LIFE AS A SECURITY ENGINEER IN 2021

www.panther.com

panther

A word from our CEO

The position of security engineer has become a pivotal role for modern security teams. These critical practitioners are responsible for testing and screening security software and monitoring networks and systems for threats or intrusions. They analyze troves of security-related data to detect and remediate threats as early as possible in the cyber kill chain. From their vantage point, they are often best positioned to evaluate security monitoring solutions and recommend security operations improvement to management.

Given that I started my career as a security engineer, I wanted to shed more light on what it is like to be a security engineer and the importance of this role. So, as we have done with other security topics, issues, and problems, we decided to ask security engineers what it's like to be a security engineer on a modern security team.

With this survey, we looked at why security engineers chose their profession, what they do on a daily basis, what challenges they face, and a host of other aspects of their work lives. Our goal is to share what makes security engineers tick and what, quite frankly, unravels them.

JACK NAGLIERI
CEO & Founder, Panther Labs

Here are some of the top insights we gained about security engineers through this survey. We take a deeper dive into each of these findings in the body of this report.

80% of engineers feel some level of burnout. Employee burnout should always be a concern for company leadership, and this finding is even more crucial to address given the pivotal role security engineers face in protecting their organizations.

Satisfaction around tools is low. Given the amount of money organizations spend on security tools, this data point may surprise management. However, the complexity and scale of data that security engineers need to analyze has exploded in recent years, putting a strain on the tools they use, and security engineers themselves.

Broad focus areas. Engineers are often familiar with a broad spectrum of security principles, best practices, and tools across several different areas of the discipline. These high-value skills undoubtedly add to their worth in the labor market.

Many are on their way out. Two-thirds of security engineers claim they plan to leave their current employer within the next 12 months. Given the importance of this role and competitive market for this skill set, organizations would be wise to get ahead of this and understand what they can do to retain these professionals.

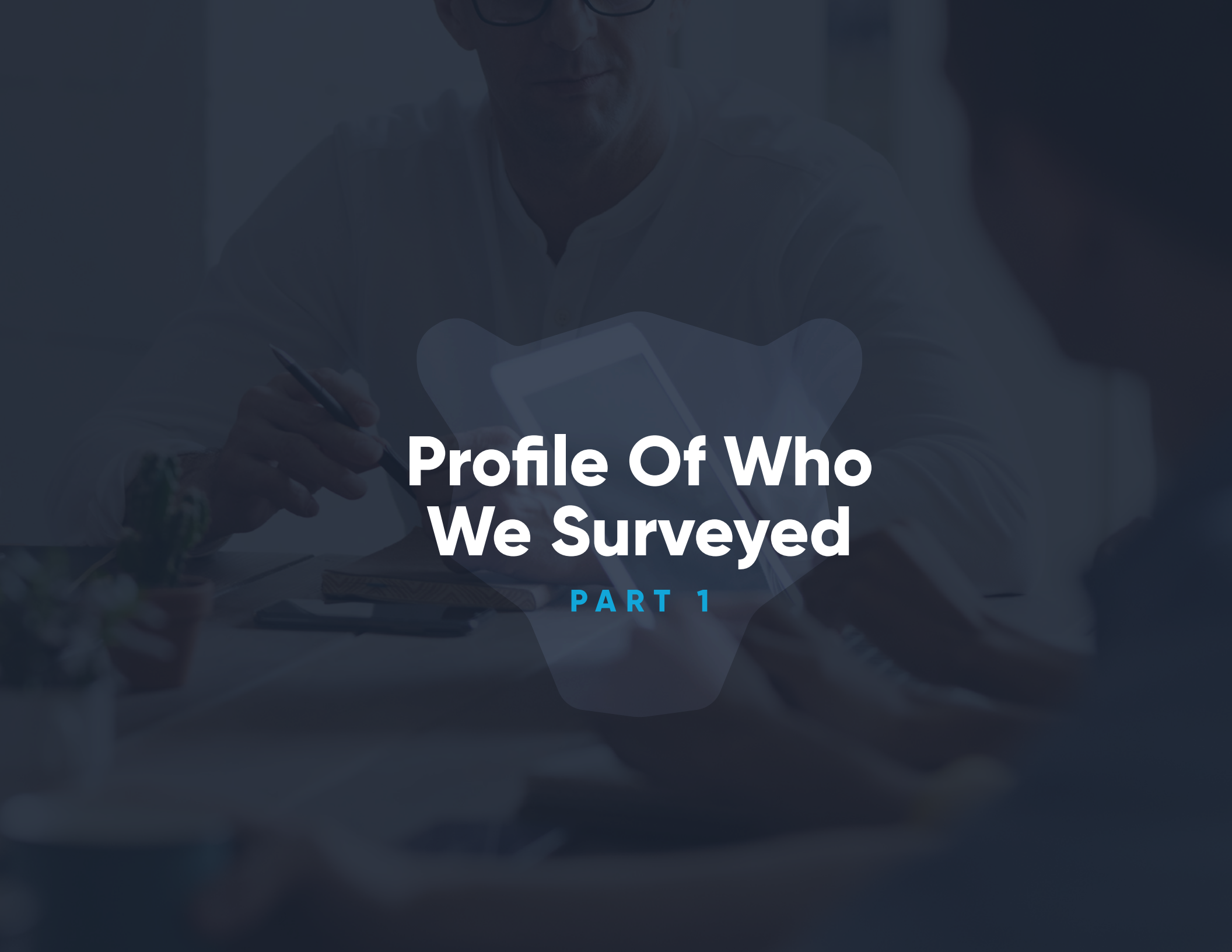
Unhappy with their pay. The largest group of those who plan to leave their current employer will do so because they feel underpaid. So, company leaders could focus here as one immediate step to mitigate the risk of losing these highly skilled individuals.

