Cobalt
Pentest as a Service

THE **STATE** OF **PENTESTING** 2023

Contents

Cobalt

Executive Summary

Disruption, transformation, volatility – whichever keyword fits your style, it all points to one fact: change is the constant security teams have had to live by for years. In 2020, the pandemic stress-tested their ability to keep data secure during the global WFH movement. In 2021 and 2022, The Great Resignation exacerbated talent shortages and slowed down vulnerability management. And this year, business pivots, restructures, and hiring freezes dominate the news and security teams' minds – how do they keep assets secure with fewer resources and more responsibilities?

For our 5th edition of ***The State of Pentesting***, we explore three key areas:

- The most prevalent security vulnerabilities in over 3,100 pentests completed in 2022 with the help of the Cobalt Core – our community of highly skilled and vetted pentesters;
- How macroeconomic shifts are affecting organizations' security standards across the US and EMEA, and;
- How teams can avoid business disruptions, extract more value from their pentests, and maximize ROI;

Top 5 most prevalent security issues

1 Stored Cross-Site Scripting (XSS)
2 Outdated Software Versions
3 Insecure Direct Object References (IDOR)
4 Lack of Security Headers
5 Insecure Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Protocols

Most Common Findings with Critical Severity

1 SQL Injection
2 Remote Code Execution
3 Using Default Credentials

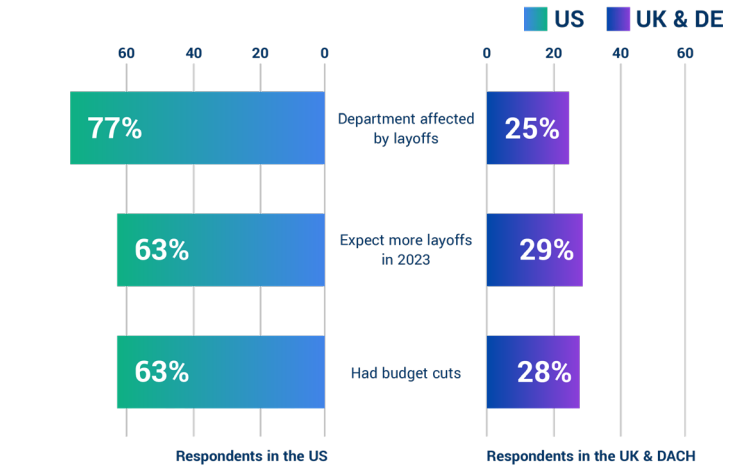
Most Common Findings with High Severity

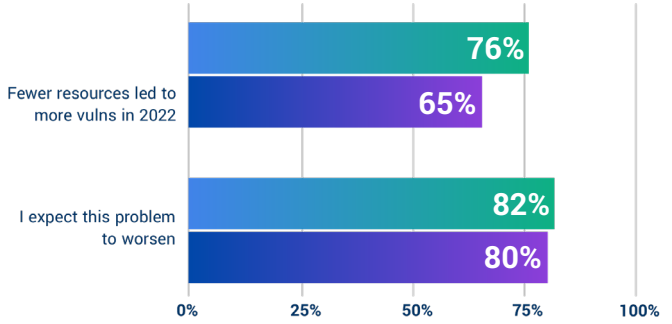
1 Stored Cross-Site Scripting
2 Insecure Direct Object References (IDOR)
3 SQL Injection

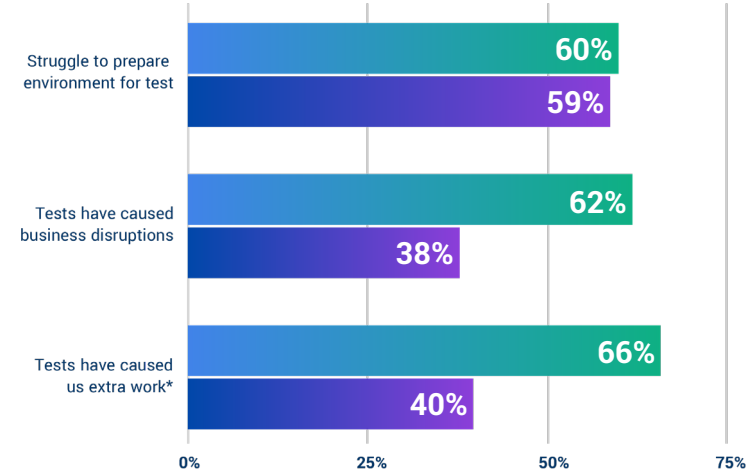
Most Common Findings with High Severity

1 Stored Cross-Site Scripting
2 Insecure Direct Object References (IDOR)
3 Reflected Cross-Site Scripting

A note on severity levels: Cobalt uses the OWASP Risk Rating methodology while calculating the severity of any reported finding. Where the application resides, what level of privilege is required, requirement for user interaction, business impact and many other factors which vary business to business determine a finding's exploit likelihood and impact. Hence, some findings will appear as the most common flaws for multiple risk levels.







* Not including fixing discovered vulnerabilities, but unexpected "clean-up" tasks after the test.

