exabeam

The Exabeam 2019 State Of The SOC Report

Contents

Overview

The Exabeam 2019 State of the SOC Report

REPORT The Exabeam 2019 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 (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 2018 State of the SOC Report.

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

Research Methodology

METHODOLOGY

Exabeam contracted Cicero Group to distribute, process and analyze responses for a 20-minute, online survey to IT professionals in two different geographies: United States of America (n=100) and the United Kingdom (n=50). The methodology used was identical to the 2018 State of the SOC Report, also conducted by Cicero Group.

SURVEY SCREENING CRITERIA

Respondents represented SOC employees with full-time, part-time, and military status. Roles were targeted in IT, operations, management, and security. This included specific targeted roles segmented by CIO / CISO, SOC managers (information security manager, security manager), SOC analysts and frontline employees (threat researchers, security architects engineers, analysts, risk officers). Use of the same broad array of industries and similar distribution used in 2018 for screening ensured no significant differences in these distributions, which enabled year-to-year comparisons of survey responses.

EFFECTIVENESS

Effectiveness scores identified Highly Effective (35%), Effective (40%), and Less Effective (25%) SOCs. Scoring was determined by averaging respondent selections of the ratings of six distinct abilities:

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

Overview

Key Findings on the State of the SOC

SOC BASICS/RESPONSIBILITIES

CIOs / CISOs are more concerned about incident response, automation, and threat hunting, while SOC analysts are spending more time on procedure and policy, monitoring security tools, and investigations.

86%

of CIOs / CISOs are involved with incident response (up from 65% a year ago)

67%

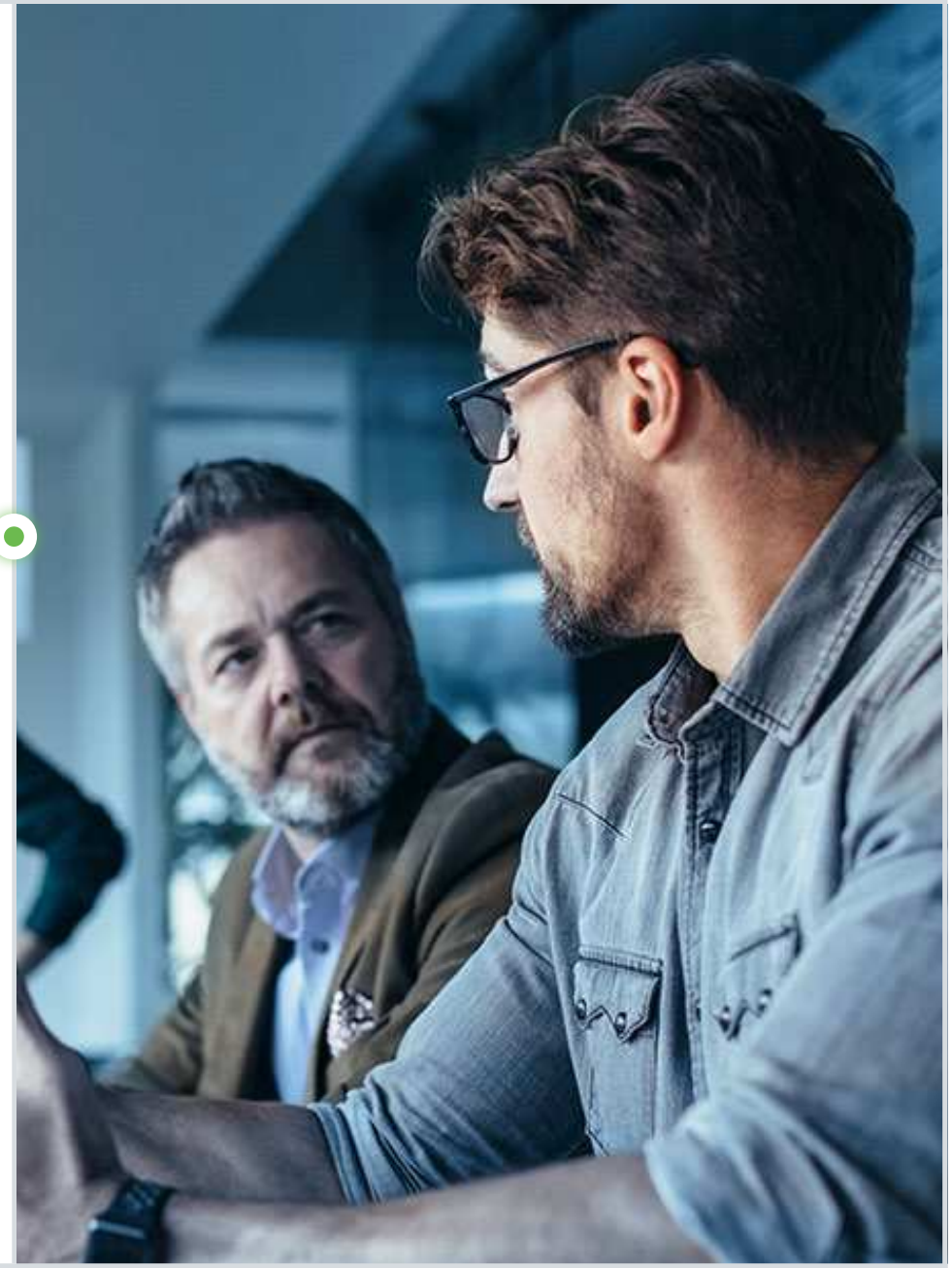
of CIOs / CISOs are involved with threat hunting (up from 51% a year ago)

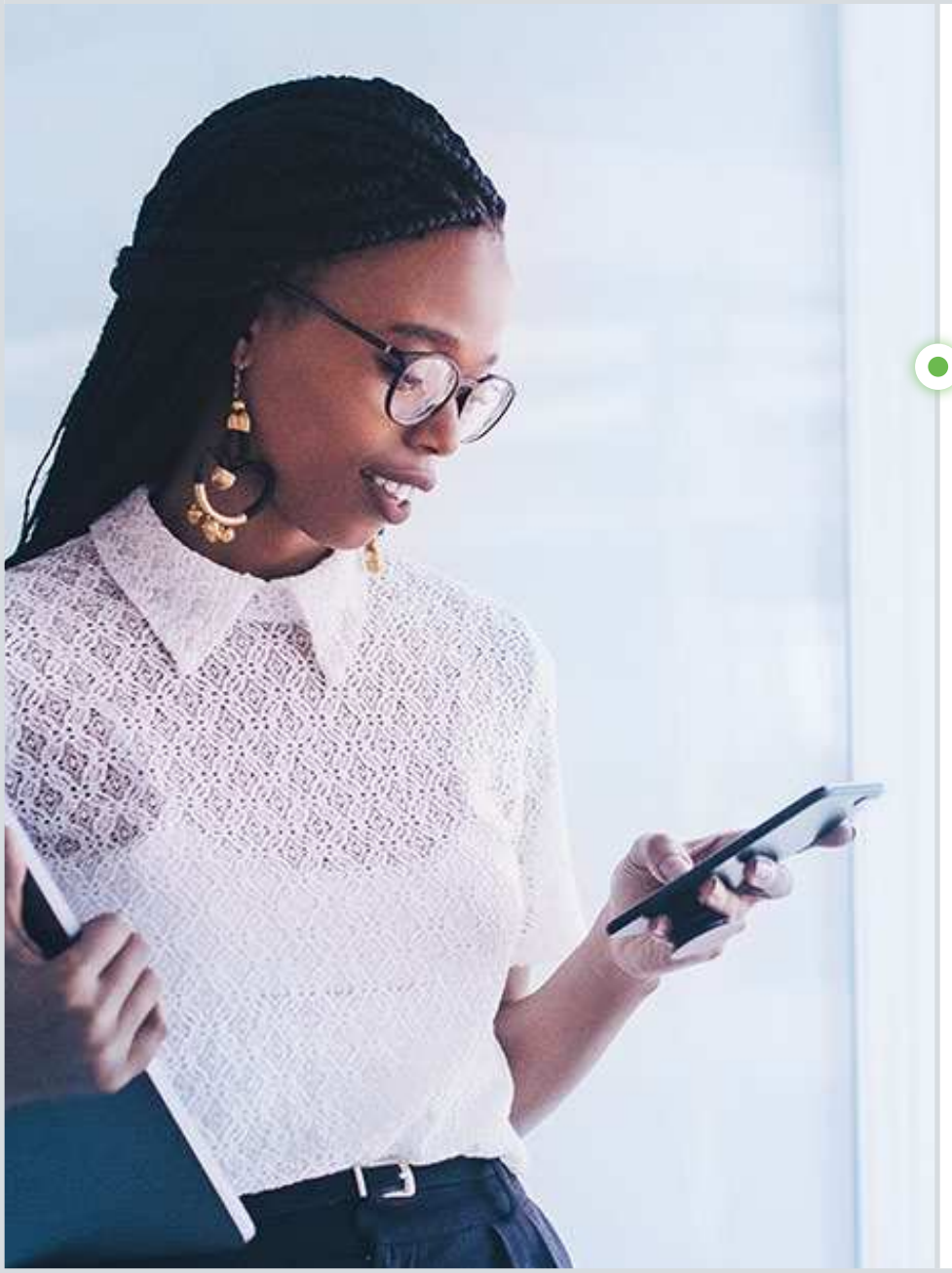
48%

of frontline SOC analysts surveyed are using automation (up from 28% a year ago)

50%

of SOC managers continue to use automation





OUTSOURCING

Almost half of SOCs surveyed continue to outsource malware analysis, threat analysis and threat intelligence, while event/data monitoring decreased as an outsourced function.

55%

outsource malware analysis expertise (up 15% from a year ago)

45%

outsource threat intelligence services (up 17% from a year ago)

37%

outsource event/data monitoring (down 10% from a year ago)

HIRING AND STAFFING

- SOC staffing remains an issue for many organizations, and is most prevalent among less effective SOCs compared to more effective SOCs.
- The highest correlation between retention in SOCs are competitive benefits and the nature of SOC work.

50%

of understaffed SOCs desire more funding for technology

46%

of less effective SOCs say they are slightly understaffed

42%

of SOCs surveyed say employees stay because of a good / challenging environment

29%

of highly effective SOCs say they are slightly understaffed

6–10

The number of employees understaffed SOCs say they need

44%

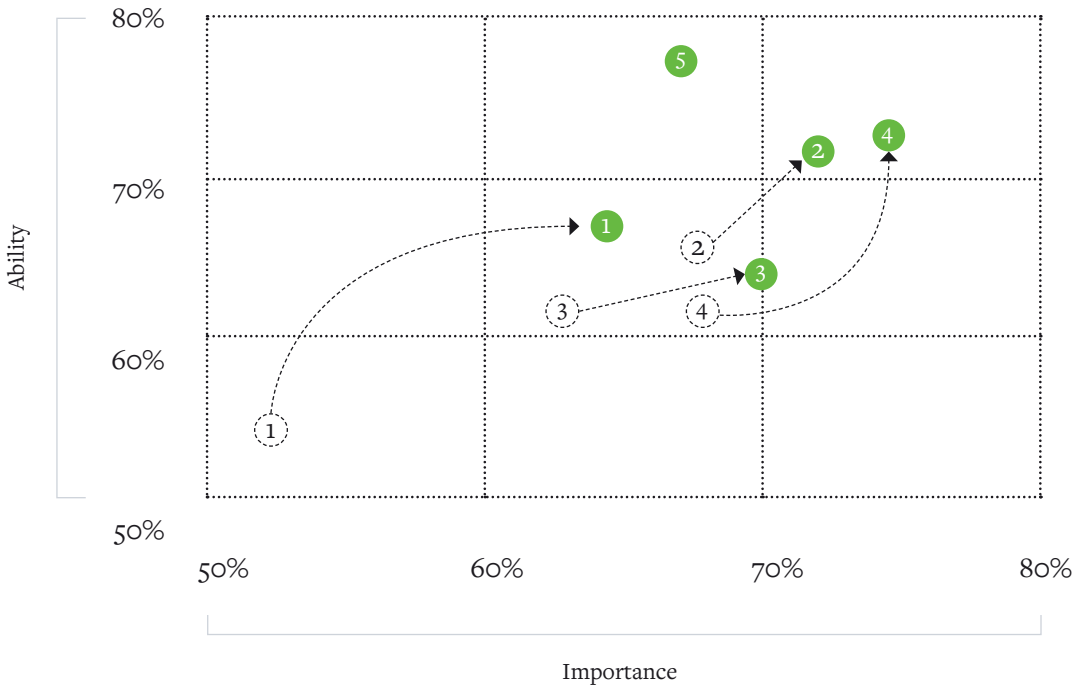
of SOCs surveyed say employees are easy to retain with workplace benefits

SOFT SKILLS

While hard skills remain critical, 65% of SOCs are placing increased emphasis on soft skills, particularly personal/social.

SOFT SKILLS - IMPORTANCE AND ABILITY - 2018 | 2019

7-point scale, (Top 2); n=150



Soft Skills	
1	Personal/social skills
2	Ability to work in teams
3	Leadership ability
4	Communication
5	Effective Management

- Personal / social skills made the most significant increase in importance and ability for SOCs, followed closely by communication skills
- SOCs currently have high confidence in employee management skills*

* Effective management was not featured in the 2018 State of the SOC survey

PROCESS

- Generally, SOC effectiveness is unchanged, but the ability to perform auto-remediation has declined in aggregate.
- The problem of inexperienced staff is greater in the eyes of CISOs/CIOs than with SOC analysts and SOC managers.
- Top pain points for SOC personnel were time spent on reporting/documentation, false positives, and alert fatigue

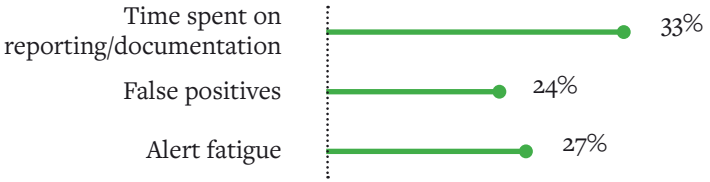
54%

of SOCs were able to perform auto-remediation (down from 68% a year ago)

71%

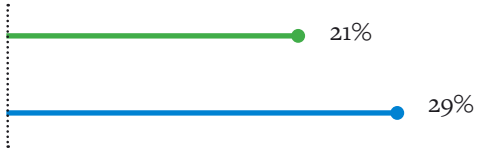
of U.S. SOCs have significantly more ability to monitor and review events than 54% of U.K. counterparts

TOP PAIN POINTS FOR SOC PERSONNEL



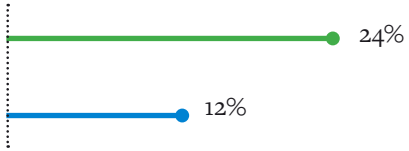
CIO / CISO

Inexperienced Staff



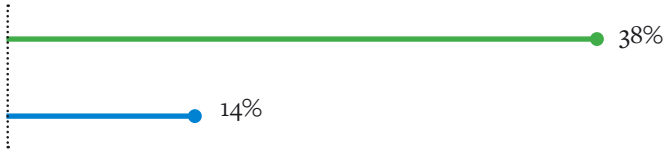
SOC MANAGERS

Inexperienced Staff



SOC ANALYSTS

Inexperienced Staff



TECHNOLOGY

- Big data analytics, endpoint detection/response, network/cloud monitoring, and identity/access mgmt. remain top technology priorities.
- Keeping up with security alerts remains the top pain point for SOCs.
- The greatest increase in technology adoption was in AI (up 4%), biometric authentication and access management (up 6%), while ML usage largely remained unchanged.