Scripting is an essential skill. Respondents ranked scripting skills and the ability to write software the highest in importance. This speaks to the convergence of software development and security operations and the frequent need for security engineers to write code to automate tasks and fill gaps in their technology stack.

Table of Contents

Methodology

On September 10, 2021, we surveyed 309 security engineers that currently work in IT security. The survey was conducted online via PollFish using organic sampling through Random Device Engagement (RDE). To access the raw data, click here. Learn more about the Pollfish methodology here.



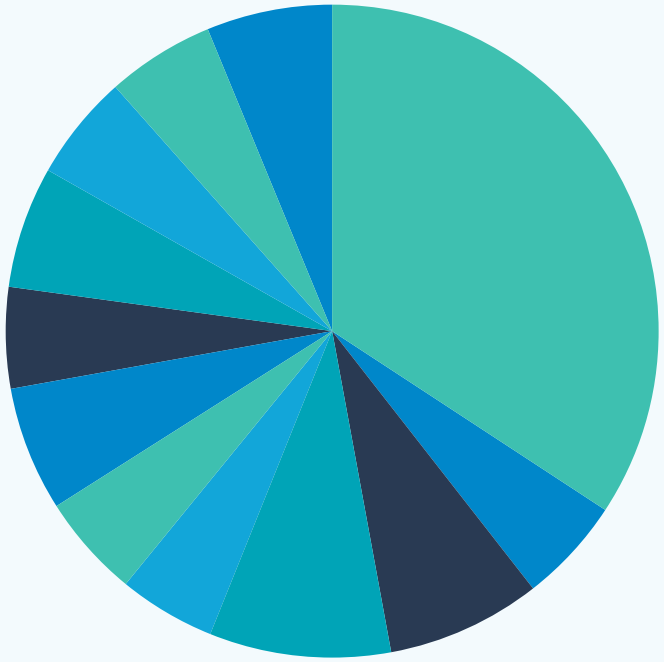
Profile Of Who We Surveyed

PART 1

Because the purpose of this survey was to learn more about security engineers specifically, rather than a broader segment of the security industry, we limited our query to only those individuals actively working in that role. By far the largest group, 34.3%, work for companies they describe as being in the technology industry, and 31.4% of the respondents work for medium-sized businesses.

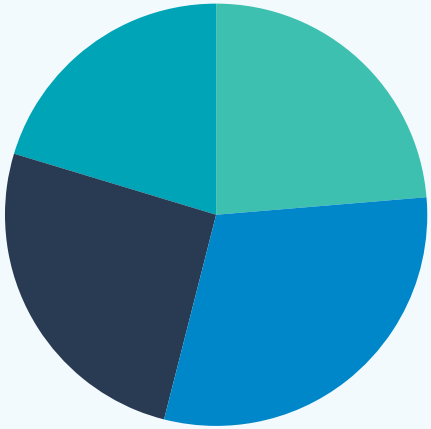
If we were to build a baseline profile of the typical respondent for this survey, it would be a security engineer who has worked for about seven years at a medium-sized, cloud-native technology company.

What Industry Does Your Company Operate In?



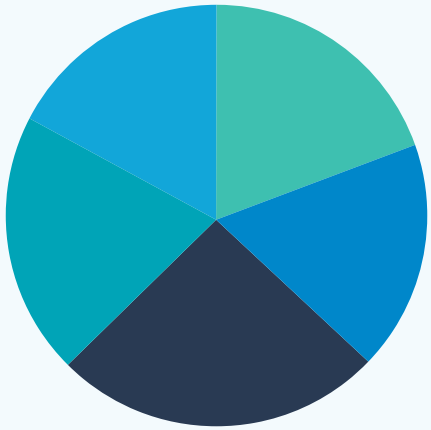
INDUSTRY	%	COUNT
Technology	34.30%	106
Finance	4.85%	15
Insurance	8.09%	25
Healthcare	8.74%	27
Utilities/Energy	5.18%	16
Federal	4.85%	15
State/Local Gov.	6.15%	19
Education	5.18%	16
Manufacturing	5.83%	18
Services	5.18%	16
Retail	5.50%	17
Other	6.15%	19

What Best Describes The Size Of The Company You Work For?



BUSINESS SIZE Number of Employees	%	COUNT
Small (1-100)	23.95%	74
Medium (100-999)	31.39%	97
Large (1,000-10,000)	26.54%	82
Major Corp. (10,000+)	18.12%	56

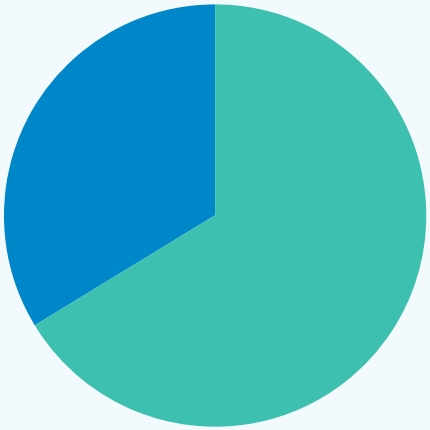
How Long Have You Been Employed As A Security Engineer At Your Current Position?