Cobalt

PART 1

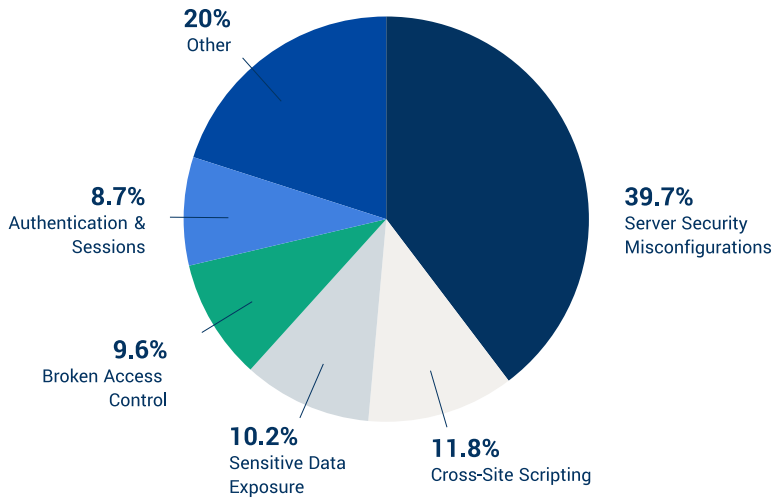
XSS, IDOR, or SQL Injection — What's Lurking in Your Systems?

The most common vulnerabilities from over 3,100 pentests.

Server Security Misconfigurations continue to dominate.

This year, nearly 40% of our findings were related to Server Security Misconfigurations, with the most common issues being Lack of Security Headers, Insecure Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Cipher Suites, and Fingerprinting/Banner Disclosure.

Other vulnerabilities we saw spanned across the following categories: Cross-Site Scripting (nearly 12% of total findings), Sensitive Data Exposure (10%), Broken Access Control (10%), and Authentication & Sessions (9%).



In fact, **Stored Cross-Site Scripting (XSS) was our most common finding for 2022**, with the vast majority of discovered flaws earning a Medium or High severity level. Any feature that allows user input can be vulnerable, because it gives attackers an opportunity to inject and store malicious content into web applications. To prevent this, Cobalt recommends treating all user-supplied input as untrusted data and accepting input in select locations. We also recommend using a well-known and secure encoding API for input and output encoding, such as the OWASP ESAPI.

Another common high-impact flaw are Insecure Direct Object References (IDOR), with Cobalt Core pentesters marking 85% as either Critical, High, or Medium severity. This vulnerability can give access to resources via user-supplied input, where attackers bypass authorization by modifying a value of a parameter that points directly to an object in your database. Use per-user or per-session indirect object references. Each time your application uses a direct object reference from an untrusted source, it should also make an access control check to ensure that the user is authorized to access the requested object.

Finally, a vulnerability we saw more of in 2022 compared to previous years is the use of **Outdated Software Versions**. When it takes dozens of apps and programs to keep a website, product, or business running, staying on top of updates for all of them can quickly spiral out of control. Despite this vulnerability having a reputation as a low-risk issue, our pentesters marked it as Critical, High, or Medium severity 14% of the time.

Most common findings per vulnerability category.

Cross-Site Scripting

- Stored XSS
- Reflected XSS

Sensitive Data Exposure

- Visible Detailed Error/Debug Page
- Disclosure of Known Public Information
- Sensitive Token in URL

Broken Access Control

- Insecure Direct Object References (IDOR)
- Server-Side Request Forgery
- Username/Email enumeration

Authentication & Sessions

- Failure to Invalidate Sessions
- Privilege Escalation
- Concurrent Logins

The top 10 vulnerabilities in the last two years.

2021

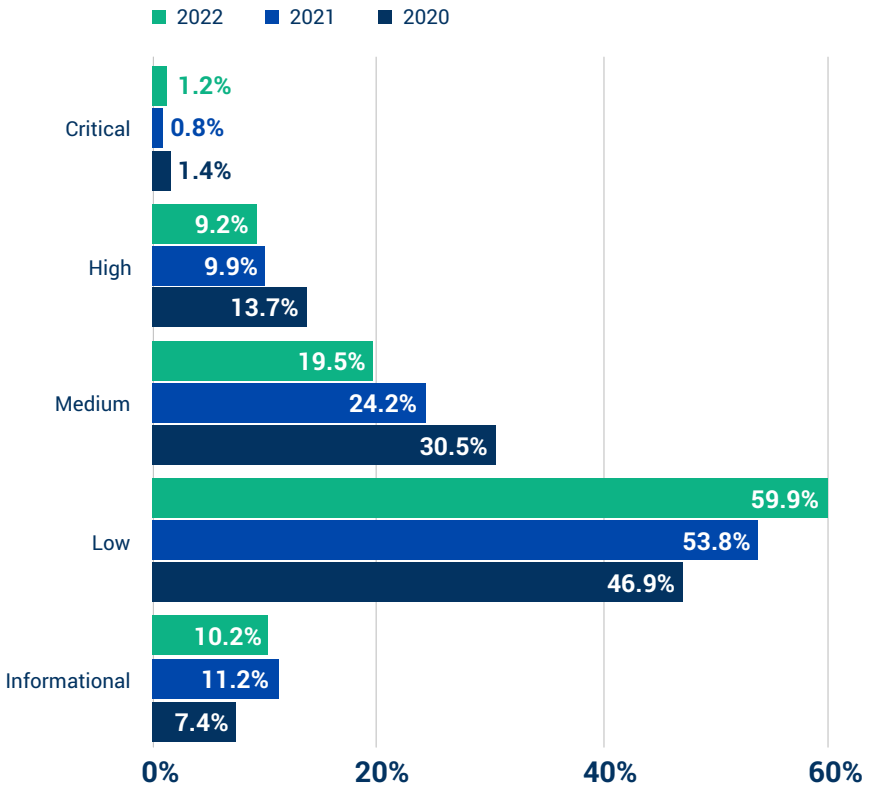
1. Stored Cross-Site Scripting (XSS)
2. Insecure Direct Object References (IDOR)
3. Outdated Software Versions
4. Insecure Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Protocols
5. Lack of Security Headers
6. Username / Email Enumeration
7. Reflected Cross-Site Scripting (XSS)
8. Insecure Cipher Suite
9. Fingerprinting / Banner Disclosure
10. Email-Triggering

