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 20% a year ago)

50%

of SOC managers continue
to use automation
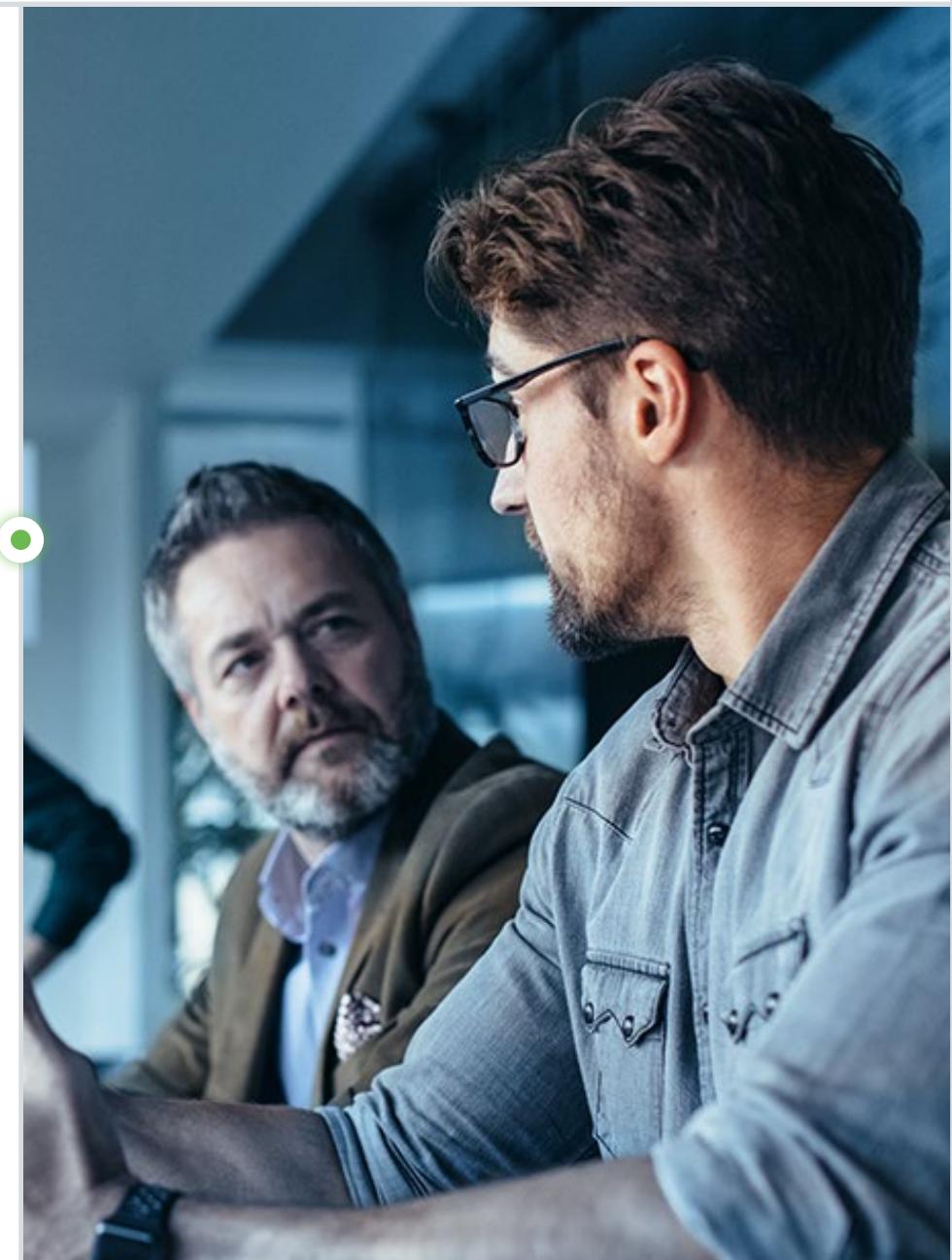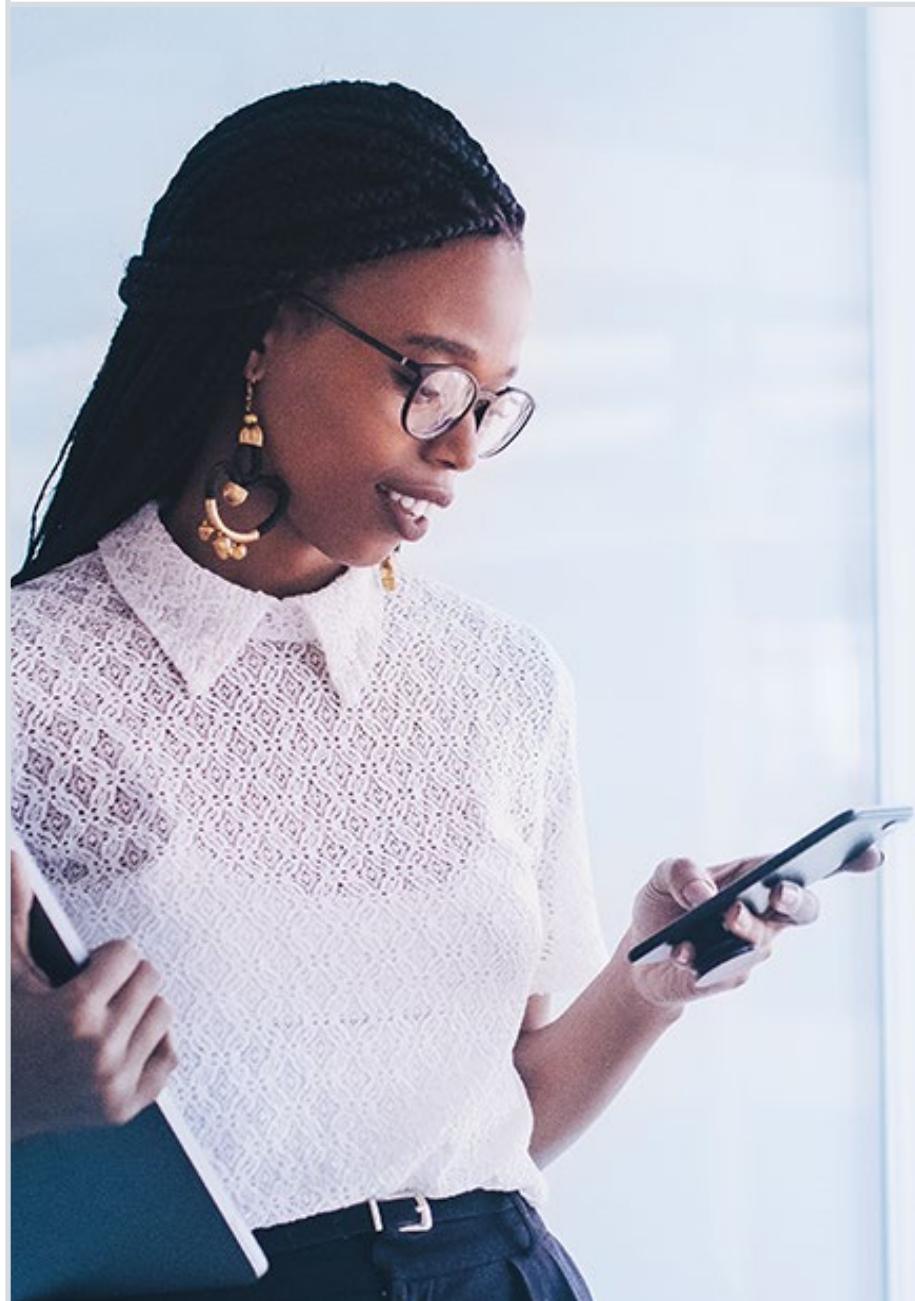
OUTSOURCING

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

29%
of highly effective SOCs say they are slightly understaffed

46%
of less effective SOCs say they are slightly understaffed

6−10
The number of employees understaffed SOCs say they need

42%
of SOCs surveyed say employees stay because of a good / challenging environment

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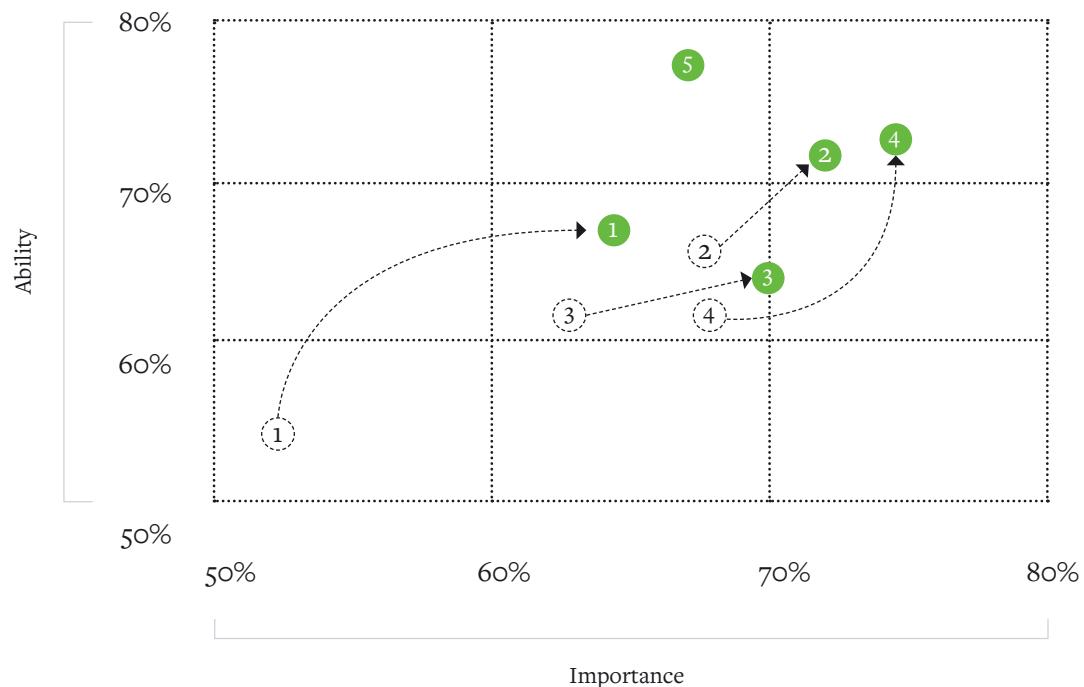
Soft Skills	
1	Personal/social skills
2	Ability to work in teams
3	Leadership ability
4	Communication
5	Effective Management

- 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

Time spent on reporting/documentation	33%
False positives	24%
Alert fatigue	27%
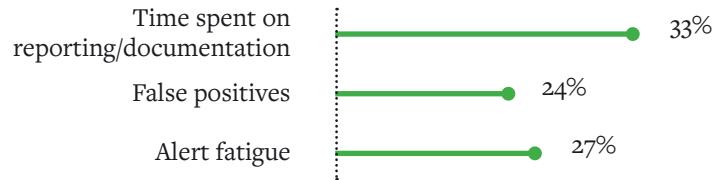
CIO / CISO
Inexperienced Staff

	21%
	29%
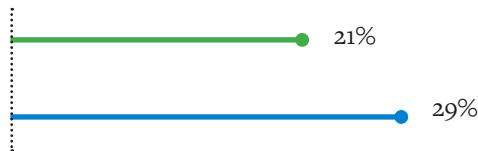
SOC MANAGERS
Inexperienced Staff