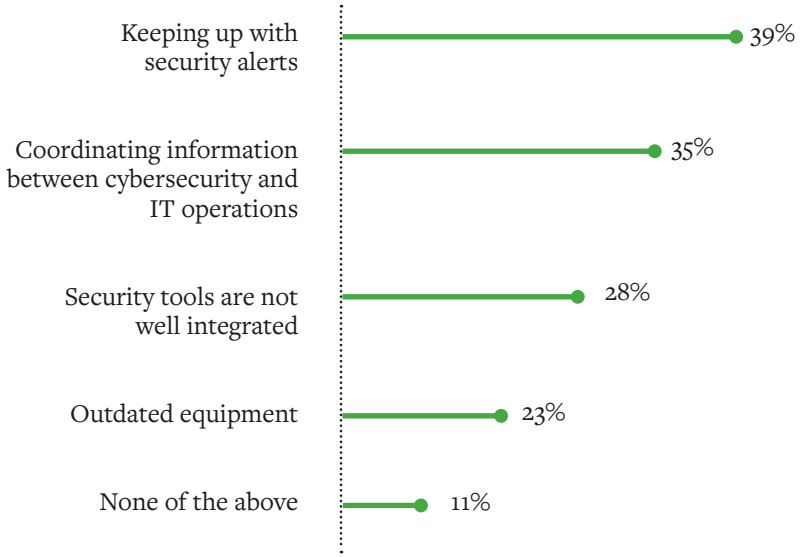
39%

of SOCs surveyed use advanced network and cloud monitoring, big data security analytics, and identity & access management

38%

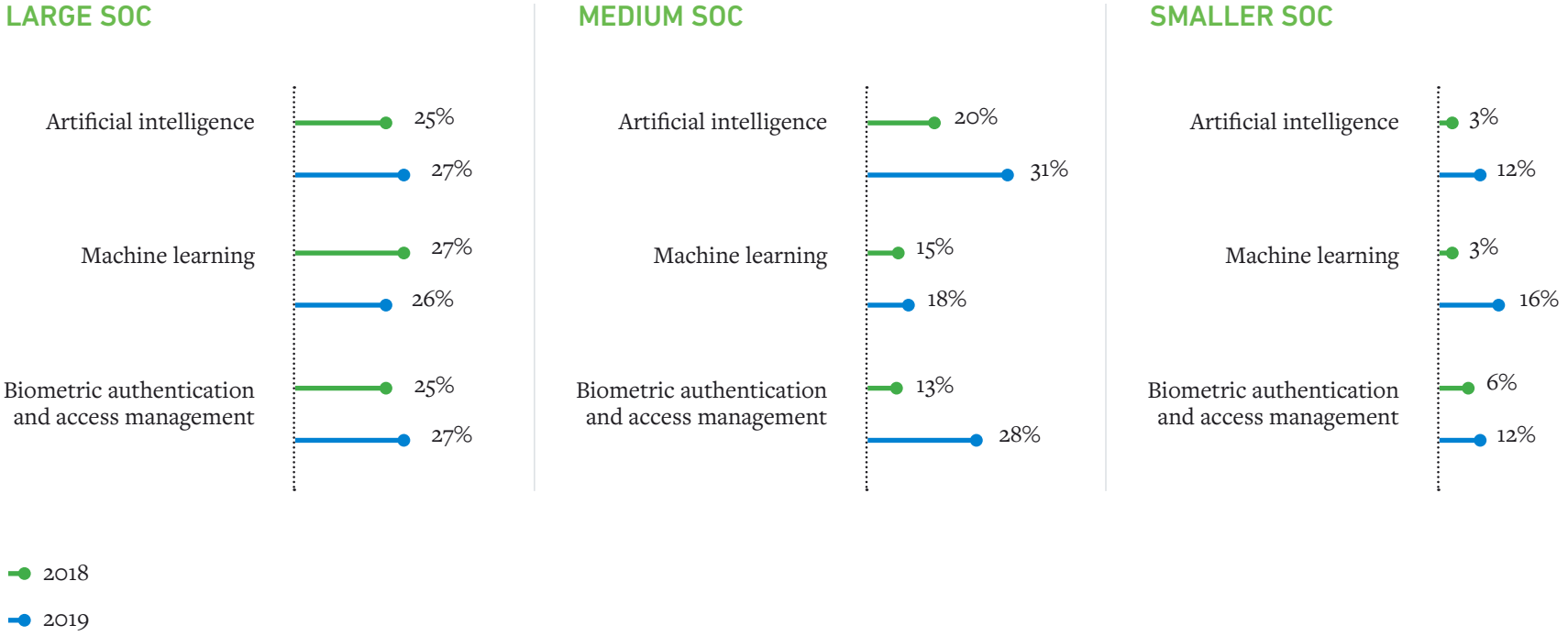
use endpoint detection and response technology (EDR)

PAIN POINTS IN TECHNOLOGY - 2019



TECHNOLOGY

Artificial intelligence and biometric authentication usage have increased, with the largest gains being made in medium-and smaller-sized SOCs.

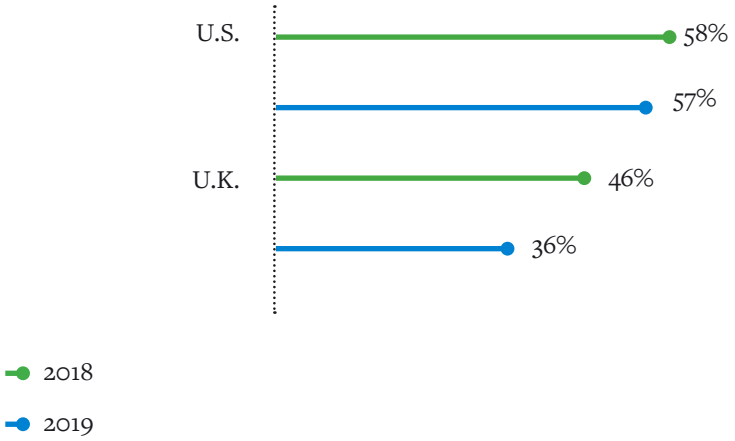


FINANCE AND BUDGET

Investment in technology, as opposed to staffing and facilities, remains the most underfunded part of the SOC; a sentiment felt much more strongly by Americans.

FUNDING DISTRIBUTIONS - 2018 | 2019

Technology



Future SOC investments are thought to be most needed in new and relevant technology, staffing, and time-saving automation.

39%

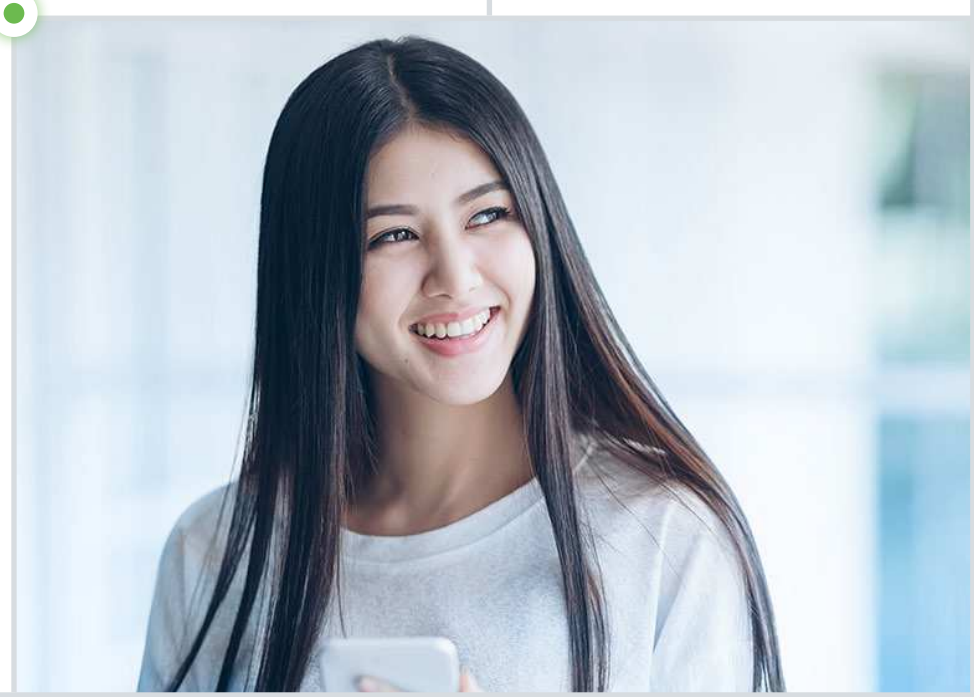
desire more investment in new/modern technology

35%

desire more funding for staffing

34%

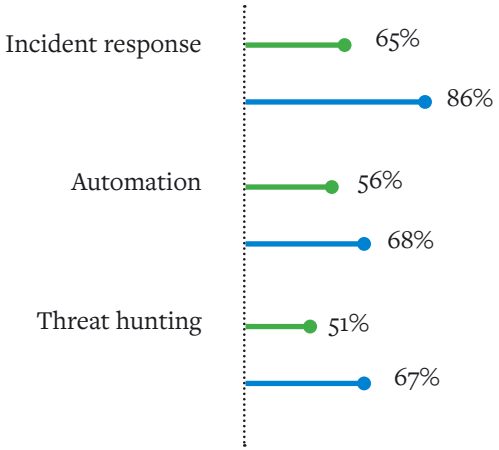
want to invest in automation to save time



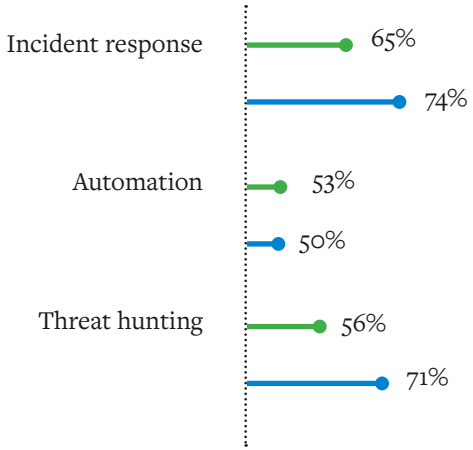
SOC Basics

CIOs / CISOs are more concerned about incident response, automation, and incident response (up 21%) and automation (up 12%).
For SOC analysts, the greatest increase is in automation (up 20%) and incident response (up 11%).

