INSIGHTS

Stanton house

CYBERSECURITY:

Salary & Recruiting Trends Guide 2023

stantonhouse.com/us

Contents

Foreword

Welcome to the Stanton House Cybersecurity Salary & Recruiting Trends Guide 2023.

This is our third edition of this insight on the US Cybersecurity jobs market, and as always we have tried to evolve the format and content to analyze deeper, communicate clearer, and generally be more useful to the security community.

If you have any feedback for us on what would improve your experience, I would love to hear from you, so please drop me a message at james.warren@stantonhouse.com

James Warren
Vice President

James.Warren@stantonhouse.com

Samantha Buckenmaier
Senior Consultant

Samantha.Buckenmaier@stantonhouse.com

Industry Insights

Market Report

James Warren

The most frequent question most recruiters in a specialist field get asked is ‘how’s the market?’

From our perspective, 2022 was one of the busiest years we’d ever seen in Cybersecurity hiring, with a sharp drop-off in Q4 in market activity.

Our client base is evenly split between start-ups and corporates, and what we saw from relatively early on in Q3 last year was the start-ups rapidly tighten their belts and move to layoffs, whereas some corporate hiring managers hung onto processes with us as late as early December before company-wide hiring freezes and staff reductions halted their plans.

It seemed a few different factors coalesced for a such a dramatic decrease in activity including inflation increasing the price of investing, firms correcting for pandemic over-hiring, and some tech stock darlings start to splutter under pressure from gaining legacy competitors.

It’s too early to say what kind of a year 2023 will be for a security professional seeking new employment, but our anticipation is that the market will rally later this year with each quarter busier than the last.

Breaking into The C-Suite

Sam Buckenmaier

Breaking into the Cyber C-suite one day is an ambition that many security individuals share, yet unfortunately, many find that vision hard to achieve.

Before we spend time discussing practical ways to move the needle a bit more toward this goal, there are a few things to think about.

Firstly, having a clear answer to the “why do you want to join the C-suite” is vital. Are you aiming for the title? Do you think you will have a stronger platform for change? Spend some time thinking about this - understanding your motivation and defining the ‘*why*’ will help you inform and tailor your search so you can understand the type of company you are ultimately seeking in the long term (see page 9 on Pros and Cons of a Start-Up).

Secondly, do your due diligence on what exactly a CISO is and what a CISO does - talk to individuals in your network, reverse engineer profiles to understand how other people have stepped up into this particular role, and ask yourself if this is *truly your passion*.

While being a CISO is indeed a well-esteemed role, it is also a calling. You will be ***THE*** go-to executive who is responsible and accountable for all the security needs of the organization and you will be the person that other people look to for guidance and strategic thinking. So - what are some tangible things you can think about as you start pursuing your next career shift?

Know your values

You will be the go-to leader for security in both a technical and professional sense. By understanding both your core personal and security values, decision-making will flow much easier and you will be able to help steer the company and the people within it, toward success. That being said, by being too rigid in your stance you can close yourself off to new ways of working or conducting security practices. The field changes fast, so while it is important to understand team values and work towards a common goal, remember to be willing to listen to those around you and be open to change.

Have a business mindset

Typically, by being at a C-level you will no longer be the most technical person in the room. You need to understand how security impacts the wider business and be able to speak to a CFO or other members of the board with clarity and ease. To do this you should engage business leaders in discussions surrounding risk - this way, it ignites an ongoing discussion and helps work toward the “security first” mindset. If you feel you are lacking in understanding the business side of security, there are lots of ways to improve. Take business classes, read books, listen to podcasts - some individuals even decide to secure their MBA as this will help fast track your knowledge and set you on the right path.

Finally, understand the business in which you are working and build a security program to meet the needs of that specific business. Don’t bend the business to security - it’s hard to get things done this way!

Cultivate your leadership skills

Work hard to learn more about the leadership and management of teams. Nobody is ever "finished" learning about leadership, so spend some time reflecting on areas you can improve and start listening to podcasts, ted talks, and reading books on the subject. We have produced a guide to help kickstart your leadership transition which includes several resources to help you on this journey that we know you will find useful, please reach out to us for your copy.