	24%
	12%
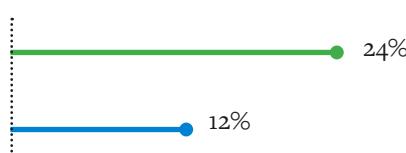
SOC ANALYSTS
Inexperienced Staff

	38%
	14%
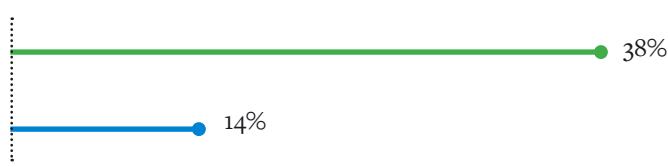
- 2018
- 2019

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

Pain Point	Percentage
Keeping up with security alerts	39%
Coordinating information between cybersecurity and IT operations	35%
Security tools are not well integrated	28%
Outdated equipment	23%
None of the above	11%
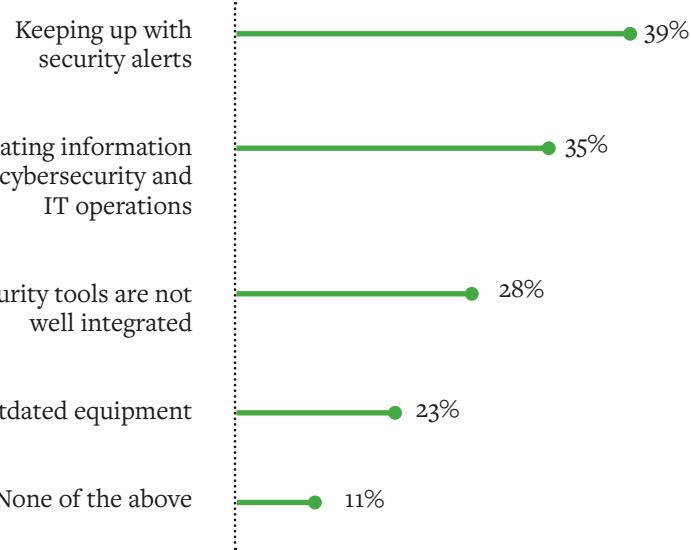
TECHNOLOGY

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

LARGE SOC

Artificial intelligence	25%
	27%
Machine learning	27%
	26%
Biometric authentication and access management	25%
	27%

MEDIUM SOC

Artificial intelligence	20%
	31%
Machine learning	15%
	18%
Biometric authentication and access management	13%
	28%

SMALLER SOC

Artificial intelligence	3%
	12%
Machine learning	3%
	16%
Biometric authentication and access management	6%
	12%
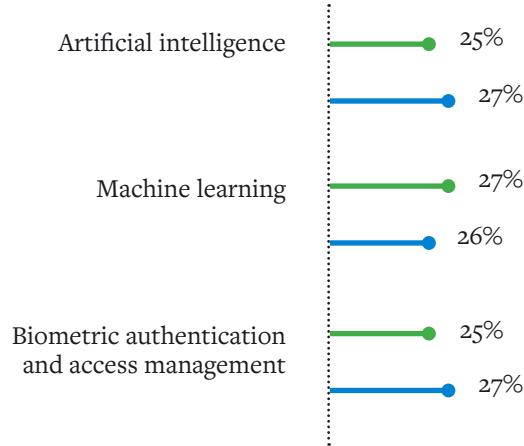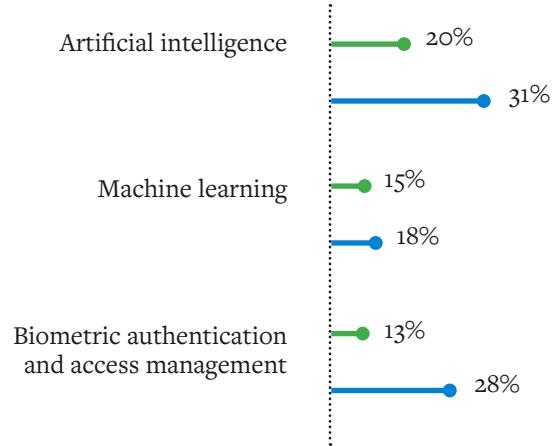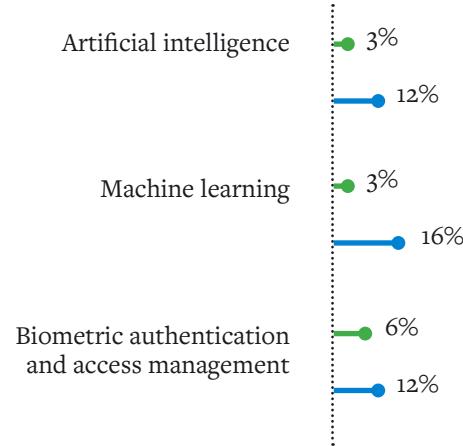
● 2018
● 2019

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

U.S.
- 58% (2018)
- 57% (2019)

U.K.
- 46% (2018)
- 36% (2019)

- 2018
- 2019

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

35%
desire more funding for staffing

39%
desire more investment in new/modern technology

34%
want to invest in automation to save time
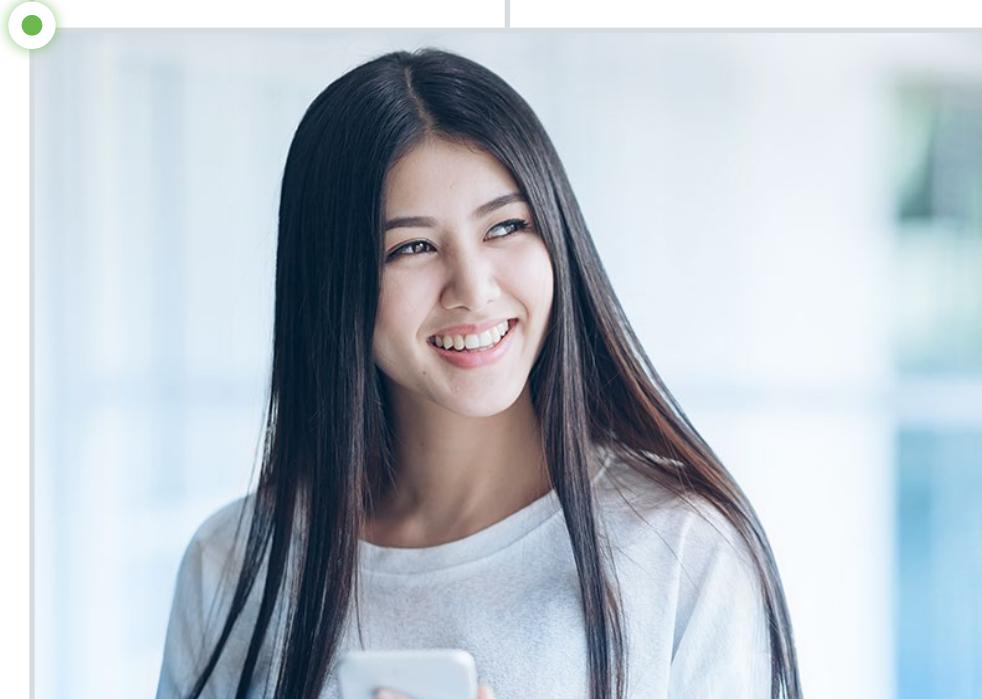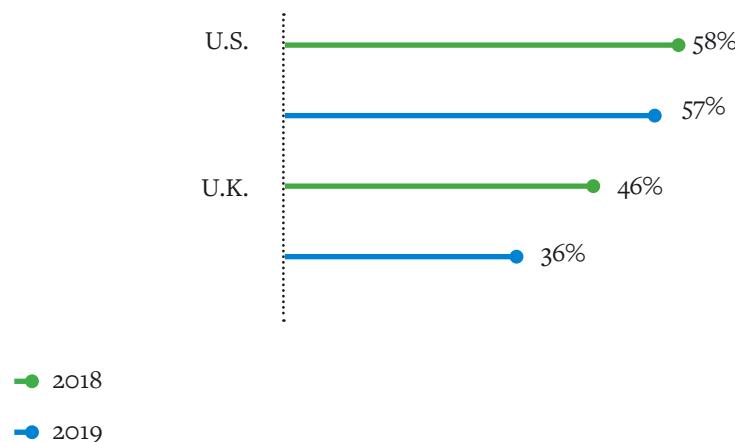
SOC Basics

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

Incident response	65%
	86%
Automation	56%
	68%
Threat hunting	51%
	67%

SOC MANAGERS

Incident response	65%
	74%
Automation	53%
	50%
Threat hunting	56%
	71%

SOC ANALYSTS

Incident response	56%
	67%
Automation	28%
	48%
Threat hunting	59%
	48%
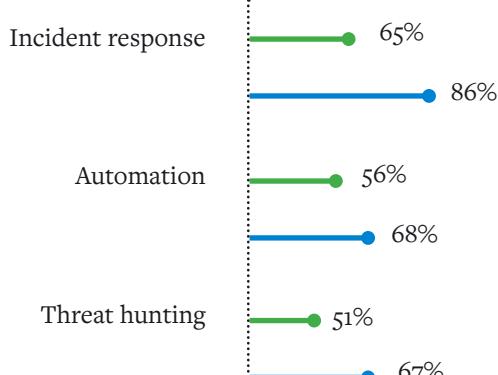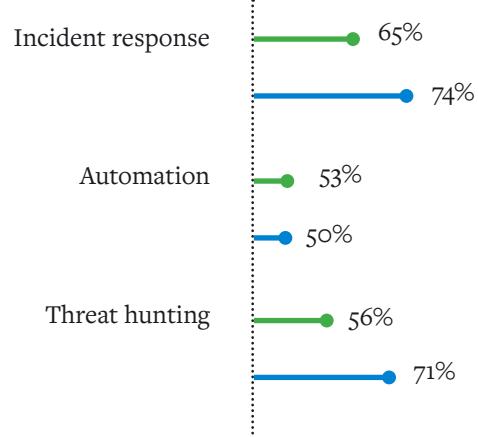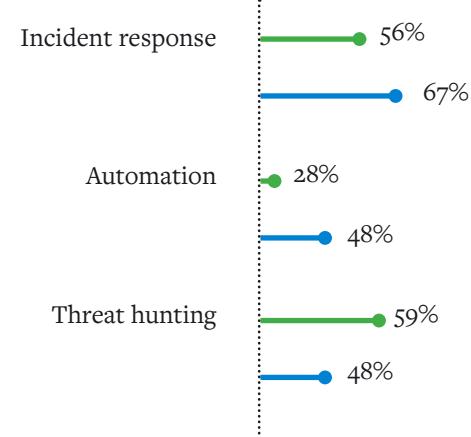
● 2018
● 2019

