

Cyber Security in Focus 2023

Exploring the trends that impact security leaders



Table of contents

ABOUT THE RESEARCH

Cyber Security in Focus explained 03

PRIMARY RESEARCH INSIGHTS

Barriers to strategy execution 04

Building cyber security teams 05

Compensation and retention 06

The business perception of security 07

Technology investment trends 08

FEATURES

The role of the CISO in focus - Chris Castaldo 09

Talent and technology in focus - Haris Pylarinos 12

SALARY BENCHMARKING

Target salaries 2023 15



Guest Contributors



Chris Castaldo

Chief Information Security Officer
Crossbeam



Haris Pylarinos

Founder & CEO
Hack The Box



ABOUT THE RESEARCH

Cyber Security in Focus explained

Based on the responses of a high-quality sample of 60 CISOs and security leaders, our research shares insight into their views and core priorities as we look to the year ahead. This report examines several key themes, including the skills shortage, barriers to strategy execution, the perception of cyber security functions, and future technology investment.

The sampled respondents were sourced from Stott and May's professional network across EMEA and North America. In addition to our primary quantitative research and findings, this report includes qualitative interviews with leading industry professionals in the cyber security space.



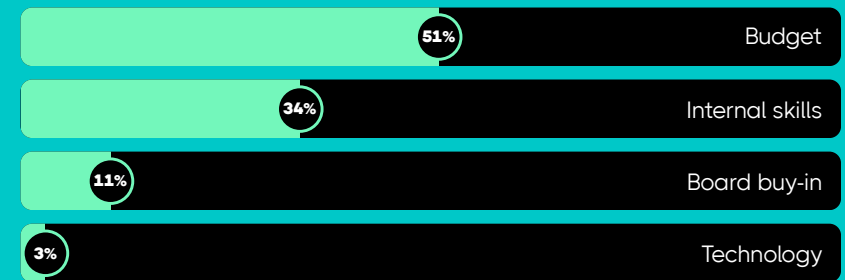
The state of the economy begins to drive a new narrative around strategy execution

For the first time in three years, budget has overtaken internal skills as the biggest inhibitor to strategy execution. 51% of today's security leaders cite this as their number one challenge, a 16% increase from last year's report. Given the state of the global economy, there will be a greater emphasis than ever on CISOs to ensure that their functions represent value for money. Security leaders will potentially place a heavy focus on consolidating tools and software investment with a renewed emphasis on getting more value from their existing providers, working to forge long-term vendor partnerships.

While a lack of internal skills may no longer be the number one obstacle CISOs face, it is still an issue that ranks highly on the whiteboard of priorities. A significant proportion of respondents (34%), down 9% year-on-year, highlighted internal skills as their biggest challenge. It should be noted that budget and headcount are intrinsically linked and not necessarily mutually exclusive. Addressing the internal skills gap will require CISOs to continue to focus on issues such as talent acquisition, security automation, and creating a culture of security across the business to meaningfully improve their overall security posture.

Board-level buy-in was seen as the largest obstacle by 11% of our sample audience, up 2% from the previous year, further highlighting the need for CISOs to truly understand and engage with the business. Only 2% of our sample saw technology as a headline barrier to strategy execution, down 11% year-on-year. As businesses remain cost-conscious throughout 2023, CISOs who understand the art of vendor and supplier management and are able to prioritize and leverage their influence across the business will be better placed to deliver on their strategic ambitions.

What do you believe is the biggest inhibitor to delivering on your cyber security strategy?



“

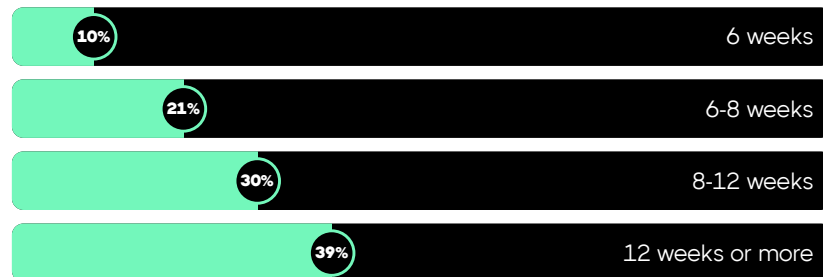
For the first time in three years, budget has overtaken internal skills as the biggest inhibitor to strategy execution.

A scarce candidate landscape calls for higher standards around talent acquisition

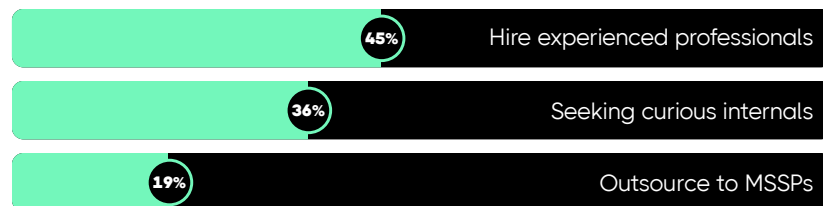
Do you face challenges in sourcing cyber security talent for your team/business?



How long does it take to fill cyber security positions in your organization?



