Stanton house

CYBERSECURITY:

US Salary & Recruiting Trends Guide 2022

Never miss an opportunity, join our LinkedIn jobs group: https://www.linkedin.com/groups/12628234/

Contents

Foreword

Welcome to our Cybersecurity Salary & Recruiting Trends Guide 2022.

For the second year in a row, the US Cybersecurity recruitment team at Stanton House have put together a salary guide, to help security leaders, talent partners and security professionals understand the market value of specific skillsets within the field.

The second half of 2021 was the busiest six months, in cybersecurity recruitment, in living memory. Positively, the growth of the market and demand for security talent shows no signs of abating this year however, skills shortages remain prevalent across North America and indeed the globe.

Alongside our salary guide, we feature a series of articles to give some colour to the cybersecurity recruiting trends, changes and developments, as we see them.

We hope you find this guide informative and very much look forward to discussing how we can support you.

James Warren
Executive Consultant, Cybersecurity
+1 773 782 0103
James.Warren@stantonhouse.com
linkedin.com/in/james-michael-warren/

CYBERSECURITY RECRUITING TRENDS 2022

Remote working is now the norm

Last year, I wrote a section titled ‘Remote working is here to stay’ and while I had an inkling that satellite security teams would become a common theme in 2021, a staggering 95%+ of our mandates were for remote opportunities.

There is of course a lot to be said for the classic, ‘all in the same room’ spirit that onsite hiring gives a team. We’ve built brilliant onsite security programs over the last few years, but, like vinyl to streaming, choosing onsite (if you have the choice) now comes at a cost.

The way I try to articulate this to our clients is; hiring onsite these days doesn’t mean you're just competing with local businesses in Chicago, NYC, or Austin. In fact, you are now competing with every business across the US that hires remotely. For example, if you are trying to hire in New York City, while you might think of the talent pool as large, it is if course dwarfed in size by the collective 48 other continental States. To add to the difficulty of the task, the major cities have seen a flood of talent relocate to more affordable States, and not every NYC based candidate wants an NYC based role.

Therefore, to secure talent tied to a specific office, even if it’s only for a couple of days a week, you will likely need to pay more than anybody else in the country for the same talent or be willing to sacrifice on quality.

It can be very uncomfortable for first time hiring managers, or for those who haven't hired in a while, to entertain the prospect of hiring remote workers. In my experience, most of this worry seems to come from the fear that they will not achieve the same team spirit, not achieve the same levels of accountability and ultimately, not get as much done.

Our counter to this is that these are simply the new leadership challenges brought about by this new era of work. The great leaders of the future will find a way for their teams to collaborate and stay productive.

Regardless, whatever your decision or situation when it comes to onsite working, our team are here to build you a great security program either way.

Author, James Warren

Security roles in focus

Application / Product and Cloud Security professionals were in very high demand throughout 2020 and last year. And, while demand hasn't exactly dwindled, Detection & Response has now overtaken everything to become the flavor of the moment.

Detection & Response experts sit in your Security Operations program and usually spend their time focused on monitoring your SIEM or responding to incidents. For the vast majority of security teams with a headcount >10, they'll form a conduit between any MSSP (Detection, Threat Intel) that supports your function, whilst providing the Tier2 and Tier3 capabilities inhouse.

They might have a combined skillset with, but are different from, Security Operations Engineers, whose job titles have evolved to refer to those who configure and maintain the tools for these teams.

In demand skillsets for Detection & Response experts include scripting for API development (usually Python), as combined and automated tools can do the work of extra heads. Incident Response experience in the Cloud is usually a big plus, too. Experience of specific tools typically has less of a focus for hiring managers as most SIEMs and EDR solutions have comparable interfaces and do very similar things.

We can provide numerous case studies of finding and placing professionals with this extremely scarce skillset into security programs across the country.

Author, James Warren

Getting your priorities straight

As we'll get into with the salary guide later, 2021 was the busiest year for security hiring ever and 2022 is shaping up to be no different. Salaries have ballooned with coastal firms now paying coastal prices for security folk in the middle of the country. With the flood of Engineers out of NYC, SF and LA, for example, those who remain behind can charge a premium and what's more, you'll have to pay more to get them into the office.

Overall, it is much, much harder than it was twelve months ago to hire security talent. For the average security leader, this presents a challenge when it comes to acquiring the right skill set. A big part of our job, and one that is more in focus this year, is educating clients on the current state of the market, and what is possible within their budget. What can you get for your money that will actually help you achieve your goals?