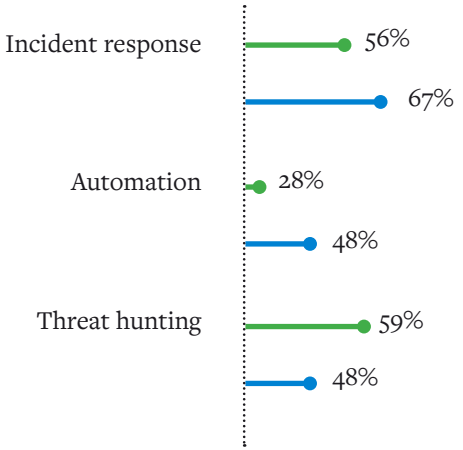
CIO / CISO



SOC MANAGERS



SOC ANALYSTS

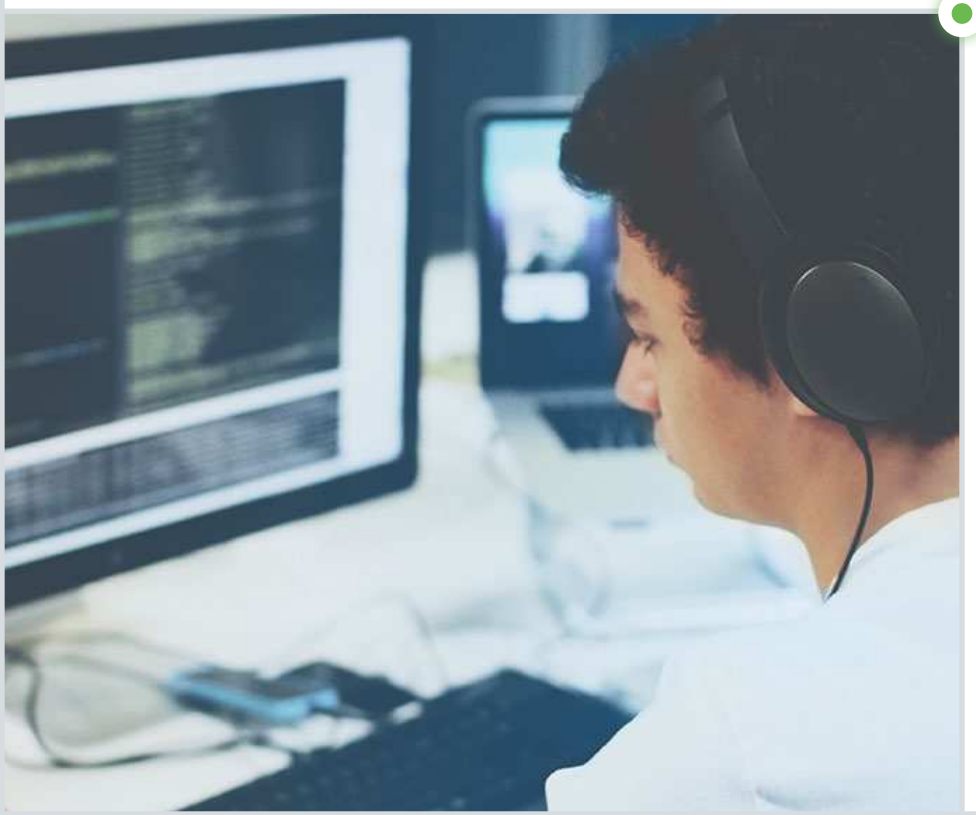


2018
2019

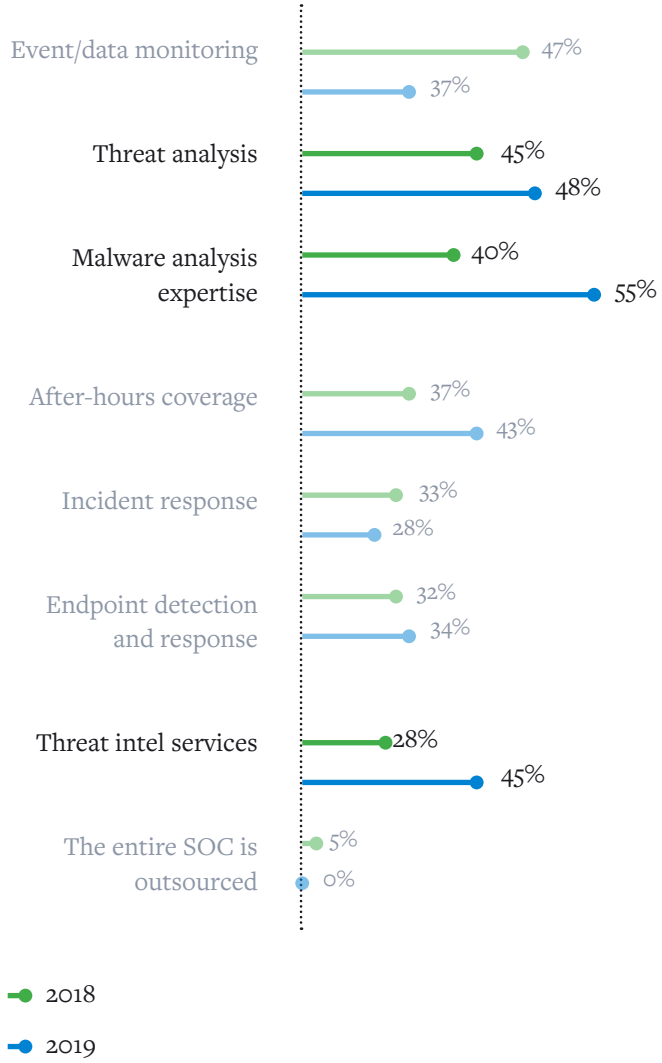
OUTSOURCING

Almost half of SOCs surveyed (43%) continue to outsource functions. Of those outsourced functions, malware analysis, threat analysis, and threat intelligence have shown the greatest increases.

SOC analysts are increasingly involved in IR and automation with a 17% increase in threat intel services; 15% increase in malware analysis.



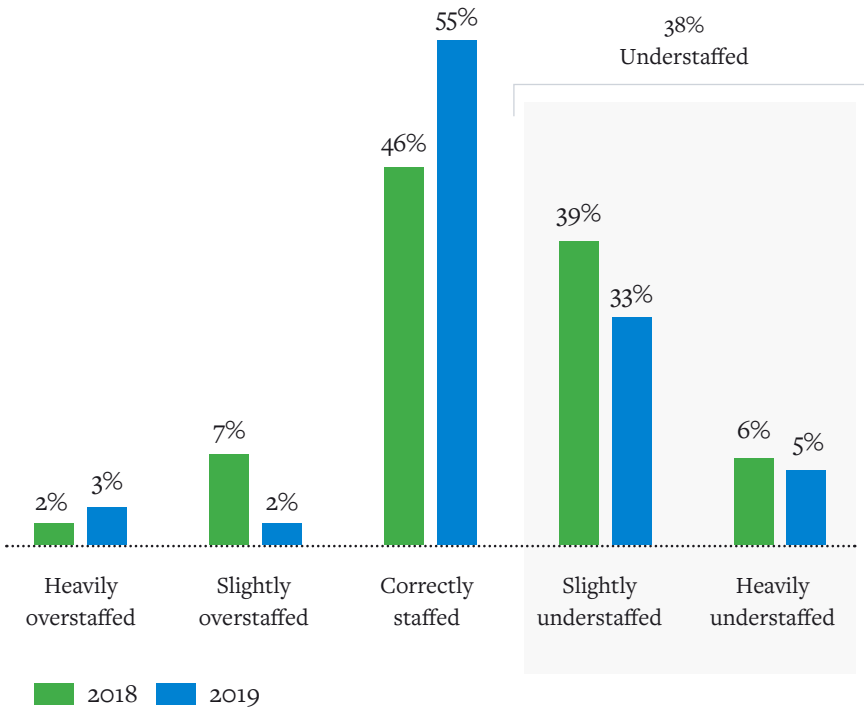
OUTSOURCED FUNCTIONS



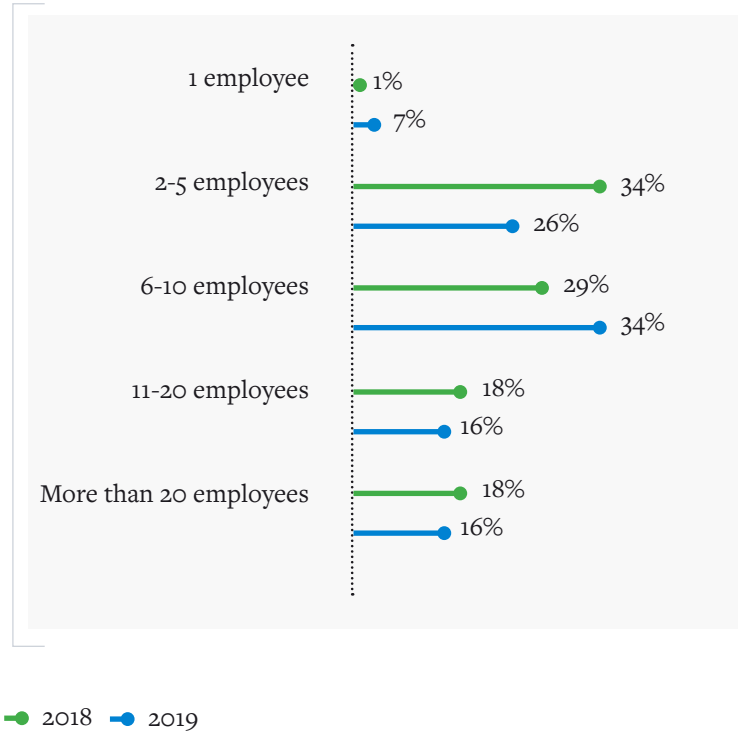
Staffing

A third of respondents feel their SOC is understaffed. Of the understaffed SOCs, the greatest staffing increment needed is between 6-10 employees.

PERCEPTION OF CURRENT STAFFING LEVELS



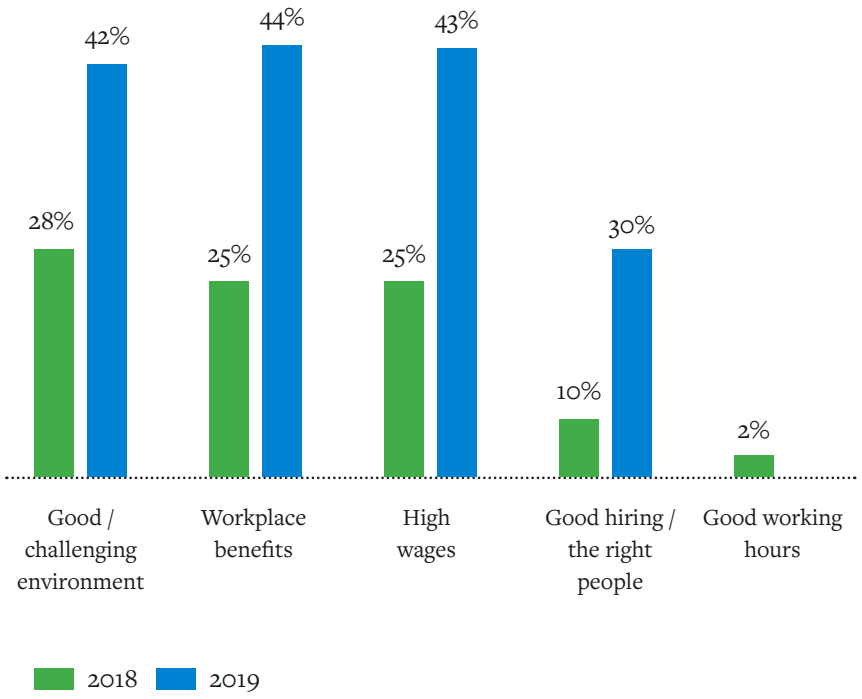
NUMBER OF EMPLOYEES UNDERSTAFFED



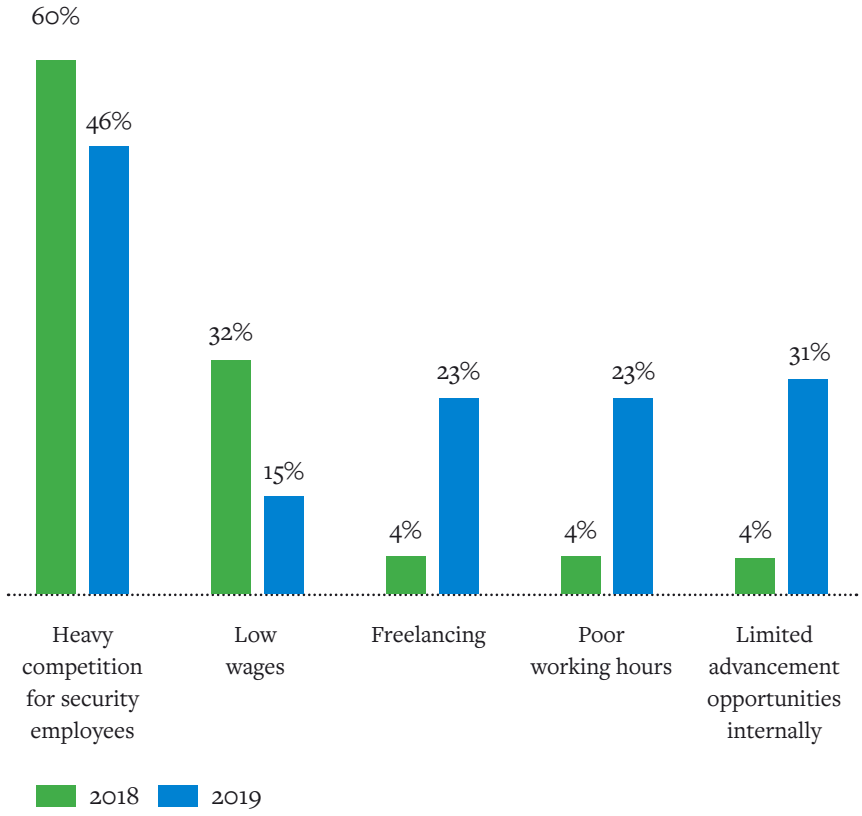
EMPLOYEE RETENTION DRIVERS

Of the SOCs reporting high employee retention, workplace benefits, high wages, and a challenging work environment continue to be drivers for many SOCs. Poor working hours and limited advancement opportunities internally showed the greatest increases from 2018 for reasons for employee attrition.

REASONS EMPLOYEES ARE EASY TO RETAIN



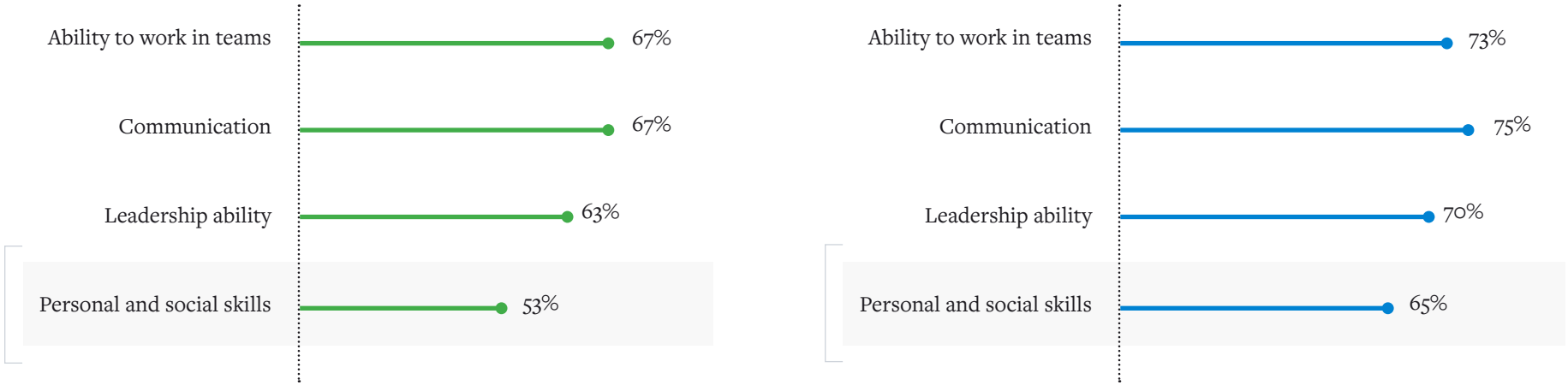
REASONS EMPLOYEES ARE DIFFICULT TO RETAIN



SKILLS

SOCs are placing increased value on employees' personal and social skills.

