SANS

A SANS Survey

Closing the Critical Skills Gap for Modern and Effective Security Operations Centers (SOCs)

Written by **John Pescatore** and **Barbara Filkins**

Sponsored by:
ExtraHop

July 2020

Analyst Program

Executive Summary

The SANS survey "Closing the Critical Skills Gap for Modern and Effective Security Operations Centers (SOCs)" was launched just two days before the World Health Organization declared COVID-19 to be a pandemic. As we know now, the pandemic has caused vast economic and political upheaval and uncertainty. The forward-looking survey results reflect this uncertainty—more security managers were uncertain about their hiring plans (40%) than planning to hire (34%). With large numbers of businesses completely shut down and others going to 100% work-from-home environments, most hiring plans are either on hold or on an emergency-only basis.

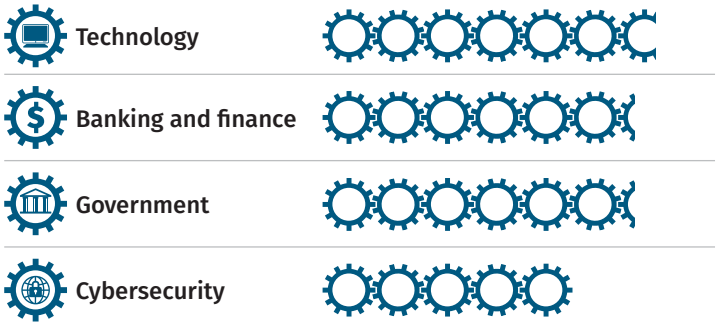
However, the survey included many questions about staff changes in 2019, qualitative responses on what skills security managers see they need, which needs they plan to staff internally and where they plan to use external service providers.

The key takeaways from the survey include:

- Other than at very small businesses and in the government vertical, turnover and attrition rates for cybersecurity staff are at or below industry averages.
- The majority of respondents plan to maintain or increase their use of external service providers, particularly for penetration testing, incident response, threat intelligence and digital forensics.
- Even though attrition is below industry averages, security managers tend to fall back on attrition as the reason for requesting staff increases. This reflects a lack of meaningful cybersecurity metrics at many organizations.
- Security operational skills were cited as most needed. Cloud security skills were rated as a higher need than network or endpoint security skills.
- The most successful source for new cybersecurity employees was the company's existing internal IT staff.
- Hiring managers would like to see new hires have more experience using the most common cybersecurity products, especially open source tools.

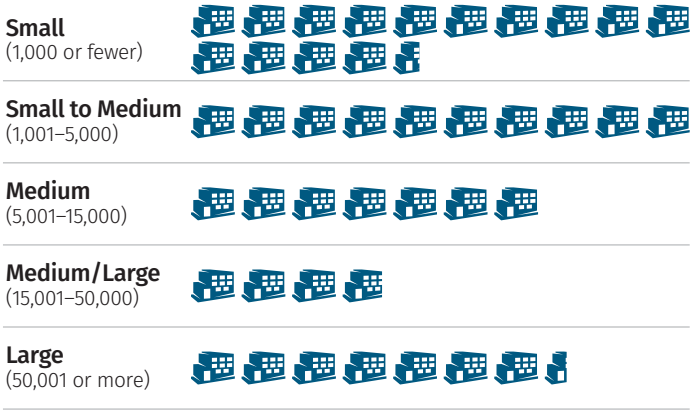
Figure 1 on the next page provides a snapshot of the demographics for the respondents to this survey.

Top 4 Industries Represented



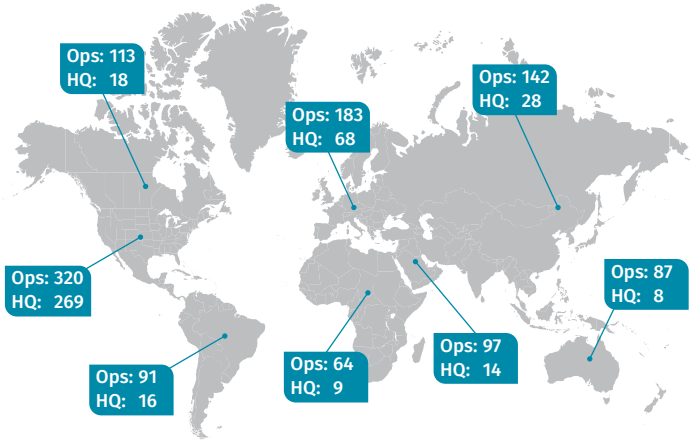
Each gear represents 10 respondents.