The first thing I usually start with is a twist on an old question: What's the 'real' objective in hiring this person? Is this a functional role to help you overcome a specific obstacle? Or is this a development hire for you to groom into a future rockstar? If you have an ISO27001 goal in three months, you might need a career GRC analyst on his or her 10th certification. If this is extra firepower for your audits, a bright spark three years out of a consultancy's compliance team might be more on the money.

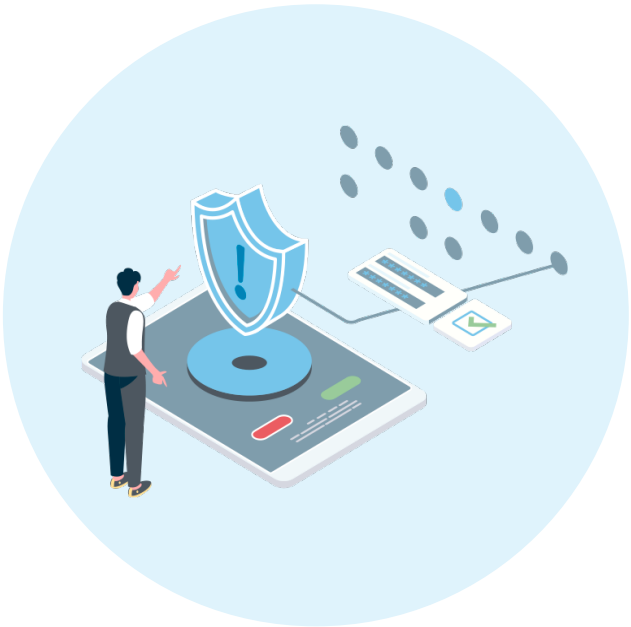
The second thing I do is really hone down and focus on the most important skill sets. Often, we'll get initial requests for somebody with Application and Cloud Security Engineering skills. In reality, a candidate who can SAST, DAST, write Infra as Code and configure Lamda is very, very rare. So, I start with, 'if you need both skill sets, would you hire one and coach the other?' If the answer is yes, you're probably going to have more luck teaching an AppSec Engineer CloudSec than vice versa, so that's where I start.

It never gets more complicated than trying to deliver the best possible solution for a hiring manager at that time.

Author, James Warren

What is a Product Security Engineer?

Product Security Engineer. You will never find a more wretched source of confusion and ambiguity. So, what does it mean to be a ProdSec Engineer?



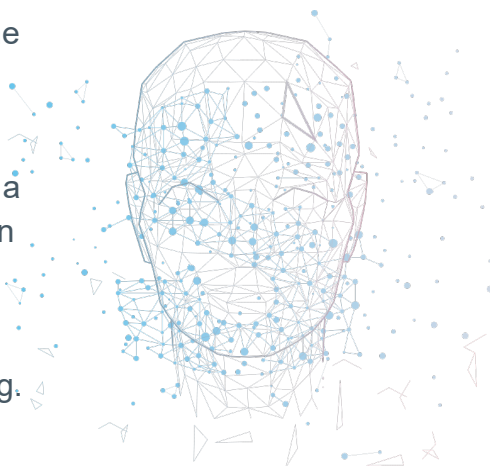
There are competing theories regarding the definition. Product Security is the securing of a product that a company offers, rather than the company environment itself, and so, a ProdSec Engineer contributes in some facet to that goal.

Some people use this interchangeably with Application Security Engineer – an employee with SAST/DAST, secure code review skills.

The purest definition of the title is probably somebody who has the above skill set but adds into it some experience of Infrastructure Security, and even Detection & Response.

Their security contributions have a broader perspective and take into account how an application interacts with underlying infrastructure, and what the threat scenarios and response would be if something did go wrong.

My recommendation if attempting to recruit this definition is typically to allow the last two elements to be skills learnt on the job. Trying to hire even one of these skill sets is a tall order in the current market.



The last definition would be to refer to any defined role within a team that focused exclusively on securing a product. I've seen Detection & Response Engineers termed 'Product Security Engineers' because they're part of this dedicated setup.

Which definition sticks will be a matter of watching and waiting.