SKILL IMPORTANCE - 2018 | 2019

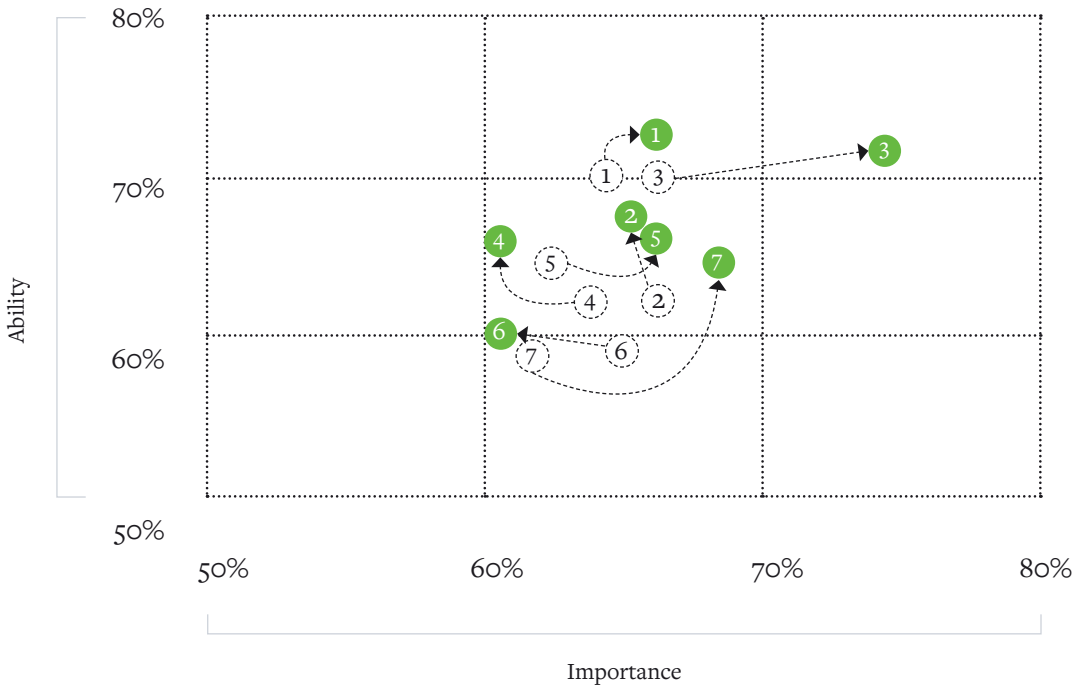


TECHNICAL SKILLS

Hard skills like threat hunting and data loss prevention are becoming increasingly important.

HARD SKILLS - IMPORTANCE AND ABILITY - 2018 | 2019

7-point scale, (Top 2); n=150



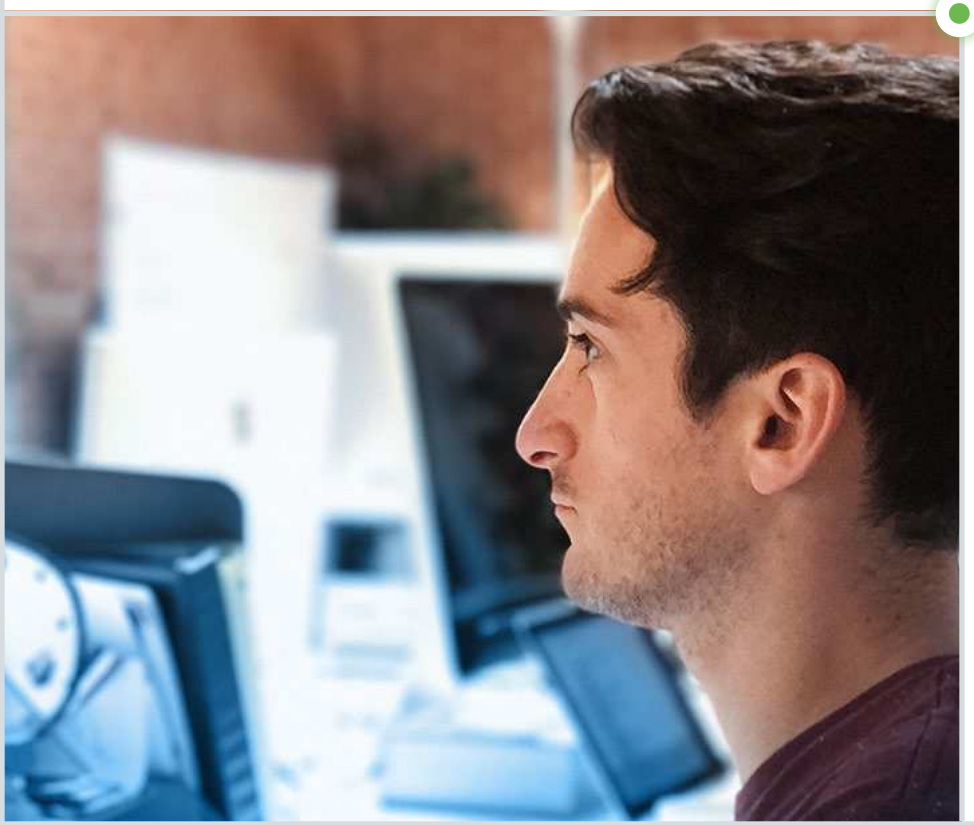
Hard Skills	
1	Network and system administration
2	Firewall architecture
3	Data loss prevention
4	Malware analysis
5	Risk management
6	Digital forensics
7	Threat hunting

- Firewall architecture, malware analysis, and digital forensics all decreased in importance to SOCs

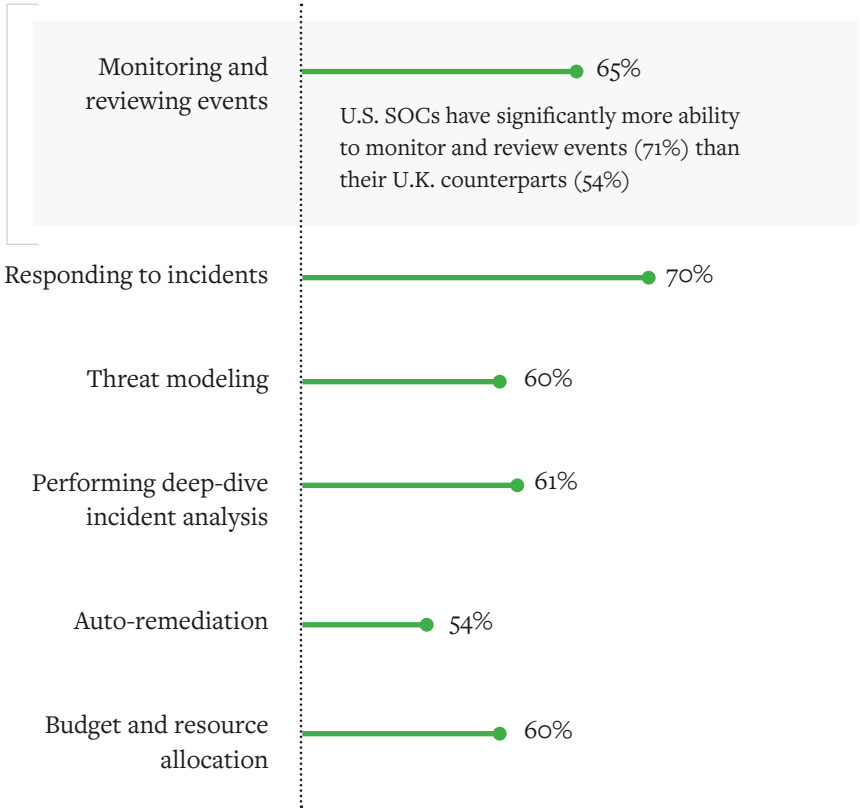
Process

EFFECTIVENESS

Generally, SOC effectiveness is unchanged, but the perception of auto-remediation effectiveness has declined in aggregate from 2018.



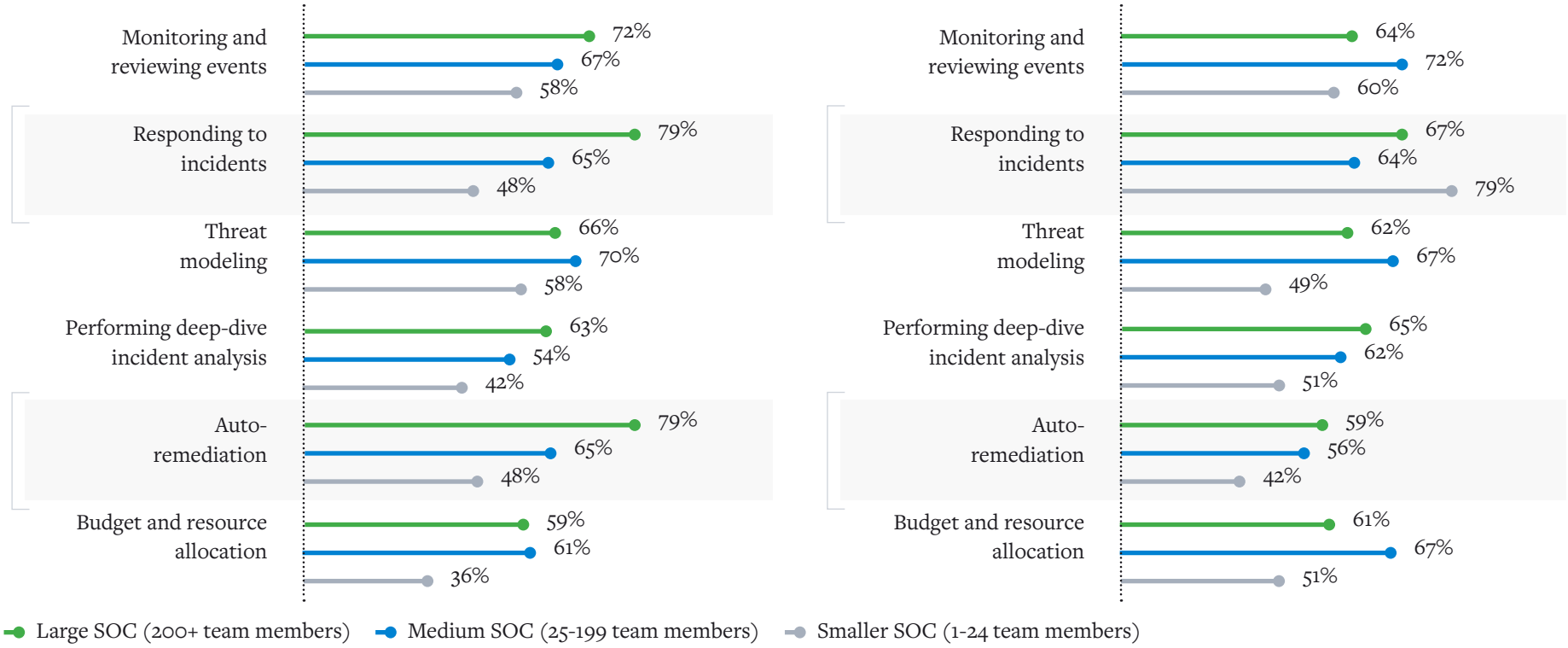
EFFECTIVENESS OF SOC TEAM



SMALLER SOCs

Smaller SOCs reported a notable increase (31%) in their effectiveness at "responding to incidents." Satisfaction and efficacy of auto-remediation has declined.

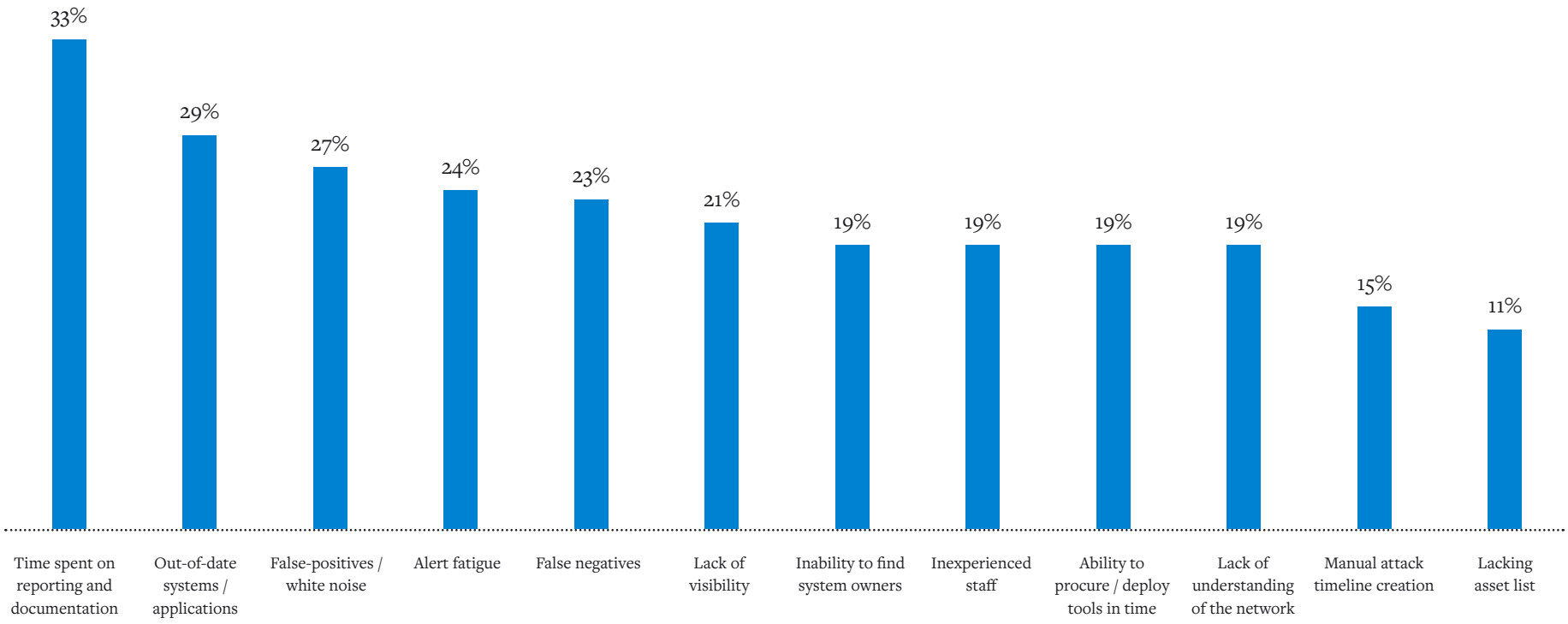
EFFECTIVENESS OF SOC TEAM - 2018 | 2019



PAIN POINTS

Time spent on reporting/documentation (33%), out-of-date systems (29%), false positives (27%), and alert fatigue (24%) are the greatest pain points for personnel.