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

Event/data monitoring — 47% / 37%

Threat analysis — 45% / 48%

Malware analysis expertise — 40% / 55%

After-hours coverage — 37% / 43%

Incident response — 33% / 28%

Endpoint detection and response — 32% / 34%

Threat intel services — 28% / 45%

The entire SOC is outsourced — 5% / 0%

2018
2019
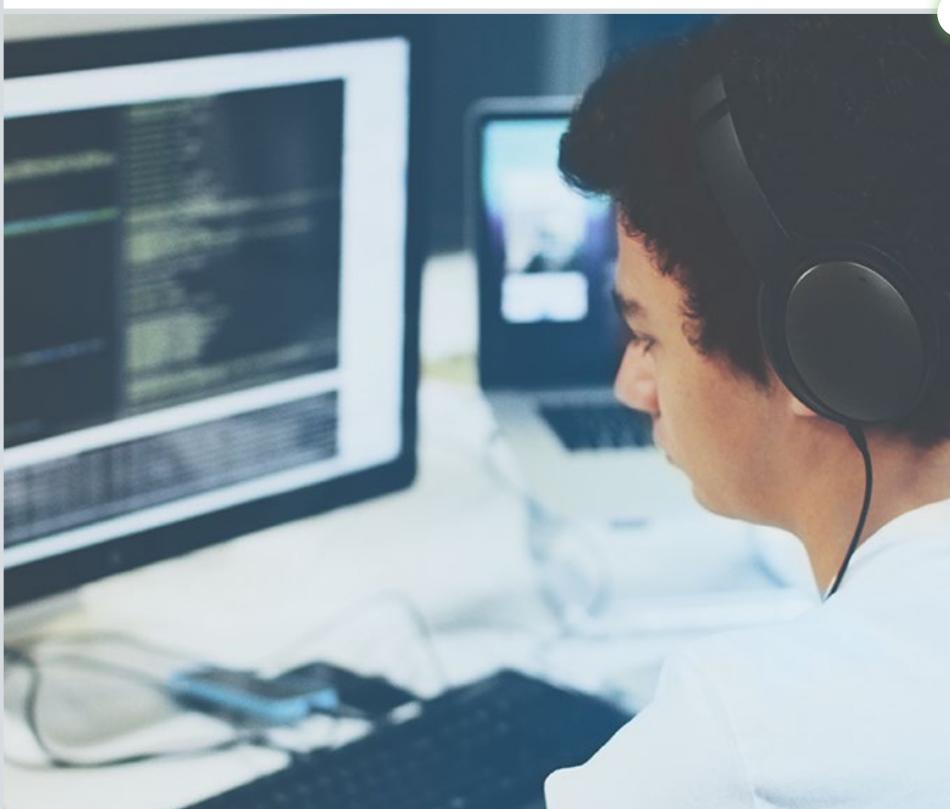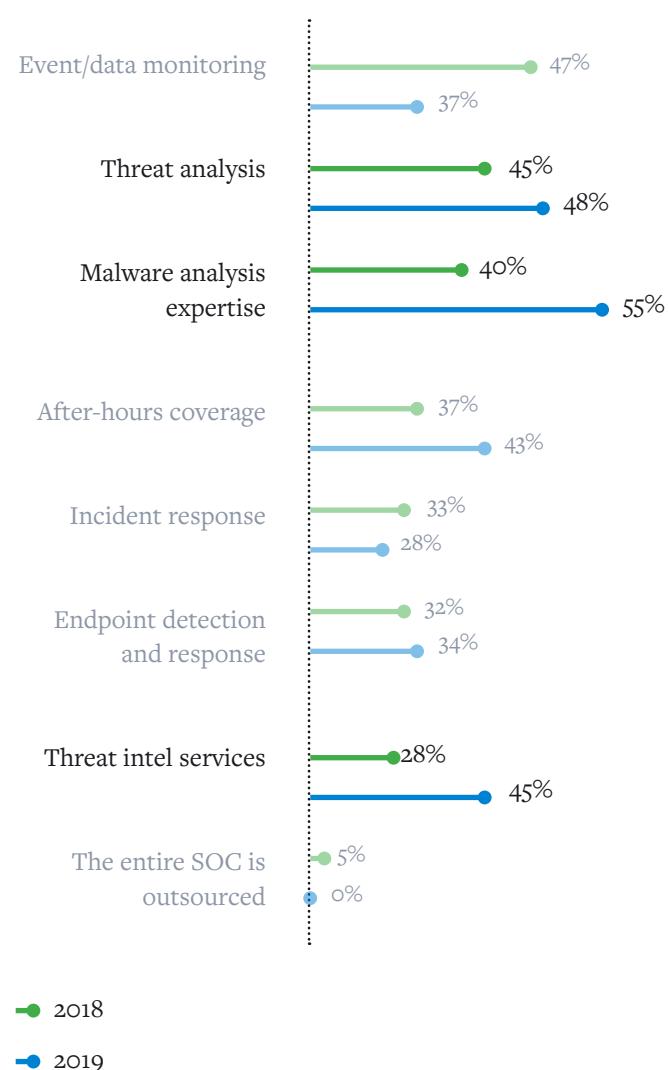
Staffing

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

38% Understaffed

	Heavily overstaffed	Slightly overstaffed	Correctly staffed	Slightly understaffed	Heavily understaffed
2018	2%	7%	46%	39%	6%
2019	3%	2%	55%	33%	5%

2018 ■ 2019 ■

NUMBER OF EMPLOYEES UNDERSTAFFED

	2018	2019
1 employee	1%	7%
2-5 employees	34%	26%
6-10 employees	29%	34%
11-20 employees	18%	16%
More than 20 employees	18%	16%

2018 2019
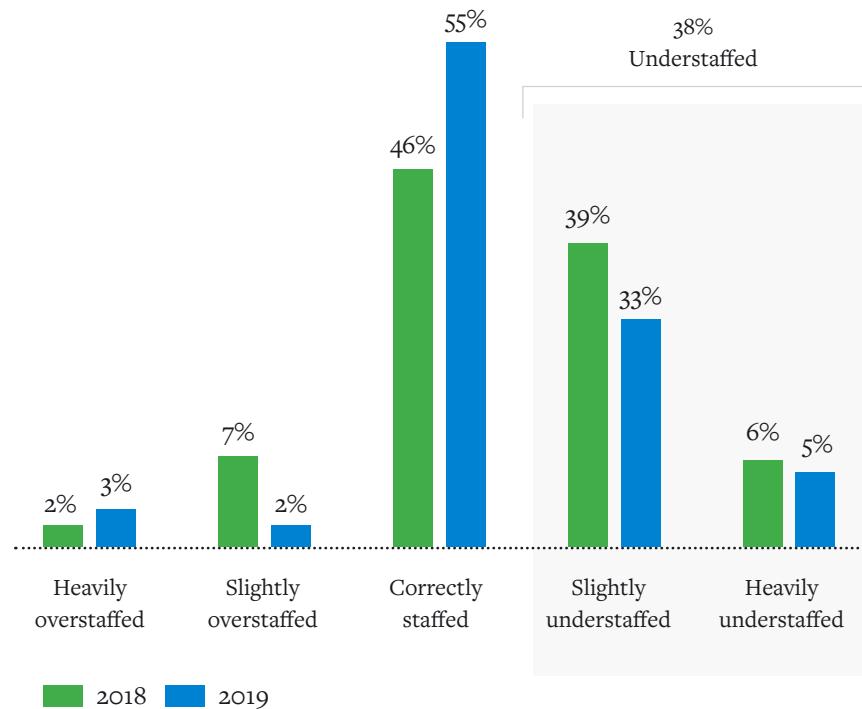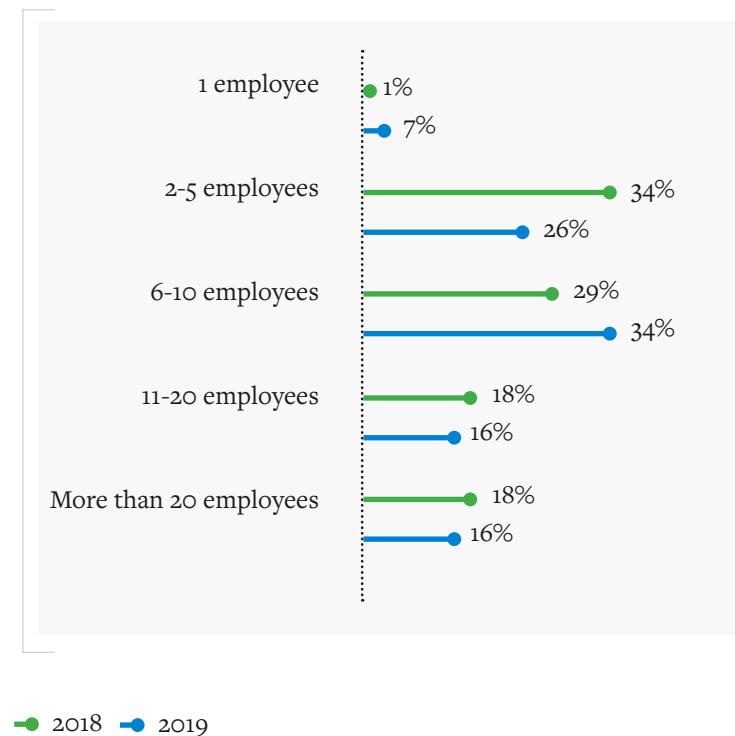
EMPLOYEE RETENTION DRIVERS

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

Good / challenging environment — 28% (2018), 42% (2019)
Workplace benefits — 25% (2018), 44% (2019)
High wages — 25% (2018), 43% (2019)
Good hiring / the right people — 10% (2018), 30% (2019)
Good working hours — 2% (2018)
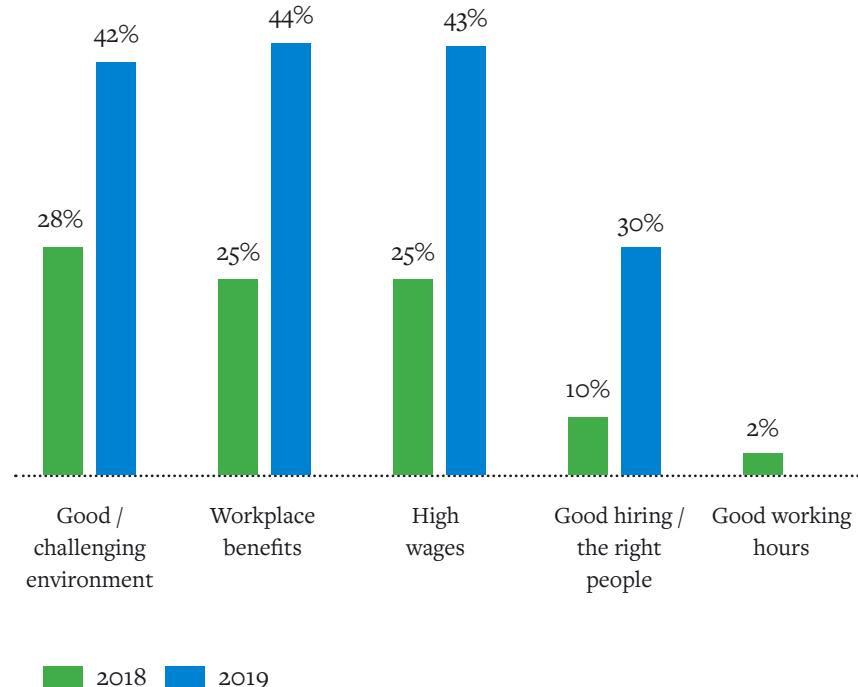
■ 2018 ■ 2019