Author, James Warren

Top cloud certifications

Looking at 2021 in retrospect, there is one trend I'm watching climb to the top of hiring managers' minds. Organizations, applications, and users alike are migrating to the Cloud, creating a demand for cybersecurity professionals with experience in Cloud security and migration, both private and public, as a hybrid environment remains the most affordable and secure solution.

For any security professional considering a new certification or area of focus, I've compiled a list of the best Cloud Certifications and tool specializations to bolster your resume.

Vendor (neutral & advanced)

For a vendor-neutral approach to Cloud Security, the ISC2 Certified Cloud Security Professional (CCSP) certification is the best to consider. It covers a variety of Cloud security topics including Cloud Application Security, Cloud Platform Security and more, in an environment that would arm you well to work for any Cloud vendor.

Here's the link to learn more.

AWS specific

If you're looking to specialize in AWS Cloud Security, the AWS Certified Security certification is top of the line. AWS is commonly the most popular public Cloud vendor among organizations because of their pay-as-you-go pricing model, so this certification will set you up for success with prospective employers, even though it's specialized. The course covers every aspect of AWS's Cloud platform and its security, associated security products and incident management.

Here's the link to learn more.

Cloud beginners

If you're relatively new to Cloud environments as a cybersecurity professional, a great jumping-off point to start expanding general Cloud security knowledge is the CSA Certificate of Cloud Security Knowledge. While this is not a certification, it is the perfect way to learn a skeleton model of Cloud security concepts in a vendor-neutral environment.

The materials will introduce you to Cloud architecture and infrastructure, and concepts such as data security in the Cloud, configuring security networks and implementing baseline controls. While the other two certifications listed have prerequisites such as years of experience in information security or AWS, this has none - making it perfect for anyone starting out.

Here's the link to learn more.

Author, Maddison Cote

Privacy out in the open

Privacy functions within a security program are often one of the most overlooked, yet quickest developing areas where we have noticed an increasing need. I've had lots of clients come to us seeking advice on where privacy specialists sit within a security program.

Based on the privacy programs that I've helped to expand, privacy professionals are typically placed near the GRC function but more often sit within the legal function of organizations, having a cross-functional interaction between the two.

Ask yourself what does privacy mean to you? The typical response to that question has blurred lines that fall quite near the definition of what security is, so what is the difference between these two very important and ever-growing topics and why does it matter to you?

As cybersecurity professionals, you must realize the importance of keeping privacy a vital part of your security function.

Security and privacy both stand at the forefront of data, the former focuses on the overall protection and assurance of data safekeeping that is collected or maintained by a company, information security wouldn't properly be named without data to protect. The latter however keeps a focus on the method of collecting data in terms of responsible use, storage, and deletion of that data.

Lack of sufficient structure and policies in established privacy programs can lead to mishandling or improper use of data. One major consequence very relevant to this topic going back a couple of years is with Meta (formerly Facebook) incurring a $5 billion fine from the FTC here in the US as well as Amazon incurring a major fine of $888 Million for GDPR violations in the EU.

Setting up a proper privacy function within your security program takes time, but with the proper understanding of just how important privacy is as a whole and how much risk you take on by not having correct procedures in place, this is something that every single security team should be implementing in their future roadmap.

Author, Alek Ostrander

Creating a culture of inclusion

"We have a big push for diversity within our hiring plans, but we have been having trouble recruiting diverse candidates."

This is one of the most common statements I hear when qualifying roles, both from existing and new clients. When I am told this, I always ask employers what their company or team is doing to create an inclusive working environment.

With more candidates starting job searches than ever before and the core values of individuals being re-evaluated, due to the forced (albeit necessary) slow-down that Covid-19 has caused, creating a culture of inclusion has never been more important.

A good culture often comes from employees feeling valued, heard, respected and included. An article in The Harvard Business Review states:

"If workers feel like they belong, companies reap substantial bottom-line benefits. High belonging was linked to a whopping 56% increase in job performance, a 50% drop in turnover risk, and a 75% reduction in sick days. For a 10,000-person company, this would result in annual savings of more than $52 million."

As a cybersecurity recruiter, specializing in finding diverse talent, I recognize that the journey to building a diverse team is not straightforward. However, the biggest piece of advice I give employers, is that a great first step is to look inwards to the core fundamentals of what it is that makes their organization a great place to work. Why should any employee want to work for you? What makes your organization or team different?