Please rank the following statements according to which best sum up your approach to building cyber security teams.



Our data reveals that filling cyber security vacancies continues to be a massive pain point for security leaders. 66% of our sample highlighted that they face challenges in sourcing talent for their business.

There also continues to be interesting debate around how CISOs should go about acquiring and developing talent within their functions. A healthy proportion of our sample (36%) are prioritizing finding and upskilling curious internal talent from adjacent disciplines like IT engineering and upskilling them through intensive training programs. Interestingly, this figure is down 7% on last year as a higher proportion (45%) of respondents turn their attention to attracting experienced cyber security hires that can add value from day one.

It's worth noting that organization size is likely to have a bearing on the approach CISOs take to this issue. Large enterprise businesses are more likely to have the luxury of a larger internal talent pool with the necessary skill sets to transition into the security space.

The challenge of building internal capability is very real. This is possibly why 19% of security leaders have a preference to outsource more to MSSPs, a 14% increase year-on-year.

Access to the skills and predictable KPIs associated with external service providers are just two of the drivers fuelling the double-digit growth of the MSSP market.

One thing is for sure. Time-to-hire remains a key challenge for security leaders. According to our data, 69% of security vacancies are unfilled within 8 weeks, 39% of which continue to remain open after a 12-week period. It's no secret that hiring experienced individual contributors in the security space is competitive. Security leaders must continue to place a sharp focus on scoping out realistic role requirements, salary benchmarking, optimizing interview process design, and really articulating the unique value proposition of the role, team, and organization to candidates.

The cyber security talent market continues to remain largely recession-proof

Despite increased pressures on the CISO around cost control, our data reveals that security leaders believe that salary levels across the industry have increased over the last year. Almost half of our sample (47%) believe that salary levels have increased by more than 11% year-on-year. A further 31% see wage inflation sitting between 6 and 10%.

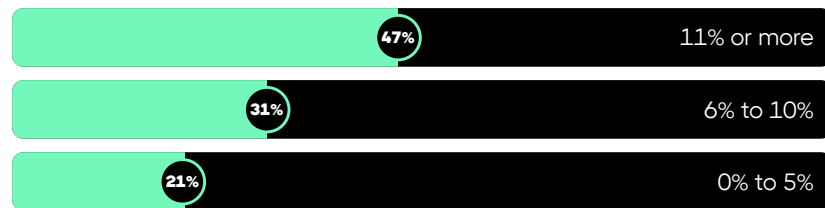
This increase in target salaries is likely to be underpinned by a combination of inflationary pressures and candidate availability for individual contributor roles. Particularly in disciplines like application and product security, detection and response, and cloud security.

Whilst it would seem that the cyber security talent market remains largely 'recession proof', the number of CISOs reporting an 11% plus increase in target salaries across the industry is actually down 7% year-on-year.

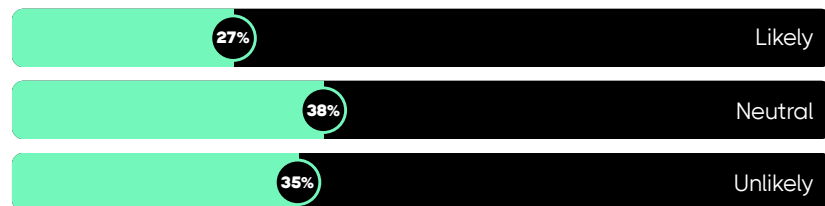
Similarly, the number of security leaders seeing a more modest wage growth of 0-5% is up 6% compared to 2022. This is some evidence to support the argument that wage growth may cool slightly in the backdrop of the current economy and short-term layoffs in big tech. However, the overarching trend points to a continued rise in salary expectations from security candidates.

Continued high demand for security talent also creates a retention challenge for CISOs. As such, our research evaluated the sentiment of security leaders towards counter-offering existing team members at the point of resignation. Our findings reveal that the highest percentage of respondents (38%) were neutral towards the issue (scored 2-3 on the propensity scale). A further 27% demonstrated a higher inclination to counteroffer (scored 4-5 on the propensity scale). Finally, 35% of security leaders were more resistant to getting involved in counter offers (scored 0-1 on the propensity scale). CISOs need to continue to be mindful of the risk of counter offers as part of their recruitment processes.