Organizational Size

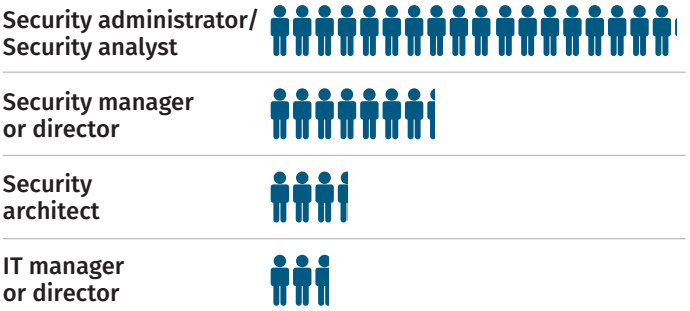


Each building represents 10 respondents.

Operations and Headquarters



Top 4 Roles Represented



Each person represents 10 respondents.

Figure 1. Survey Demographics

Top Findings

Thirty-four percent of respondents said that their organization would be adding security staff in 2020 (see Figure 2). However, a strikingly high percentage (40%) expressed uncertainty as to whether they would be expanding their security workforce.

Data captured for this survey effectively started the week of March 9, 2020. The World Health Organization (WHO) declared the pandemic on March 11, 2020. Therefore, the results reflect security managers facing economic uncertainty while simultaneously dealing with changing security demands due to a rapid transition of their organizations to nearly a 100% work-from-home environment—including the security team. See Figure 3 on the next page.

Do you plan to add security staff in 2020 and, if so, how many?

