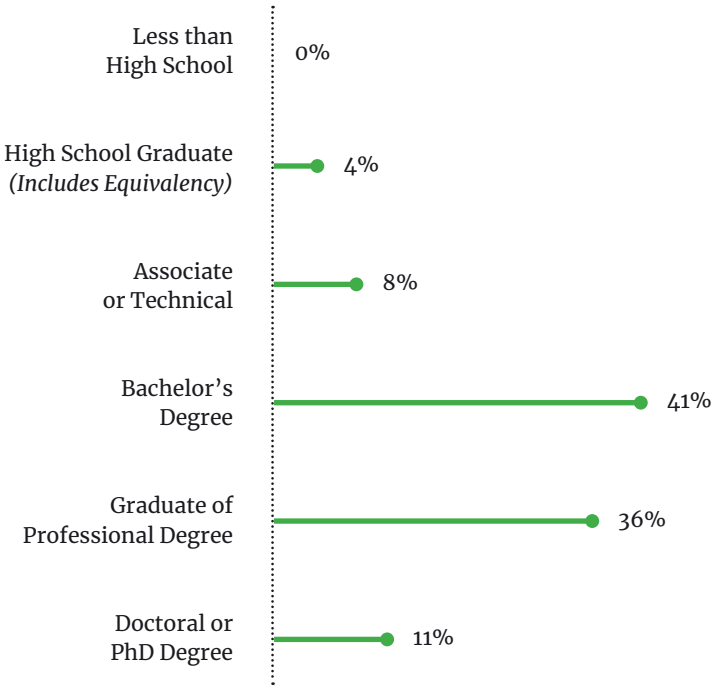
Survey Participant Demographics

The State of the SOC Survey targeted both U.S. and U.K. security professionals in roles across the entire organization from CIOs and CISOs, to SOC managers, to frontline security analysts. All respondents were either full-time or part-time employees in a SOC.

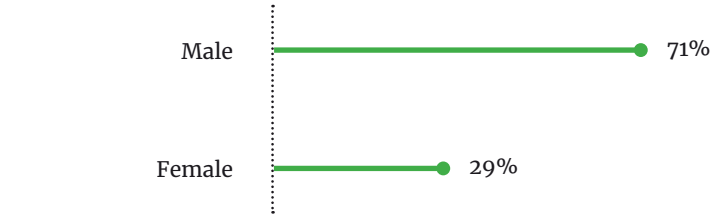
PROFILE OF PARTICIPANT JOB TITLES

- CIO
- CISO
- Information Security Officer
  (Analyst, Manager, VP of Security, Director)
- Threat Research Analyst/Officer
- Security Architect
- Security Engineer/Manager/Analyst
- Risk/Compliance Officer
- Cybersecurity Analyst