Feedback is vital to nurture your leadership skills. Discussing ways to improve with your team, leaders, or peers will help highlight gaps in your knowledge that you may not have noticed. Remember - feedback is a gift so it should always be treated as such!

Be patient

Just like you aren't born an adult, you aren't starting your career at the top of the ladder as a CISO. These leadership roles take time to achieve, and for a good reason. To build or maintain the strongest security program, you will need all the experience and confidence to do so. Nurture your skills and prepare yourself over time for this level of responsibility.

Have a mentor. Having someone in your corner to guide you through your career growth is crucial. If you don't have anyone who immediately comes to mind, there are other ways to find a mentor, you could try:

- CISO networking groups
- Asking for a referral from your current CISO/CIO
- Ask us!
- Find someone on LinkedIn and message them for an introduction (make sure you build a rapport with them first, before you directly ask for mentorship - their time is very valuable!)

These are all key aspects to start thinking about as you begin your exploration of the C-suite. The last piece of advice I'll leave you with is to ensure that you prioritize other things that are meaningful to you outside of work. A balance of work and life is imperative for long-term success.

Corporates vs Start-Ups

Alek Ostrander

Having a robust Cybersecurity program is a necessity in all industries. Whether it be a small tech-focused start-up or a massive fortune 500 company, everyone needs a cyber program in place. So, what are the best goals to aim for when thinking of fast-tracking success in your cyber career?

Whether it's a role building out the cyber program from the ground up as a CISO, or being one of the vital analysts or engineers that aid in daily operations, both corporate and start-up environments have their pros & cons.

Start-ups allow for major exposure

It's widely known that start-ups try to operate with leaner teams as they attempt to scale up and secure more funding in their growth journey. This is a great chance for someone, especially in an IC role, to begin to take on more responsibilities. Sometimes you might not feel initially comfortable with the tasks given, but by accepting these tasks and pushing yourself to learn and expand your skill set, you will be well-placed to take on more challenging opportunities later down the line.

Corporate environments will allow you to specialize in one major focus

A common theme that we've followed as a recruitment firm is that the more specialized someone becomes in a particular field (i.e. detection and response or cloud security) the more compensation and buzz they generate from the market. In a corporate setting, the team around you is going to be large, with many sub-projects within the overall cyber program, which will allow you to specialize in a niche area and thrive.

Flexibility and "new-age" culture is going to be very present in a start-up

Perks like remote work, flexible hours, mental health days, or free snacks/lunches are the things people picture when thinking about what working in tech may look like. For many hyper-growth companies, this is going to be true, getting the culture right early will allow them to attract great talent. For those that take a chance on doing this, it will be a great way to differentiate themselves against the competition and attract incredible talent.

Not all start-ups are built the same

Joining a smaller, less established environment isn't always filled with butterflies and ponies. Start-ups fall on hard times too. With funding running out and budget cuts it can take a turn for the worst, if not managed correctly. The best way to judge whether a start-up is right for you is to think of the number of competitors there are in the space, compared to your current organization, do you truly believe in the company mission or product they are selling in order to stay there for the long term and ride out potential bumps?

Making your mark on a program can have a major impact

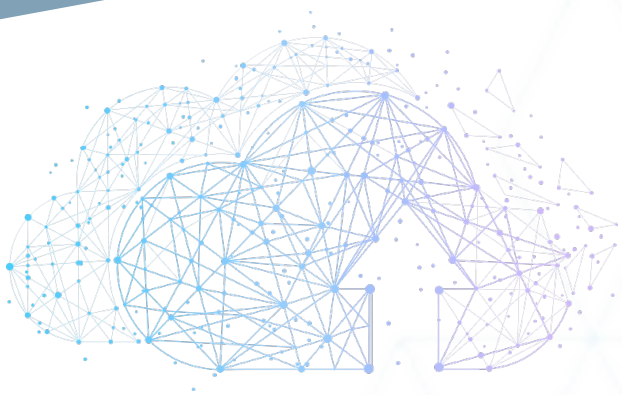
No matter what route you go down, you're part of a larger team, all putting your collective efforts into advancing the functionality of a cyber program and protecting the overall business. In larger, more complex environments, you'll be working on smaller projects pertaining to a program subgroup, and building that out will be your focus over the next few years. In smaller, more agile environments, even as an engineer, you'll be tasked with really bringing forth the vision and building blocks of the entirety of the security program.