PAIN POINTS - 2019



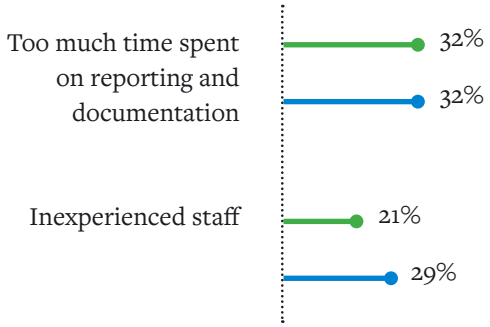
SOC MANAGERS

SOC Managers report the largest issue with time spent on reporting / documentation. This is likely due to the immense burden of creating audit and compliance artifacts.

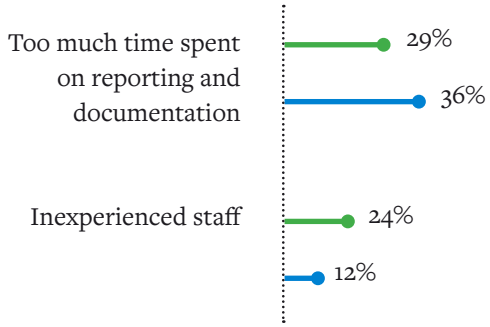
29% of CIOs and CISOs surveyed say inexperienced staff is a problem, indicating the issue is more relevant with C-level executives.

PAIN POINTS BY ROLE

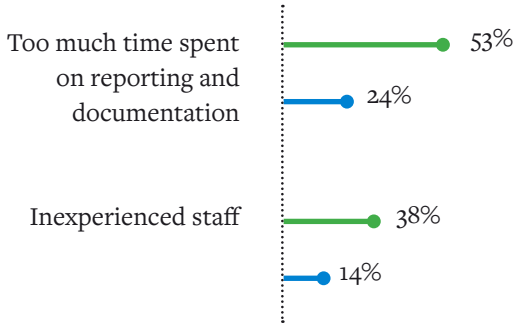
CIO / CISO



SOC MANAGERS



SOC ANALYSTS



2018
2019

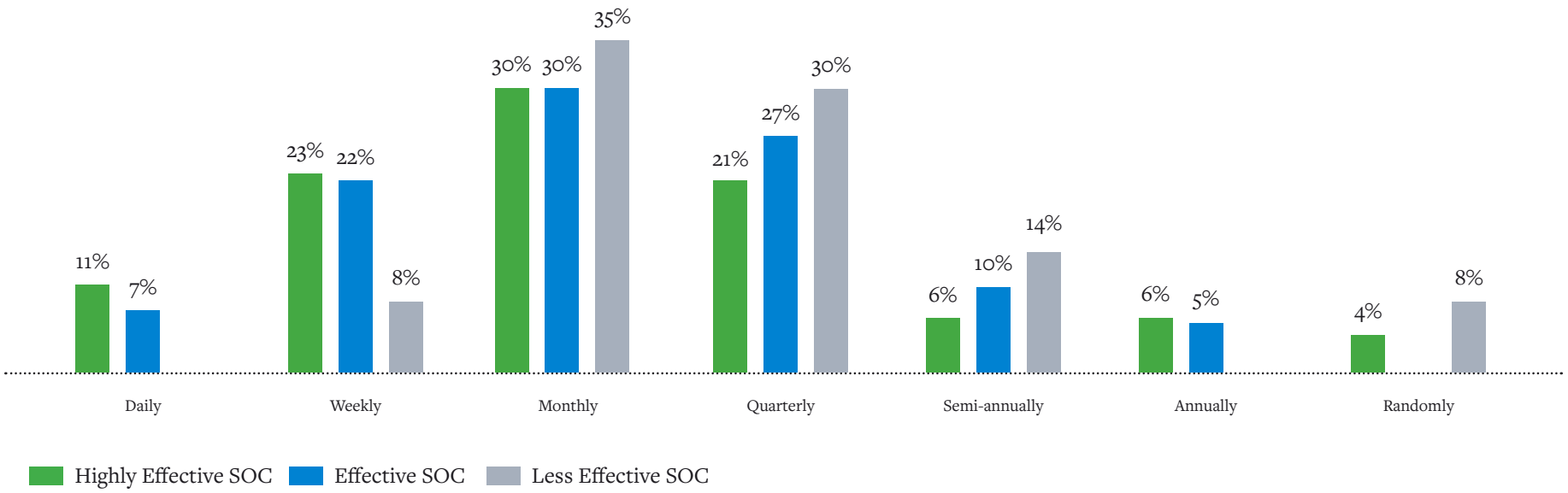
TRAINING

Regular training helps make SOCs more effective; the majority of Highly Effective and Effective SOCs held training at least on a monthly basis.

U.S. SOCs are much more likely to have quarterly trainings (32%) than their U.K. counterparts (12%).

U.K. SOCs are slightly more likely to conduct training on an ad hoc or as needed basis..

PAIN POINTS - 2019



SURVEY RESPONDENTS ON TRAINING IN THEIR ORGANIZATIONS

"I think because our training is done primarily in-house, it helps trainees get a feel for how our organization operates."

ISO, U.S., 9-10 YRS., > $20 BILLION, FINANCE AND INSURANCE

"The training is very effective in getting employees prepared, and the online seminars make it way more convenient for our schedules."

CIO, U.S., 3-5 YRS., $50-99 MILLION, CONSTRUCTION

"Our training is adequate, but would be better if done more frequently."

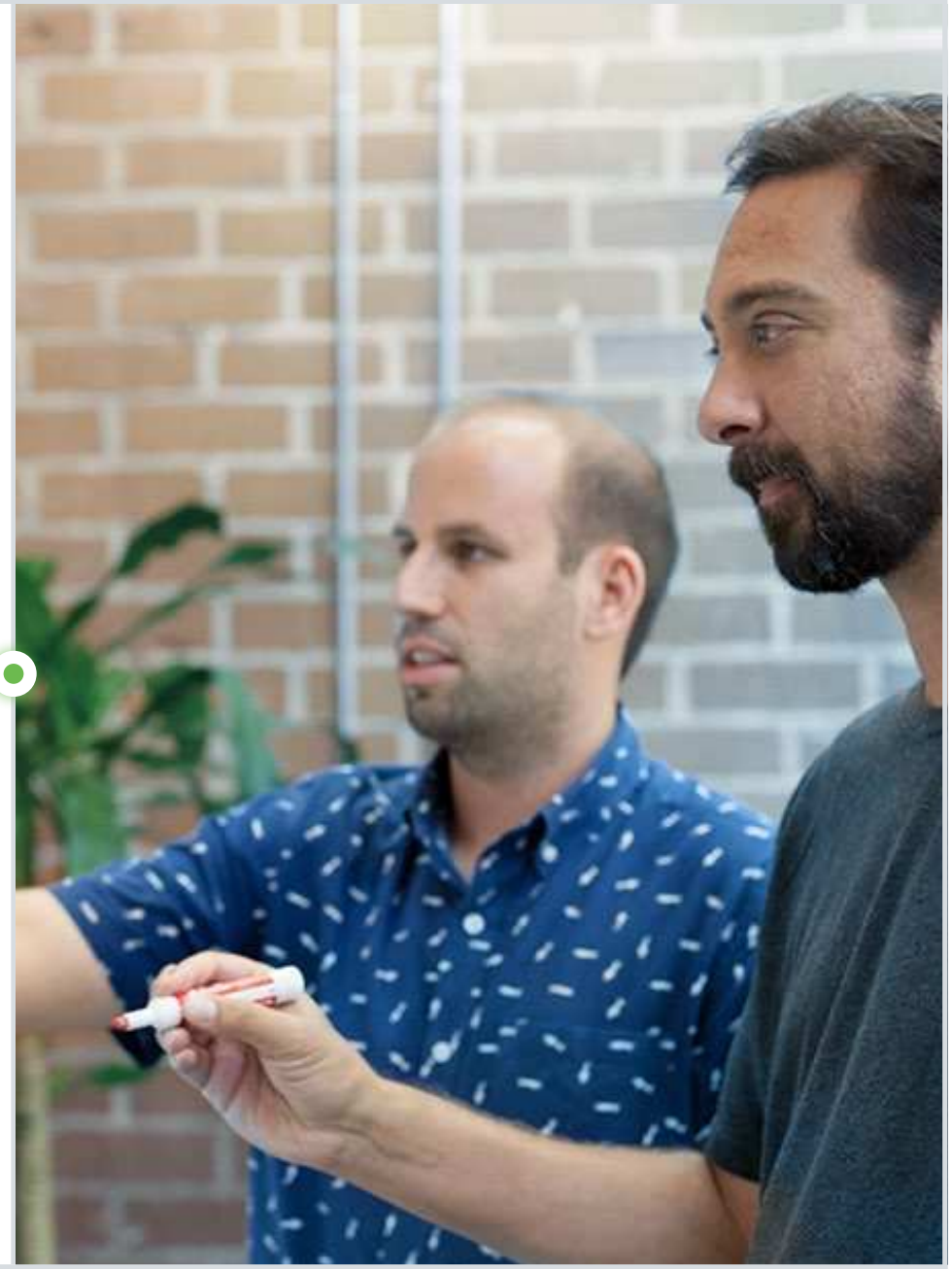
ISO, U.K., 16-20 YRS., $1-4.99 BILLION, CONSULTANCY

"Our training could be better. I think management is so worried about lost work time that it sometimes blinds them from helping us be more effective."

CIO, U.S., 16-20 YRS., $100-299 MILLION, OTHER EDUCATION INDUSTRY

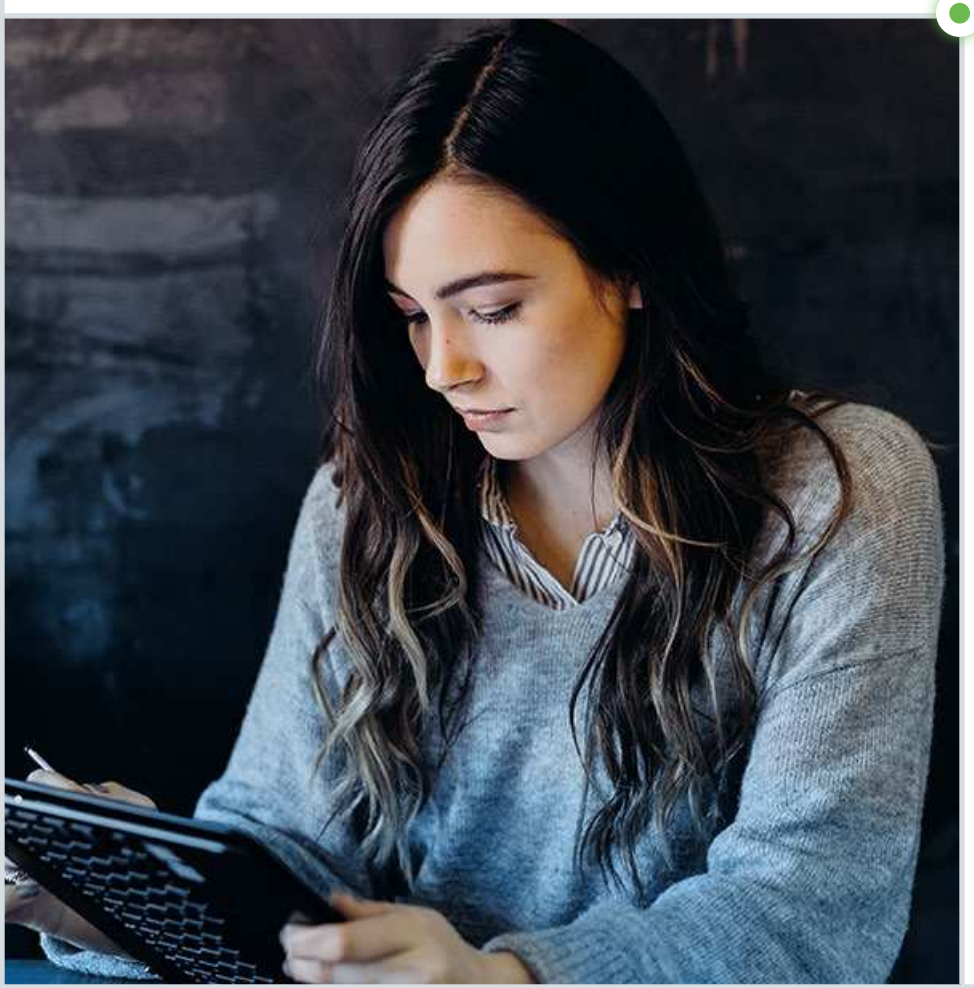
"We need to expand the frequency and scope of training to cover more staff and keep them updated with the technical know-how they need to do their jobs."

ISO, U.S., 9-10 YRS., $1-4.99 BILLION, FINANCE AND INSURANCE

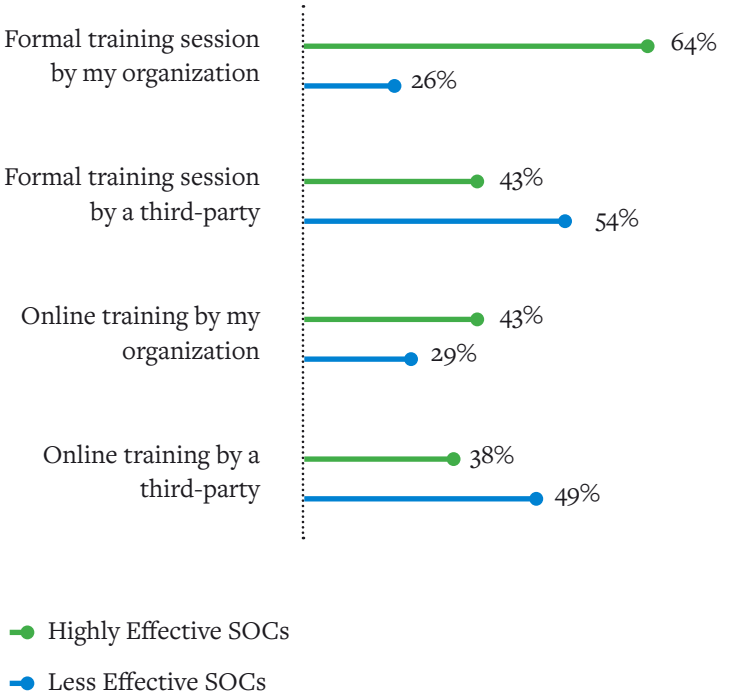


TRAINING IN HIGHLY EFFECTIVE SOCs

Highly Effective SOCs are more likely to handle their own employee training, jumping from 45% in 2018 to 64% in 2019.