Defining and articulating this will not only help sell your company to potential candidates, but the constant re-evaluation and communication of your company culture as part of your EVP (Employee Value Proposition) will help with the retention of top talent. A lot of companies say they have an amazing culture, but when taken further than face-value, hiring managers soon realize they have deeper-seeded issues than they first thought.

However, the first step to building an inclusive culture is simple – create a space where empathy, vulnerability and truthfulness are encouraged, then communicate your initiatives to existing and prospective employees.

Author, Samantha Buckenmaier

Executive compensation

So, how much should a CISO get paid? This is a question I get asked all the time and one that is very difficult to answer. The accurate answer to that question is anywhere between $180,000 and $5,000,000 per year depending on the job. More than any other executive job I have recruited for over the years, the CISO role is difficult to benchmark as there are SO many variables, including the size of the company, the size of the team, the value of the company's data, whether it's post-breach and whether it's a board-level role or not, to name but a few.

In this salary guide, I have attempted to give you a bracket to help guide your thinking, but it's important to point out that of all the salary guidance we've given you, this one is the most variable. What I can tell you is that in a smaller business you should be pushing for equity / stock options if that interests you and in a larger organization, there should be a substantial bonus component to your package linked, at least in part, to personal deliverables.

Navigating your way through negotiating an offer, or perhaps a pay rise, for a CISO role is a tricky thing. My plea to anyone reading this is: CALL US! Even if we don't know you, we are more than happy to help. Whether it's help with understanding if an offer is good enough, or if you're being underpaid, we can help you work it out. Drop our Vice President, Henry Yeomans a text on 312-859-7132. He will be very happy to hear from you and can arrange a time to speak at your convenience.

Author, Henry Yeomans

CYBERSECURITY SALARY GUIDE 2022

The elephant in the room

Our salary guide, in years past, has always split the US up into a grid pattern demarcating salary ranges by location. After some careful thought, we've decided to abandon this concept this year, in favor of a new model.

The issue, with defining salaries by location, is that salaries have levelled out across the country as a consequence of increased remote working. San Fran firms will pay San Fran prices in Ohio for a role they've been trying to fill for months, and over the last two years, that's had a domino effect on the price of hard-to-find skill sets, wherever they may be.

So, this year, we've tried to talk about ranges, with some detail for individual contributor positions regarding extra elements that would make a candidate more valuable.

As always, there are a million things that will dictate where a candidate sits on a range at any one time. Years of experience, location (it still plays a small part), competing offers, technical skill details etc.

This is impossible to fit onto one piece of paper, so this year we're going for simplicity and a promise that when it comes to building your team, we will do our utmost to provide context and success with our experience in the market.

Individual contributors

Role	Low End Base ($)	High End Base ($)	Expense Multipliers
Application / Product Security Engineer	170-190	200-220	• Dev exp • Cloud exp • Container exp
Application / Product Security Architect	180-200	210-230	• Cloud exp • Container exp • Dev exp
Cloud Security Engineer	180-200	210-230	• IaC exp • Container exp • Scripting/automation
Cloud Security Architect	180-200	210-230	• IaC exp • Container exp • Multi-cloud exp
Detection & Response Engineer	150-170	180-200	• Deep forensics exp • Cloud exp • Scripting/automation
GRC / Information Security Analyst	130-150	160-180	• Lead audit exp • CISSP/CISA/CISM • Cloud compliance
Information Security Architect	170-190	200-220	• Cloud compliance • CISSP/CISA/CISM
Enterprise Security Architect	180-200	210-230	• Breadth of knowledge
IAM Engineer	130-150	160-180	• Dev exp
Penetration Tester	140-160	170-190	• Web app focus • Dev exp • Cloud exp
Privacy Analyst	120-140	150-170	• Legal exp
Threat Researcher	160-180	200-220	• Cloud threat exp • Scripting/automation

Leadership

Role	Low End Base ($)	High End Base ($)
CISO / Chief Information Security Officer	250-300	350-400
Director / Head of Information Security	200-220	240-260
Manager / Director Application/Product Security	200-220	240-260
Manager / Director of Cloud Security	200-220	240-260
Manager / Director Security Operations	180-220	240-260
Manager / Director of GRC	160-180	200-220
Manager / Director IAM	170-190	200-220
Manager / Director Penetration Testing	170-190	200-220
Manager / Director Security Engineering	200-220	240-260
Manager / Director of Privacy	150-170	190-210

Never miss an opportunity, join our LinkedIn jobs group: https://www.linkedin.com/groups/12628234/

CLIENT TESTIMONIALS

James and the team provided an exceptional recruiting experience for United providing great candidates and managing the process effectively. I would recommend him and Stanton House to anybody looking to recruit.

