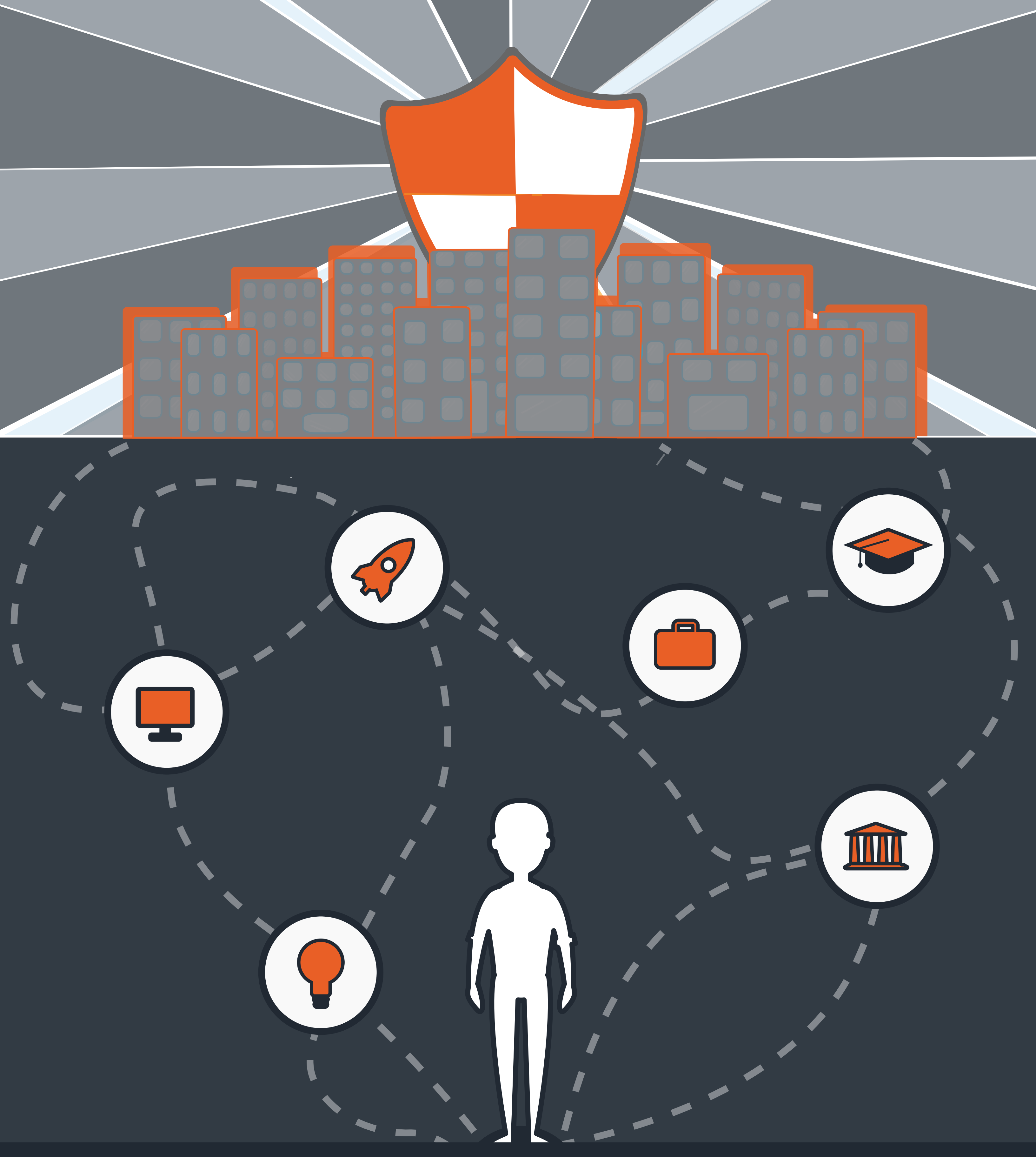

DEFINING YOUR CAREER PATH AS A SECURITY PROFESSIONAL

Table of Contents

SECURITY:
SO HOT RIGHT NOW

What You Need to Know About a Career in Security

Security is a hot field today, and with good reason.

Technology is expanding, enterprises and SMBs alike are digitizing, and security teams are tasked with protecting additionally environments, networks, and endpoints now more than ever. In fact, Cybersecurity Ventures predicts global cybersecurity spending will exceed $1 trillion from 2017 to 2021.

Accordingly, the demand for security professionals is booming. Symantec's CEO Michael Brown notes that the number of positions for cybersecurity workers is expected to grow to 6 million worldwide by 2019, with 1.5 million of those jobs going unfilled. There simply aren't enough security practitioners to go around right now.