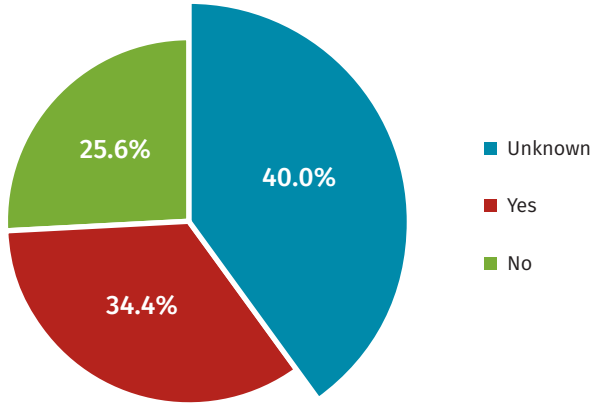


Figure 2. Security Staff Hiring Plans

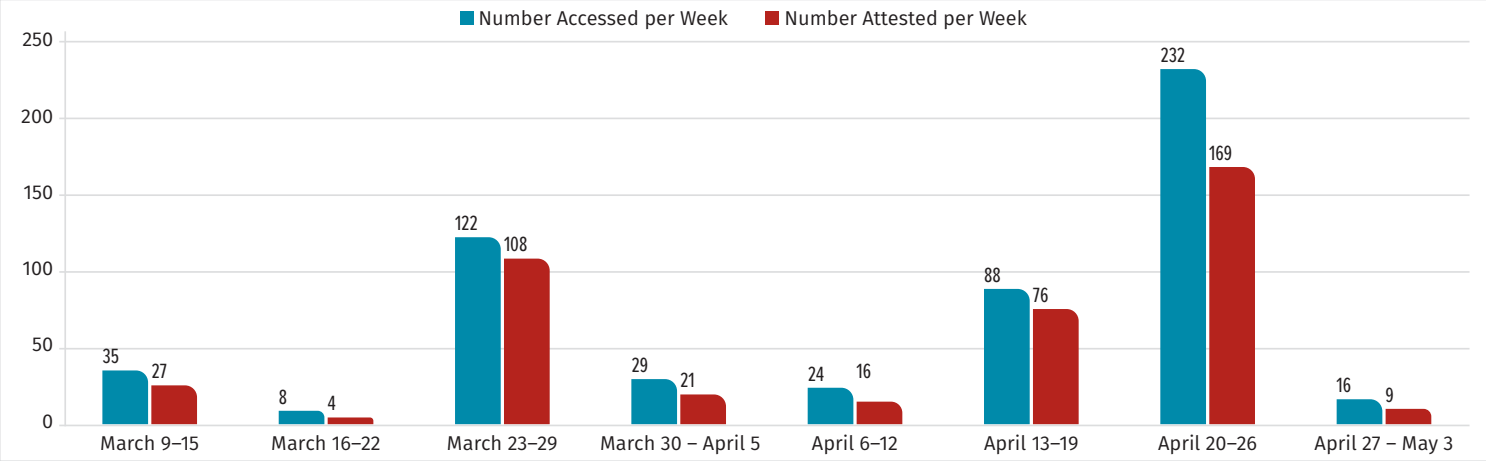


Figure 3. Weekly Survey Response Rates

The average team size—for IT and security—is shown in Table 1. This is based on a weighted average and shows a larger security staff than typical overall averages that we have seen across the SANS community. One consideration here may be that two of the verticals—technology and cybersecurity—represent service and/or product providers (which also have support services), skewing the results toward this higher security staff size.

Interestingly, of the top four verticals, government respondents indicated the highest uncertainty in the status of staff hiring in 2020, with slightly over half (52%) expressing their uncertainty in 2020 hiring.

Table 1. Average Team Size for Top 4 Verticals

	Rank	Average IT Team Size	Average Security Team Size
Technology	1	285	123
Banking and finance	2	381	199
Government	3	265	125
Cybersecurity	4	130	103

Looking at team size by size of the organization, other patterns emerge. Overall, both IT and security team sizes increase with increasing workforce, but in larger organizations, the ratio of security staff to IT staff at Medium–Large and Large companies is much higher than SANS typically sees across organizations. See Figure 4.

The most likely reason for the unusually high security-to-IT staff ratios at Medium–Large and Large companies is a high number of respondents near the edge of the data categories, which drove the weighting algorithms to overestimate. In line with typical industry averages,[1] we would expect to see ratios closer to 1 security person for every 20 to 30 IT staff.

What is your internal staffing for both your IT and security operations, expressed in terms of actual person count? *Include both employees and in-house, dedicated 1099 contractors who function as employees in your organization.*

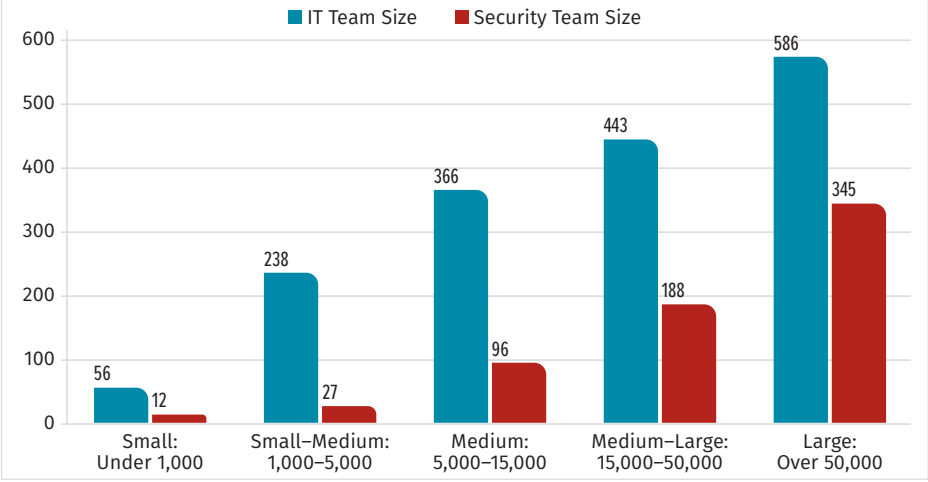


Figure 4. Average Team Size by Organization Size

[1] "IT Security Personnel Drop as a Percent of IT Staff," www.computereconomics.com/article.cfm?id=2558

SANS also analyzed staff turnover, asking respondents to estimate their turnover in internal staff during 2019. Looking at how turnover impacted staff size changes—in terms of both verticals represented and organizational size—we see that, for the most part, hiring offset staff that left, government being an exception to this.