TIMEFRAME	%	COUNT
Less than a year	20.06%	62
1-3 years	16.50%	51
4-10 years	29.13%	90
11-20 years	19.74%	61
20+ years	14.56%	45

Would you describe the copany you work for as a cloud-native organization?

The company has only ever existed within the cloud from its inception - not a company with a cloud-first strategy.



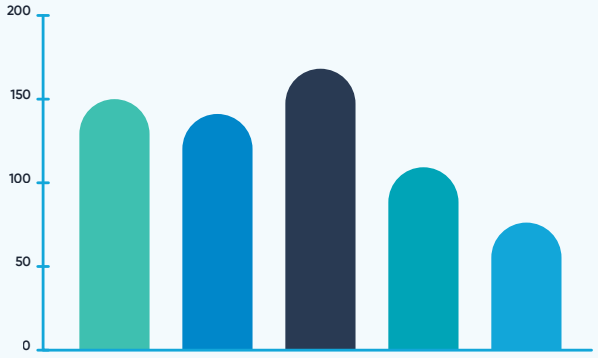
ANSWERS	%	COUNT
Yes	69.58%	215
No	30.42%	94

The majority of security engineers have earned a master's degree.

If our survey represents the industry at large, and we designed it to do just that, it suggests that most security engineers (56%) earned a master's degree before obtaining that role. Professional security certifications (49.2%) are also common among those in this segment of security practitioners.

So, as we continue to build upon the profile of the typical security engineer, we can add that they tend to be well-educated, both from the perspective of university-level studies and more specific knowledge based on industry certifications.

Before Getting Your Job As A Security Engineer, What Type Of Education Did Your Receive?



EDUCATION	R%	%	COUNT
Certifications (ex. SANS)	49.19%	23.14%	152
Undergraduate Degree	46.28%	21.77%	143
Masters Degree	55.99%	26.33%	173
Trade School	35.60%	16.74%	110
On-The Job Training	25.57%	12.02%	79

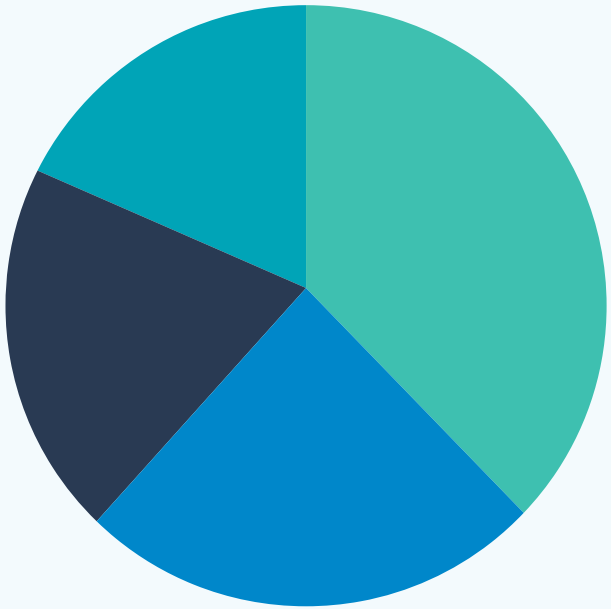
R% = Respondants Percentage

Pay and job stability are essential, but so is passion.

We asked the respondents to indicate the primary reasons they decided to pursue a career as a security engineer. The top two reasons were good pay (35%), followed by job stability (25.9%).

Passion for cybersecurity ranked third (21.7%), but only slightly behind job stability as the primary reason for becoming a security engineer. This speaks to the mission-driven nature of cybersecurity and the rewarding aspects of thwarting attacks.

If You Had To Choose One, What Is The #1st Reason You Decided To Become A Security Engineer?



REASONS	%	COUNT
Good pay	34.95%	108
Good job and stability	25.89%	80
Passion for Cyber Security	21.68%	67
Passion for Software Engineering	17.48%	57

Experience Working As A Security Engineer

PART 2

Introduction

We crafted this portion of the survey to illuminate those aspects of working as a security engineer that practitioners find fulfilling and frustrating. We look at job satisfaction and how that may cross over into other parts of the life of a security engineer.

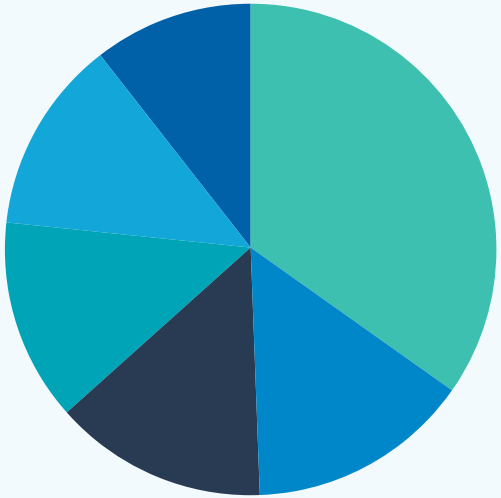
From compensation to COVID, we'll provide insights into what employers should know about why security engineers are content, happy, and productive, and in some cases, not so much.

Keeping their company secure is what they enjoy the most about their job.