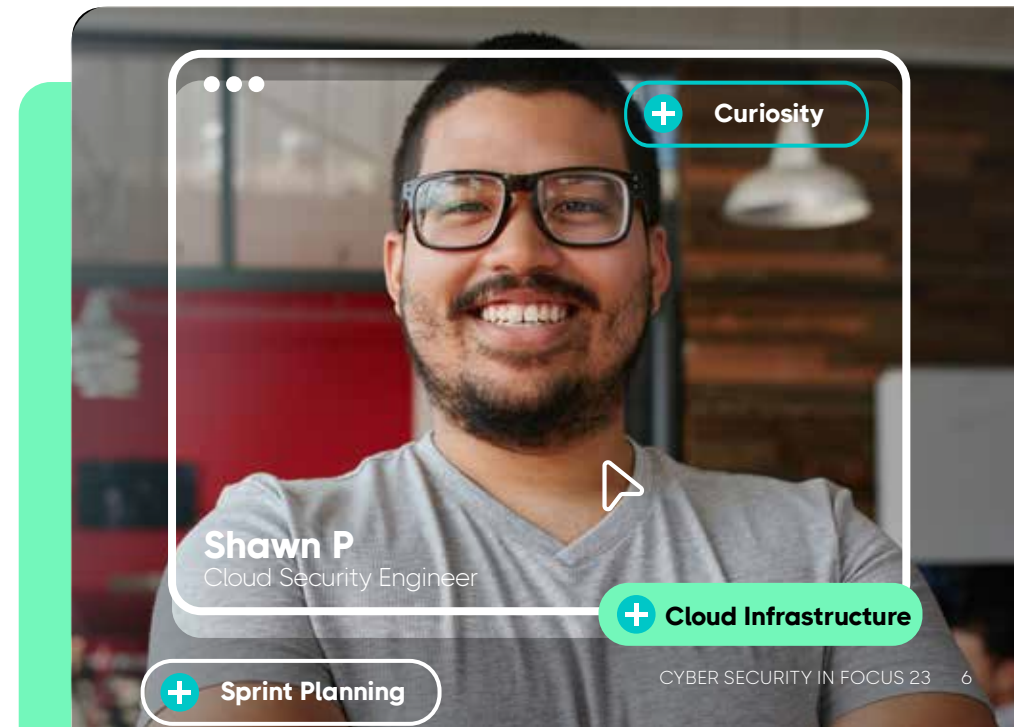
In your view, what % change in salaries has the security industry seen in the last year?



How likely are you to counteroffer a team member?

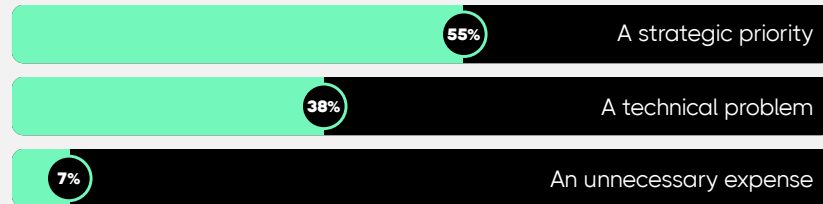


Based on aggregated results from a propensity scale, ranging from 0-5. 0-1 comprises the 'Unlikely' score, 2-3 comprises the 'Neutral' score, and 4-5 comprises the 'Likely' score.



The focus turns to positioning security impact in business terms

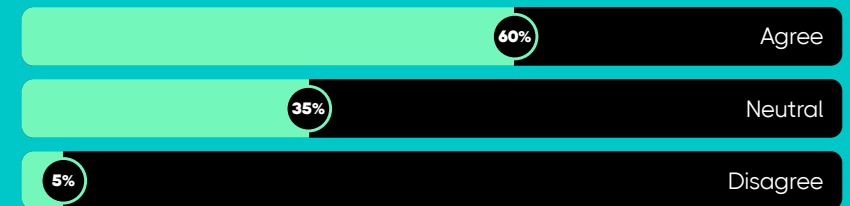
How does your business perceive cyber security?



It's fair to say that high-profile data breaches, increasing regulatory complexity, and more educated customers have significantly increased the profile of security functions over recent years. It's cemented its place as a board-level issue. However, CISOs need to continue to be conscious of the importance of developing a culture of security across the business and translating security risk in terms that align with the broader business strategy. 55% of our sample cited that their business perceives security as a strategic priority. This is a material decrease of 25% from the year before when the pandemic brought the security function to the very forefront of business operations. As perception and awareness of the security function drop back towards pre-pandemic levels, CISOs must continue to place a sharp focus on articulating the business impact of key initiatives.

The opportunity for CISOs to contribute towards the value proposition of the business remains. That's according to 60% of our respondents, who outlined that their business feels the security function improves the overall proposition to customers. In fact, only 5% of security leaders from our sample stated it has no major impact. The size and shape of the opportunity for CISOs to package up the value of the security function will vary from industry to industry. CISOs from SaaS software businesses or highly regulated organizations will arguably find this easier. Whilst the CISO role will always be highly operational in nature, it's important for security leaders to continue to seek out opportunities to positively influence customer demand.

Do you agree with the following statement: 'My business feels that the cyber security function improves the overall proposition to customers'?



Based on aggregated results from a propensity scale, ranging from 0-5. 0-1 comprises the 'Disagree' score, 2-3 comprises the 'Neutral' score, and 4-5 comprises the 'Agree' score.

REPORTING LINES IN FOCUS

What is the ideal reporting line for a **Chief Information Security Officer**?



Strategic investment continues in cyber security but there's little room for experimentation

There has been a trend towards businesses making cyber security their priority technology investment area in recent years. Many of these projects and investments are strategic, long-term, and tightly aligned to the broader digital transformation strategy.

Our findings demonstrate a continued appetite to invest in cyber, with 56% of CISOs reporting that they expect to see their budgets increase in 2023. 29% expect to do more with the same, and only 15% anticipate having to find cost efficiencies in their budget.