TYPES OF TRAINING

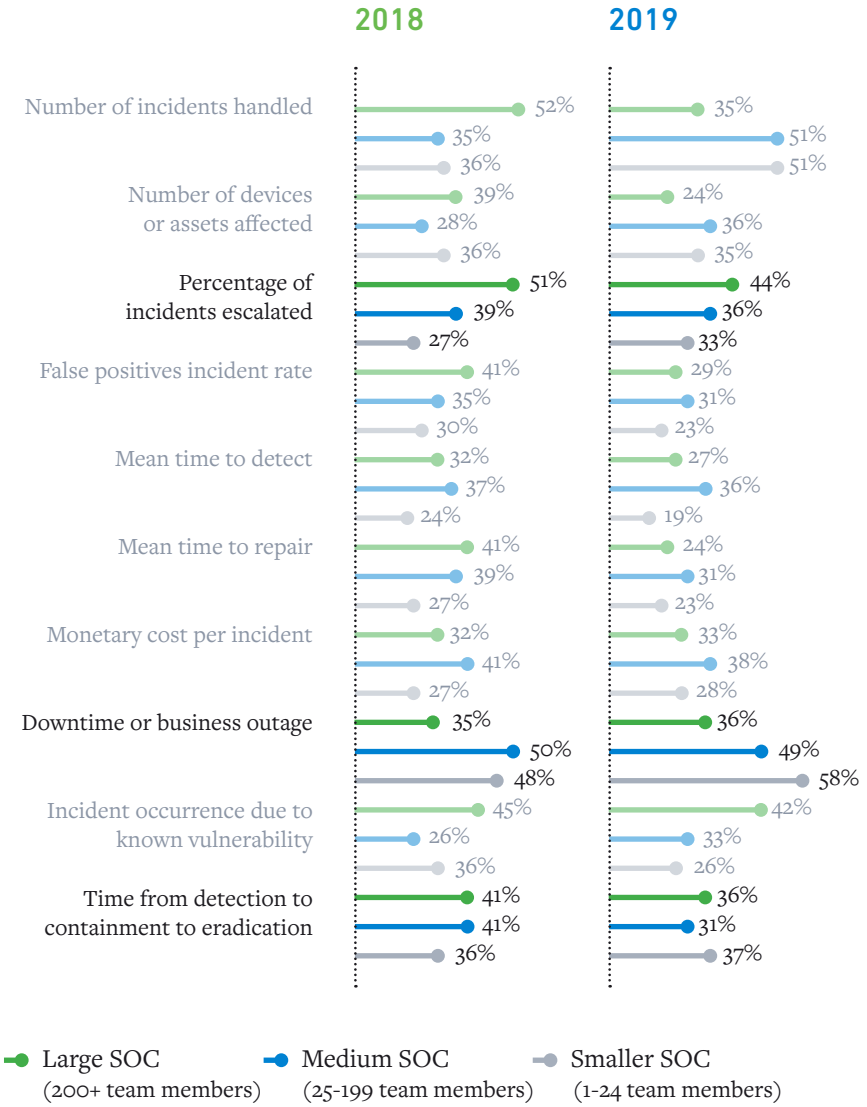


METRICS

Smaller SOCs are more likely to use downtime or business outages as metrics. This often occurs in smaller organizations where an outage is seemingly a greater threat than a cyberattack.

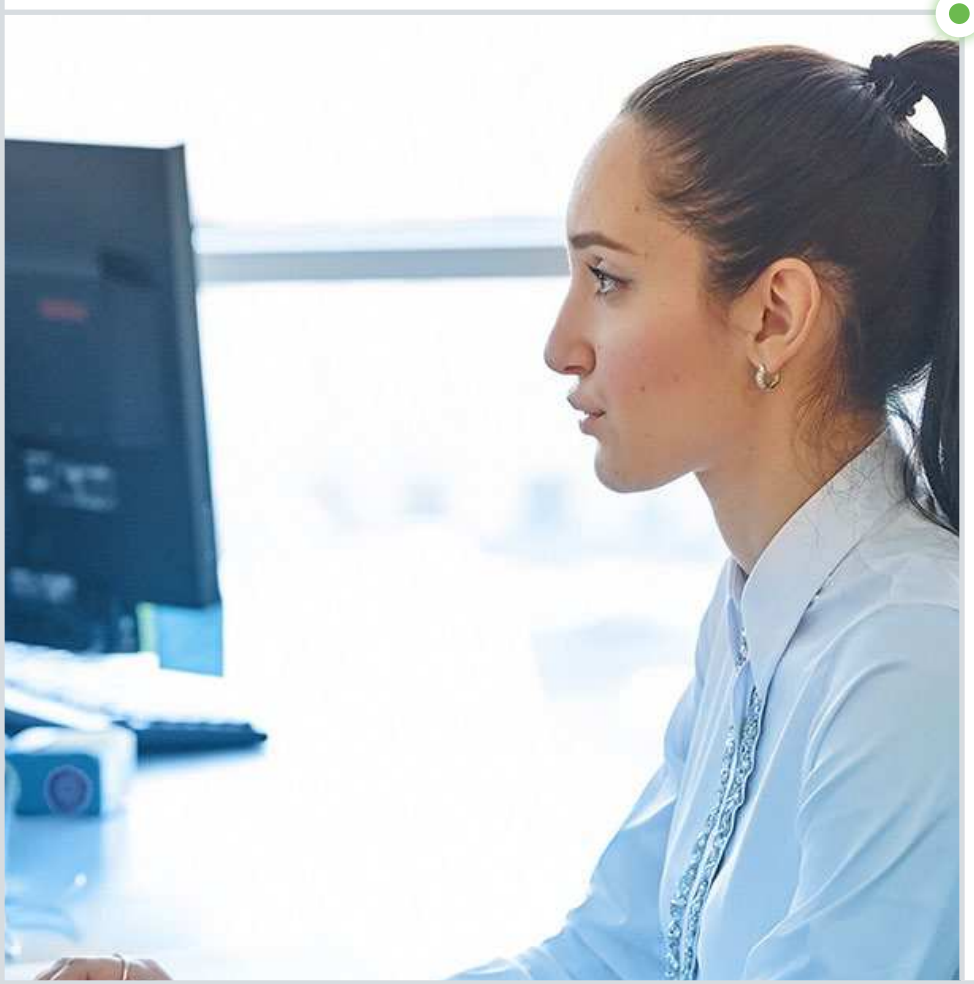
Large SOCs are using incident counts and mean-time-to-repair less in 2019. They are most concerned with number of incidents escalated, downtime, and time from detection to eradication.

METRICS TRACKED BY SOC SIZE - 2018 | 2019

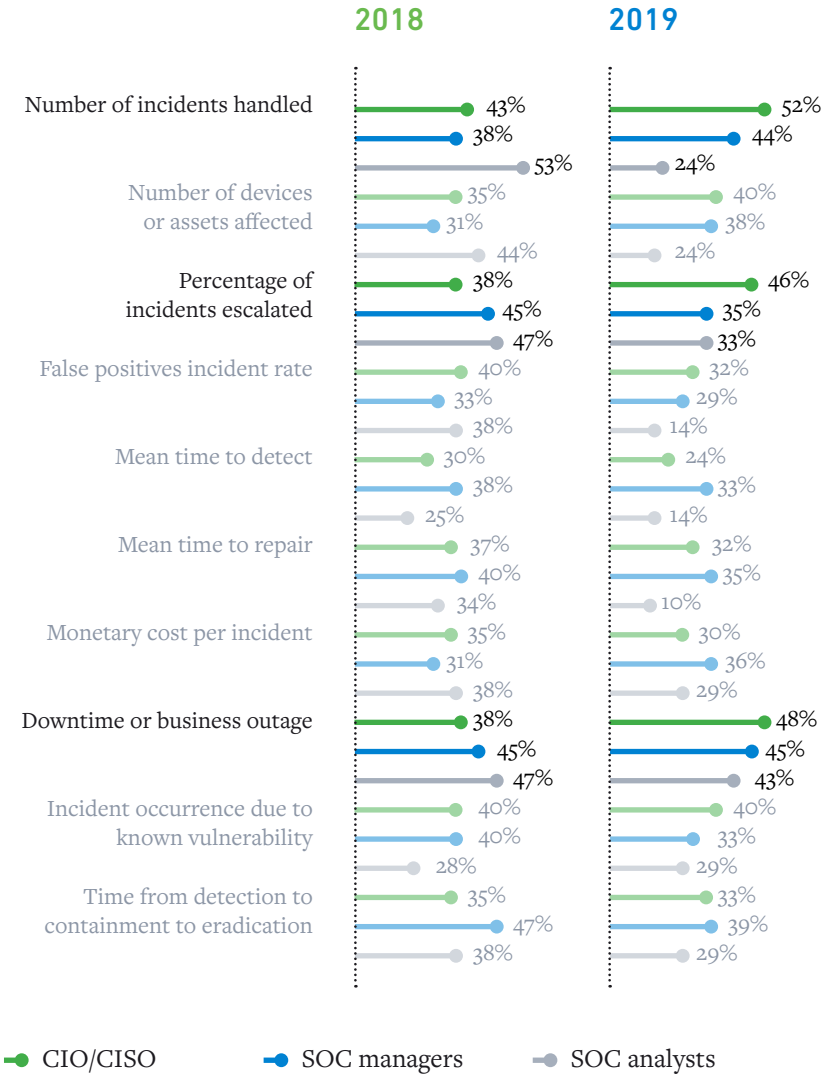


ROLES AND RESPONSIBILTIES

CIOs / CISOs are still focused on the number of incident tickets, while SOC analysts are more focused on down time and business outage.



METRICS TRACKED BY ROLE - 2018 | 2019

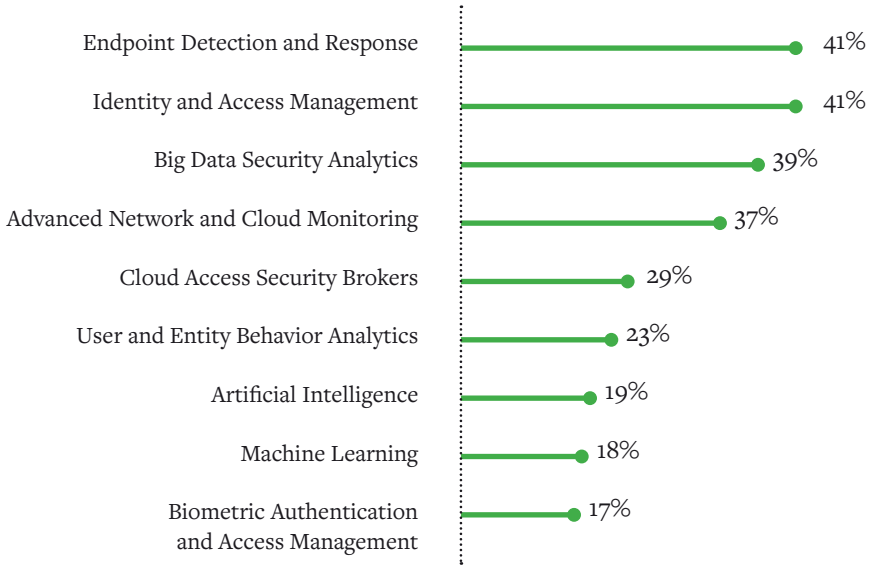


Technology

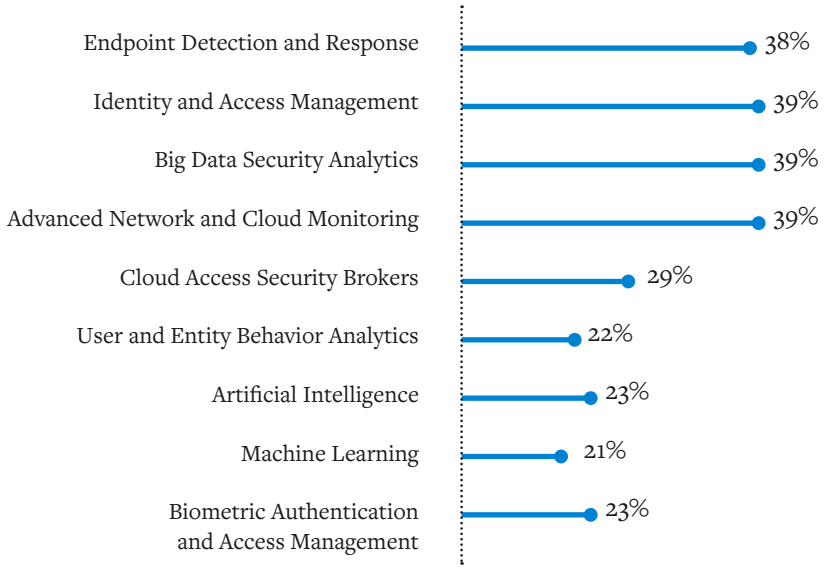
Big data analytics and UEBA remained strong, while artificial intelligence and machine learning made marginal gains in usage. The biggest jumps were in medium and smaller SOCs.