Turnover rates across industries and company sizes varied quite a bit. At the summary level, the key takeaway is that attrition of security staff is significantly lower than industry averages in most segments. Industry averages for total annual employee turnover range from 10% to 15%, with the technology industry typically at the high end of the range at 14%.[2]

Only the government vertical exceeded that at 14%, with the cybersecurity sector close behind at 12.1%. However, contrary to the popular narrative, technology (7%) and banking/finance firms (3%) had security staff attrition rates that were well below industry averages. See Table 2.

Table 2. Staff Turnover for Top 4 Verticals

Turnover by Security Team Size (% Count)					
				Gain	
	Hired	Promoted	Left	Hired – Left	Hired – (Pro + Left)
Technology	11.3%	5.4%	6.5%	4.8%	–0.6%
Banking and finance	4.2%	3.0%	3.3%	0.9%	–2.1%
Government	8.6%	6.9%	14.0%	–5.3%	–12.3%
Cybersecurity	24.9%	19.4%	12.1%	12.9%	–6.6%

Government salaries are typically below industry salaries, and with cybersecurity skills in demand, "brain drain" in the government sector has been high for several years. The cybersecurity sector vertical is largely made up of security product firms and security consultancies that are, in general, volatile, with opportunities for skilled cybersecurity people to join startups or change jobs without having to relocate.

Looking at turnover by company size, however, provided a slightly different perspective. Small companies were near the IT industry average turnover rate with 13%; the other segments were 8% or below. See Table 3.

Table 3. Turnover Rates

Turnover by Company Size (% Count)					
				Gain	
	Hired	Promoted	Left	Hired – Left	Hired – (Pro + Left)
Small: < 1,000	25.5%	11.2%	13.1%	12.4%	1.2%
Small–Medium: 1,000–4,999	12.8%	7.9%	5.8%	7.0%	–0.9%
Medium: 5,000–14,999	17.5%	17.2%	8.4%	9.1%	–8.1%
Medium–Large: 15,000–50,000	5.1%	3.6%	2.2%	2.8%	–0.7%
Large: > 50,000	9.6%	8.5%	7.4%	2.2%	–6.3%
Average Overall	9.9%	7.8%	5.9%	4.0%	–3.8%

The bottom line is that turnover rates related to attrition in the cybersecurity industry are not above common rates for technology professionals and *in most segments are well below average*. This is good news: SANS has seen that the longevity of a staff is a leading indicator of a strong cybersecurity program, because teams that work together longer work more effectively and more efficiently. No matter how much technology is used, and no matter how well-documented security processes and playbooks are, security teamwork is needed to work across the business to avoid vulnerabilities, to quickly react to new threats and to develop new techniques and processes.

[2] "What's Driving the Tech Sector's Extreme Turnover Rate?," www.informationweek.com/strategic-cio/team-building-and-staffing/whats-driving-the-tech-sectors-extreme-turnover-rate/a/d-id/1334920#:~:text=Today%2C%20tech%20has%20the%20highest,business%2C%20no%20matter%20the%20size

Organizations should have a goal of minimizing security team turnover, and (again, contrary to popular myth) constantly increasing salaries isn't usually the most effective approach. The common factors SANS has seen in security teams with high time together at a company include:

- A well-defined career path to avoid "alert burnout" and demonstrate advancement
- Sufficient funding for training and skills enhancement
- Opportunities to play with and develop new security tools and techniques

On average, 34% of respondents reported they would be hiring in 2020, although the uncertainty factor varied. Not surprisingly, large organizations had the greatest uncertainty about hiring staff in 2020, with close to 56% of respondents from large organizations indicating uncertainty. On the other hand, respondents from small organizations were much more certain as to their organization's hiring practices in 2020—only 29% expressed uncertainty as to their organization's direction.