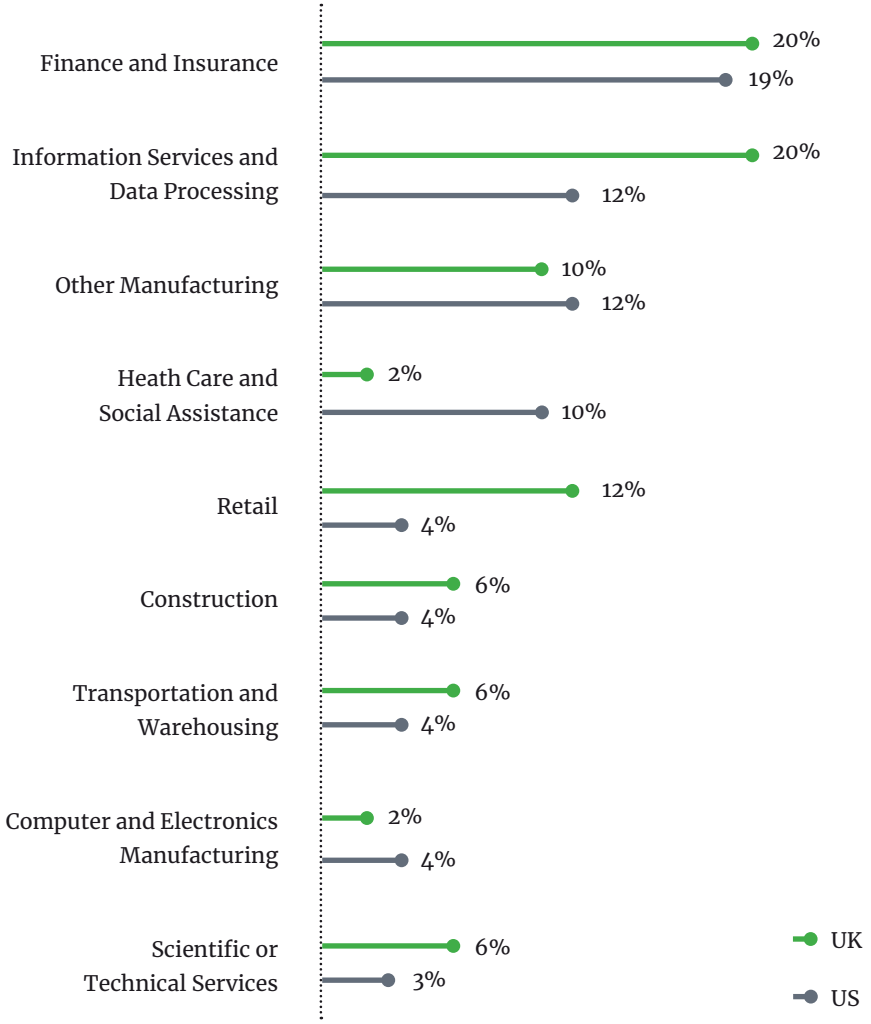
HIGHEST EDUCATION LEVEL



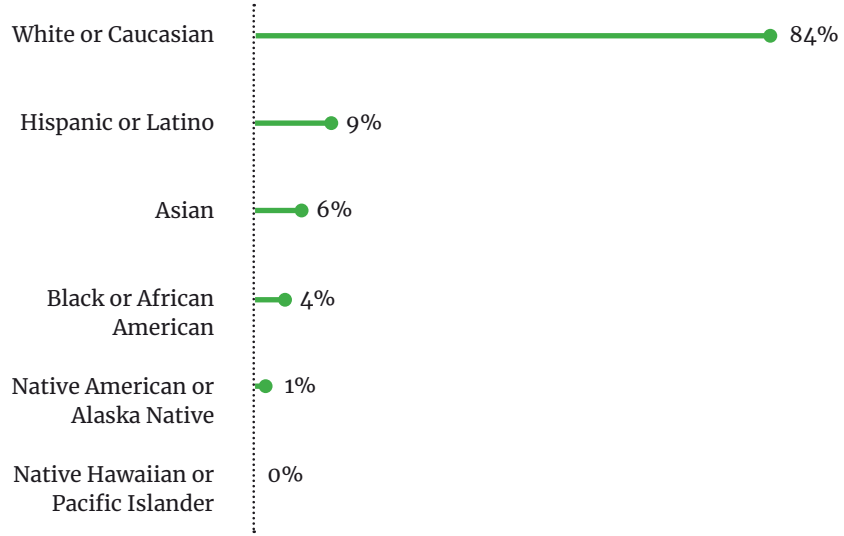
GENDER



THE RESEARCH WAS SPREAD ACROSS MANY DIFFERENT INDUSTRIES



ETHNICITY



Exabeam provides security intelligence and management solutions to help organizations of any size protect their most valuable information. The Exabeam Security Intelligence Platform uniquely combines a data lake for unlimited data collection at a predictable price, machine learning for advanced analytics, and automated incident response into an integrated set of products. The result is the first modern security intelligence solution that delivers where legacy SIEM vendors have failed. Built by seasoned security and enterprise IT veterans from Imperva, ArcSight, and Sumo Logic, Exabeam is headquartered in San Mateo, California. Exabeam is privately funded by Norwest Venture Partners, Aspect Ventures, Icon Ventures, Lightspeed Venture Partners, and investor Shlomo Kramer. Follow us on Twitter and LinkedIn.

2 Waters Park Dr., Suite 200
San Mateo, CA 94403

1.844.EXABEAM
info@exabeam.com