Technology Recruitment PMO, United Airlines

Samantha is a true professional. Throughout my career, I've had the chance to work with many people in her field, and Samantha is far and away the best. I strongly recommend her as an excellent resource – she's thorough, honest, and a joy to work with.

Principal Consultant, ACA Aponix

Not all recruiting executives are cut from the same cloth. James's expertise in information security recruitment was beyond what I have experienced in past interactions within my career. To further that notion, his prompt and professional communication was nothing short of top notch. If you ever have the opportunity to work with James, you will be happy.

Director of Product Security, DataRobot

James sets the bar for excellence in acquiring talent in the extremely competitive cybersecurity market. His insights help companies find candidates that provide immediate impact, while aligning people in situations to unleash their full potential. James is a great advisor and strategic partner. I welcome opportunities to collaborate with him.

CISO, Hologic

Stanton House has been an invaluable resource in helping me find talent. They combine a deep understanding of the security landscape and market and how to sell our proposition to secure Grade A talent and have formed a true partnership with our talent team as a trusted adviser. I would highly recommend Stanton House for your recruitment.

CISO, East West Bank

Samantha and James 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, but they also 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 requirements, I would highly recommend engaging them.

Senior Technical Recruiter, Datto

Stanton House provided an invaluable service during the search for an application security resource. While our requirements were strict and standards were uncompromisingly high, the team was able to find the right fit for our organization on an accelerated schedule. Their knowledge of the application security space in particular and information security in general are true assets, and I would not hesitate to engage their services for future information security roles.

CISO, ErisX

Never miss an opportunity, join our LinkedIn jobs group: https://www.linkedin.com/groups/12628234/

CANDIDATE TESTIMONIALS

Maddison is great to work with and made my job search painless. She always laid out clear expectations for what was coming next. Even though my interviews took place during the heart of the holiday season, she was still quick to respond any time I had a question. I 100% would work with her again.

Security Architect, New York Presbyterian Hospital

Samantha is top-notch. She went above and beyond to help me throughout the whole process of joining a new team and made sure all my questions and concerns were handled. She made sure I was prepared for each step of the interview process, so I wasn't walking blind into any part of it. I would highly recommend her to other developers or information security professionals looking for a new role!

Application Security Engineer, Sectigo

James recruited me for a GRC role in late 2021. He and I had built rapport over time, and he came to understand what I sought in a role and what was a good fit for me. I thoroughly enjoyed working with him and am very happy with his efforts. He was supportive, personable and professional every step of the way.

Security Analyst, DRW

Samantha was absolutely amazing in referring me to a new position. Her drive and dedication to providing the best possible service is second to none. Samantha was extremely open and communicative throughout the entire process and took care to ensure absolute satisfaction. I would highly recommend her to anyone who needs her services in any capacity.

Senior Cloud Security Engineer, Frame.io

These are the things that were great about working with Maddison:

*1. **Communication.** She responded to my questions and requests for updates usually within 24 hours.*
*2. **Honesty & helpfulness.** My resume was a mess, I was still using the same template from college. She was able to guide me as to what the employer wanted to see and what looked better overall.*
*3. **Transparency & dedication.** Both of the above points tie into this point. Maddison explained the salary range, what the employer was looking for, and searched for an appropriate candidate that would be the best match. Maddison does her due diligence when looking for candidates, which drastically increases her success rate.*

When I was offered the position, Maddison seemed about as excited as I was. We gave each other a virtual high-five. The sheer amount of professionalism demonstrated by Maddison and Stanton House has left an everlasting impression on me. I will always forward her contact information to. my colleagues and peers.