1,000,000,000,000
SPEND IN CYBERSECURITY 2017-2021

6,000,000
GROWTH IN CYBERSECURITY WORKFORCE BY 2019

1,500,000
OF THE 6MM WILL GO UNFILLED

If you're a security professional today, then that may be good news. Being in high demand means you have **excellent job security, strong compensation, and plenty of options** if and when you're ready for a change. If you haven't settled on a career path yet or are considering a career change, these statistics are ample reason to consider security as an avenue.

Today, information technology has a major impact on every area of our culture and our individual lives. **There are security ramifications to anything that involves a computer or the internet**, so the need for security pros isn't going anywhere anytime soon.

Beyond the high demand and excellent career prospects, the best part about a career in security is that there is **no shortage of complex and interesting work**. No day is exactly the same, and if you pick the right organization—one that values human input and knows when to automate and orchestrate routine tasks—you're in for a challenging, rewarding, and exciting career.

With that said, breaking into the industry and finding a niche that suits your unique personality, skills, and interests can be challenging. So we put together this eBook that will offer you a clearer picture of what it means to build a career in security, what potential paths look like, and how to navigate some of the bumps along the way.

> *Success is loving what one does the majority of the time.*
>
> DEIDRE DIAMOND

In this eBook, we'll share with you:

- **What a career in security looks like**
- **How to follow the "typical" track**
- **How to explore more unusual avenues**

We have interviewed several seasoned security pros, who shared a good deal of wisdom and anecdotes about their time in the trenches. We'll impart their advice and offer a glimpse into how they have shaped their own careers. Alongside our own in-house security pros, these experts have "been there and done that," and they offer helpful and sage advice about how to navigate a career as a security

CAREER PATHS: ON AND OFF THE BEATEN TRACK

Overview

There's no one-size-fits-all track for a security career. Unlike, for example, becoming a doctor, the educational requirements, training, and expectations for a security professional are not always clear-cut. But that's not necessarily a bad thing. Part of what makes security so interesting is that there are many paths you can take. We think it helps to have a good understanding of what a more typical or traditional career path looks like, as well as taking a look at some of the more unusual ones.

Deidre Diamond of CyberSN notes, **“The biggest mistake I see is not doing the research on all the different jobs out there and picking a role that isn’t inspiring to the individual.”** This is why, as Scott Roberts of GitHub noted when we interviewed him, **“Broad exposure early on is a really big deal. There are a lot of niches, and you don’t want to go down a path too early and hold yourself back. There is so much variety in the world of security that there’s really no reason to do something you’re not 100 percent in love with.”** We couldn’t agree more.

Is Security Right For You?

Before we hop into what typical and atypical career paths in security may look like, we want to talk about what type of person is a good fit for the security industry.

Maybe you have a stereotype in mind of what a security professional is like—perhaps a surly, antisocial brainiac? While it’s true that certain personality types gravitate towards certain careers, the dominant stereotype of security professionals doesn’t paint a very nuanced or accurate picture.

As Scott Roberts put it, **“Anybody could get into security and find something worthwhile and a good fit. It comes down to curiosity, love of learning.”** Moreover, there’s a huge variety of roles, organizations, and paths that you can explore as a security professional. So if one particular aspect doesn’t appeal to you, it doesn’t mean it’s not the right field for you.

Scott says, **“Saying ‘I want to be in security’ is like saying ‘I want to go shopping for a car.’ That doesn’t narrow it down a lot. A Smart car is a car and a Winnebago is a car. But they are two very different things and fit different people.”**

So what does make for a successful security professional? Everyone we spoke to had pretty much the same response: curiosity and a willingness to learn. It’s also good to know that, today, security is at the center of many teams, from operations to development and beyond. Whereas it used to be a function that was “off in a corner” doing its own thing, many organizations today recognize and uphold the central role that security needs to play.

Another point to consider about the security field—and this may be a positive for some and a negative for others—is that it is a vast and quickly changing landscape. As Scott put it, **"You can get a full view of what accounting looks like, but you can never really do that for security."** If you are the type of person who really needs to understand everything, it may not be the best career. But if the idea of tackling something new every day gets you excited, security is the place to be.

Finally, it's important to realize that you don't necessarily need a degree or expensive equipment to start teaching yourself security skills. Scott says, **"If you have a $200 laptop and a $150 Amazon gift card, you could start a pretty killer security career with what's out there right now."** If security is something that appeals to you, don't let resource constraints hold you back. Start getting your hands dirty. Follow that natural curiosity and see where it leads.

> *Always strive to be the dumbest person in the room.*
>
> SCOTT ROBERTS

Sectors

If you're interested in a career in security, there are a few different directions you can go in terms of the type of organization that you work for. Below are some of the broad categories you may find yourself choosing from, with a general discussion of what it's like to work at each. While of course this can vary a great deal from organization to organization, this should give you a pretty good sense of what to expect.