Compensation structures are going to differ, think cash today vs the long-term potential

It's no secret that larger, more stable businesses are typically going to be able to offer more cash compensation to begin with (base + bonus). Whereas a start-up may lack the capital to pay higher compensation packages to its employees.

However, start-ups will of course make up for it with Long Term Investments (typically stock options). LTIs can be a big question mark that could either gift you with early retirement or could be completely worthless in the long run. On the other hand, and perhaps rather sneakily, if and when a company eventually finds itself in the Fortune 500, compensation packages may decrease overall as companies believe that just having the brand name on your resume is worth enough on its own, so always be ready to weigh up your options.

At the end of the day, both routes offer various benefits and drawbacks, and the decision will be totally dependent on your appetite for risk and what you decide you want to make of your career in cyber security in the future. Want to risk it all with the ability to be part of the founding group of the next revolutionary security program? Or would you rather play it more conservatively, specialize in one focus area and grow your career that way?



How to get into Cloud Security

Christina Paluscio

Being in such a highly competitive and highly specialized market, a very common question we get asked is something along the lines of ***"How can I get into cloud security?"*** or ***"What skills do I need to take the next step up in my security career?"***

In a nutshell, a Cloud Security Engineer's job is to create security policies and best practices to ensure a secure infrastructure. They do this by recognizing where threats can come from in regards to identity and access, monitoring the environment through automation, and data encryption, among other things.

The higher you climb in Cloud Security, the more your role will take a wider, more holistic approach to architecture. At the Product Security level, you'll also start to consider things like application code scanning and threat modeling.

When it comes to cloud security, most candidates break into the cloud from one of two backgrounds: network security or security operations.

Through Network Security

Network security engineers make an easy jump to cloud security because the fundamentals of the jobs are very similar. Both require things like increased storage and constant monitoring, and both are solutions to the question of who can access an organization's data. Cloud Security is taking a much wider step, but the fundamentals are very similar, making the transition easier.

If you're currently in the Network Security space, here are a few ways you can make the jump into cloud roles:

- **Obtain certifications**
  - Examples: AWS Cloud Computing, AWS Security Specialty, Terraform
- **Work with developers**
  - Cloud security overlaps with many different teams, but development teams are a big piece of that puzzle. A lot of companies see it as a huge plus if you can "speak developer". Understanding their flow and how they work will give you a leg up in obtaining a cloud security role.
- **Begin learning cloud-native tools**
  - IAM, monitoring, and automation tooling

Through Security Operations Engineering

Coming into cloud security from security operations gives you a different type of advantage than network security, outlined above. Many modern SOC's will have cloud-native tooling for you to familiarize yourself with, as well as the knowledge of threat detection and response, which is at the heart of cloud security.

If you take a look at the AWS security tooling stack, they focus on monitoring, scanning, and restricting access. If you've worked in a SOC and have an understanding of where threats originate and when they're escalated, making the transition into cloud security is not too far away. The hands-on experience in a SOC will give you the incident response knowledge that a lot of cloud security professionals work with. What it ultimately comes down to is learning new tools, strengthening programming/scripting skills, and beginning to work across multiple security teams like DevOps, Application Security, IAM, etc.

If you're currently in the Security Operations space, here are a few ways you can make the jump into cloud roles:

- Learn a cloud security tooling stack
    - AWS is the most common and the easiest to learn
- Pick up Infrastructure as Code and other programming languages

How to get ahead in Cloud Security

When it comes to moving up through cloud security into higher-level and higher-paying positions, it really depends on the route you want to go. A natural transition for cloud security engineers is to make the leap into architecture. If you have management aspirations, an architect position can be a good stepping stone from a highly technical individual contributor role, to taking a step back and looking at projects with a wider scope.