Promotion Matters

Realistically, staff promotion also should be considered when reviewing the net staff turnover. The promotion of junior staff to fill senior positions vacated by staff leaving means that the junior positions still need to be filled. When this is considered, almost all organizations see either no gain or a slightly negative gain—meaning organizations need to prioritize hiring or adopt services and technology to make their workforce smarter with fewer internal resources.

Not surprisingly, small organizations see the least impact when promotions and staff leaving are considered together. Small companies tend to be attractive to security professionals, especially those involved in state-of-the-art practice technology and cybersecurity; they also tend to be more fluid in their hiring practices.

External Service Use Will Grow—Focus Is on Penetration Testing Services

Organizations often use external consultancies or managed service providers to augment their own staff. These services run the gamut from retainers for incident response to one-time projects, such as penetration testing or full policy audits, to real-time vulnerability and incident monitoring. Typically, organizations outsource more external threat–facing roles (incident response, penetration testing, threat intelligence, etc.) than inward-facing roles (policy, architecture, data monitoring), because the latter requires more detailed knowledge of business operations.

Excluding the 19% who weren't sure, nearly 64% of the remaining respondents are currently using some form of external service provider. Of these, 24% plan to maintain the current level of services, 22% plan on increasing usage, and less than 7% plan to decrease their use. This indicates strong growth in demand for managed services. See Figure 5.

What are your plans for using managed security service providers (MSSPs) or independent consultants to augment your internal staff and capabilities?
Select the most appropriate answer.

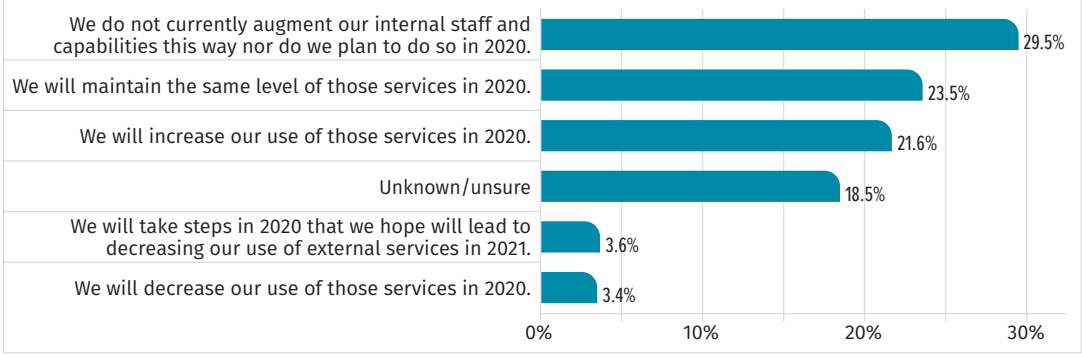


Figure 5. Plans for External Service Provider Usage

There are a variety of reasons why organizations decide to use external services:

- Inability to attract and hire needed skills
- Management headcount limits or hiring freezes, especially during times of economic uncertainty
- Filling what are considered to be intermittent or unpredictable needs or surge staffing requiring deep and narrow skills, such as incident response and forensics and penetration testing

Respondents' plans for specific external services use matches the rationale detailed previously. The top four services to be acquired required deep external threat knowledge:

- Penetration testing (34%)
- Incident response (32%)
- Threat intelligence (29%)
- Forensics (26%)

The services least likely to be outsourced are the ones requiring deeper internal knowledge: compliance and policy (16%) and architecture and engineering (13%).

Security hygiene and operations fell in between those extremes at 22%. SOC analysts and cyberdefense operations personnel generally require a balance of skills that includes a strong working knowledge of threats and a deep knowledge of the internal workings of corporate networks and servers. Organizations will often use managed service providers for first-line monitoring of perimeter alerts, while using staff for maintaining and operating internal security controls. See Figure 6.