REASONS EMPLOYEES ARE DIFFICULT TO RETAIN

Heavy competition for security employees — 60% (2018), 46% (2019)
Low wages — 32% (2018), 15% (2019)
Freelancing — 4% (2018), 23% (2019)
Poor working hours — 4% (2018), 23% (2019)
Limited advancement opportunities internally — 4% (2018), 31% (2019)
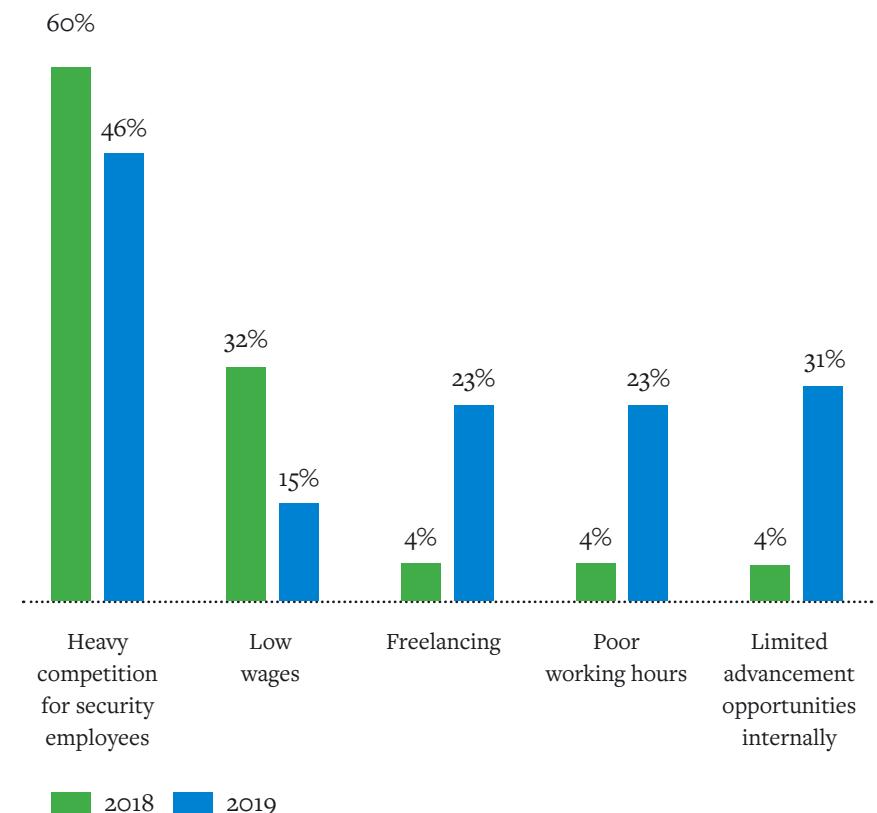
■ 2018 ■ 2019

SKILLS

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

SKILL IMPORTANCE - 2018 | 2019

2018

Skill	
Ability to work in teams	67%
Communication	67%
Leadership ability	63%
Personal and social skills	53%

2019

Skill	
Ability to work in teams	73%
Communication	75%
Leadership ability	70%
Personal and social skills	65%

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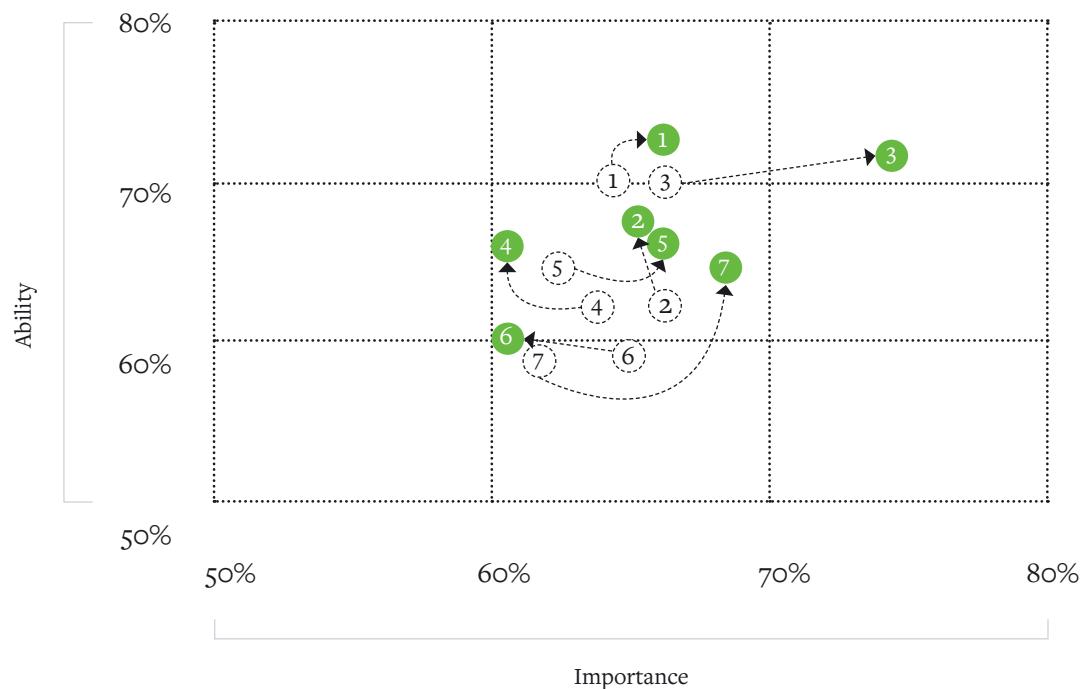
Hard Skills	
1	Network and system administration
2	Firewall architecture
3	Data loss prevention
4	Malware analysis
5	Risk management
6	Digital forensics
7	Threat hunting

- 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

Monitoring and reviewing events — 65%

U.S. SOCs have significantly more ability to monitor and review events (71%) than their U.K. counterparts (54%)

Responding to incidents — 70%

Threat modeling — 60%

Performing deep-dive incident analysis — 61%

Auto-remediation — 54%

Budget and resource allocation — 60%
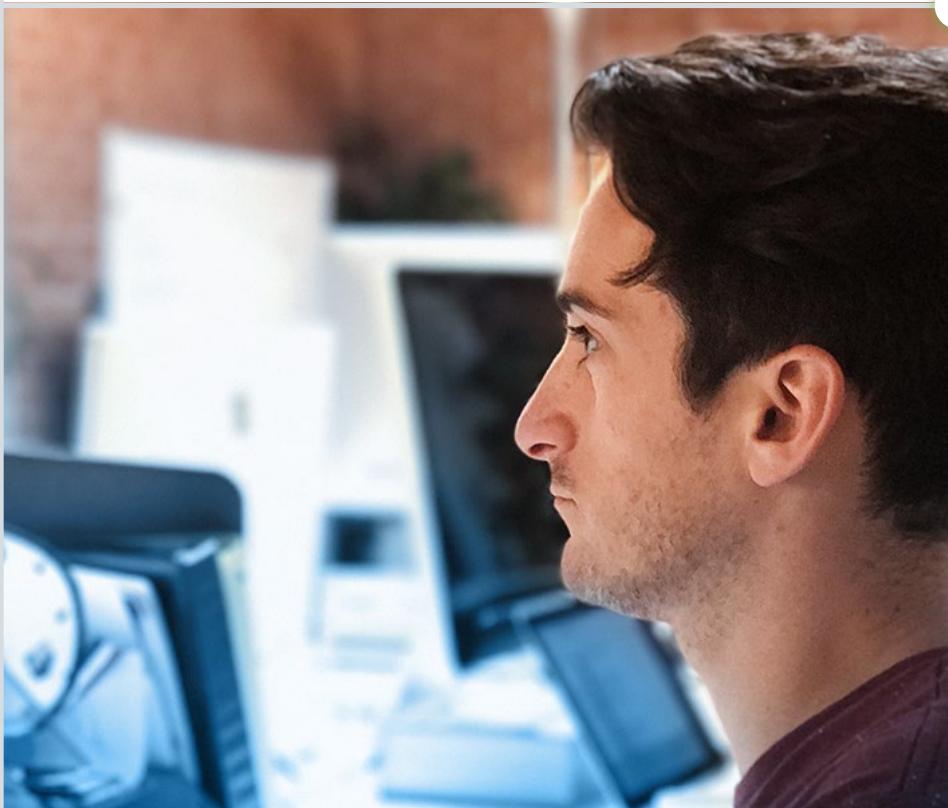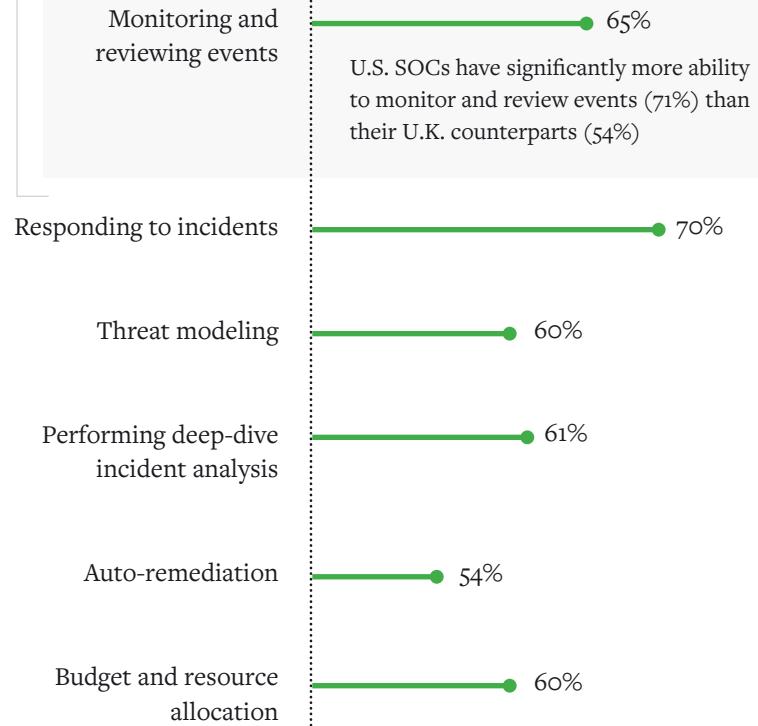
SMALLER SOCs

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

2018

Monitoring and reviewing events	72% / 67% / 58%
Responding to incidents	79% / 65% / 48%
Threat modeling	66% / 70% / 58%
Performing deep-dive incident analysis	63% / 54% / 42%
Auto-remediation	79% / 65% / 48%
Budget and resource allocation	59% / 61% / 36%