But the acceleration towards digital transformation is creating challenges for some CISOs as they seek to implement the necessary controls to defend their critical assets. 47% of security leaders in our sample reported that they felt cyber security investment is struggling to keep pace with digital business.

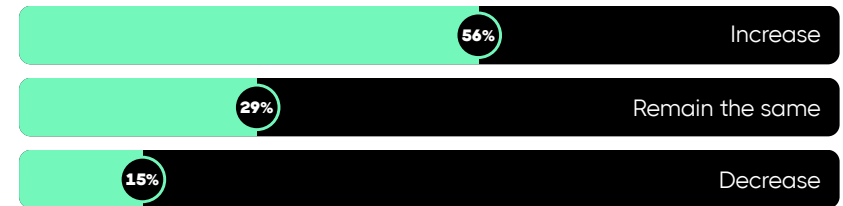
As the rate of change continues, CISOs need to double down on efforts to drive meaningful alignment with key stakeholders. Prioritization should be given to translating risk in business terms and doubling down on efforts to support collaboration between developers and security teams.

CISOs will always prioritize their technology investment in the areas that will have the biggest impact on their organizations' overall security posture. Our findings suggest that cloud security is the number one focus area for security leaders this year; 25% of CISOs are making this their priority.

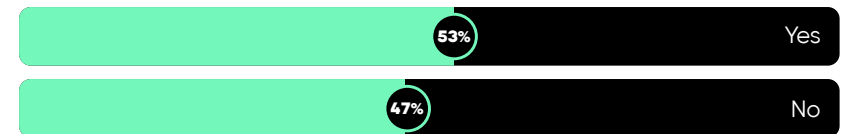
The increasing number of businesses moving to the cloud for increased flexibility, scalability, and cost-effectiveness is leading to a growing number of security concerns for the CISO. Security leaders need to defend a larger attack surface and ensure data in the cloud is properly secured and protected while adhering to regulatory standards.

The issue of protecting sensitive data is also driving significant investment in identity access management, with 20% of our respondents focusing on projects in this space. Based on qualitative feedback, it's unlikely that CISOs will introduce a lot of experimental or unproven technologies into their budgets this year.

Select the most applicable statement for your cyber security function. "My budget for 2023 will..."



Is investment in cyber security keeping pace with the drive towards digital business?



What would be your #1 technology investment area in the next 12 months?



The role of the CISO in focus

Chris Castaldo - CISO
Crossbeam



Chris Castaldo is an industry-recognized CISO with over 20 years of experience in cyber security. He is currently the CISO at Crossbeam, the world's first and most powerful partner ecosystem platform. It acts as a data escrow service that finds overlapping customers and prospects with your partners while keeping the rest of your data private and secure. He is also the author of *Start-up Secure: Baking Cybersecurity into your Company from Founding to Exit*. Chris is also a Fellow at the National Security Institute - George Mason University's Antonin Scalia Law School.

Q. What do you see as the key challenges sitting in front of the CISO community in 2023?

I definitely think that the economy is going to be at the top of everybody's mind. CISOs in startups that are very burn conscious may have a slightly different perspective to those that are in publicly traded companies, who will still have reporting requirements, but the economy is going to be a key challenge for everyone. If you're a CISO in a B2B SaaS company and your sales team is not hitting the numbers every quarter, then you're unlikely to be procuring new security tools, for example.

This will ultimately culminate in CISOs needing to do more with less and ensuring that their security functions represent good value for money. You're probably going to see some of those 'nice to have' elements dropping off the security roadmap. The focus will be on the 'need to haves'. If you're in a regulated industry, for example, do you need to have this tool going into the year? Do you need that FTE, or can we get by one more calendar year without that hire or without that tool? Is that a risk we can accept? That being said, I think that narrative offers lots of

opportunities for CISOs in 2023. There is a real opportunity to shine in the role. A large proportion of our job as CISOs is operational. It's about managing risk for the business. So this will be the year that CISOs really earn their keep in that regard. Not everybody knows what an EDR is or DSPM, or CSPM, for example, so that's your job as a CISO to demystify these things and make sure the business understands the risks that you're telling them to accept.

Q. How can the security function position itself as an enabler rather than an obstacle to innovation and growth?

I think it's really going to come down to CISOs embedding themselves into the business and making sure that they fully understand all of the operational components. That's one of the biggest hurdles that CISOs face. They often come in and try to solve things from a control or technical level when it really has to be flipped on its head and come from the business side. Whether you're in a B2B or B2C company, you need to understand exactly how your sales and revenue team works and why people buy your product in the first place. You need to earn that spot by showing

how well you understand the business and how well you can operate cross-functionally.

Coming back to that theme of doing more with less and being that enabler. Look for opportunities to align with the engineering team and potentially make use of their headcount. Is there someone that can spend a quarter of their time a month working on engineering security problems? It could be a useful alternative to simply saying we can't do that because we don't have the budget for a principal security engineer.