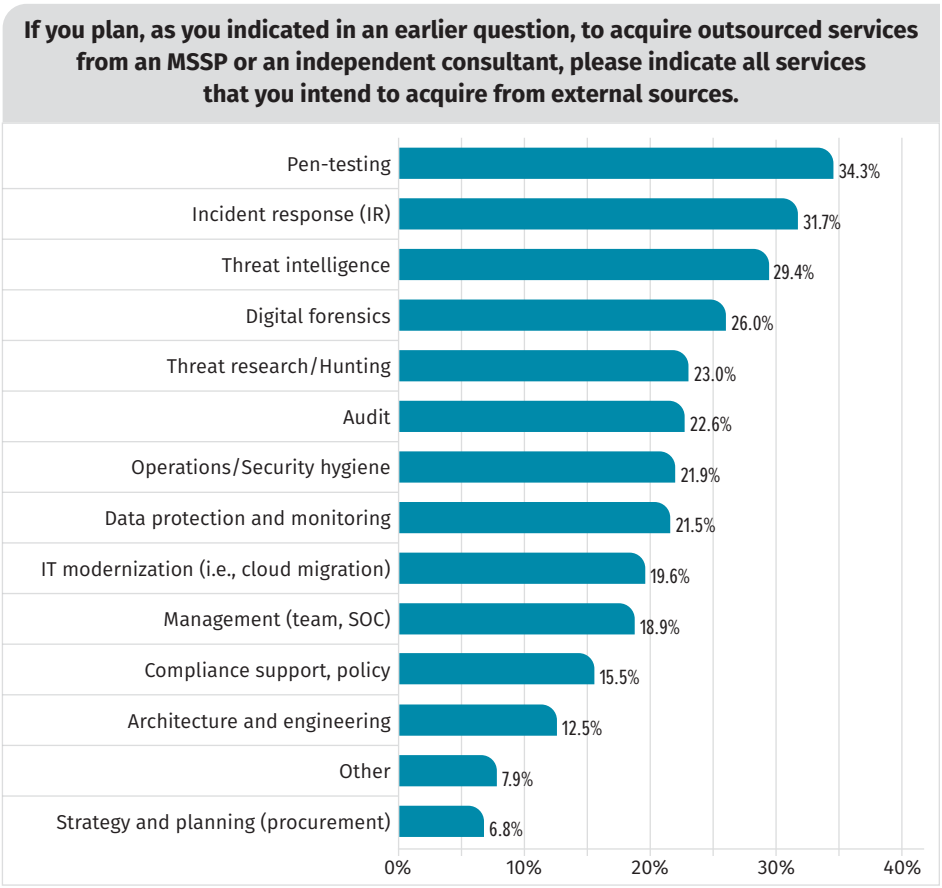


Figure 6. Services Acquired from External Sources

What Influences Hiring (People/Process/Technology)

Justifying a new hire in any company or agency can be a complex process. In some areas, well-understood metrics exist—so many millions of dollars in sales per account executive, source lines of code per day per programmer, teacher-to-student ratios, and so forth. However, SANS surveys consistently show that fewer than half of security organizations collect metrics that would allow them to justify resource needs.[3]

[3] "Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey," www.sans.org/reading-room/whitepapers/analyst/common-practices-security-operations-centers-results-2019-soc-survey-39060, p. 17, Figure 20 [Registration required.]

Without metrics, organizations often fall back on attrition or turnover replacement ("We had 20 people, lost 2, we need to hire 2 more") as justification. The actual turnover rates reported earlier in this report are below industry averages, yet replacing for attrition was cited by survey respondents as the top driver. This indicates the lack of metrics effect.[4]

The second most popular hiring motivation, "hiring to reduce workload on existing staff," also requires data and metrics to justify. When management hears, "My employees are overworked," their two questions are usually, "How can you tell?" and, "Is there no other way than hiring more employees?" The answer to the first question requires metrics such as events closed per analyst per shift, time to detect, time to respond, time to restore, and so on.