Here are a few broad topics a Cloud Security Architect might be in charge of:

- Understanding both technical and business needs/requirements
- Python/scripting knowledge
- Cloud migrations
- Creating operation procedures
- Leading enterprise changes for cloud adoption
- An increased focus on future plans

As an architect, you will be expected to help push projects along, communicate progress to other teams as well as stakeholders, and serve as an escalation point if necessary. **Soft skills will be just as important as technical abilities in this role.**

Moving into a people management role is a straightforward path from security architecture. You might have your sights set on a Cloud Security Engineering team, DevSecOps team, or even a CISO title in the future. If that's the case, our main piece of advice would be to start building your network of people in cybersecurity, both in and outside of your organization. Higher-level management roles tend to be filled through connections, so it's never too early to start networking.

How to get into Application Security

Maddison Cote

The demand for application security talent in 2022 was the highest we've ever seen, and based on cybersecurity trends, that need is only going to grow in the coming years. I've had the pleasure of talking to application security and offensive security talent at a variety of seniority levels, and the questions I get most often are "how do I transition into this space?" or "what is the next step for my skillset?"

To bring you the most value, I've taken the time to roadmap each path for both first-timers and veterans in the application and offensive security world.

At a high level, Application Security Engineers work closely with development teams to help them follow a secure software development lifecycle (SDLC). Their primary function is to test applications for security vulnerabilities, add secure features to prevent threats from said vulnerabilities, and shift security practices left in the development lifecycle.

Given the basics of an Application Security Engineer's role, Software Engineers and Developers can make an easy jump into an entry-level Application Security role. Both roles require knowledge of object-oriented coding languages, experience conducting code reviews, and working knowledge of the software development lifecycle. If you're considering the transition into Application Security from a software engineering or development background, here are some ways to make the jump:

- Highlight your knowledge of various languages on your resume
- Elaborate on your experience automating tasks using code
- Seek out these resources that will introduce you to some of the security fundamentals:
    - OWASP WebGoat: An application made deliberately vulnerable so you can use it to practice various security tests, exploits, and tools.
    - OWASP Cheat Sheet Series: A collection of high value information on over 65 specific application security topics.
    - OWASP Security Knowledge Framework: An extensive knowledge base you can use to learn how to integrate security by design in an application. It even has examples and best practices on how to prevent attackers from exploiting your app.

Getting ahead in Application Security

The more senior you become in Application Security, the more your responsibilities will focus on that “shift left” mentality, adopting secure application architecture and collaborating with development teams to implement said secure architecture at the start of all development lifecycles.

Not everyone in Application Security comes from a background in development, but knowledge of code is one of, if not the most desired skill set for these roles. If you’re already in this field, pursuing coding knowledge will help you break into that next tier of seniority and compensation. If you’re someone looking to upskill from this point, here are some ways to make take that next step:

- Pursue projects in a cloud environment; this combo skill set is becoming more and more in-demand (see next section for some cloud certifications)
- Explore and obtain your CSSLP - Certified Secure Software Lifecycle Professional gives you the fundamentals to incorporate security practices into every stage of the software development lifecycle (SDLC)
- Gain experience in other areas of Application Security that will increase the value of your combined skill sets:
    - Threat modeling
    - Secure application architecture
    - Testing source code
    - Remediating vulnerabilities
    - Penetration testing

How to get into Penetration Testing

Maddison Cote

Simply put, Penetration Testers are authorized hackers that use a variety of tools to perform simulated cyberattacks. Their primary function is to evaluate the security of a web application, network, cloud environment, etc. Given the crossover between Application & Offensive Security, I also work closely with web app & network security penetration testers. Here I get the question, “what are hiring managers looking for the most” from professionals that are either taking their first step into penetration testing or trying to break into the next tier of offensive security talent.

Entering the Field:

At the associate or junior level for penetration testing, most employers look for experience penetration testing in one of two ways; in an educational environment for new graduates or in a home lab environment. For someone established in their career, the most common background we see for penetration testers are software engineering/development, network administration/engineering, or security administration. Having a passion for penetration testing, and a demonstrated knowledge of its fundamentals, are the common requirements for an entry-level position in penetration testing.