CURRENT TECHNOLOGY USAGE - 2018 | 2019

2018



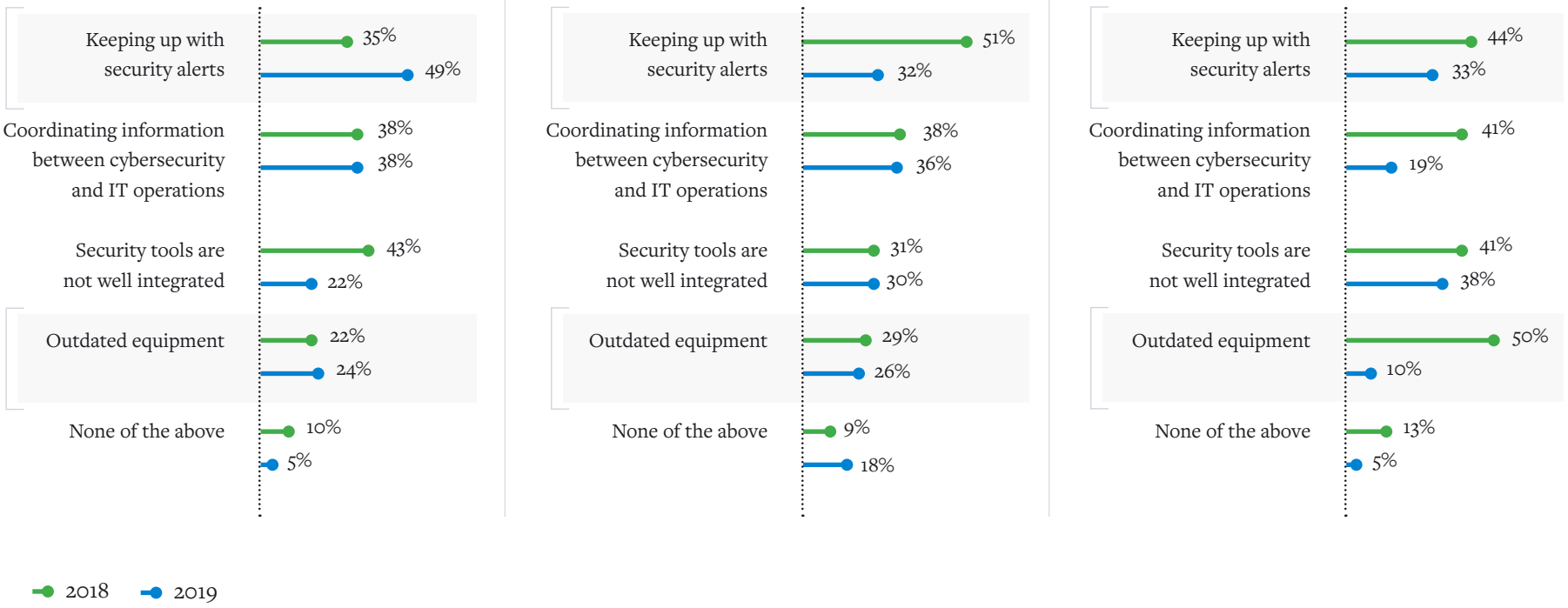
2019



TECHNOLOGY PAIN POINTS

Keeping up with security alerts is the leading pain point experienced by all SOC personnel. SOC analysts see outdated equipment as the greatest pain point in 2019.

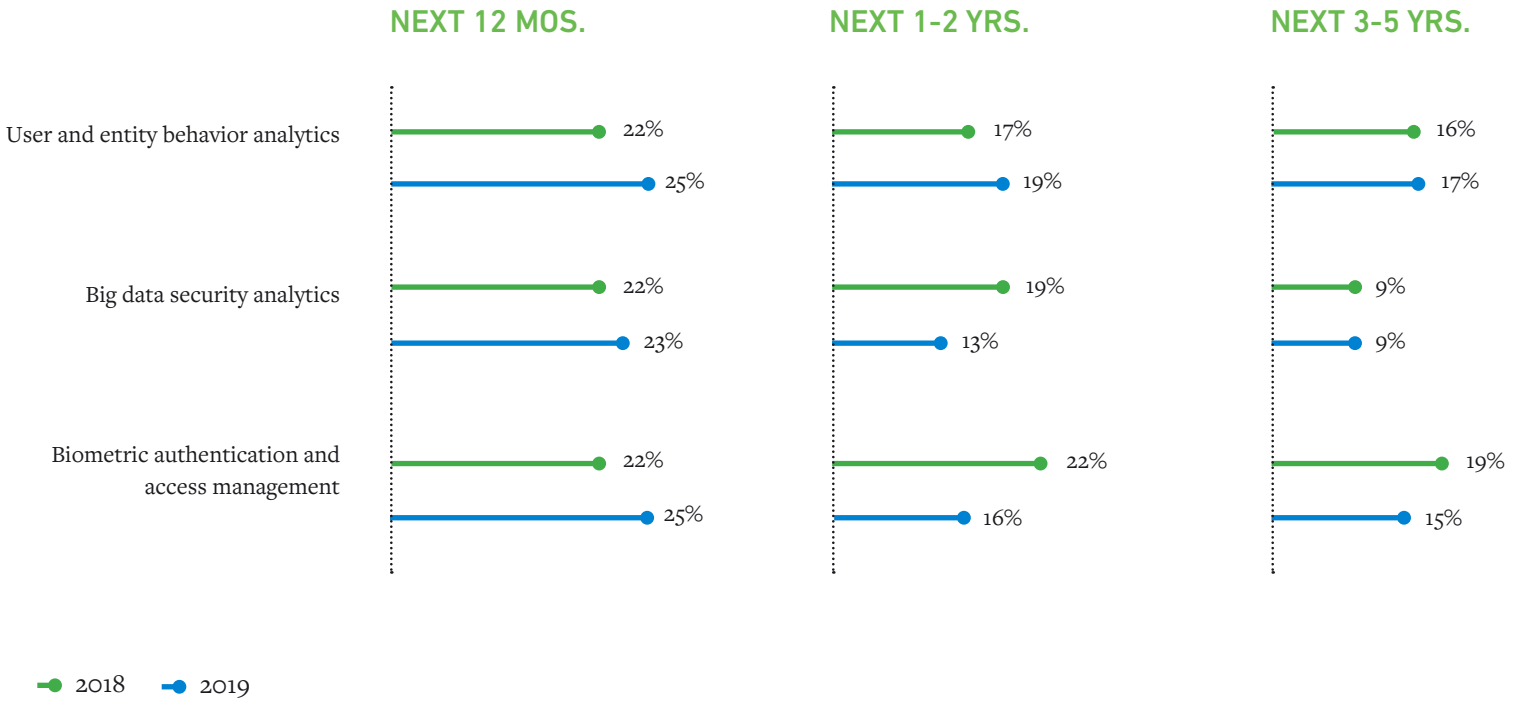
PAIN POINTS IN TECHNOLOGY BY ROLE - 2018 | 2019



TECHNOLOGY PAIN POINTS

User and entity behavior analytics and biometric authentication and access management lead usage expectations in the next 12 months.

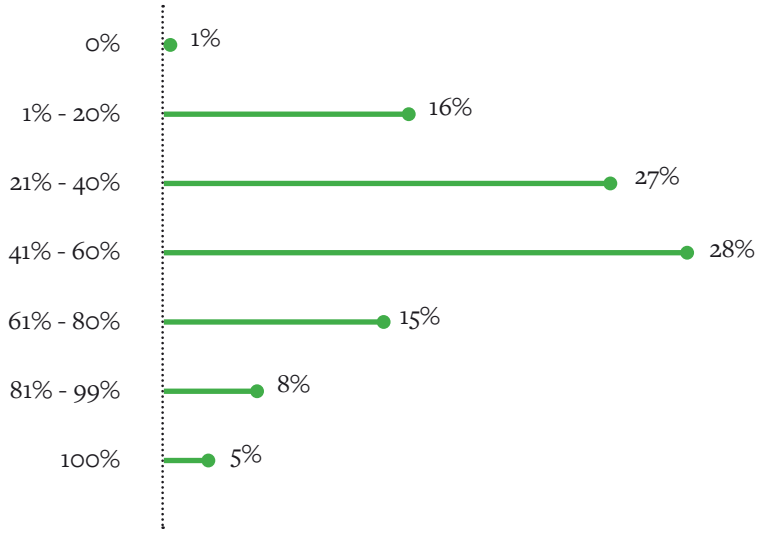
USAGE EXPECTATIONS



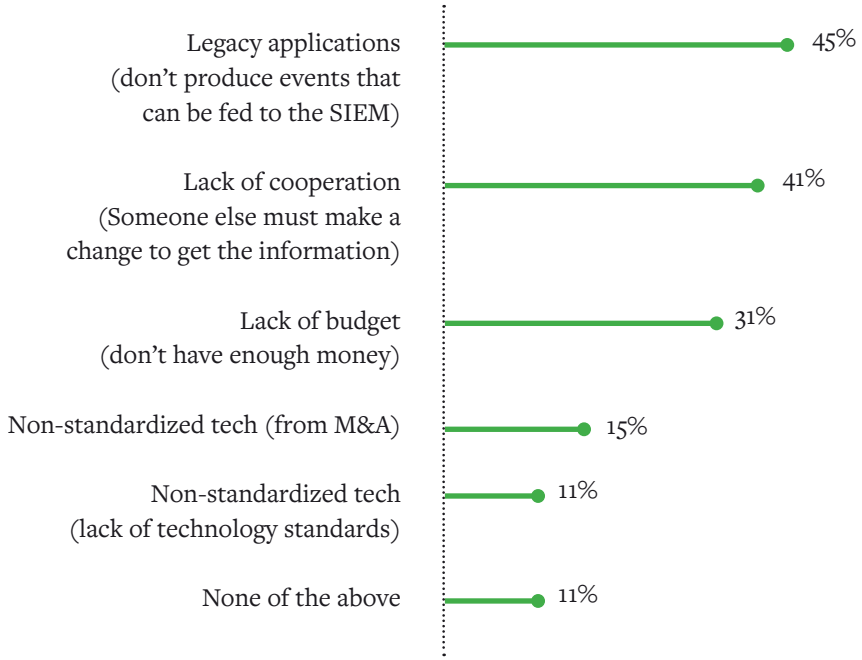
DETECTING SECURITY EVENTS

Just 5% of SOCs say they see what they need to. The greatest reasons given for not logging more events into the SIEM are systems that don't produce events that can be fed to the SIEM and lack of cooperation.

PERCENTAGE OF EVENTS SEEN IN SIEM



REASONS FOR NOT LOGGING MORE EVENTS IN SIEM



Finance & Budget

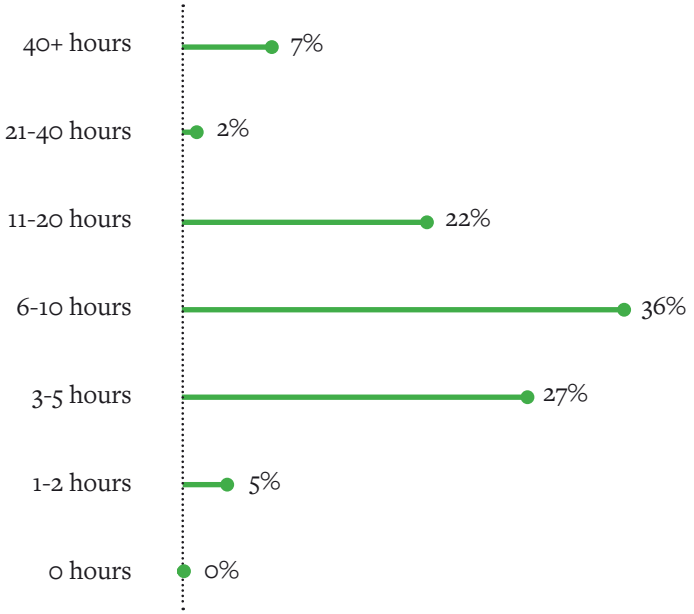
Technology is the area most frequently cited for insufficient funding. This is most strongly felt by American SOC personnel.

FUNDING DISTRIBUTIONS - 2018 | 2019

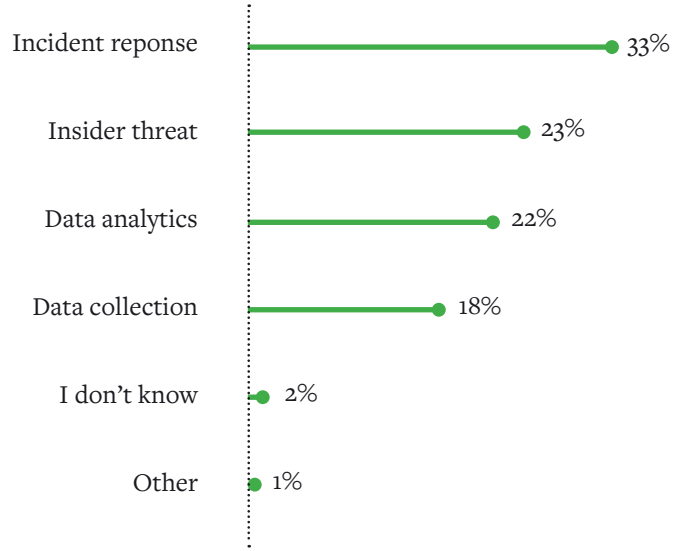
CYBER RISK INSURANCE

More than a third of respondents say they are not aware of (29%) or don't know (8%) about their organization's cyber risk insurance policy. Yet 9% of SOCs spend more than 21 hours on preparation when renewing cyber insurance policies, and 22% spend between 11-20 hours. Details are reported in the graph below.