2019

Monitoring and reviewing events	64% / 72% / 60%
Responding to incidents	67% / 64% / 79%
Threat modeling	62% / 67% / 49%
Performing deep-dive incident analysis	65% / 62% / 51%
Auto-remediation	59% / 56% / 42%
Budget and resource allocation	61% / 67% / 51%
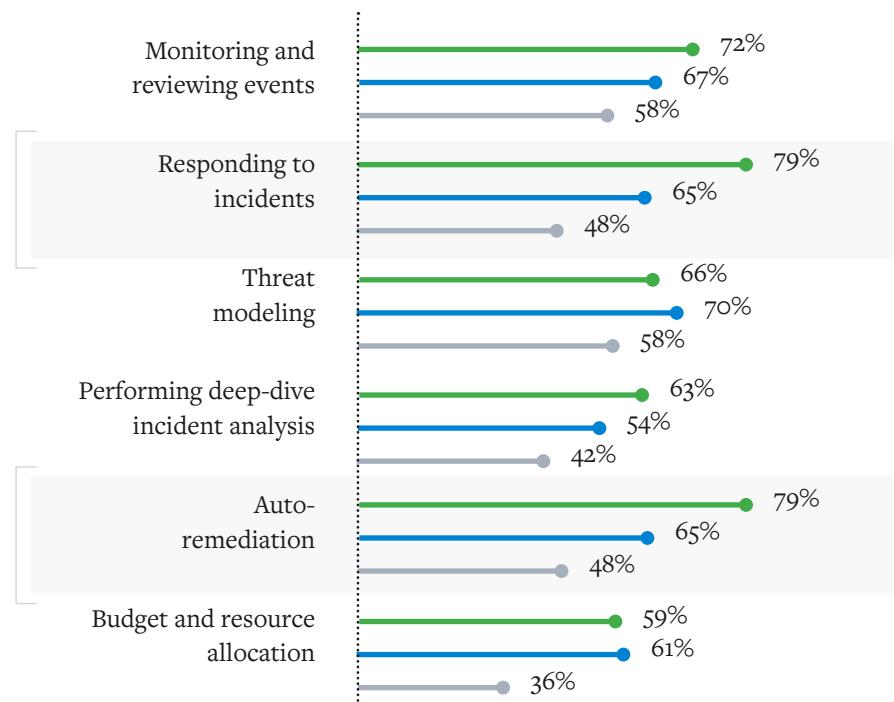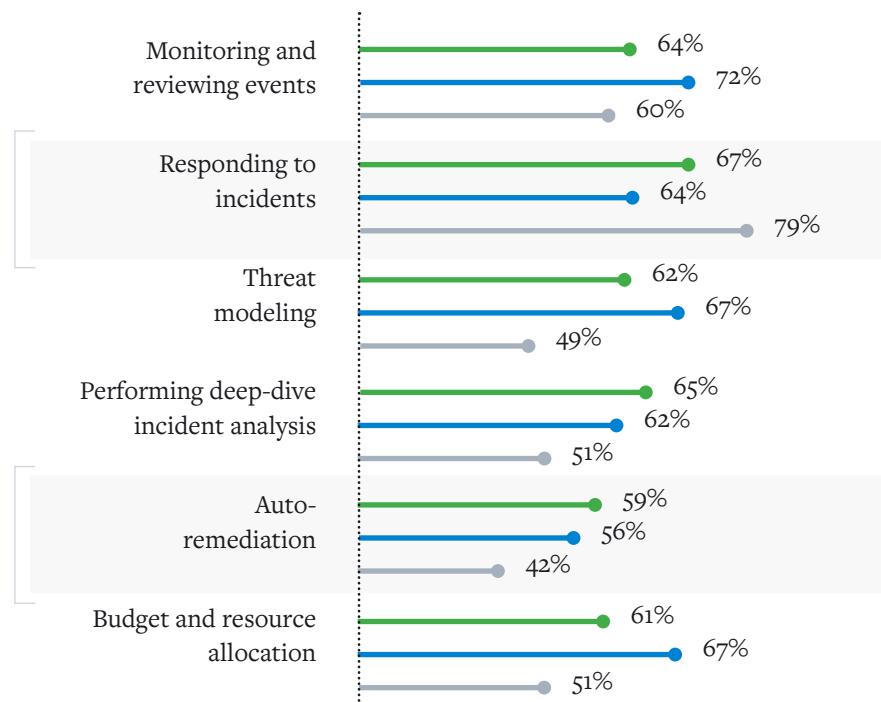
● Large SOC (200+ team members)   ● Medium SOC (25-199 team members)   ● Smaller SOC (1-24 team members)

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

Pain Point	%
Time spent on reporting and documentation	33%
Out-of-date systems / applications	29%
False-positives / white noise	27%
Alert fatigue	24%
False negatives	23%
Lack of visibility	21%
Inability to find system owners	19%
Inexperienced staff	19%
Ability to procure / deploy tools in time	19%
Lack of understanding of the network	19%
Manual attack timeline creation	15%
Lacking asset list	11%

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

Too much time spent on reporting and documentation — 32%
— 32%

Inexperienced staff — 21%
— 29%

SOC MANAGERS

Too much time spent on reporting and documentation — 29%
— 36%

Inexperienced staff — 24%
— 12%

SOC ANALYSTS

Too much time spent on reporting and documentation — 53%
— 24%

Inexperienced staff — 38%
— 14%
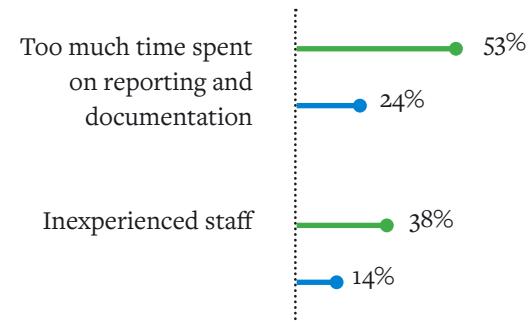
- 2018
- 2019

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

	Daily	Weekly	Monthly	Quarterly	Semi-annually	Annually	Randomly
Highly Effective SOC	11%	23%	30%	21%	6%	6%	4%
Effective SOC	7%	22%	30%	27%	10%	5%	
Less Effective SOC		8%	35%	30%	14%		8%

■ Highly Effective SOC ■ Effective SOC ■ Less Effective SOC
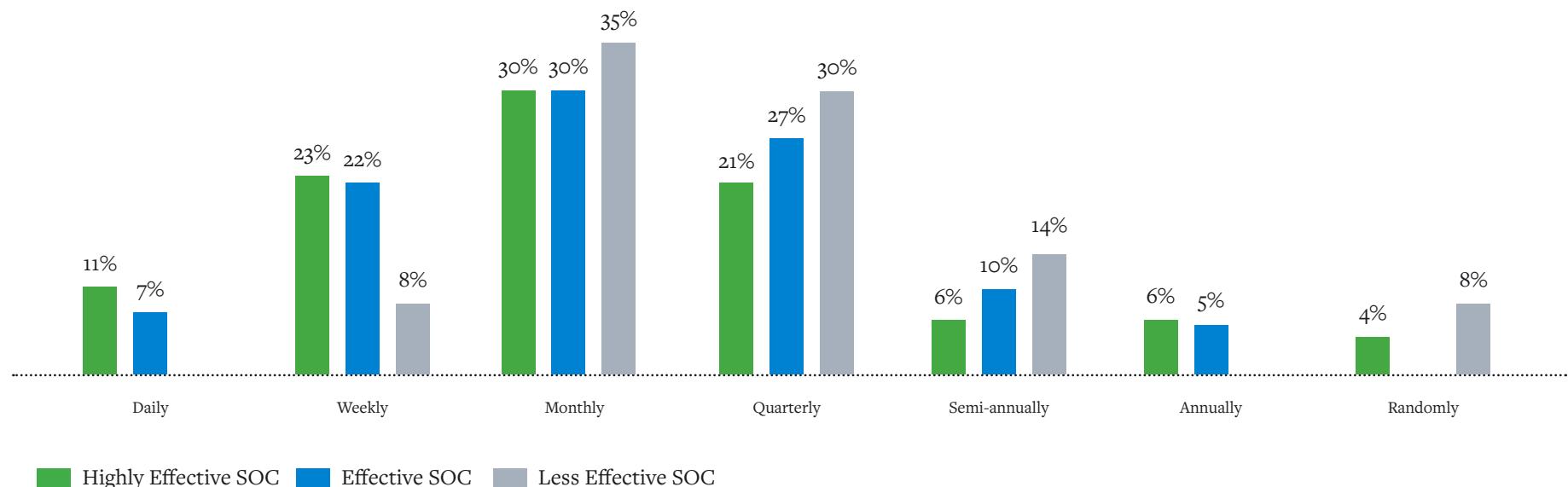
SURVEY RESPONDENTS ON TRAINING IN THEIR ORGANIZATIONS

"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
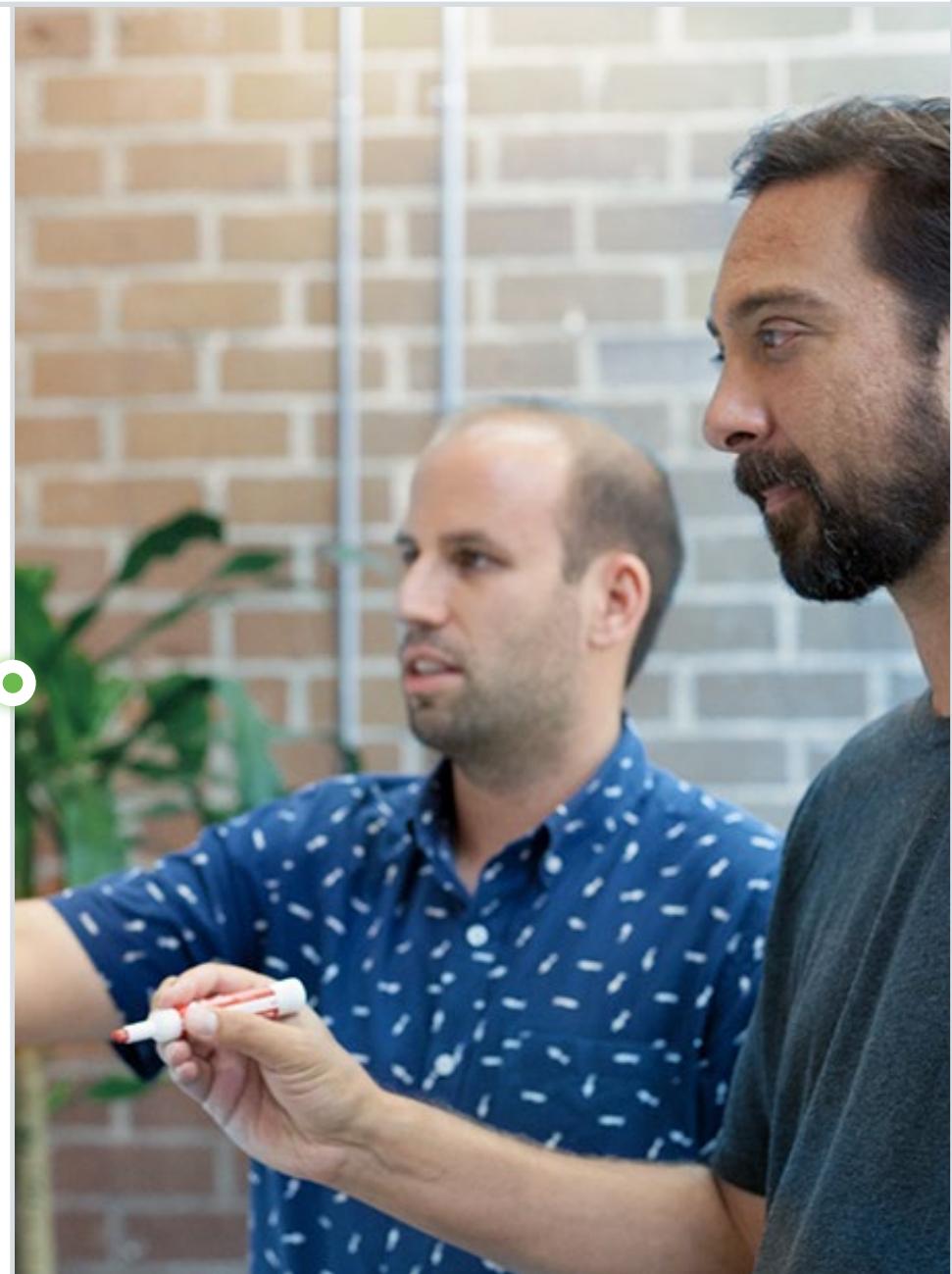
TRAINING IN HIGHLY EFFECTIVE SOCs