How to get ahead in Penetration Testing

If you are a penetration tester looking to step into the next tier of seniority and compensation, there are a few avenues that will take you there. One that does not require additional technical pursuits, is leadership/mentorship experience. Often we see these professionals level up by playing an active leadership role on a team, acting as the point person for penetration tests, and proactively taking on leadership tasks. These are effective methods to communicate to your leaders that you're interested and able to perform as a leader in your next role.

There are also technical routes you can take if you're looking to level up as an individual contributor.

Pursuing projects that take you outside of just the day-to-day and diversify your skillset are a great way to stand out as a desirable candidate for a senior role. There are multiple cross-functional routes to take such as:

- Bug Bounty Programs
- Collecting Open-source Intelligence
- Proprietary attack programs
- Staying current on the latest trends in hacking techniques and popular exploited vulnerabilities

Penetration Testing Certifications

Multiple professional certifications are highly valued in this field, especially for more senior positions such as:

- Certified Ethical Hacker (CEH) – A vendor-neutral and theoretical approach for offensive security and is great to explore as an entry-level option
- Offensive Security Certified Expert (OSCE) - A more advanced offering from Offensive Security, and focuses on exploit development and mastery of penetration testing skills
- Offensive Security Certified Professional (OSCP) - Focuses primarily on penetration testing over white-hat hacking and acts as the lowest-level certification offered by Offensive Security
- Offensive Security Web Expert (OSWE) - Made for application penetration testers and focuses on white box application assessments, knowledge of advanced source code reviews, and exploiting vulnerabilities in web applications

The Salary Guide

How to read our salary guide

This guide is a rough approximation of what it would cost to hire any of the included skill sets with an experienced candidate. Please bear in mind that this does not necessarily reflect the average across the industry. In our experience, given the clients we work with, these figures simply represent our professional advice on where to start.

The figures represent the base salary and an estimate for remote workers. For positions located in the San Francisco Bay Area, New York City, Seattle, or another similarly high-cost urban center, you can add between 10-30% extra.

We provide a range of salaries that look at the lower, median, and high ends based on the skills needed for each position. The lower ends may need to compromise on background, location, or years of experience for example. The high ends, with few compromises, will likely be offered to candidates that check most, if not all, of the desired boxes for the role.

The bonuses added to these salaries vary, but we typically see between 10-25%.

Extra components like RSUs or equity also vary.

The leadership roles in this guide are calibrated for running teams of approximately 5-15. There are jobs running larger security teams in industries like Banking or Big Tech that may have significantly higher salaries.

CISO salaries are quite a complex topic, so we'd always advise discussing them one on one with one of our consultants.

Definitions of terms

Application Security Engineers run static and dynamic testing and manual secure code review on applications. Typically, an important hire for any business building a large amount of proprietary software. This is a difficult skill set to get from a vendor partner, as it normally requires a full-time commitment to understanding the codebase of your applications. They may have some DevSecOps abilities.

DevSecOps Engineers integrate automated vulnerability scanning tools into a CI/CD pipeline. They do not typically do manual secure code review.

Application Security Architects are usually experienced Application Security Engineers whose influence has shifted to the left of the application development process. An Application Security Architect who specializes in cloud-hosted applications should be referred to as an Application Security Architect as opposed to a Cloud Security Architect.

Cloud Security Engineers configure tooling focused on cloud security compliance. Their focus is often weighted toward technical implementation and less towards knowing the frameworks themselves. An extremely important role in cloud-native security teams, particularly to achieve cloud security compliance standards. Often one of the first 3 hires into a SaaS security team.

Cloud Security Architects design solutions for cloud security compliance. Their skill set is less focused on implementation and more on understanding relevant frameworks and determining what solution(s) could work for a given area. They are typically seen in larger security teams, when the environment becomes complex enough to have to plan carefully for.

Detection & Response Engineers operate SIEMs and respond to incidents. They may have Security Operations Engineering or Threat Intelligence Analyst abilities. D&R Engineers are very common in smaller security teams, even if the rest of their SOC is outsourced, as they will usually spearhead coordinating with vendor partners.

Security Operations Engineers configure SIEMs and detection and response tooling. They are often hired alongside Detection & Response Engineers in medium to large security teams where Detection Engineering requires a full-time approach.