Government

Governments have plenty of need for security professionals, as you surely will not be surprised to learn. **Options include working for local, state, or national governmental agencies, or being employed by a government contractor.** There is a particular need in the defense sector. The defense industry—whether in-house at an agency or at a defense contractor—can be interesting, as you'll likely be exposed to varied and sophisticated attacks. On the negative side, **you may find that there is a lot of red tape in this sector**.

Additionally, it can limit your geographical options, especially if you want to work at the federal level. Because governments are beholden to their constituents, sometimes they do not move as quickly as private enterprises, so you may find that the pace is not as fast.

However, you will often get to use some of the **latest-and-greatest, larger budget tools out there, and you could be involved in some very cutting-edge research**. These types of roles also often come with reasonable working hours and good benefits. Government work often does not pay as well as private enterprise, but the trade-offs in lifestyle and the impact you can make may well be worth it.

Startup

You could say startups are having a moment. Whether you're looking at Silicon Valley, New York, Boston, or any other city with a thriving tech scene, startups can be a great place to hone your skills as a security professional. **They often pay well**, and you may even get some equity that could turn into a big windfall later on (although don't count your chickens before they hatch!)

The downside of working for startups often comes in the form of **long hours and high expectations**. If you're interested in really immersing yourself in the world of security and **learning quickly by rolling up your sleeves and wearing many hats**, then a startup might be just the place for you. Just be prepared to be scrappy and learn to do whatever it takes to get the job done. On the other hand, if you're looking for more work-life balance, you may want to consider a later-stage startup, an established business, or go a different direction altogether.

Enterprise

There is plenty of need for security professionals at large companies. They experience high volumes of attacks, and their stakeholders are often focused on ensuring security. If you want the **high pay and exciting work** of a private sector company **without the long hours of a startup**, then enterprise might be just the place for you.

Additionally, many enterprises have their own security operations center (or SOC), and this can be the perfect place to get your feet wet. SOCs often encounter many different threats, and they require a team of people working closely together. You'll have a good opportunity to learn from those around you, get exposed to a variety of security protocols, and explore different tasks and areas that appeal to you. Especially early in your career, working at an enterprise can be a great way to get that broad range of exposure that Scott recommends.

A Typical Career Path

There's no single path that everyone must or will take when it comes to a career in security. But we can make some generalizations based on what is most common.

Education

Many security professionals start out by getting an undergrad degree in a field like **computer science, information technology, or even security**. Others start out on a math or science track and then discover an interest in security, either through extracurricular exploration or a project for a class.

You don't have to pick one of these majors, but if you know for a fact that you're interested in getting into security, they are a good bet. On the other hand, Chris Sanders of Applied Network Defense notes that cybersecurity degree programs are not always up to par these days. **"I don't recommend people go into these programs,"** says Chris. **"You're better off going into something that teaches you to think more broadly and pursuing security training on your own."** He says people should consider majoring in engineering, computer science, physics, or even English or philosophy.

That said, the majority of security professionals do have an undergraduate degree. Deidre says, **"Degrees open doors and command higher salaries."** She advises that cybersecurity or comp sci degrees are a good bet if you want to pursue a more technical role, though she notes you can also increase your qualifications through various certification courses. Just make sure you do plenty of research into the particular degree program you are looking at, its outcomes, and reputation in the larger industry.

Of course, **a completed degree isn't 100% necessary**. For example, Scott Roberts has built an impressive career after leaving college mid-way through. He tried out three schools, discovered a passion for security, and then landed a coveted internship with Symantec's SOC. Scott figured the point of school was to get him a job he wanted, and with that in his pocket, why continue? He determined that he had learned what he could in the classroom and that he'd have more opportunities to grow in a real world setting.

While leaving before you finish a degree isn't the ideal path for everyone, it may be helpful to know that, even if you don't love classroom learning, there's no reason you can't make a living as a security professional. Beyond a bachelor's degree, some folks will go on to get a master's or even a Ph.D. in a security-related field. However, this is less common, especially if you don't plan to go into a research or academic role. More typically, you will finish your undergrad degree and then look for a first job.

Entry-Level and Early Career Roles

Next up is that first job. Scott Roberts had some excellent wisdom to share with us about choosing your first few jobs. **"Get as much exposure as you can early on,"** he says. **"Later you can do a deep-dive into a particular set of skills and really specialize."** Here are some things to think about early on in your career.

Red Team vs. Blue Team

One specific criteria you may also want to start considering and exploring early in your career is whether you prefer **offensive (red team)** or **defensive (blue team**) security. Do you like to tinker with things, take them apart and put them back together? Then you might be cut out for offensive work. Does catching bad guys sound thrilling? You might be a good fit for defensive work.