HOURS SPENT ON RENEWALS



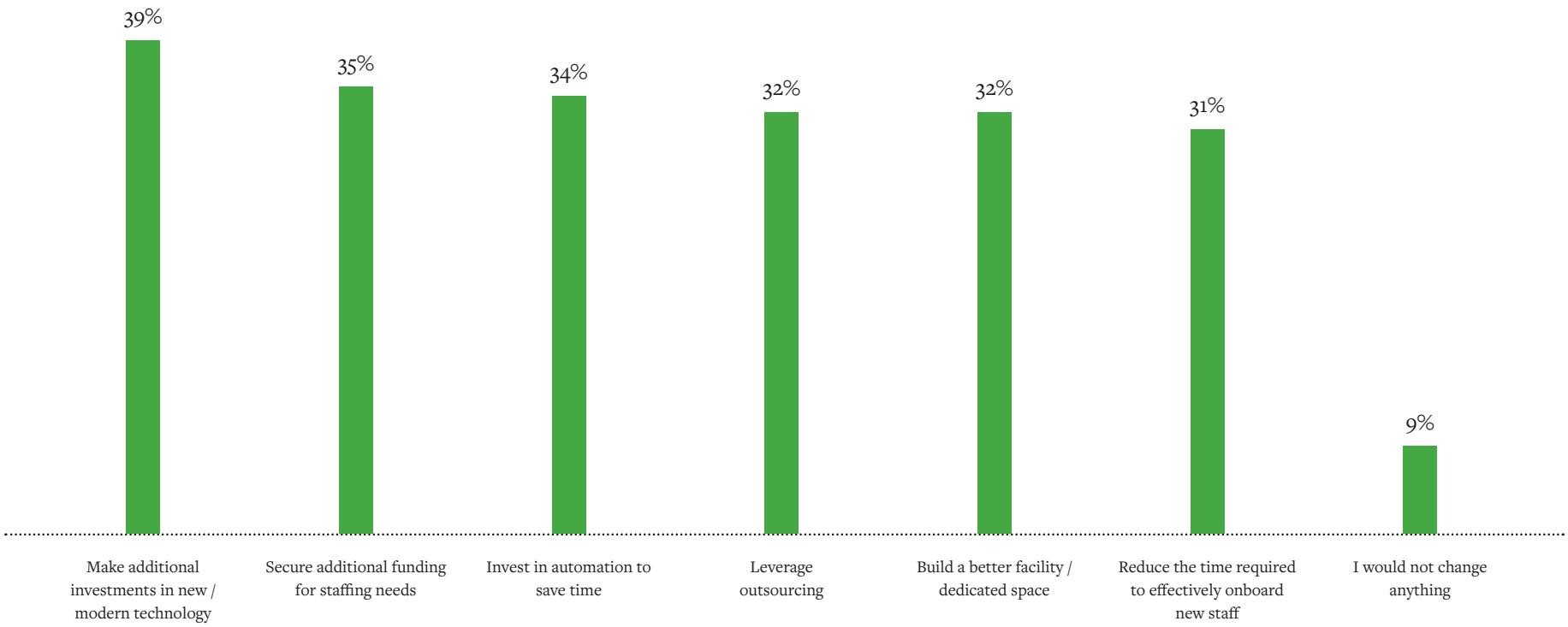
MOST IMPORTANT INSURANCE ISSUES



FUTURE INVESTMENTS

Among respondents, modern tech, staffing, and automation were considered the most needed for future investments in the SOC.

CHOSEN METHODS TO IMPROVE SOC



Demographics

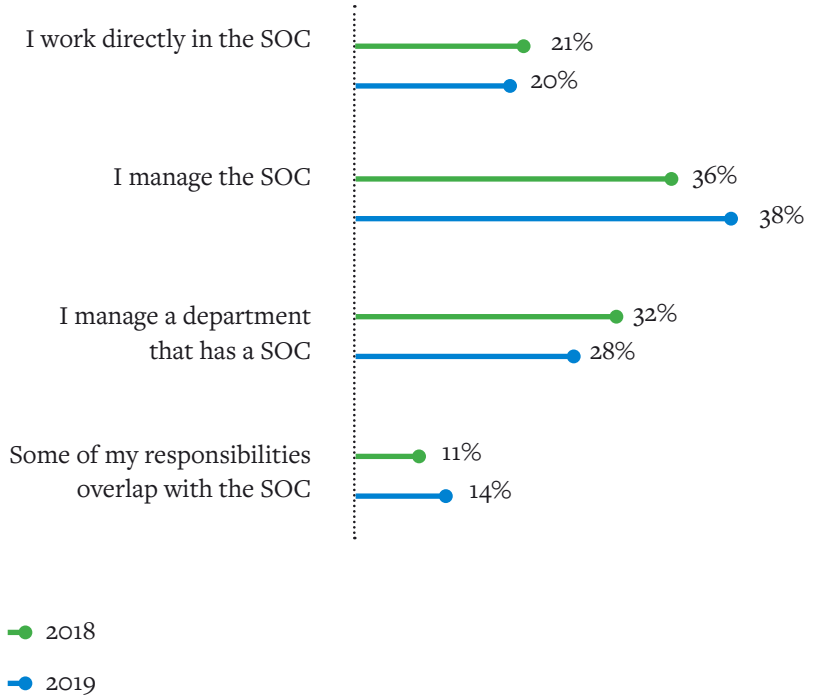
The Exabeam 2019 State of the SOC Report

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.

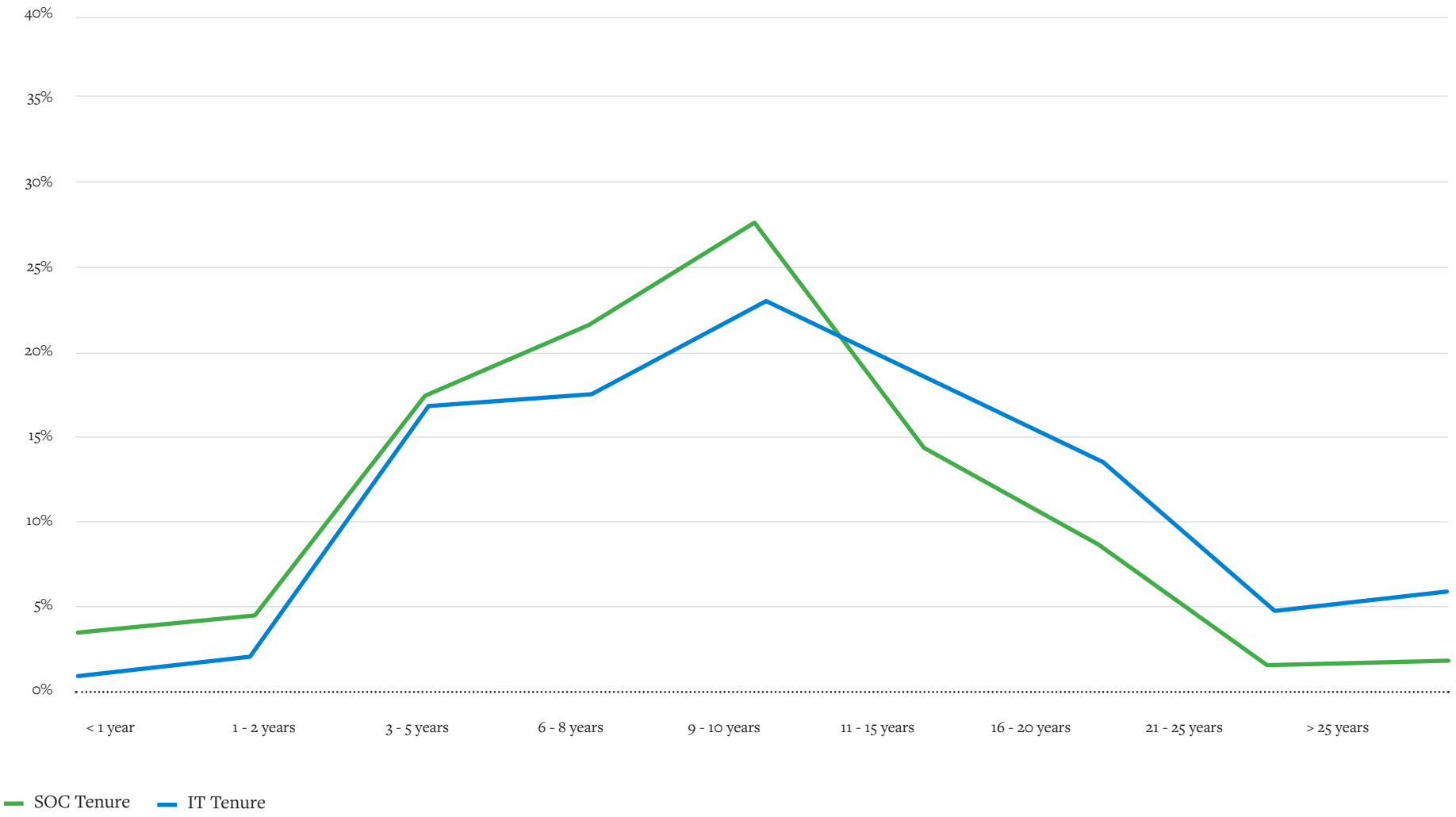
PROFILE OF PARTICIPANT JOB TITLES

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

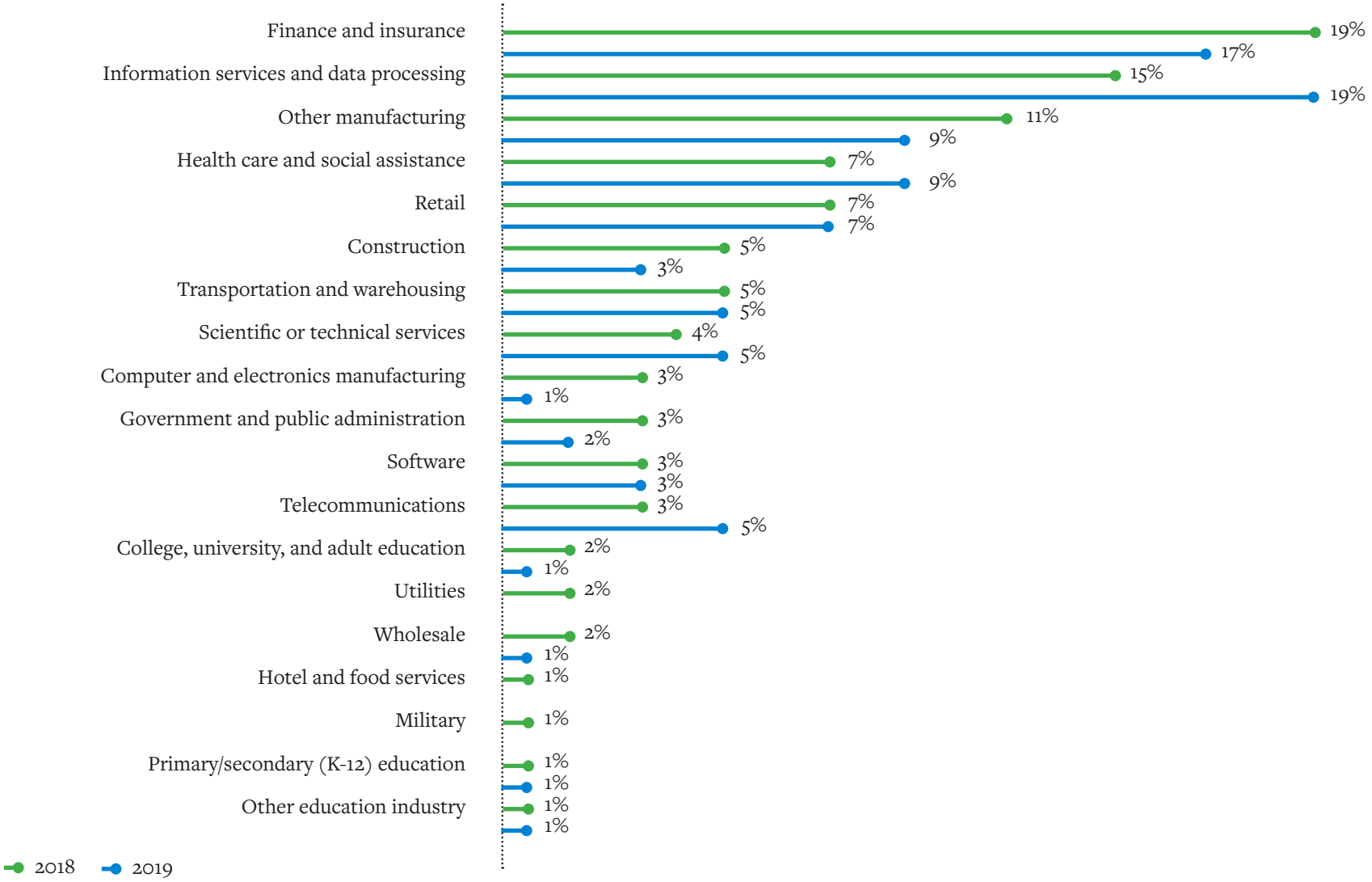
RELATION TO SOC



SOC INVOLVEMENT



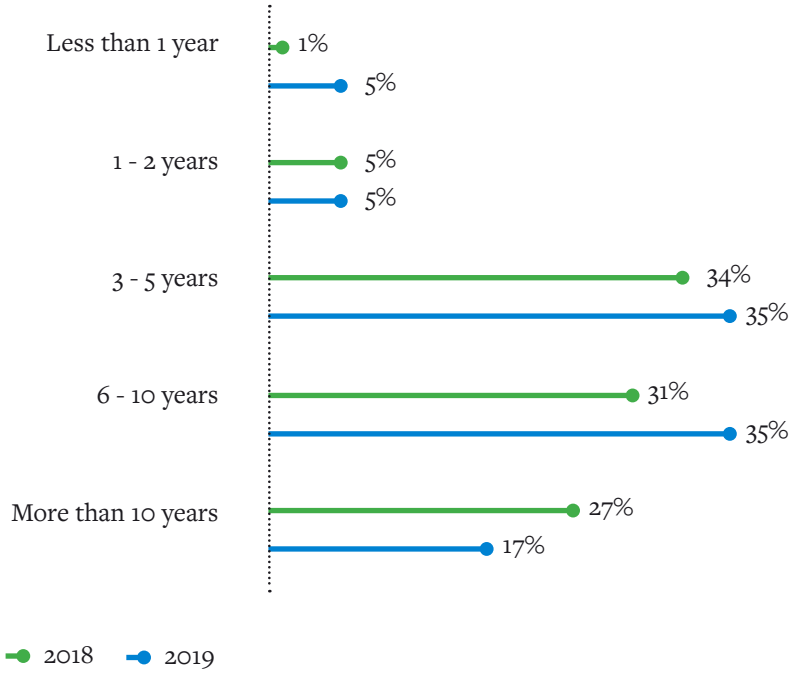
SOC EMPLOYEE INDUSTRIES



SOC OPERATIONAL HISTORIES

Most SOCs have operated between 3 and 10 years.

LENGTH OF TIME HAVING AN SOC - 2018 | 2019



Exabeam is the Smarter SIEM™ company. We empower enterprises to detect, investigate, and respond to cyberattacks more efficiently so their security operations and insider threat teams can work smarter. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the 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. www.exabeam.com.

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

1.844.EXABEAM
info@exabeam.com