When asked what they enjoy most about being a security engineer, the most popular response by far was that they derive personal satisfaction from keeping their company safe (33%). This speaks volumes about the character of these individuals, and relates back to our earlier finding that passion for cybersecurity is a key reason they pursued this career path.

The second most frequently chosen answer — learning about new technologies (16.8%) — signifies their curiosity and desire to be learning continually. Given how rapidly cybersecurity evolves, it makes sense that the people drawn to this role enjoy the challenge of learning new things.

Outside Of The Salary And Stability Benefits, What Do You Enjoy The Most About Working As A Security Engineer?

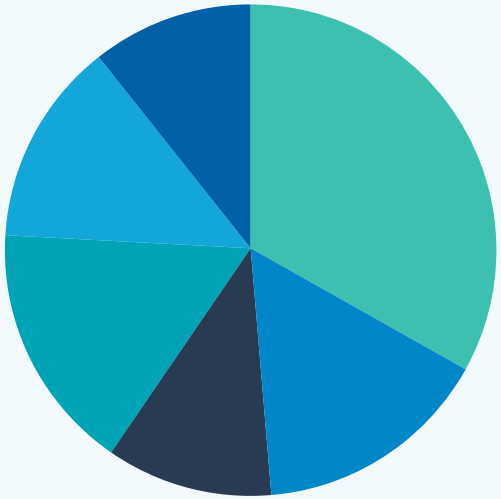


ANSWERS	%	COUNT
Keeping my company secure	33.01%	102
Learning about new technologies	16.83%	52
Tracking the evolving threat landscape	14.24%	44
Working with cloud technology	12.94%	40
Writing software to improve security	12.30%	38
Detenting and investigating breaches	10.68%	33

Keeping up with constantly changing technology is their number one challenge at work.

It is interesting to note that while many of the security engineers surveyed indicated that they enjoy learning about new technologies, many (32.7%) also indicated that "constantly changing technologies" was their biggest challenge. The explosion in cloud and SaaS applications is a good example of a fundamental shift that is driving a fast-growing and ever-changing attack surface, and new challenges for security engineers.

What Do You Find Most Challenging About Being A Security Engineer?



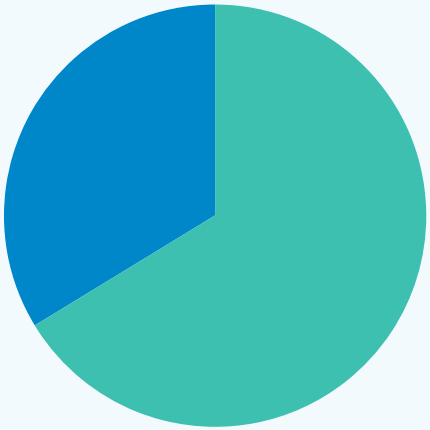
REASONS	%	COUNT
Constantly changing technologies	32.69%	101
Constantly evolving threats	15.86%	49
Collaborating with outside teams	12.62%	39
Proving security value to the organization	14.56%	45
Work/life balance	13.59%	42
Employment dissatisfaction	10.68%	33

Most feel well compensated, but we shouldn't ignore that a full third do not.

Hiring managers in the security industry often struggle to fill open roles due to the overall skills gap when it comes to security. As a result, salaries have increased for security engineers, meaning that organizations that don't (or can't) keep up with salary requirements will have trouble retaining their staff. As a result, organizations would be ill-advised to ignore the fact that a third (34%) of their security engineers feel underpaid.

But let's focus on the positive for a moment. It is a credit to the security industry that most — in fact, two-thirds (66%) — of security engineers indicated that they feel they are compensated fairly. This investment in security talent is well worth the return, given that security engineers play a crucial role in protecting their organizations' ability to operate effectively.

Do You Feel You're Compensated Fairly For The Value You Bring To Your Organization?



ANSWERS	%	COUNT
Yes	66.02%	204
No	33.98%	105

Security engineers get their information from a broad spectrum of sources.

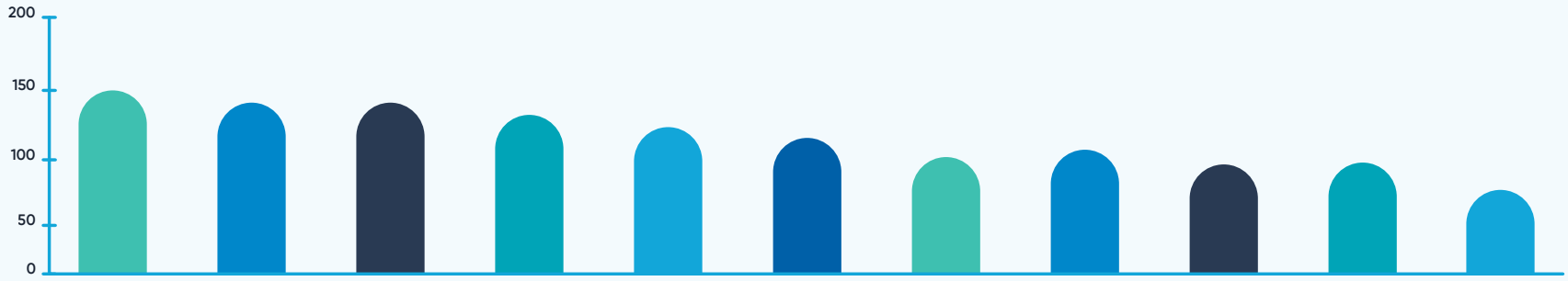
We asked security engineers what their primary source of information is for keeping their knowledge up to date. The answers paint a picture of a group of professionals who leverage a variety of information sources. Blog posts are the number one resource security engineers use for information. Many security bloggers have built their reputation over years of providing credible and useful information to the security community, and therefore have become a trusted resource.