It's worth noting that there are many more jobs for defense. Scott said, **"On the defensive side, you are always exposed to something new. It's like playing a game of cops and robbers, getting ahead of the bad guys and showing them they aren't as clever as they think they are."** If that's appealing to you, definitely look at defensive career paths, which will offer more opportunities while providing plenty of challenges and excitement.

Common Entry Level Titles

Entry-level roles in security can vary quite a bit, but often these include either IT admin or security analyst titles. **One common place to start is as an analyst or incident responder.** Another direction, if you have or plan to develop coding skills, is to become a security engineer. The role you choose depends on your interests and skill set. Generally, analysts and responders are given tasks that require immediate attention, such as alert handling and incident response. Security engineers, on the other hand, generally handle the "bones": security architecture and engineering matters. We'll explore both of these common roles below.

Security Analyst

Other Common Titles: Tier1 - Tier3 Analyst, Incident Responder, Incident Handler; May also come in more specific flavors like Malware Analyst or Intrusion Detection Analyst

Security analysts are, in many ways, the foot soldiers of an organization. Their job is to detect, investigate, and respond to incidents. They may also be involved in planning and implementing preventative security measures and in building disaster recovery plans. Depending on the vulnerabilities your organization faces and the nature of your security program, analysts may need to be on-call at various times to handle incidents as they arise.

Analysts may also be responsible for recommending new technologies and installing them, as well as training other team members to use them. Many organizations break security analysts out by levels or tiers, where the rank indicates the skill level (and experience) of the analyst. Higher-ranked analysts will handle escalated events or more complicated incidents that junior analysts may not be prepared for and perform proactive hunting for threats that may have escaped their alerting systems.

Security Engineer

Other Common Titles: Security Architect, SIEM Engineer, Security Device Engineer

Another potential path is the more technical route of becoming a security engineer. Depending on the size, composition, and needs of an organization, it may have a variety of engineers and/or architects on the security team. While the broadest job title is “security engineer,” there may also be people on the team who specialize in SIEM, endpoint security, and other specific areas of security engineering.

Team members in this role are responsible for building security architecture and engineering security systems, as well as working closely with DevOps teams to ensure continuity and speed of releases. They should also be able to document the requirements, procedures, and protocols of the architecture and systems they create.

> *It's easy to talk about stuff, but security is a career for people who are doing stuff.*
>
> SCOTT ROBERTS

Mid-Career Roles

As you move along in your security career, you may become more specialized, particularly if you happen upon an area that really lights your fire. In other cases, you may move into a management-focused role, where you are responsible for building and running a team of security pros. Below is the most common role for a mid-career security pro.

Security Manager

Other Common Titles: SOC Manager, Security Director, SecOps Lead

If an organization has a security operations center (SOC), this is the person who will oversee it. If the org don't have an official, traditional SOC, this person will still be in charge of directly managing the security team. This role involves creating a vision for hiring, building processes, and developing the technology stack. A security manager should have a background in and significant experience with running a security team, and should be able to provide both technical guidance and managerial oversight.

Senior Career

As they move deeper into your career, most security pros either specialize in something that they excel at (and hopefully really enjoy doing), or they will pursue more of a management and leadership track. A specialized team member might be something like a senior security infrastructure engineer, a senior incident response manager, or a high-level pentester. More common is the leadership track, which we'll describe in more detail below.

Chief Information Security Officer (CISO)

Other Common Titles: CIO, CSO, Head of Security

Whether an organization has a dedicated CISO or a general CIO, this person is responsible for defining the organization's entire security posture. The CISO (or CIO) should be the one to put together the strategy, programs, policies, and procedures to protect the organization's digital assets, from information to infrastructure and more. A CISO is sometimes responsible for compliance, as well, which may require additional strategies, programs, policies, and procedures on top of the security-related ones.

Reporting to the CEO or CIO, CISOs have direct contact with the rest of the C-suite. They represent the interests of the security team to the rest of the business. A C-level security representative should focus on clearly communicating the business case for security, and on developing a complete strategy that covers prevention, detection, and response.

A good CISO will know and understand the information and systems they're protecting. They'll know the threat landscape and be able to identify, create, and maintain policies to help mitigate risk, as well as enabling rapid response to incidents. It often takes decades to ascend to a role like this, and you will have quite a bit of responsibility and power if you decide to pursue this route.

An Atypical Career Path

Of course, as we mentioned, every career path is different—and that's a good thing! You may find yourself moving along a more typical journey, or you may find yourself taking a fork in the road to explore an interesting opportunity or chase a new passion. Below, we'll explore what some of those forks in the road might look like.