Monitoring Analysts monitor SIEMs and help escalate possible incidents up the chain. Generally hired into MSSPs and larger security teams who have their own end-to-end Security Operations setups.

Privacy Analysts help you comply with privacy regulations. Privacy is sometimes covered as an auxiliary specialism by GRC Analysts, but the field is becoming dense enough in some industries to necessitate specialists. May in some organizations report into legal.

GRC Analysts focus on security compliance. They may have some Privacy Analyst knowledge. Usually the most common first CISO hire. GRC Analysts will help take paperwork out of a security leader's hands and allow them time and space for other things.

Threat Hunters focus on proactively seeking out threats that have evaded the automated Detection tooling scanning your environment. Usually very experienced Detection & Response Engineers who have developed this specialization.

Threat Intelligence Analysts research the latest threats using a variety of methods. Very rarely hired into smaller security teams and usually found in MSSPs or very large security teams, as they often rely on collective knowledge.

Enterprise Security Architects are generally experienced ICs who help a security leader map out their organization and help them put together a program. Found usually in large security teams where the org is so complex the CISO needs birds-eye support.

IAM Engineers specialize in identity and access management installation and configuration. They quite often have a developer skillset and intimate knowledge with one or more IAM platforms. Becoming more common as businesses mature into cloud infrastructure.

Penetration Testers learn to infiltrate networks and web applications to test a business's security defenses. Less commonly found in smaller security teams these days, as the work is often project based and can be outsourced to consultancies.

Product Security Engineer is a term that may be used to refer to Application Security Engineers with experience in securing the way the application interacts with the underlying infrastructure, but this skillset has become expected of strong Application Security Engineers, and the term is now arguably interchangeable with Application Security Engineer.

Role	Many compromises	Some compromises	Few compromises	Coveted skills
Application Security Engineer	$150k	$175k	$200k	• Software Dev. • Cloud • Container
DevSecOps Engineer	$140k	$165k	$190k	• API scripting • Cloud • Container
Cloud Security Engineer	$160k	$190k	$220k	• Writing IaC • Container • API scripting
Detection & Response Engineer	$140k	$160k	$180k	• Cloud • API scripting
GRC Analyst	$120k	$150k	$180k	• Lead audit exp. • CISSP, CISA, CISM • Cloud compliance
Security Operations Engineer	$140k	$170k	$200k	• API scripting • Cloud
Threat Hunter	$150k	$170k	$190k	• Cloud exp.
Threat Intelligence Analyst	$160k	$180k	$200k	• Cloud threat exp
IAM Engineer	$130k	$150k	$170k	• Software dev exp.
Privacy Analyst	$130k	$150k	$170k	• Legal exp. • EU exp.
Penetration Tester	$150k	$180k	$210k	• Web applications • Software Development • Cloud • Container

Role	Many compromises	Some compromises	Few compromises	Coveted skills
Cloud Security Architect	$170k	$200k	$230k	• IaC • Container • Multi-cloud
Application Security Architect	$170k	$190k	$220k	• Cloud • Container • Software dev exp.
Enterprise Security Architect	$180k	$205k	$230k	• Breadth of knowledge
Monitoring Analyst	$80k	$100k	$120k	• Yrs. exp.
Application Security Leader	$200k	$230k	$260k	• Hands on exp. • Yrs. leading
Cloud Security Leader	$200k	$230k	$260k	• Hands-on exp. • Yrs. leading
Security Operations Leader	$180k	$210k	$240k	• Hands-on exp. • Yrs. leading
GRC Leader	$170k	$200k	$230k	• Yrs. leading • Audit track record
Security Engineering Leader	$190k	$220k	$250k	• Yrs. leading • Hands-on exp.
Penetration Testing Leader	$180k	$210k	$230k	• Yrs. leading • Hands-on exp.
IAM Leader	$180k	$210k	$240k	• Yrs. leading • Hands-on exp.

For security contractors

Stanton House is able to provide contract security professionals for a variety of different engagements.

In 2022 we provided contract Penetration Testers to help pass audits, GRC professionals to support with compliance crunches, Application Security Engineers for a CISO who couldn't afford one full time, and several vCISOs who helped clients build entire security programs.