Equally, it's important to remember that as a CISO, you have an essential role to play in the growth of the business. Security is becoming more and more important to the value proposition. If you did a survey of CISOs in B2B SaaS businesses, for example, I would be shocked if they were not getting security questions from their customers in the pre-sales process. I am yet to see a deal in any of the companies that I've worked at over the last 5-years that does not have some type of security question from sales prospects. Whether that's 'do you have any security at all,' through to 'here's a spreadsheet with 1,600 security



questions to fill out'. It is so critical now to get that right. Particularly for SaaS companies, because you're selling the product multiple times to multiple personas in multiple accounts, which means that ensuring the security narrative is tight, targeted, and well-packaged throughout the sales cycle will be hugely commercially valuable.

Q. What are the major barriers that you see CISOs struggling with when it comes to executing their security roadmaps?

Not understanding the business. That's the main barrier. Everyone that I talk to that's trying to implement some new tool or a new process or new policy and meets resistance typically hasn't spent enough time trying to understand what those stakeholders really care about and tailoring that message to them. For example, there should be no question that every company on the planet needs EDR. It should come with the cost of doing business. But I still hear from peers that are struggling to buy and deploy EDR in their environment. To me, that comes down to the blocker of not understanding the business. It's really not the job of individual stakeholders to understand what EDR is. It's your job to translate it in the context of their role and what they care about. They need to understand the implications of a breach. What does it mean for their ability to close deals? What does it mean for a potential IPO? This is part of the tooling that de-risks that for the business.

This whole business understanding piece unlocks a lot of the other common elements that CISOs are challenged with on the execution side. Lack of budget. Inability to acquire the right level of internal skills. All of these things are linked to understanding the business and shaping a strong narrative that resonates with key stakeholders.

Q. How do you see the role of the CISO evolving over the next 5 years?

I would say the role will continue to be a highly business-focused position. The engineering side, I think, will come along with it. I know plenty of amazing CISOs with no engineering background that are leading functions at Fortune 100 companies really successfully. So I don't think having an engineering background or a business background is necessarily a prerequisite, but you need to have one or the other. Then it's about finding that balance or blend of the two over time.

I also see regulatory understanding as being a really important area for CISOs both now and over the next 5 years. You don't need to be a lawyer. Most CISOs will have a general counsel to lean on, but having the ability to really dig into those critical operational components of the business will be a key skill, given the complexity we face.

Q. What performance metrics do you think are most useful to use when articulating the progress of the security function to the board?

I'm of the opinion that CISOs should forget about KPIs and metrics; this is an operational role. The legal team doesn't present metrics, the people ops team doesn't present metrics, and neither should you. You're an operational function of the business. You're managing, reducing, avoiding, and accepting risk for the company. I really think we've done ourselves a disservice to want to push some type of metric in order to compare ourselves to sales, engineering, or IT. Ultimately, their performance is easy to measure; you either hit your sales numbers or you didn't. It's very black and white.

Typically, when I present to boards, I focus on the operational components. What have we done? What has been accomplished? How are we impacting the business in a positive way? But outlining how many phishing emails we have blocked doesn't mean anything to a board member. Equally, outlining the number of detections we got in our EDR that were blocked isn't that useful either. We're going to be attacked all the time; there will always be vulnerabilities in software that's built by humans. I just don't think presenting that information is a useful way to use board members' time. They are there to govern the business. Use those minutes wisely. Instead, focus on how we're progressing on the roadmap and the narrative of the function's direction of travel.



Lack of budget. Inability to acquire the right level of internal skills. All of these things are linked to understanding the business and shaping a strong narrative that resonates with key stakeholders.



Q. What do you think will be the number one technology investment area for CISOs over the next 12 months?

It's quite hard to come up with one single answer. On the enterprise side, there will be investment in big-ticket items like EDR and DSPM; the latter is a new space. I describe it as EDR but for your data. We also talked earlier about security having a positive impact on the value proposition, and I can certainly see more tools like SafeBase popping up. It's a product that centralizes security information for customers and prospects, enabling sales cycles to be faster, more valuable, and much more streamlined.

I don't think we are going to see massive investment into newer technology. Again, with the economic situation, there won't be much experimentation or room for 'nice to haves'. Instead, CISOs are going to be focused on investing in the things that keep the lights on and keep the right level of compliance.


Automation is, however, a space that I am definitely excited about. There's a lot happening. We initially saw it with SOAR, and that's evolving into new technology popping up like Tines and Torq. It's a really interesting area. I think the concept of low/no-code security-focused automation will really resonate and have an impact. There's possibly an opportunity for CISOs to do a bit of horse-trading here where you can't quite get that FTE, but you might be able to allocate some budget to find an automation tool to do some of those tasks. It'll also be useful to startups who are buying all these toolsets that typically don't integrate and can't connect, and you need something that will bring it all together. Security automation was already trending, but I expect in the economic environment, there will be a renewed focus on doing more with less.

Q. What advice do you have for CISOs that are being asked to do more with the same budget?

My advice is to make it work. That's what we are here for as CISOs. The rest of the C-suite is experiencing the same thing; it's not unique to us. Everyone is being asked to do the same thing: triple-check if you need that headcount and quadruple-check if you need to buy that software.