It is telling to note that there is not much difference in the number of security engineers that use the top three answers: blog posts (49.2%), research papers (42.4%), and forums (42.4%). Social media (40.1%) also ranks high as a source of information, which is not surprising considering that social media is a good source for new and developing information — zero-day cyber threats, for example.

What's Your Primary Source Of Information You Use For Your Job?

SOURCE OF INFORMATION	%	%	COUNT
Blog posts	49.19%	12.15%	152
Research papers	42.39%	10.47%	131
Forums	42.39%	10.47%	131
Social Media (Twitter/LinkedIn)	40.13%	9.91%	124
Conference talks	38.51%	9.51%	119
Podcasts	36.25%	8.95%	112
Mentors	33.01%	8.15%	102
Friends in other companies	33.33%	8.23%	103
Certifications	31.39%	7.75%	97
Higher education	32.69%	8.07%	101
Technical documentation from vendors	25.57%	6.31%	79

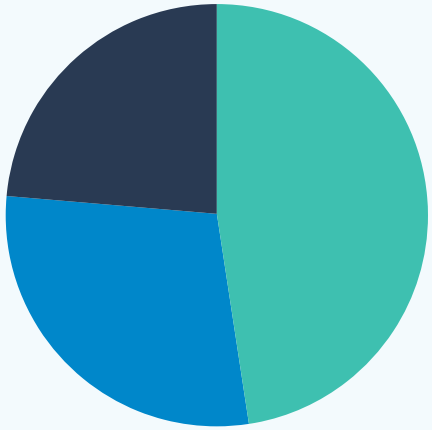
R% = Respondants Percentage



49% say COVID has made their jobs more stressful.

For many companies, the answer to keeping their employees safe during the pandemic was to have them work from home. This sudden and near-total shift to WFH caused an exponential increase in the size and shape of the attack surface for most companies. Security engineers were at the forefront of finding ways to keep their organization's networks, endpoints, and sensitive information protected, no matter where employees were working. Therefore, it comes as no surprise that 48.5% of security engineers responded that COVID has made their lives more stressful.

How Did COVID Impact Your Workload?



ANSWERS	%	COUNT
COVID made my work more stressful	48.54%	150
COVID made my work less stressful	29.13%	90
COVID did not impact my stress at work	22.33%	69

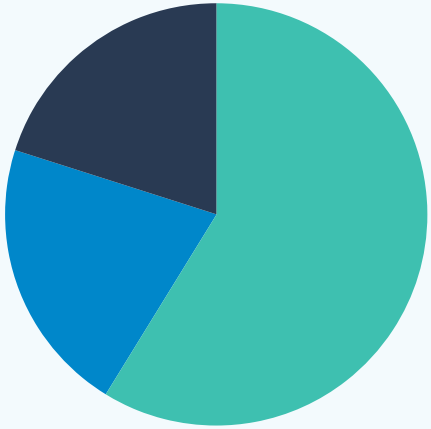
57% are very engaged, but almost half say they feel very burned out.

The ability to stay engaged in work is a key indicator of job satisfaction. When employees are unsatisfied, they find it much more difficult to stay engaged.

Because the responsibilities of security engineers are critical for protecting their organizations, it is encouraging that 57.3% indicate they are very engaged in their work.

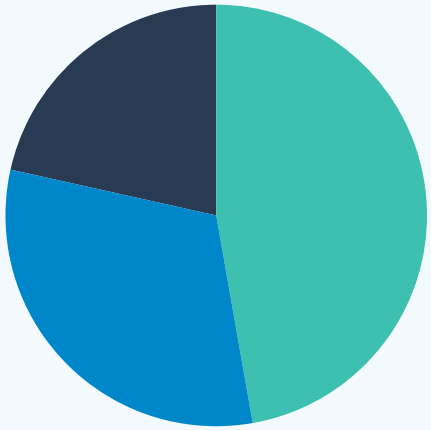
However, the survey results also show that a significant portion (48.2%) feel very burned out. Given the important (and often stressful) role played by security engineers, it is not surprising that it can take a toll in terms of burnout. Organizations need to be cognizant of this, and actively work on solutions to support employee health, retain their security staff, and prevent cumulative exhaustion from introducing risk to the organization.

How Engaged Would You Say You Are In Your Work As A Security Engineer?



ENGAGEMENT LEVEL	%	COUNT
Very engaged	57.28%	177
Somewhat engaged	22.98%	71
Not very engaged	19.74%	61

Which Of The Following Is Most Accurate?