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

TYPES OF TRAINING

Formal training session by my organization — 64%
Formal training session by my organization — 26%

Formal training session by a third-party — 43%
Formal training session by a third-party — 54%

Online training by my organization — 43%
Online training by my organization — 29%

Online training by a third-party — 38%
Online training by a third-party — 49%

● Highly Effective SOCs
● Less Effective SOCs

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

	2018	2019
Number of incidents handled	52% / 35% / 36%	35% / 51% / 51%
Number of devices or assets affected	39% / 28% / 36%	24% / 36% / 35%
Percentage of incidents escalated	51% / 39% / 27%	44% / 36% / 33%
False positives incident rate	41% / 35% / 30%	29% / 31% / 23%
Mean time to detect	32% / 37% / 24%	27% / 36% / 19%
Mean time to repair	41% / 39% / 27%	24% / 31% / 23%
Monetary cost per incident	32% / 41% / 27%	33% / 38% / 28%
Downtime or business outage	35% / 50% / 48%	36% / 49% / 58%
Incident occurrence due to known vulnerability	45% / 26% / 36%	42% / 33% / 26%
Time from detection to containment to eradication	41% / 41% / 36%	36% / 31% / 37%

Large SOC (200+ team members)
Medium SOC (25-199 team members)
Smaller SOC (1-24 team members)

26

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.
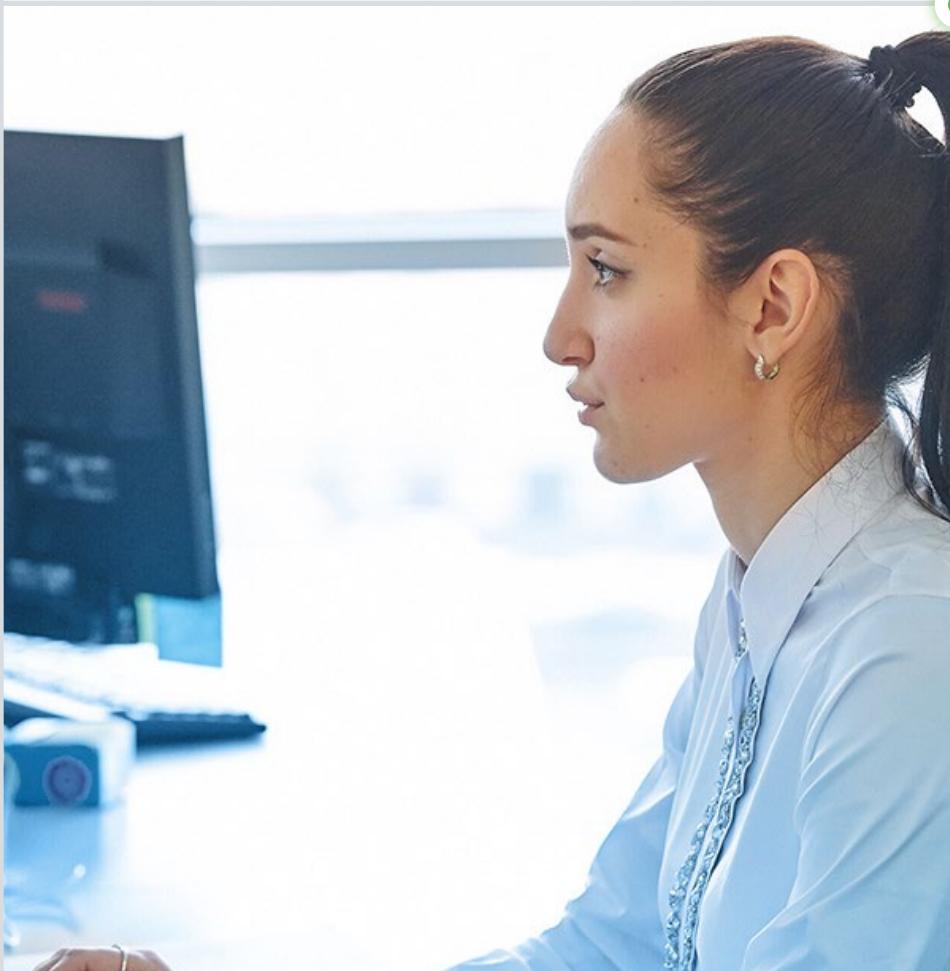
METRICS TRACKED BY ROLE – 2018 | 2019

2018 **2019**

	2018	2019
Number of incidents handled	43% / 38% / 53%	52% / 44% / 24%
Number of devices or assets affected	35% / 31% / 44%	40% / 38% / 24%
Percentage of incidents escalated	38% / 45% / 47%	46% / 35% / 33%
False positives incident rate	40% / 33% / 38%	32% / 29% / 14%
Mean time to detect	30% / 38% / 25%	24% / 33% / 14%
Mean time to repair	37% / 40% / 34%	32% / 35% / 10%
Monetary cost per incident	35% / 31% / 38%	30% / 36% / 29%
Downtime or business outage	38% / 45% / 47%	48% / 45% / 43%
Incident occurrence due to known vulnerability	40% / 40% / 28%	40% / 33% / 29%
Time from detection to containment to eradication	35% / 47% / 38%	33% / 39% / 29%

● CIO/CISO   ● SOC managers   ● SOC analysts

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

Technology	%
Endpoint Detection and Response	41%
Identity and Access Management	41%
Big Data Security Analytics	39%
Advanced Network and Cloud Monitoring	37%
Cloud Access Security Brokers	29%
User and Entity Behavior Analytics	23%
Artificial Intelligence	19%
Machine Learning	18%
Biometric Authentication and Access Management	17%

2019

Technology	%
Endpoint Detection and Response	38%
Identity and Access Management	39%
Big Data Security Analytics	39%
Advanced Network and Cloud Monitoring	39%
Cloud Access Security Brokers	29%
User and Entity Behavior Analytics	22%
Artificial Intelligence	23%
Machine Learning	21%
Biometric Authentication and Access Management	23%

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

CIO/CISO

| Pain Point	2018	2019
Keeping up with security alerts	35%	49%
Coordinating information between cybersecurity and IT operations	38%	38%
Security tools are not well integrated	43%	22%
Outdated equipment	22%	24%
None of the above	10%	5%

SOC MANAGER

Pain Point	2018	2019
Keeping up with security alerts	51%	32%
Coordinating information between cybersecurity and IT operations	38%	36%
Security tools are not well integrated	31%	30%
Outdated equipment	29%	26%
None of the above	9%	18%

SOC ANALYSTS

| Pain Point	2018	2019
Keeping up with security alerts	44%	33%
Coordinating information between cybersecurity and IT operations	41%	19%
Security tools are not well integrated	41%	38%
Outdated equipment	50%	10%
None of the above	13%	5%

● 2018 ● 2019

29

TECHNOLOGY PAIN POINTS

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

USAGE EXPECTATIONS

	NEXT 12 MOS.	NEXT 1-2 YRS.	NEXT 3-5 YRS.
User and entity behavior analytics	22% / 25%	17% / 19%	16% / 17%
Big data security analytics	22% / 23%	19% / 13%	9% / 9%
Biometric authentication and access management	22% / 25%	22% / 16%	19% / 15%

● 2018   ● 2019
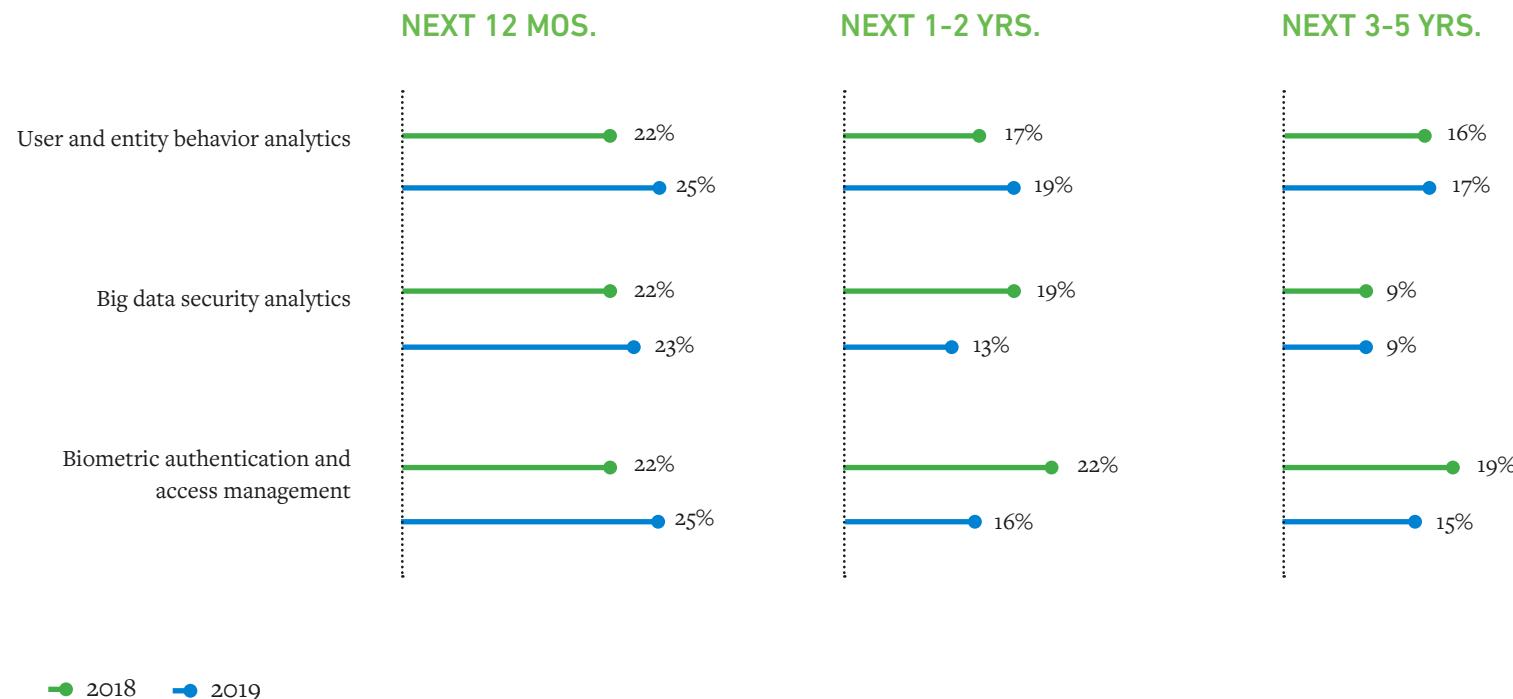
DETECTING SECURITY EVENTS