If you've already frozen headcount, then the next step is to look at software spend. You could assess whether your licenses for GRC and third-party risk tools are really that necessary. Bug bounty platforms might not be the best use of your budget, so there are spaces for some trimming from a budget perspective. You have options, but of course, you can't cut the cost of licenses you don't have.

Equally, CISOs need to look at getting more value from their existing software providers and really work with them to forge a partnership rather than a transaction. Perhaps also looking towards startups that are willing to give a little more on the services side. I'd say there's definitely an art to vendor or supplier management in these times of cost control.



Oscar J
CISO

Candidate shortlist

	Sarah W Security Architect	★ 4.8
	Joshua K Security Architect	★ 4.7
	Jane P Security Architect	★ 4.8
	Edward S Security Architect	★ 4.6



Talent & technology in focus

Haris Pylarinos - Founder & CEO
Hack The Box



Haris Pylarinos is an experienced professional in Networking and Software Architecture. He is skilled in systems engineering due to his many years of experience as a SysAdmin in the Maritime and is a Security Expert with over 15 years of experience in the IT and Cyber Security industry. In 2017 he founded Hack The Box, a leading online fully-gamified cyber security upskilling, certification, and talent assessment platform that enables individuals, businesses, government institutions, and universities to sharpen their offensive and defensive security expertise through fully guided and exploratory learning solutions addressing red, blue, and purple teams. Having recently secured a Series B investment of \$55 million, the company has scaled to 180+ employees and over 1.7 million platform members since launch.

Q. What are the top challenges associated with building a high-performing security function?

The challenge I often see that stands in the way of high-performing security functions is the ability to stay outward looking and ensure that internal skills stay up to date. You can hire the best security professionals out there with field experience, but the problem is that this knowledge can degrade over time because cyber security is evolving at such a rapid pace. You need to be conscious that when security professionals join your team, they become purely focused on your organization. That means they miss a lot of experience and context they would otherwise gain if they were, say, working for a vendor providing services to multiple organizations. As a result, we are seeing the higher-performing security functions invest more heavily and more consistently in upskilling and reskilling. Security leaders could take a few immediate actions to tackle this challenge. Investing in an upskilling and reskilling platform would be a positive start. You could also consider hosting internal competitions based on fictional scenarios, mimicking an incident to keep your team sharp and aware. Another obvious challenge for CISOs is the basic fact that there aren't enough experienced professionals out there

to fill internal positions. The current global cyber security shortage stands at 3.4 million. Many organizations are responding to that challenge by reskilling people. They may target talent from similar functions with adjacent skill sets. For example, you could take an IT engineer and fast-track them through cyber security training to allow you to fill tier-one SOC Analyst roles or possibly even Junior Penetration Testing roles.

This is a smart move in the current climate if you can't hire all the cyber security professionals you need. CISOs should attempt to find a good balance between making experienced hires, where there is candidate availability, and having a plan for those IT engineers who have an appetite to upskill and evolve into cyber security roles.

Q. What changes do you see in the attack landscape this year, and how should CISOs respond to those trends?

Undeniably ransomware is still here. As long as there is a financial incentive for cyber criminals, ransomware will continue to get more and more sophisticated. Cloud also remains a focus. While very secure in terms of infrastructure, you can, as an organization, be insecure based on your

configuration. Some unique attack methods span from the out-of-the-box functionality provided by vendors. I see the risk rising in the cloud overall; the more we migrate, the more cybercriminals will definitely target it. IoT also presents lots of threats. Things like smart offices, smart lamps, and meeting rooms will all be targeted. They already are, and this will continue because the more we make our lives easier through automation, the more we expose ourselves to highly creative cyber criminals. The more we merge the physical world with the virtual, the more risk there is.

Given the evolution of the attack landscape, the number one thing I would focus on as a CISO is employee awareness. Around 80% of all attacks start with a phishing attempt. Even with 2FA, if employees are not fully aware of the nature of cybersecurity threats and how they can jeopardize organizational security, the risk is still there.

I've heard stories of breaches where the hacker bypassed the 2FA simply by relentlessly spamming it. After countless requests, eventually, internal employees will accept a notification just to make it stop. So internal understanding and security awareness are key. Taking that a step further, when looking at the security team, it's essential that everyone, from Security Engineers to SOC analysts, have at least some knowledge of offensive security and how an attacker operates. After all, the best person to tell you how to secure your house from a thief is a thief. Offensive security knowledge is necessary; we must think and act like attackers to better protect ourselves.

Q. How can CISOs improve internal security awareness initiatives and drive a higher level of maturity when it comes to security thinking?

First of all, it needs to start from the top. If the issue of security is taken seriously at a board level, the rest will follow. If it's treated as a compliance exercise, it won't be seen as a priority for the organization or the people working within it. So that's point number one around security awareness - ensure you have a high level of executive sponsorship.