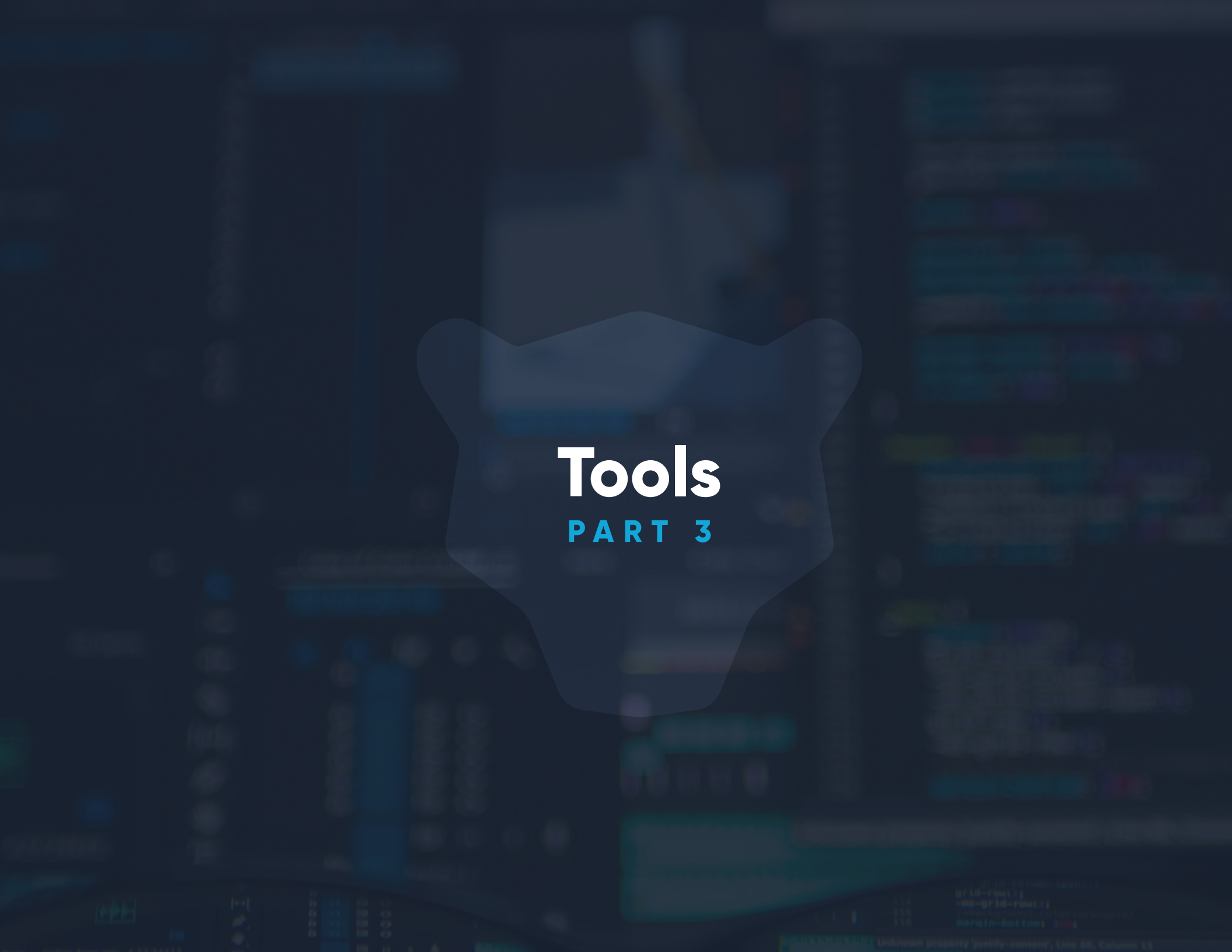


TIMEFRAME	%	COUNT
I feel very burned out at work	48.22	149
I feel somewhat burned out at work	32.04%	99
I don't feel burned out at work at all	19.74%	61

Summary

Our picture has become more apparent as we have looked deeper at what provides security engineers a sense of satisfaction at work, what they enjoy about their jobs, and what challenges they encounter. We know from their answers that they love a good challenge. They're curious and like to gather information from a wide variety of sources. And, most feel engaged in their work, however burnout is a common challenge.

Let's now pivot to look at the tools they use, how satisfied they are with their tools, and what tools they wish they had.


Tools
PART 3

Introduction

The tools security engineers have access to and how well those tools perform have a major impact on their ability to do their jobs well. In this section, we look at tools and their capabilities.

Three tools engineers are most happy with in terms of capabilities.

In order of satisfaction, the top three security tools are:

It is also interesting to note that a sizable percentage of respondents indicated that they would like to have access to these tools but do not (13.9% for CASB, 11.9% for EDR, and 11.7% for SIEMs). For organizational leaders wanting to improve their security teams' effectiveness, ensuring they have access to these three categories of tools could be an excellent place to start.

Three tools engineers are least happy with in terms of capabilities.

Our respondents were least satisfied with the capabilities of:

The fact that SIEMs and EDR show up in the top three tools that security engineers are most and least satisfied with indicates that there is a wide disparity in the capabilities of available products, and/or the requirements of different security teams vary broadly.

Please rank how you feel about the capabilities of the following tools you use in your work as a security engineer.