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

Range	Percentage
0%	1%
1% - 20%	16%
21% - 40%	27%
41% - 60%	28%
61% - 80%	15%
81% - 99%	8%
100%	5%
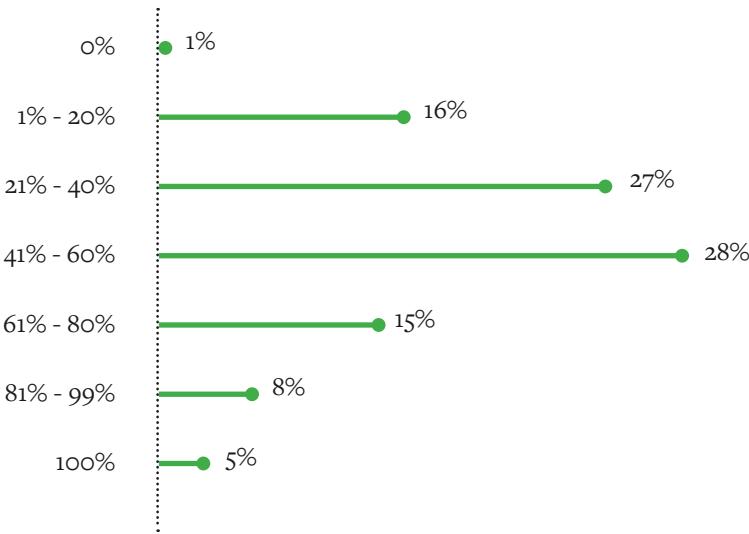
REASONS FOR NOT LOGGING MORE EVENTS IN SIEM

Reason	Percentage
Legacy applications (don't produce events that can be fed to the SIEM)	45%
Lack of cooperation (Someone else must make a change to get the information)	41%
Lack of budget (don't have enough money)	31%
Non-standardized tech (from M&A)	15%
Non-standardized tech (lack of technology standards)	11%
None of the above	11%
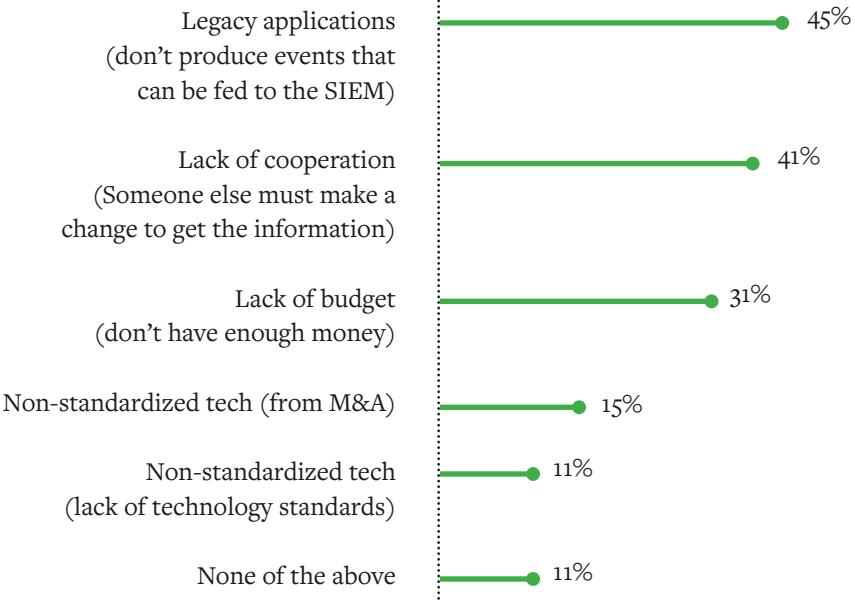
Finance & Budget

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

FUNDING DISTRIBUTIONS – 2018 | 2019

Legend: ■ 2018 ■ 2019

Technology — U.S.: 58% (2018), 57% (2019); U.K.: 46% (2018), 36% (2019)
Staffing — U.S.: 32% (2018), 28% (2019); U.K.: 44% (2018), 32% (2019)
Facilities — U.S.: 29% (2018), 20% (2019); U.K.: 28% (2018), 20% (2019)
Management — U.S.: 24% (2018), 29% (2019); U.K.: 26% (2018), 32% (2019)
None of the above — U.S.: 20% (2018), 17% (2019); U.K.: 16% (2018), 30% (2019)
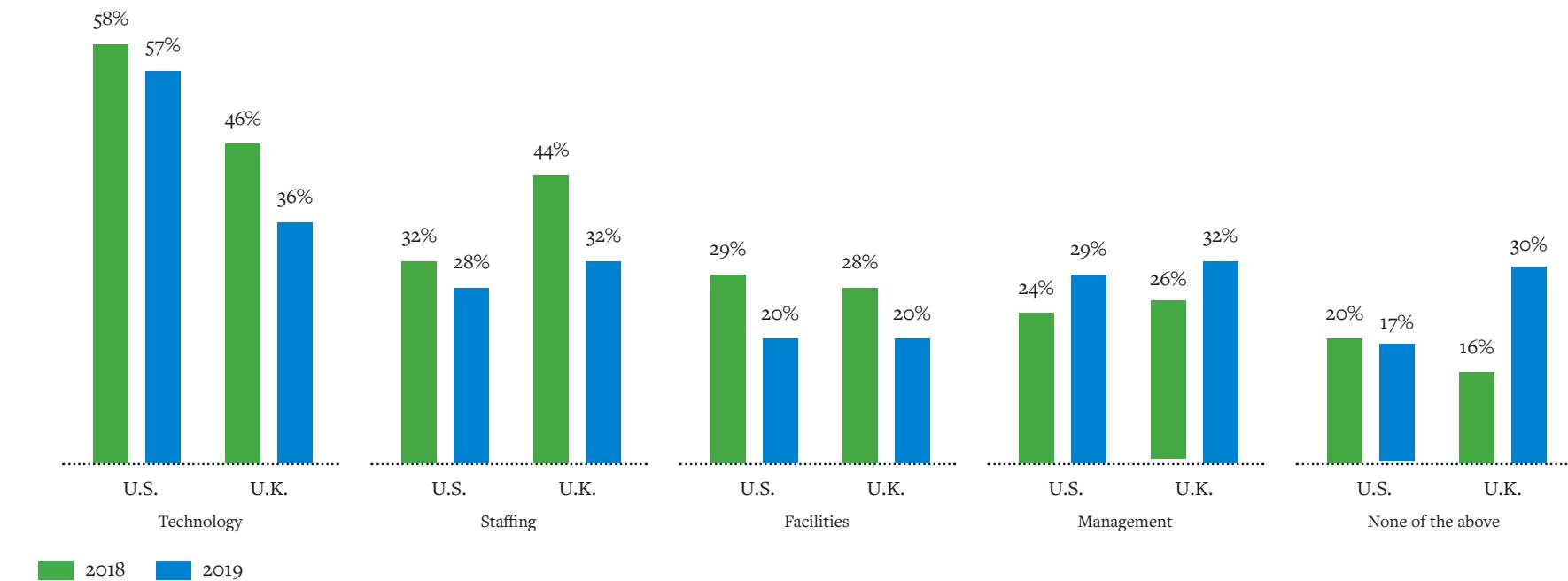
CYBER RISK INSURANCE

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

40+ hours	7%
21-40 hours	2%
11-20 hours	22%
6-10 hours	36%
3-5 hours	27%
1-2 hours	5%
0 hours	0%
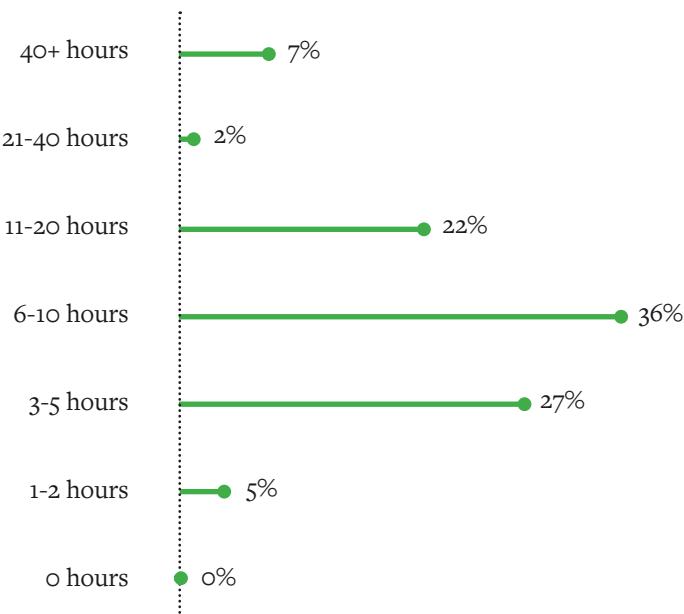
MOST IMPORTANT INSURANCE ISSUES

Incident reponse	33%
Insider threat	23%
Data analytics	22%
Data collection	18%
I don't know	2%
Other	1%
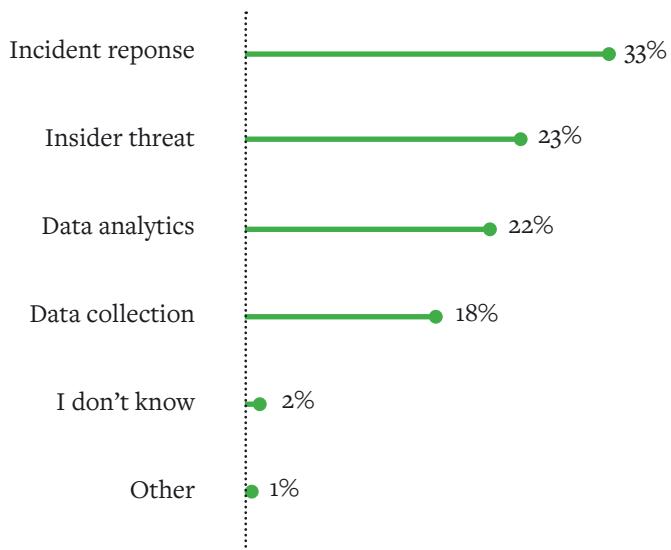
## FUTURE INVESTMENTS