Starting Elsewhere, Moving into Security

As Deidre Diamond remarks, **"Security is such a new industry that many of us stumble upon it while doing a different job."** Plus, she notes, very few organizations are hiring entry-level security professionals today. So even if you wanted to follow the more traditional track, that could prove to be tricky, and you may be better off starting elsewhere (or wherever you happen to be today!) and making the move to security later. A common place to start is in an IT role.

Deidre says, **"Starting out by getting a job in IT is always a good path, as a lot of those in IT roles are now being held accountable to having some security knowledge."** In other words, going into IT means getting exposure to security, and while you hold that role you'll have a good opportunity to explore the field and see if you enjoy the work.

Another place to start is in a more traditional intelligence field (such as in a government agency). **Scott says he has seen a lot of folks come out of the intelligence world and successfully apply their skills to cybersecurity.** "That's a good thing," he says, "because it means they bring with them a different school of thought." The broader perspective and honed skill set can be very valuable.

Perhaps the most "underrated but powerful" role for security folks to grow from? The IT help desk, says Scott. This role gets exposure to many challenges on a daily basis—ranging from a computer crashing to an employee falling for a phishing scam. Scott says that some of the best folks he's known in security are those who started out troubleshooting.

People with experience behind the help desk are also often quite good at remembering that, in every security incident, there are human beings on both sides of the equation. If you spend your whole career in security, says Scott, it can be easy to forget this. This knowledge can help them act more empathetically, and also make better strategic decisions.

Academia and Education

Chris Sanders has had one of the most interesting and unusual career paths that we've come across. After starting his career as a sysadmin, he moved into IT security. He worked at the Department of Defense for some time before joining InGuardians and FireEye/Mandiant.

Recently, he developed an interest in cognitive psychology and how it applies to the challenges faced by security practitioners. He is currently pursuing a PhD in psychology, and has started his own security training program, Applied Network Defense. His goal is to provide information security training and education that is effective, affordable, and tailored.

Chris got into the world of academia and education after recognizing that his passion lay in studying and improving how security analysts are trained, how security tools are developed, and how investigations are conducted. His varied and complex career path is a great example of how you can pursue your own passions and, over time, hone in on what makes you happy in a professional context.

Often, in many fields, not just security, people find themselves later on in their careers wondering, "What next?" Sometimes there is burnout, and other times you just feel ready for a new challenge. When this begins to happen, it's a good idea to pursue training courses and continuing education, since this may help keep the spark alive for you or open your eyes to new ways of thinking and doing your job.

But you may also want to consider getting into education yourself, as both Chris Sanders and Scott Roberts (who teaches for SANS) have done. It may be that teaching others about the ins and outs of security is just the thing to stoke your fire.

Consulting and Contracting

For some people, working in-house for your whole career may become tiresome. Becoming a contractor or consultant has many benefits: You can:

- **Make your own hours**
- **Set your own pay scale**
- **Choose clients and projects that interest you**

This type of freedom may be appealing to folks, especially those who are in their mid-late career arc.

If you're considering getting into consulting or contracting but have a full-time job now, you might think about doing some moonlighting (just make sure it's ok and legal with your day job) to get a feel for it and make sure it is the right next step. The downside to contract work, of course, is that your income and client load can vary from month to month and year to year.

It doesn't offer the level of stability that an in-house job may. However, the good news is that, with the security talent shortage, there's never been more need for security pros, and many organizations are more than happy to bring in outside help.

> *Approach security with a sense of humility and the idea that there's always something new to learn. You never know who you're going to learn from.*
>
> SCOTT ROBERTS

The Security Career Paths Matrix

Sometimes it can be difficult to picture what a certain role entails and what it takes to get that type of job. Below, we offer a security career paths matrix that covers a variety of common positions, the responsibilities each entails, and the key skill sets required—as well as some notes on what makes each role unique and notable.

ROLE	RESPONSIBILITIES	KEY SKILL SET	WORTH NOTING
ADMINISTRATOR			
Subcategories: • Systems Administrator (Sysadmin) • Security Administrator • Network Administrator • IT Administrator	Maintain the company's IT network, servers, and/or security systems Ensure upkeep, configuration, and reliable operation of computer systems	Familiarity and fluency with computer systems, servers, and networking equipment Ability to troubleshoot and solve both common and unusual problems Detail-oriented	Sysadmins, IT admins, and network admins may start out in a more general IT-focused role and transition into security later in their careers. This role is an ideal way to get familiar with computer systems and prepare for a successful security career.
SECURITY ANALYST			
Subcategories: • Intrusion Detection Analyst • Firewall Analyst • Malware Analyst • Cyberthreat Intelligence Analyst • Cryptanalyst • Vulnerability Analyst	Maintain the company's IT network, servers, and/or security systems Ensure upkeep, configuration, and reliable operation of computer systems	Familiarity and fluency with computer systems, servers, and networking equipment Ability to troubleshoot and solve both common and unusual problems. Detail-oriented	Sysadmins, IT admins, and network admins may start out in a more general IT-focused role and transition into security later. This role is an ideal way to get familiar with computer systems and prepare for a successful security career.
INCIDENT RESPONDER			
Other titles: • CSIRT Engineer • Intrusion Analyst	Actively monitor systems and networks for intrusions Identify security flaws and vulnerabilities Address and manage the aftermath of a security breach or attack Plan proactively to defend against and mitigate future attacks.	Ability to develop a clear procedural set of responses to security incidents Ability to produce detailed incident reports and technical briefs Cool under fire and quick to respond Strong verbal and written communications	An incident responder is like a paramedic, arriving on the scene as quickly as possible in the aftermath of an attack and doing everything possible to halt progress, mitigate damage, investigate and resolve the incident, and safely return systems to normal. Ideally, this role will also spend some time focused on proactive measures and planning for future incidents.