TOOLS	Very happy	Somewhat happy	Not happy at all	I don't use this tool or need it	I'm not provided this tool but I wish I was
SIEMs	126 40.78%	48 15.53%	47 15.21%	52 16.83%	36 11.65%
Penetration testing tools	114 36.89%	56 18.12%	45 14.56%	56 18.12%	38 12.30%
Cloud Security Posture Management (CSPM)	114 36.89%	60 19.42%	46 14.89%	42 13.59%	47 15.21%
Data Loss Prevention (DLP)	122 39.48%	64 20.71%	37 11.97%	47 15.21%	39 12.62%
Intrusion Detection System (IDS)	112 36.25%	52 16.83%	47 15.21%	44 14.24%	54 17.48%
Cloud Security Access Broker (CSAB)	132 42.72%	44 14.24%	43 13.92%	47 15.21%	43 13.92%
Web Application Firewall (WAF)	114 36.89%	53 17.15%	61 19.74%	46 14.89%	35 11.33%
Firewalls, switches, routers	121 39.16%	62 20.06%	40 12.94%	50 16.18%	36 11.65%
Static code analysis tools	105 33.98%	62 20.06%	54 17.48%	42 13.59%	46 14.89%
Dynamic code analysis tools	112 36.25%	55 17.80%	45 14.56%	57 18.45%	40 12.94%
Endpoint Detection and Response (EDR)	128 41.42%	56 18.12%	47 15.21%	41 13.27%	37 11.97%

Tool Capabilities Rating

Responsibilities

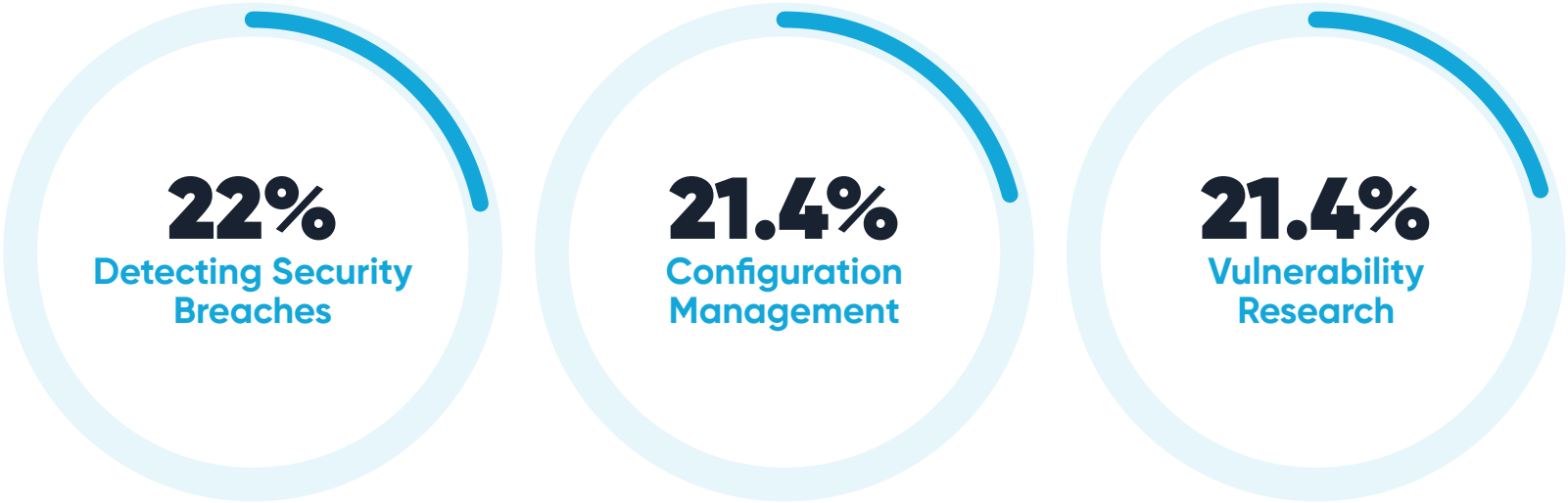
PART 4

Introduction

In the previous section, we asked security engineers about their satisfaction with specific categories of tools. In this section, we explore how well they think they can perform specific functions of their role with the tools they have.

Security engineers are very unsatisfied with three critical functions.

Over 20% of security engineers are very unsatisfied with the tools provided for each of the three responsibilities below. Challenges performing these critical functions will make it difficult for security teams to adequately protect their organizations.



The functions of testing system vulnerabilities, fielding customer security questions, and security automation all fared better in the survey results. Still, even these top three garnered significantly less than 50% of engineers that could say they were very satisfied with the tools available to them.

Please rank how you feel about your ability to do the responsibility listed below with the current tools your company provides.

RESPONSIBILITIES	Very satisfied	Somewhat satisfied	Very unsatisfied	Skip This is not my responsibility
Testing system vulnerabilities	141 45.63%	53 17.15%	62 20.06%	53 17.15%
Implementing and upgrading security controls	116 37.54%	75 24.27%	65 21.04%	53 17.15%
Detecting security breaches	122 39.48%	69 22.33%	68 22.01%	50 16.18%
Investigating security breaches	123 39.81%	65 21.04%	62 20.06%	59 19.09%
Fielding customer security questions	135 43.69%	59 19.09%	63 20.39%	52 16.83%
Configuration management	127 41.10%	57 18.45%	66 21.36%	59 19.09%
Vulnerability research	129 41.75%	65 21.04%	66 21.36%	49 15.86%
Security information	130 42.07%	62 20.06%	57 18.45%	60 19.42%

Tools Provided To Do Tasks Successfully Rating

Outlook for the Future

PART 5

Introduction

In Part 5, we look down the road to see what security engineers and their employers might expect in the next year, and the skills needed to thrive as a security engineer

67% are planning to leave their job in the next year.