CISOs could raise visibility around their security program by gamifying the experience for end-users; it's about making security fun, relevant, and engaging. In my last company, we decided to send phishing attempts internally to our employees as a security awareness exercise. The first time we ran this exercise, lots of people took the bait. The second time, more people remembered it and became cautious and more likely to report external phishing attempts. So the takeaway is to use gamification and role-play to make security principles more accessible to the everyday user. Don't pass it off as a mandatory awareness course;

that's not the way. Articulate why security is a serious issue, provide some analogies, and use real-world examples of breaches so that they understand that cyber security attackers are not just targeting huge organizations; they're attacking everyone. Users need to question and challenge everything that is presented to them - whether in the physical world or the virtual one.

Finally, look for opportunities to make the security function more visible. This could revolve around messaging and internal communications and go all the way through to having an internal security brand. I've seen companies engage with end-users and increase visibility by handing out branded security swag. I'm not sure how scalable that is, but it's another example of security leaders becoming more creative about how they engage with the broader business.

Q. How far along the maturity curve do you think CISOs are with automating areas like security operations?

I think there will ultimately always be limitations around just how far we can go with security automation. For example, there are often multiple ways to remediate a vulnerability, and not all remediations work in the same environments in the same way. You've also got to consider the business impact of any remediation, which will vary from organization to organization. I wouldn't trust a computer to patch everything for me; I would want a human to review it and manually test it afterward. So at the moment, there are limitations to where this automation journey can go.

However, I do see lots of value in automation. Vulnerability scanning, for example, is amazing and saves a lot of time, but you'll still need a person to classify what's critical and what's not. Still, in principle, the more you automate, save

time, and eliminate legwork, the more you can prioritize your resources on higher-value tasks.

Q. In terms of personal development in the security space, what topic areas do you see the most demand for?

We naturally see a lot of demand around cloud security. It's a hot topic and highly relevant to security professionals right now. I'd say there's also emerging interest in AI hacking, which is probably more future-focused. Incident response and threat hunting will also continue to be key topic areas due to the importance of these roles both now and in the future. If we don't seek out threats, they will only multiply.



CISOs could raise visibility around their security program by gamifying the experience for end-users; it's about making security fun, relevant, and engaging.



Q. In your view, what security roles will be hardest to fill this year, and why?

I think it's important to define what we mean by 'hardest to fill.' Are we talking about areas where we have a real acute shortage of candidates? Or the most complex hire you will make for your security function?

If you are looking at it from a candidate scarcity perspective, then Penetration Testers will be fairly high on the list of tough positions to recruit for. It's a difficult role and requires a lot of dedication. It's a way of living - not just your profession. You don't finish your job at 5 pm; you continue to think about your work and study more. Those types of individuals are hard to find. It's also not always seen as an easy discipline to break into. However, this is changing as crowdsourced bug bounty platforms provide an entry point to develop experience and build credibility.

If we move away from the candidate scarcity debate and drill into the importance of making the right hire, then the CISO position really needs to come into the spotlight. It's arguably the most important hire you will make for a security function, which by default makes it an extremely difficult role to fill. There are more CISO candidates in the market, but they will come in different shapes and sizes, so finding the right fit for your organization is key. Ultimately, you will be ten times more careful hiring a CISO than an individual contributor.

Q. What tips do you have for CISOs to manage the impact of candidate scarcity?

First of all, we have to rethink the way we hire. We should move away from a traditional hiring model that focuses solely on university degrees and specific certifications. I

know many very skilled individuals and professionals who don't have any of the above, but they are very good at what they do. So we really need to look at how we assess candidates in this industry. For example, you could send them through assessment tests, have them do a demo, or have them prove their skills through a practical exercise. I don't mind how it's done, but relying solely on a university degree will actually sabotage your hiring efforts because it's such a scarce candidate environment.

Another obvious coping mechanism we've already discussed is building and growing your own security talent. Hire IT Engineers and upskill them through an intensive 3-month training program. Trust me; if you do it right, you'll get Cyber Security Engineers on the other side. Automation is obviously another option to do more with less, but I feel lots of organizations have already realized as much of the efficiencies that they are going to see in this space.

In this new world of work, there is also an opportunity to broaden the search radius for scarce skill sets. Even before the pandemic, our policy was to hire talent from wherever the talent is. It was less about location and more about candidate quality for us. If you can create a global talent pool, it is better than having a local one. The only thing to consider is depending on the location, there may be timezone constraints. This could cause collaboration challenges, for example, so individual CISOs must be mindful of that. But if we're talking about individual contributors who can deliver their work on their own timeline, it's excellent. Clearly, there are additional security considerations with remote work, but at the end of the day, you'll be able to attract top cyber security talent on a global scale by hiring remotely rather than just relying on a local talent pool.