ROLE	RESPONSIBILITIES	KEY SKILL SET	WORTH NOTING
SECURITY ENGINEER			
Other Titles: • (Information) Systems Security Engineer • Cybersecurity Engineer • Information Security Engineer • IT Security Engineer • Network Security Engineer Subcategories: • Application Security Engineer • Forensic Engineer • Reverse Engineer	Design and build secure IT systems. Develop systems that can respond robustly to disruption, particularly security incidents.	Strong development skills Comprehensive understanding of vulnerabilities and threats landscape Ability to work closely with the security team and communicate technical requirements and limitations	A security engineer is charged with analyzing computer networks, ensuring they are running securely, and trying to predict future security issues. It requires both refined development skills and a clear understanding of the threat landscape, as well as an ability to think strategically and proactively.
SECURITY RESEARCHER			
Other Titles: • Cybersecurity researcher • • Subcategories: • Malware researcher • Vulnerability researcher	Proactively research threats and vulnerabilities Track and respond to incidents in real-time Understand the who, what, when, where, and why of attacks Gather information to support security strategy and incident response	Impeccable research skills Persistence and passion for threat hunting Ability to work independently and doggedly to chase down new threats	Security researchers are always on the cutting edge, identifying and chasing down new threats and vulnerabilities. They are charged not only with conducting the research, but with producing reports for the organization and even taking follow-up measures such as gathering details for a prosecution.
PENETRATION TESTER			
	Penetration testers are charged with testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit	Detailed understanding of computer systems, servers, and networks Deep familiarity with threat vectors and cutting-edge attacks Ability to think creatively and inhabit the "bad guy's" perspective	Pentesting is a complex role that requires you to be able to put yourself in the shoes of the attacker and think outside the box, in order to identify and patch any and all soft spots before a bad guy finds them.

ROLE	RESPONSIBILITIES	KEY SKILL SET	WORTH NOTING
SECURITY AUDITOR			
	Security auditors provide an audit of security systems used by an organization They also provide detailed reports outlining whether the system runs efficiently and effectively This can help the company make changes where necessary to improve the integrity of their system	Experience performing security audits and risk analysis Testing of policies to determine whether they are sufficiently secure Ability to team interview members to learn about security risks and other complications within the company Ability to review security plans, including security gap assessments, policies, procedures, playbooks, training and testing	Some auditors may work as part of a team to determine the integrity of the security system for a company or they may conduct the audit on their own Auditors may be contract or in-house, depending on a variety of factors, so it's a good idea to spend some time considering your preferences if this is a career path that interests you
CRYPTOGRAPHER			
Subcategory: · Cryptanalyst	Develop algorithms, ciphers, and security systems that encrypt sensitive information and ensure security and privacy Protect important information from interception or deletion Detect weaknesses and design strong security systems to patch them Develop and test mathematical models and cryptography theories Decode encrypted messages (particularly cryptanalysts—who must often do this without knowing the key or algorithm)	Excellent critical thinking skills Top-notch mathematical and analytical reasoning skills Ability to think strategically and proactively Strong organizational skills and attention to detail Ability to think like a bad guy Hunger for learning and desire to stay on the cutting edge	Cryptography is a highly specialized skill set that is essential to the security of organizations of all shapes and sizes. Those with a very strong aptitude for mathematics and logical reasoning—and who love to solve puzzles—may find a satisfying career in the world of cryptography or cryptanalysis.