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

CHOSEN METHODS TO IMPROVE SOC

|	
39%	Make additional investments in new / modern technology
35%	Secure additional funding for staffing needs
34%	Invest in automation to save time
32%	Leverage outsourcing
32%	Build a better facility / dedicated space
31%	Reduce the time required to effectively onboard new staff
9%	I would not change anything
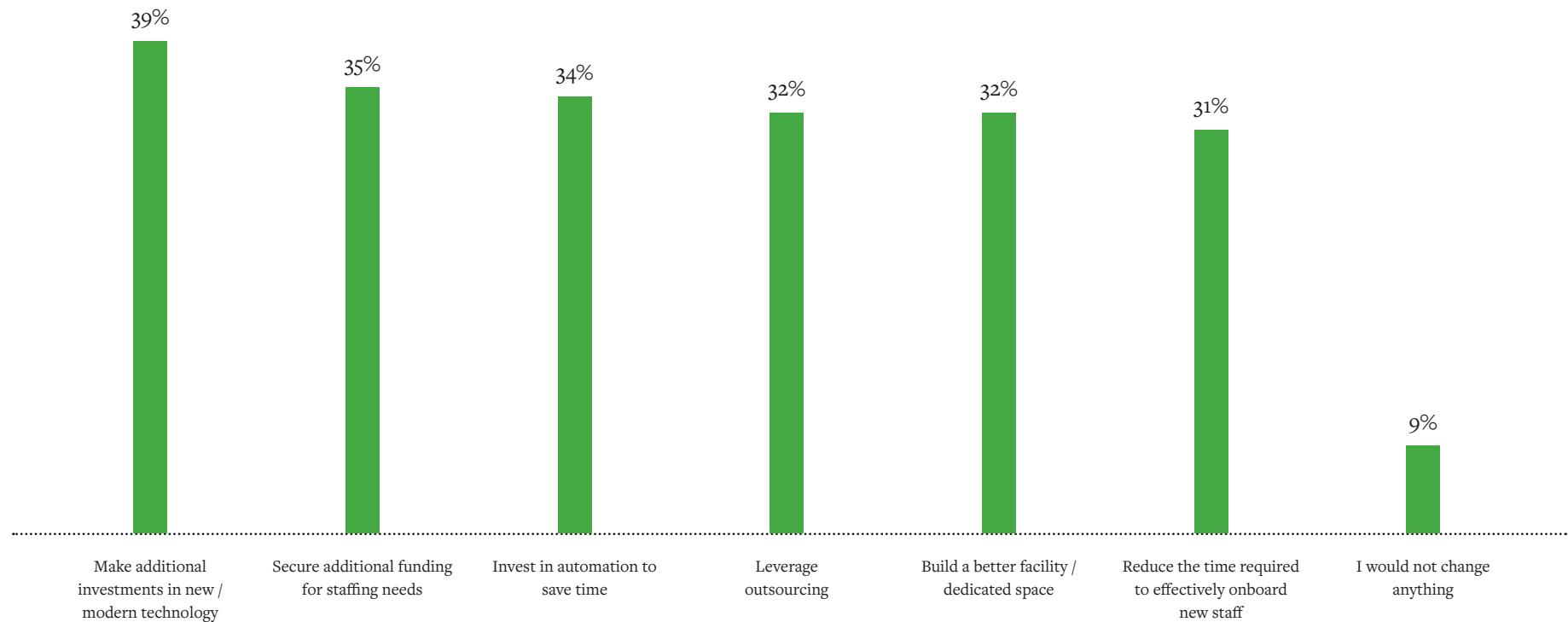
Demographics

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

I work directly in the SOC
21%
20%

I manage the SOC
36%
38%

I manage a department that has a SOC
32%
28%

Some of my responsibilities overlap with the SOC
11%
14%

- 2018
- 2019

SOC INVOLVEMENT

Legend: SOC Tenure, IT Tenure

X-axis: < 1 year, 1 - 2 years, 3 - 5 years, 6 - 8 years, 9 - 10 years, 11 - 15 years, 16 - 20 years, 21 - 25 years, > 25 years

Y-axis: 0%, 5%, 10%, 15%, 20%, 25%, 30%, 35%, 40%
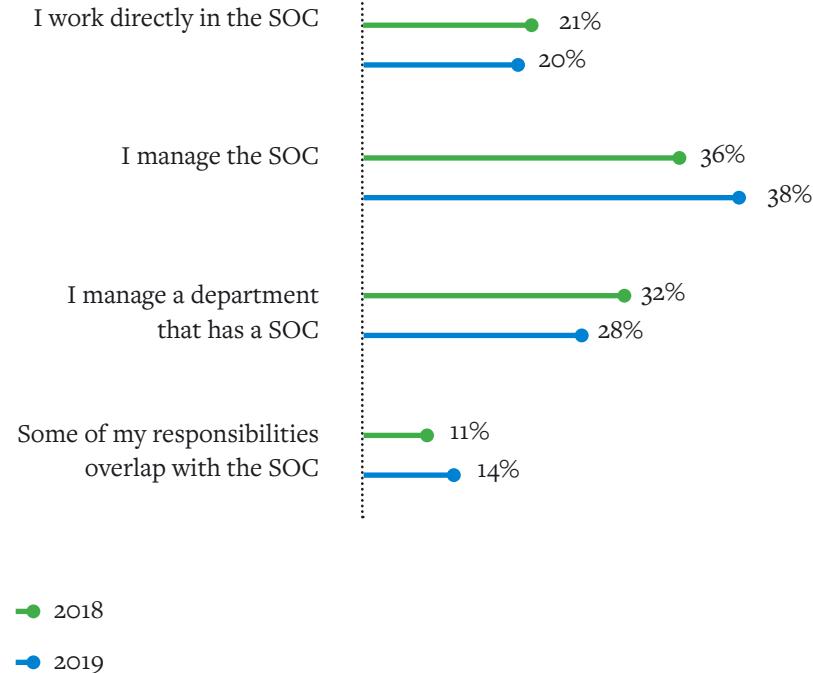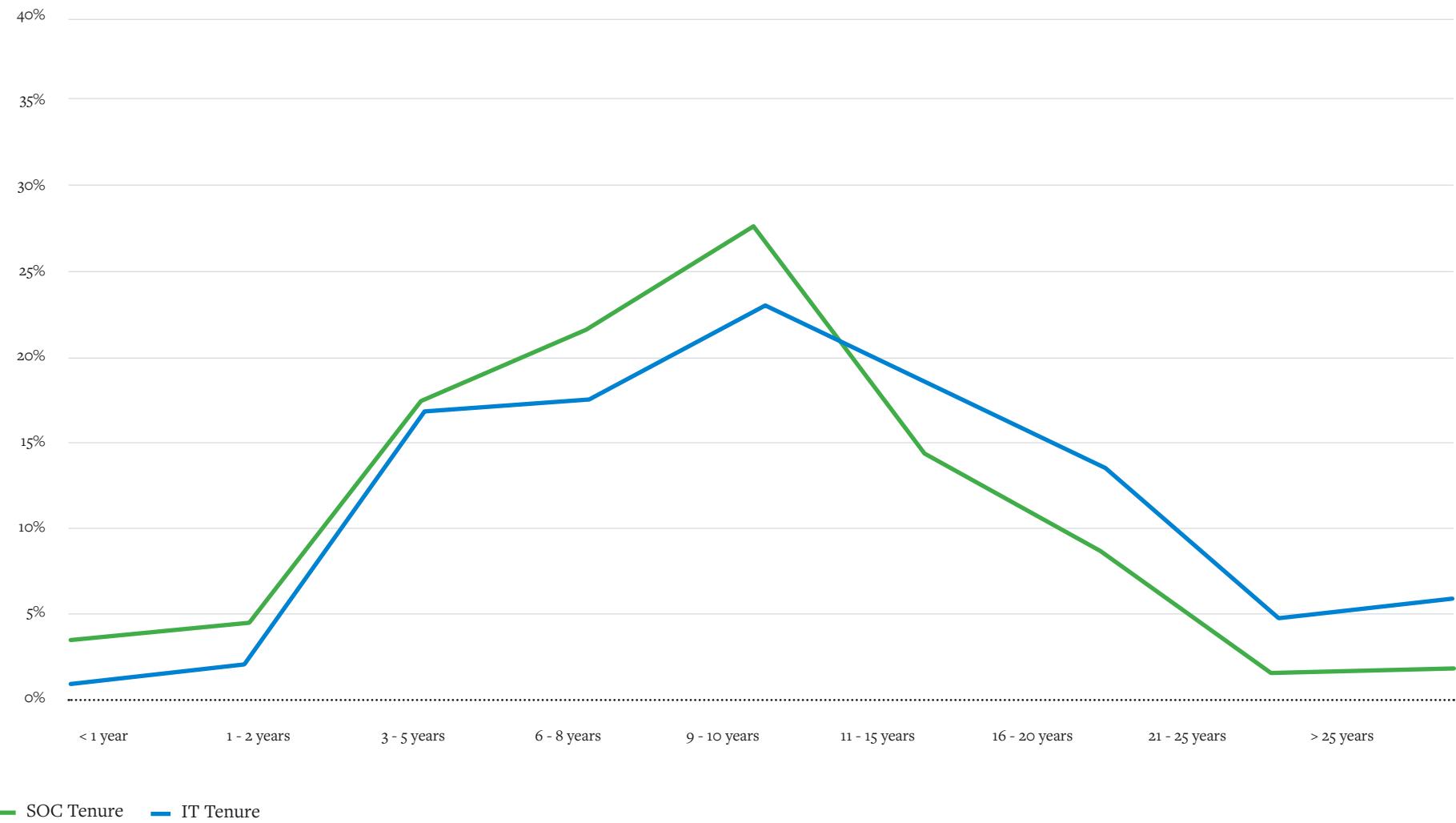
SOC EMPLOYEE INDUSTRIES

Industry	2018	2019
Finance and insurance	19%	17%
Information services and data processing	15%	19%
Other manufacturing	11%	9%
Health care and social assistance	7%	9%
Retail	7%	7%
Construction	5%	3%
Transportation and warehousing	5%	5%
Scientific or technical services	4%	5%
Computer and electronics manufacturing	3%	1%
Government and public administration	3%	2%
Software	3%	3%
Telecommunications	3%	5%
College, university, and adult education	2%	1%
Utilities	2%	
Wholesale	2%	1%
Hotel and food services	1%	
Military	1%	
Primary/secondary (K-12) education	1%	1%
Other education industry	1%	1%

● 2018 ● 2019

## SOC OPERATIONAL HISTORIES

Most SOCs have operated between 3 and 10 years.

LENGTH OF TIME HAVING AN SOC – 2018 | 2019

	2018	2019
Less than 1 year	1%	5%
1 - 2 years	5%	5%
3 - 5 years	34%	35%
6 - 10 years	31%	35%
More than 10 years	27%	17%

● 2018   ● 2019
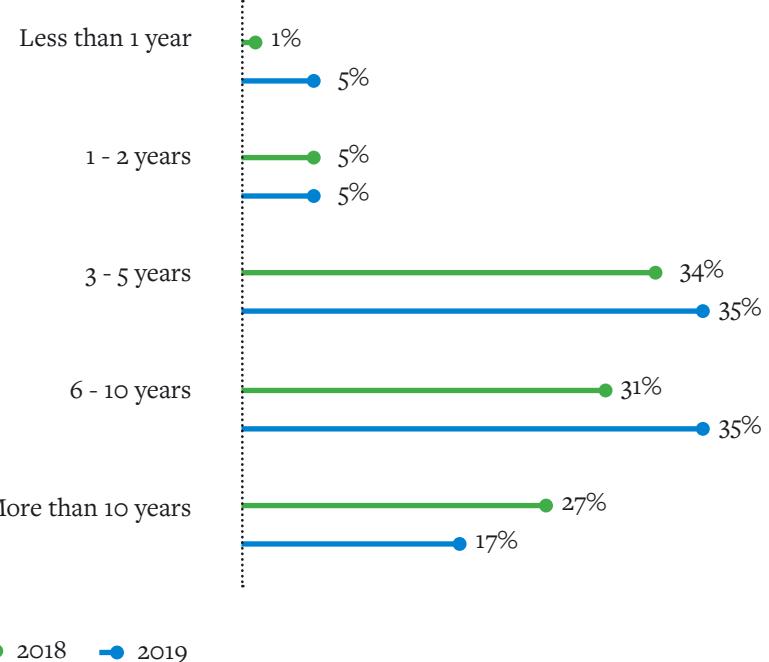
exabeam

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