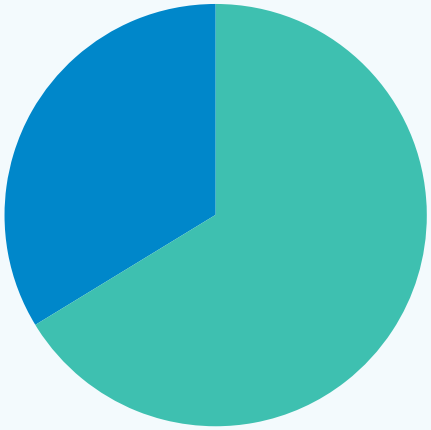
One of the most alarming findings from this survey is that the majority of security engineers (67%) indicated they plan to leave their job in the next year. There is rarely a single reason why employees plan to change workplaces. Still, unhappiness with their pay (29.5%) is the biggest reason security engineers gave, by nearly a two-to-one margin.

Dissatisfaction with their company's culture (15.9%) and how much importance their employer places on security (15.5%) are two additional reasons engineers cite as significant factors for leaving their job.

Overall, engineers take their responsibility to protect the organization they work for very seriously. Being a security engineer for a company that does not put enough emphasis on security or provide adequate support to their security teams can be very difficult.

It is also reasonable to attribute some turnover to the fact, as discovered by question 14, that 80.2% of security engineers feel at least somewhat burned out in their jobs.

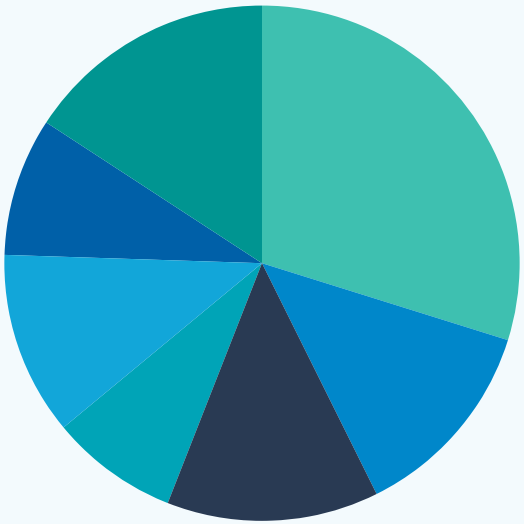
Do You Plan On Leaving Your Current Employer In The Next 12 Months?



ANSWERS	%	COUNT
Yes	66.99%	207
No	33.01%	102

If Yes, What's The Primary Reason Why?

REASONS	%	COUNT
Unhappy with pay	29.47%	61
Unhappy with culture/co-workers	15.94%	33
Unhappy with my manager/supervisor	11.11%	23
Unhappy with the tools we are provided	7.73%	16
Unhappy with my chance of being promoted	11.59%	24
Unhappy with my chance of growing/learning more in this company	8.70%	18
Unhappy with the importance they give to security overall	15.46%	32

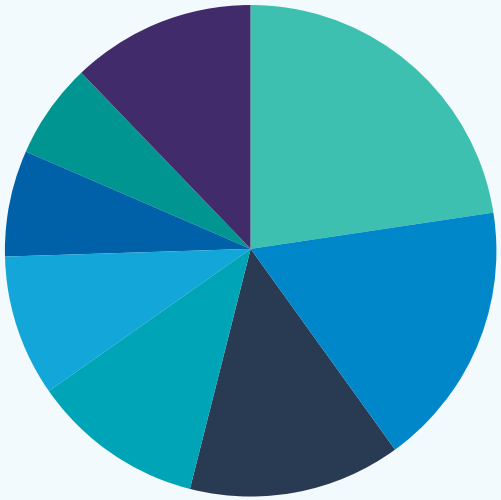


Scripting, writing software, and cloud computing are the top three skills for the future.

Looking forward from the security engineer's perspective, adding scripting to their list of skills should be a priority, as reported by 22.7%. The need to have a firm grasp on the security aspects of cloud computing is a predictable answer to a question about future skills. Still, the number one answer (scripting) and number two answer (writing software, at 17.8%) are fascinating.

This speaks to the convergence of software development and security operations and the frequent need for security engineers to write code to automate tasks and fill gaps in their technology stack.

In The Future, What Will Be The #1 Most Important Skill A Security Engineer Shoud Have?



ANSWERS	%	COUNT
Scripting	22.65%	70
Writing software	17.80%	55
Cloud computing	12.62%	39
Linux system administration/knowledge	11.33%	35
Windows system administration/knowledge	10.68%	33
Penetration testing	7.77%	24
Policy creation	7.12%	22
Technical documentation	10.03%	31

Summary

As we've seen from this section, many security engineers may choose to change jobs in the coming year, and many will continue to acquire new skills to enhance their abilities. Organizations should take steps to retain these valuable employees by recognizing the importance of security, offering competitive salaries, and providing the tools security engineers need to do their jobs well.

The Life as a Security Engineer 2021 survey results offer insights into one of the more technical roles within security teams.

We all could have guessed that COVID and the resulting work from home culture have put additional stress on security teams, yet most security engineers continue to feel engaged in their work. Burnout is certainly a risk, as is the chance of turnover, especially for organizations that don't demonstrate that they value cybersecurity. Employers can't do much to alleviate the stress caused by COVID, but they can evaluate what new tools their security teams need to do their jobs well and ensure that the company culture emphasizes the importance of security.

Experienced security engineers are in high demand, and that trend will no doubt continue in the future. Organizations would be wise to evaluate how they can best retain their security staff as this is essential to protecting their business from disruptions caused by a breach.


panther
Life As A Security
Engineer In 2021 Report
www.panther.com