ROLE	RESPONSIBILITIES	KEY SKILL SET	WORTH NOTING
LEADERSHIP			
Subcategories: · Director of Security · Compliance and Risk Manager · CISO · CSO · CPO (Privacy)	Build organizational security strategy Communicate security priorities to rest of leadership team Oversee staffing, resource allocation, budgeting, and more Interface with the board, investors, shareholders, and other constituents Communicate with the public about security precautions and any breaches that take place	Broad and deep familiarity with the security and threat landscapes Ability to lead and inspire teams Strong analytical, critical thinking, and problem solving skills 10+ years of experience in the security or compliance field Top-notch written and verbal communication skills, and ability to work well with other leaders	If you stick with security long enough to get a C-level title or become a director, then you are probably capable of handling a heavy load of responsibility. CISOs and CSOs are charged with leading the entire organizational strategy and communicating priorities to key parties. They are also often public-facing, especially in the event of a security incident or breach, and so must be cool under fire.

A DAY IN THE LIFE OF A SECURITY TEAM

Overview

If you ask a security professional what they do on a day-to-day basis, you can bet you'll get a wide variety of answers. While there is generally some overlap when it comes to strategy, department goals, and common tasks, the actual day-in, day-out work of different roles at different company tends to vary wildly—and the same role may even change quite a bit day to day and over time. After all, every organization is unique, including its security threats, workforce makeup, regulatory requirements, and IT environment. And that type of "never know what's next" adrenaline is part of what attracts many to the security field in the first place!

To give you a glimpse into what a day in the life of a security professional looks like across different roles and organizations, we spoke with two highly respected security pros to get an inside look at their roles within the world of security.

Doug DePerry and John Swanson have different sets of goals and responsibilities, but both can shed light on these often-misunderstood roles while helping us think more holistically about how security fits into a business's overall strategy. Below is a condensed version of our full Q&A with Doug and John, explaining what they do day-to-day, and the goals and challenges they face as security pros in today's business climate. (If you'd like to read the full interview, check it out **here.**)

	 Doug DePerry **Director, Product Security** **Datadog**	 **John Swanson** **Incident Response Analyst** **GitHub**
Daily Goals & Focus	· Increasing security visibility · Maintaining a secure environment for developers and customers · Preventing problems before they start and baking security in as early as possible · Recruiting new team members	· Increasing security visibility · Maintaining a secure environment for developers and customers · Preventing problems before they start and baking security in as early as possible · Recruiting new team members
Daily Tasks	· Learn about new security services · Conduct code reviews · Review and design secure architecture · Leverage automation · Address time-sensitive incidents as needed	· Generate new detection and prevention methods · Create and fine-tune alerts · Research and compile threat intelligence · Address malware and account compromises · Conduct security awareness training · Evaluate and implement new tools

Roles They Work Closely With	· Site reliability engineers · Development team · Broader organization (especially as a liaison with development)	· Security operations engineers · AppSec team · Governance, risk management, & compliance (GRC) team · Support team · Platform health team · Legal/privacy team · Public relations
Common Security Challenges	· Not enough hours in the day · Scope creep and complexity · AWS and other resource constraints	· Distributed team · Responding quickly to time-sensitive issues · Keeping processes clear and smooth · Data telemetry across tools

As you can see, John and Doug have quite different day-to-day tasks and responsibilities, but their overall goals are similar. Every security team wants to keep the organization secure while also facilitating the speed and efficiency with which modern teams need to run to be successful. Hopefully this glimpse into John and Doug's day-to-day helps you imagine what it would be like to be a security professional, and in particular to inhabit one of these two roles.

A Day in the Life of a Security Team

READ THE FULL ARTICLE

FINAL WORDS OF WISDOM

Final Words of Wisdom

Finally, we want to leave you with some words of wisdom from a few of the experts we interviewed for this eBook. Security can be both challenging and rewarding, and it's always a good idea to learn from those who came before.

Keep an Open Mind

Scott Roberts says, "One of my favorite, but also the most frustrating thing about security is that you can never fully wrap your head around it. The second you figure it out, the bad guys go and do something completely different that you've never seen before." If that sounds exciting to you, then the good news is you're probably well cut-out for a career in security.

Prioritize Soft Skills

Deidre Diamond recommends that you, "Focus on soft skills as much as hard skills. Regardless of what role you choose, they all require team skills. Team skills include the ability to communicate with anyone, and the ability to stay calm, cool and collected. Team skills also include the ability to interact and educate those older and younger than you. People who have a mix of technical and soft skills go much further than those who have one and not the other." She also recommends that you search out mentors who can help you develop those soft skills over time.

Deidre also emphasizes, "Make sure you like the people you choose to work for and make sure they have a plan for your growth."

> *Hold on to the coattails of someone who occupies the role you aspire to occupy.*
>
> DEIDRE DIAMOND

Hack Yourself

Chris Sanders explains that, for many people, 10 to 15 years into a career in security, burnout may start to set in. If that happens to you, Chris advises, “It’s all about hacking yourself. Ask yourself what are the things you don’t like, and figure out how you can position yourself to eliminate those things.” He also suggests that you consider changing specialties, trying out a new field, or pursuing entrepreneurship. The latter in particular can really help make it exciting for you again, especially if you have a big idea—which you very well might after several years in the trenches (that’s how Komand came into existence!)