There are also many options for enabling existing staff to meet demands. Security organizations that have been able to convince IT operations to use secure server configurations, limit administrative privileges and patch faster generally can maintain higher levels of security with smaller security staffs. Investing in training for security staff can provide a double benefit by directly making staff more productive, but also giving them the skills to use advanced tools and techniques such as Security Orchestration, Automation and Response (SOAR) and machine learning.

Hiring to obtain skills was the third most frequently cited motivation. One common pushback against security training is a belief that employees will get trained and then leave the company for a higher paying job. However, the below-average attrition rates disprove this, and SANS' qualitative interviews with SOC managers tend to show that the highest skilled teams stay at their companies the longest.

We also asked who in the management chain has the authority to hire. Organizational size, however, shows a battleground between the CISO and CIO in terms of hiring security staff. A large number of respondents cited HR as a major player in the execution of hiring plans. However, HR—especially in large corporations—is responsible for making sure that an offer is presented in accordance with the law, as well as making sure that candidates are qualified and so forth. Responsibility for approving the hire, however, appears to lie with either the CIO or CISO, as shown in Table 4.

Table 4. Hiring Authority

	Organization Size				
	Small: < 1,000	Small–Medium: 1,000–5,000	Medium: 5,001–15,000	Medium–Large: 15,001–50,000	Large: > 50,000
My manager who is not the CIO or CISO	8.1%	5.8%	5.6%	2.6%	4.2%
CISO	6.3%	7.9%	7.2%	4.4%	6.3%
CIO	5.8%	8.6%	7.7%	2.8%	4.2%
COO	3.3%	1.6%	0.5%	0.2%	1.2%
HR manager	7.0%	6.5%	4.7%	2.1%	4.9%
CEO	10.2%	4.4%	1.4%	0.9%	1.4%
Board of directors or equivalent	6.0%	4.9%	2.1%	1.2%	2.8%
Other	4.0%	1.6%	0.7%	0.7%	0.2%

[4] HR Metrics: How and Why to Calculate Employee Turnover Rate?," www.talentlyft.com/en/blog/article/242/hr-metrics-how-and-why-to-calculate-employee-turnover-rate#:~:text=According%20to%20the%20U.S.%20Bureau,above%20the%20average%20turnover%20rates

In small organizations, the role of the CIO/CISO may be subsumed by the CEO or another member of the C-suite, especially if the organization is service (MSSP) or product (technology) focused. So, it is not surprising the survey results show that the CEO retains approval authority for security staff in small companies.

What is interesting, however, is the transition from CIO to CISO as companies increase in size, with the CISO seeing increasing authority in larger organizations (e.g., with a workforce of more than 15,000).

When it comes to hiring, it's who you know that matters. The two leading, most successful sources for finding potential new hires were existing employees in the IT organization, followed by referrals for new staff from existing employees. At the bottom of the heap was job fairs. These trends appear universal, connected to neither industry nor organizational size. See Table 5.

Table 5. Ranking of Hiring Sources
(3 = Most successful, 1 = Least successful)

Hiring Source	Rank
Existing employees in our IT organization	2.0
Referrals for new staff from existing employees	1.8
Online job boards	1.5
Commercial placement/Headhunter companies	1.5
Intern programs	1.4
Existing employees in other areas of our company	1.4
College recruiting	1.2
Job fairs	0.8

The Criticality of the Cloud

When asked about the most critical infrastructure areas for skills, 45% of respondents pointed to overall security operational skills, and 41% selected a central element of all SOCs, the SIEM product. Significantly, the next highest rated area was the cloud, coming in just ahead of network and endpoint. This data point rings true with the demand for cloud security "up-skilling" that SANS sees from enterprises and government agencies. The basics of security still apply for cloud-based systems, but the way security controls are architected, deployed and managed requires new skills. Moving systems to the cloud without investing in cloud security skills can lead to large gaps in security coverage.

Tools and Technologies

Like most organizations, security teams tend to have a pyramid-like structure: large numbers of lower-skilled analysts performing more routine functions, with smaller numbers of higher-skilled security analysts and engineers. Bringing in an entry-level analyst often requires disruptive on-the-job training, because a more experienced security engineer spends time showing the new employee how things work and how to use the various security tools and technologies. This places a premium on entry-level hires that are already familiar with the products in use.