Gerry Q
VP Security

Candidate shortlist

	Steve J Penetration Tester	★ 4.6
	Eric B Penetration Tester	★ 4.6
	Sue P Penetration Tester	★ 4.8
	Mary S Penetration Tester	★ 4.9

Salary benchmarking 2023

Manager/Executive Level	US - West Coast (\$)			US - East Coast (\$)			UK&I (£)		
	Low	Median	High	Low	Median	High	Low	Median	High
CISO	230,000	325,000	550,000	240,000	300,000	500,000	130,000	200,000	350,000
Deputy CISO/BISO	200,000	260,000	315,000	220,000	250,000	350,000	110,000	150,000	200,000
Head of Information Security (Early Stage)	200,000	230,000	300,000	200,000	240,000	300,000	120,000	150,000	170,000
Head of Information Security Risk	215,000	250,000	370,000	220,000	250,000	350,000	110,000	130,000	160,000
Director Security Engineering	250,000	300,000	350,000	220,000	280,000	350,000	100,000	130,000	180,000
Director Application Security	225,000	275,000	325,000	220,000	280,000	320,000	115,000	135,000	200,000
Director Incident Response & Security Assurance	180,000	230,000	300,000	175,000	230,000	280,000	100,000	130,000	170,000
Director Security Operations & Threat Management	190,000	240,000	300,000	180,000	240,000	280,000	105,000	120,000	160,000
Director Identity & Access Management	175,000	225,000	280,000	180,000	230,000	300,000	100,000	115,000	140,000
Application Security Manager	180,000	220,000	275,000	170,000	220,000	250,000	120,000	130,000	160,000
Product Security Manager	180,000	220,000	275,000	180,000	220,000	250,000	90,000	100,000	125,000
Cloud Security Manager	190,000	230,000	275,000	180,000	220,000	250,000	100,000	120,000	140,000
Detection and Response Manager	190,000	230,000	270,000	190,000	225,000	260,000	100,000	120,000	140,000
Offensive Security Manager	160,000	190,000	225,000	160,000	180,000	220,000	100,000	115,000	130,000
Senior Manager, Information Security Risk	215,000	235,000	310,000	210,000	225,000	280,000	95,000	100,000	120,000
Security Operations Manager	150,000	190,000	250,000	160,000	200,000	250,000	80,000	95,000	125,000
Security Architecture	Low	Median	High	Low	Median	High	Low	Median	High
Chief Security Architect	225,000	255,000	350,000	220,000	260,000	320,000	95,000	130,000	180,000
Application Security Architect	200,000	225,000	315,000	190,000	220,000	300,000	100,000	110,000	140,000
Infrastructure Security Architect	190,000	235,000	295,000	190,000	230,000	290,000	80,000	95,000	120,000
Product Security Architect	205,000	250,000	295,000	190,000	240,000	280,000	95,000	100,000	135,000
Network Security Architect	180,000	240,000	270,000	170,000	220,000	240,000	60,000	75,000	110,000
Enterprise Security Architect	225,000	260,000	320,000	200,000	240,000	280,000	80,000	100,000	130,000
DevSecOps Architect	200,000	255,000	310,000	200,000	250,000	290,000	100,000	125,000	140,000
Cloud Security Architect	200,000	250,000	305,000	200,000	240,000	285,000	70,000	95,000	140,000
GRC Information Security Architect	200,000	255,000	290,000	190,000	230,000	280,000	60,000	80,000	130,000

Salary benchmarking 2023

Security Engineering	Low	Median	High	Low	Median	High	Low	Median	High
Security Automation Engineer	160,000	200,000	240,000	160,000	200,000	240,000	90,000	110,000	140,000
DevSecOps Engineer	170,000	210,000	240,000	160,000	210,000	240,000	95,000	130,000	140,000
Detection Engineer	160,000	200,000	235,000	160,000	200,000	240,000	65,000	75,000	90,000
Security Data Engineer	160,000	200,000	235,000	160,000	195,000	225,000	65,000	75,000	90,000
Corporate Security Engineer	140,000	180,000	225,000	130,000	165,000	215,000	55,000	70,000	90,000
SIEM Engineer	130,000	170,000	220,000	120,000	160,000	210,000	90,000	100,000	120,000
Product Security Engineer	170,000	200,000	240,000	160,000	200,000	230,000	90,000	115,000	130,000
IAM Engineer	120,000	165,000	225,000	125,000	160,000	220,000	45,000	75,000	115,000
Cyber Threat Hunter	140,000	165,000	185,000	140,000	165,000	190,000	60,000	80,000	115,000
Threat & Vulnerability Engineer	140,000	170,000	200,000	130,000	170,000	190,000	55,000	80,000	100,000
Penetration Tester	120,000	165,000	200,000	125,000	160,000	200,000	50,000	90,000	130,000
Software Security Engineer	170,000	200,000	240,000	165,000	200,000	250,000	70,000	80,000	115,000
Cloud Security Engineer	170,000	200,000	240,000	160,000	190,000	240,000	55,000	90,000	120,000
Application Security Engineer	170,000	200,000	240,000	160,000	200,000	240,000	80,000	100,000	120,000
Incident Response Engineer	160,000	185,000	225,000	160,000	180,000	210,000	50,000	85,000	115,000

About Stott and May

Founded in 2009 Stott and May are a professional search firm with a passion for helping leaders achieve complete confidence that they have hired the right talent, first time in fiercely competitive markets. We believe you should never have to make the choice between quality of candidate and time-to-hire. As a result, our business has been founded on the principle of offering a premier standard of search service delivered in vastly accelerated timescales. Because after all this is about more than just recruitment, it's about turning your business vision into reality.

stottandmay.com



More on [Hack The Box](#)

More on [Crossbeam](#)