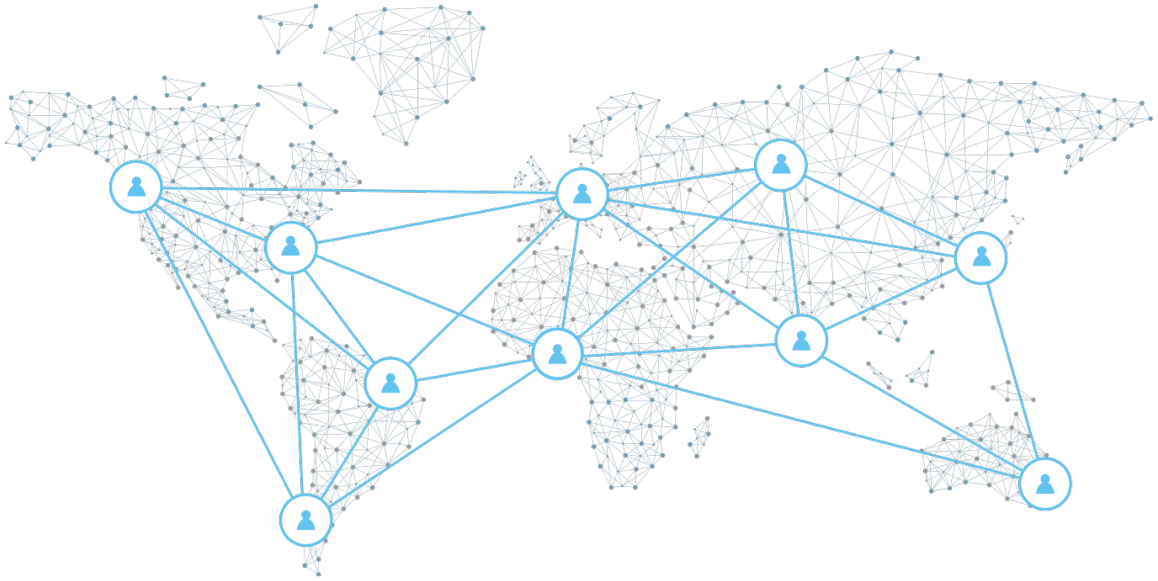
Enterprise Security Manager, Hinge

James is, without doubt, the most experienced and knowledgeable recruitment consultant I've met in the 15+ years I've been in the industry. He helped me in finding the right job and was there with me all the way through the onboarding process. He also followed up with me post onboarding until I felt comfortable working for my new employer. I have referred several colleagues and friends of mine in the industry to James.

GRC Manager, Zoll

I worked with James exclusively on a role for a fitness company in Austin, Texas. James truly separates himself from other recruiters in that he is a straight shooter and does what he says he will do. His communication skills are fantastic. He was very transparent about the entire hiring process and spent an extra hour of time preparing me for the interview. As an Infosec veteran, James uses his experience in the process to help all of his candidates. I can't recommend James enough and look forward to working with him on future roles.

Head of Information Security, F45 Training



About us

Stanton House is a global search consultancy and provider of specialist recruitment solutions within Cybersecurity and Cybersecurity Sales.

Since launching in 2010, we have established offices in the US, UK and Asia Pacific, and grown to $45M revenues, developing a customer-focused proposition that has laid the foundations for consistent success.

From our established office in Chicago, we help organizations across North America find exceptional Permanent and Contract talent from across the globe. Our joined-up international teams offer deep technical and local market expertize, and we take great pride in having an opinion on the topics that will shape the future of Cybersecurity.

Our unique set of values truly differentiates us from the competition and our Purpose of creating exceptional customer experiences is central to all that we do.

We believe in getting close to our customers and building trusting relationships with clients and candidates alike. This enables us to fully understand motivations, requirements and objectives and deliver exceptional outcomes.

sh INSIGHTS

Never miss an opportunity, join our LinkedIn jobs group: https://www.linkedin.com/groups/12628234/

CONTACT US
CONNECT WITH US

The more of our team you connect with on LinkedIn, the greater your chance of seeing our full breadth of opportunities.

Henry Yeomans
Vice President

+1 312 859 7132

Henry Yeomans

Henry.Yeomans@stantonhouse.com

James Warren
Executive Consultant

+1 733 782 0103

James Warren

James.Warren@stantonhouse.com

Samantha Buckenmaier
Consultant

+1 312 520-0374

Samantha Buckenmaier

Samantha.Buckenmaier@stantonhouse.com

Alek Ostrander
Associate Consultant

+1 312 859 7132

Alek Ostrander

Alek.Ostrander@stantonhouse.com

Maddison Cote
Recruiter

+1 773-848-1701

Maddison Cote

Maddison.Cote@stantonhouse.com

Grace Lysell
Associate Consultant

+1 312 465 3226

Grace Lysell

Grace.Lysell@stantonhouse.com