In the survey, the hiring managers cited familiarity with network detection and response (NDR) and endpoint detection and response (EDR) technologies as their top need, closely followed by SIEM technology. The lowest-ranked areas were AI/machine learning, playbooks, system management and SOAR technologies. This represents a recognition that entry-level employees will likely not be skilled enough to use those complex technologies as opposed to the technologies not being useful.

We also asked respondents to tell us what specific tools they would like entry-level new hires to be familiar with on day one. (See Table 6.) The only commercial security product cited was Splunk for SIEM use. The other top products were all open source products or available as both proprietary and open source versions. Qualitative interviews conducted as part of the 2019 SANS SOC survey showed that security operations groups with the highest use of open source tools had the lowest rates of attrition.[5] The belief was that the internal time and effort spent on maintaining those tools both kept SOC staff up to date on threats, tactics and techniques and increased their job satisfaction compared with simply monitoring commercial products. The question asked specifically about tools, which likely caused the Mitre ATT&CK framework and YARA rules not to be mentioned at all—both are commonly in use by security operations teams.

Table 6. Top Products for Entry-Level New Hires

Product	Open Source/Commercial	Category
Wireshark	Open source	Monitor/analyze
Splunk	Commercial	SIEM
Nessus	Open source/commercial	Vulnerability assessment
NMAP	Open source	Discovery
MetaSploit	Open source/commercial	Penetration test
PowerShell	Internal	OS tools
BURPSuite	Open source/commercial	Application security testing
Python	Open source	Scripting
Volatility	Open source	Forensics
SNORT	Open source/commercial	IDS
TCPDUMP	Internal	Internal
ELK Stack	Open source/commercial	SIEM

Conclusions and Advice

> **"Uncertainty is the only certainty there is, and knowing how to live with insecurity is the only security."**
>
> —John Allen Paulos[6]

The global impact of the COVID-19 pandemic means that any forward-looking projections include a large "cone of uncertainty." However, we know some form of normal will emerge, and SANS' long history with cybersecurity managers and teams across decades of technology or conflict-driven changes have shown there are some constants:

- The most efficient and effective security teams are the ones that stay together the longest. Investment in skills advancement and security tools is a key driver of low attrition rates.
- Business-relevant security metrics are needed to justify investments in cybersecurity people, processes and technology.
- Basic security hygiene is always a foundational requirement. The staffing, skills and tools for continuous visibility into vulnerabilities and threats will always be in demand.
- New technologies drive new needs for basic security hygiene skills—business use of the cloud is driving requirements now.
- "Force multiplier" tools that enable security staff to rapidly identify and focus on high-risk/high-business-impact areas are key to both effectiveness *and* efficiency.

[5] "Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey," www.sans.org/reading-room/whitepapers/analyst/common-practices-security-operations-centers-results-2019-soc-survey-39060 [Registration required.]

[6] www.goodreads.com/quotes/504787-uncertainty-is-the-only-certainty-there-is-and-knowing-how

As businesses reopen and hiring resumes, this survey pointed out that the top two success factors hiring managers quoted were:

- **Using your company's internal IT staff as the starting point—**Detailed knowledge of the company's IT systems and business environment reduces the time for new hires to get up to speed.
- **Highly weighting candidates' experience with security products and open source tools—**Hiring managers need new hires who can sit down at SIEM and visibility product consoles, work with threat intelligence feeds, and take advantage of automation and integration tools to reduce time to detect, respond and restore.

About the Authors

John Pescatore joined SANS as director of emerging security trends in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and "the occasional ballistic armor installation." John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

Barbara Filkins, SANS Analyst Program Research Director, holds several SANS certifications, including the GSEC, GCIH, GCPM, GLEG and GICSP, the CISSP, and an MS in information security management from the SANS Technology Institute. She has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, plus the legal aspects of enforcing information security in today's mobile and cloud environments, particularly in the health and human services industry, with clients ranging from federal agencies to municipalities and commercial businesses.

Sponsor

SANS would like to thank this paper's sponsor:

ExtraHop
Rise Above the Noise.