Whether you need a Red Teamer for 30hrs over two weeks, or a vCISO for 20hrs a week for two years, contact us at cybersecurity@stantonhouse.com to discuss your need.

TESTIMONIALS

WE LOVE PARTNERING WITH INTERNAL TALENT TEAMS

"I recently partnered with Stanton House to assist our company in staffing niche IT Security roles. James and the team worked incredibly well, resulting in multiple, successful hires, including a Director, Analyst and Engineer. From the intake/kick off through screening/interviewing and the offer process, James and the Stanton team was spot on in terms of understanding our needs, communication, thoroughness, pace and quality."

- AVP, Talent Acquisition, Ascena Retail

"James Warren and Samantha Buckenmaier represent a best in class recruiting firm that has benefitted Datto in many ways. Not only did they help us with three extremely hard to fill roles, they brought a sense of humor and diligent professionalism along with it. Security is no doubt the most in demand portion of the candidate market right now, and by loving their craft and being subject matter experts in this field they deliver on time results. If you are a hiring manager with niche needs I would highly recommend engaging them."

- Staff Technical Recruiter, Datto

"James is truly the epitome of AMAZING customer service and ensuring that he not only helps staff the best candidates for open reqs, but builds relationships with his clients. I never felt that our organization was just another number or a quota to be filled. We have always been treated with grace, humanity and is always so flexible and friendly to our staff. We truly feel valued working with James and look forward to our continued relationship with him and his team."

- Head of Human Resources, GetInsured

"Maddison was an invaluable partner last year. We partnered on some tough searches -- her industry expertise, problem solving skills, and tenacity led us to hire some excellent people. I'd love to work with Maddison again and would recommend her to anyone looking to work with a cybersecurity recruiter as either a hiring manager or job seeker."

- Technical Recruiter, Hinge

"It was a wonderful experience working with James and the team at Stanton House. Stanton House is very knowledgeable in the security market. Their detailed insights coupled with their customer-first mentality has made them a trusted partner of Lenovo's. We look forward to a long lasting partnership."

- Senior Talent Acquisition Partner, Lenovo

"Samantha was a wonderful partner to our recruiting team. I looked forward to each interaction, and the candidates we received through Sam and Stanton House were the cream of the crop! Can't recommend her enough, and can't wait to partner with her again for our Security hiring needs! :)"

- Senior Talent Partner, Frame.io

"James and the team provided an exceptional cyber security recruiting experience for United providing great candidates and managing the process effectively. I would recommend he and Stanton House to anybody looking to recruit in Cyber Security."

- Technology Recruitment PMO, United Airlines

"Maddison is awesome to work with. She really gets the info you need and really collaborates with the internal folks to not only get running, but to also get us over the finish line."

- Senior Technical Talent Acquisition Partner, Hinge

"I have had the opportunity to work with Samantha on a few hard to fill Product Security roles. Samantha found great candidates and she is a pleasure to work with! I highly recommend Samantha and Stanton House!"

- Senior Recruiter, SailPoint

More testimonials from candidates & hiring managers on our website

CONTACT US

For a general inquiry about our services, please email us at:

cybersecurity@stantonhouse.com

Join our LinkedIn Jobs group where we post every opportunity

Follow us on LinkedIn at #SHCyberJobs

Browse our website for new roles

Samantha Buckenmaier
Senior Consultant

James Warren
Vice President

Alek Ostrander
Consultant

Chaz Spicer
Associate Consultant

Maddison Cote
Senior Recruiter

Application & Offensive Security

Christina Paluscio
Recruiter

Cloud & Network Security

Sabrina Powers
Associate Recruiter

Detection & Response + Security Operations Engineering

While we recruit anything under the banner of information security, we recruit some roles enough to have specialist recruiters for those positions. If you are a candidate seeking one of those roles, please contact your specialist recruiter. If you don't see your specialism, please email us at cybersecurity@stantonhouse.com

Maddison.Cote@stantonhouse.com

Christina.Paluscio@stantonhouse.com

Sabrina.Powers@stantonhouse.com

Stanton house

WE BUILD WORLD CLASS CYBERSECURITY TEAMS™

stantonhouse.com/us