Give Back

One of the most important things that you can do if you pursue a career in security is to give back to the wider community. Especially with the security talent shortage raging on, it’s invaluable for those who have been there and done that to contribute their knowledge back to the community, whether in the form of intel-sharing or mentorship. Mentorship is particularly important because it can help bring new blood into the world of security and give young talent a leg up in a competitive and fast-paced world. If you have spent a few years in the security space, it’s a good idea to start looking around you and identifying ways that you

RESOURCES

Overview

As we mentioned earlier, the key to being a successful security professional is to cultivate a natural curiosity. You want to continually absorb new information and fresh ways of thinking, as well as educating yourself on news, trends, and developments both in security and in the broader context (especially the geopolitical context, says Chris.) Below are some resources that the experts we have quoted throughout recommend highly.

Courses

SANS courses; recommended by Scott* & Deidre

*Scott teaches SANS courses occasionally, so if you may be able to learn from him in-person!

(ISC)^2 courses; recommended by Deidre

Applied Network Defense: Chris Sanders' training program

Books

DEF CON Book List; recommended by Komand

Incident Response and Computer Forensics; recommended by Scott

Intelligence-Driven Incident Response; recommended by Komand

Conferences

As a general piece of advice, Chris Sanders recommends smaller, local conferences, especially for folks who are just getting started. The more intimate venues can be less overwhelming and more helpful than large, traditional shows like DEF CON.

BSides (Local Events) - recommended by Chris and seconded by the Komand team

BrrCon (Minneapolis, MN) - recommended by Chris

Security Onion Conference (Augusta, GA) - recommended by Chris

Free Shared US Cybersecuriy Event Calendar

Get The Calendar Now →

Other Resources

Cybrary: Free cybersecurity learning center; recommended by Deidre

NPower: NPower creates pathways to prosperity by launching digital careers for military veterans and young adults from underserved communities; recommended by Deidre

Peerlyst: A community of security professionals; recommended by Komand

SecurityTube.net: Free videos (think YouTube for security); recommended by Chris

The Forensic Lunch podcast; recommended by Scott

Women's Society of Cyberjutsu: Nonprofit dedicated to advancing women in security; recommended by Deidre

Security Professionals to Follow

Alex Stamos	@alexstamos
Allison Miller	@selenakyle
April C. Wright	@aprilwright
Dan Guido	@dguido
Dave Kennedy	@HackingDave
Erin Jacobs	@SecBarbie
Geoff Belknap	@geoffbelknap
Heather Mahalik	@HeatherMahalik
Jack Daniel	@jack_daniel
Jen Andre	@fun_cuddles
Jen Ellis	@Infosecjen
Jessy Irwin	@jessysaurusrex
Joshua Corman	@joshcorman
Katie Moussouris	@k8em0
Kelly Lum	@aloria
Leigh Honeywell	@hypatiadotca
Lesley Carhart	@hacks4pancakes
Magen Wu	@infosec_tottie
Matt Bromiley	@mbromileyDFIR
Paul Asadoorian	@securityweekly
Phil Hagen	@PhilHagen
Rebekah Brown	@PDXbek
Richard Bejtlich	@taosecurity
Rob M. Lee	@RobertMLee
Robert Graham	@ErrataRob
Swift on Security	@SwiftOnSecurity
Troy Hunt	@troyhunt
Wendy Nather	@wendynather

Follow the Experts from this eBook

Chris Sanders
Founder, Applied Network Defense and Rural Technology Fund

Twitter: @chrissanders88
LinkedIn: linkedin.com/in/chrissanders88
Website: chrissanders.org

Deidre Diamond
Founder and CEO, CyberSN and #brainbabe

Twitter: @deidrediamond
LinkedIn: linkedin.com/in/deidrediamond
Website: cybersn.com

Scott Roberts
Bad Guy Catcher, GitHub

Twitter: @sroberts
LinkedIn: www.linkedin.com/in/scottroberts
Website: www.sroberts.github.io

Doug DePerry
Director of Product Security, Datadog

Twitter: @dugdep
LinkedIn: linkedin.com/in/douglas-deperry-959aab8

John Swanson
Incident Response Analyst, GitHub

Twitter: @swannysec
LinkedIn: linkedin.com/in/john-swanson-57347613

About Komand

Komand, by Rapid7, is a IT and security orchestration and automation platform that gives your team the power to quickly automate and optimize IT and security operations, with no need for code. Connect your tools, build workflows, and utilize human decisions to accelerate incident response and move forward, faster.

www.komand.com

komand
by RAPID7