2022

		% marked Critical/High/Medium severity
1.	Stored Cross-Site Scripting (XSS)	94%
2.	Outdated Software Versions	14%
3.	Insecure Direct Object References (IDOR)	85%
4.	Lack of Security Headers	2%
5.	Insecure Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Protocols	9%
6.	Insecure Cipher Suite	2%
7.	Fingerprinting / Banner Disclosure	0.6%
8.	Username / Email Enumeration	4%
9.	Email-Triggering	6%
10.	Descriptive Stack Trace	1.5%

Stored XSS and IDOR introduce high levels of risk.

As we work with customers to improve their security posture, we observe fewer and fewer vulnerabilities marked as high, medium, or critical severity. The majority of our 2022 findings were on the lower end of the risk scale, with nearly 60% being Low severity.



And yet, teams need to remain vigilant. In 2022 we discovered more than 16,000 findings, and while the majority posed minimal impact, two of the three most repetitive flaws — Stored Cross-Site Scripting and Insecure Direct Object References — had the potential for serious damage, with pentesters marking them frequently as Medium or High severity. We recommend proactively checking for these flaws, whether through internal reviews or via a targeted pentest.

Most Common Findings with Critical Severity	1	SQL Injection
	2	Remote Code Execution
	3	Using Default Credentials
Most Common Findings with High Severity	1	Stored Cross-Site Scripting
	2	Insecure Direct Object References (IDOR)
	3	SQL Injection
Most Common Findings with Medium Severity	1	Stored Cross-Site Scripting
	2	Insecure Direct Object References (IDOR)
	3	Reflected Cross-Site Scripting

A note on severity levels: Cobalt uses the OWASP Risk Rating methodology while calculating the severity of any reported finding. Where the application resides, what level of privilege is required, requirement for user interaction, business impact and many other factors which vary business to business determine a finding's exploit likelihood and impact. Hence, some findings will appear as the most common flaws for multiple risk levels.

Critical: Includes vulnerabilities such as administrative access, remote code execution, financial theft, and more.

High: Includes high probability vulnerabilities with a high business impact.

Medium: Vulnerabilities that are "Medium risk <> Medium impact," "Low risk <> High impact," or "High risk <> Low impact."

Low: Specifies common vulnerabilities with minimal impact on their own, but possibly dangerous if chained.

Informational: Notes vulnerabilities of minimal risk to your business.

Top vulnerabilities for different asset types.

Web App

- Stored Cross-Site Scripting (XSS)
- Outdated Software Version
- Insecure Direct Object References (IDOR)
- Lack of Security Headers
- Reflected Cross-Site Scripting (XSS)

API

- Lack of Security Headers
- Descriptive Stack Trace
- No Rate Limiting on Form
- Fingerprinting / Banner Disclosure
- Insecure Cipher Suite

Mobile App

- Lack of Jailbreak Detection
- Screen Caching Enabled
- Absent SSL Certificate Pinning
- User Password Persisted in Memory
- Lack of Obfuscation

Internal Network

- Outdated Software Version
- Using Default Credentials
- Insecure SSL and TLS Protocols
- Insecure Cipher Suite
- Fingerprinting / Banner Disclosure

External Network

- Insecure SSL and TLS Protocols
- Outdated Software Version
- Fingerprinting / Banner Disclosure
- Insecure Cipher Suite
- Using Default Credentials

Cloud Configurations

- Outdated Software Version
- Sensitive Application Data Stored Unencrypted
- Stored Cross-Site Scripting (XSS)
- Weak Password Policy
- Non-Sensitive Application Data Stored Unencrypted

(all data since 2017)

A large portion of vulnerabilities remain unaddressed at each severity level.

As we help customers remediate vulnerabilities, we can observe how teams react to these findings. The scenarios we see are:

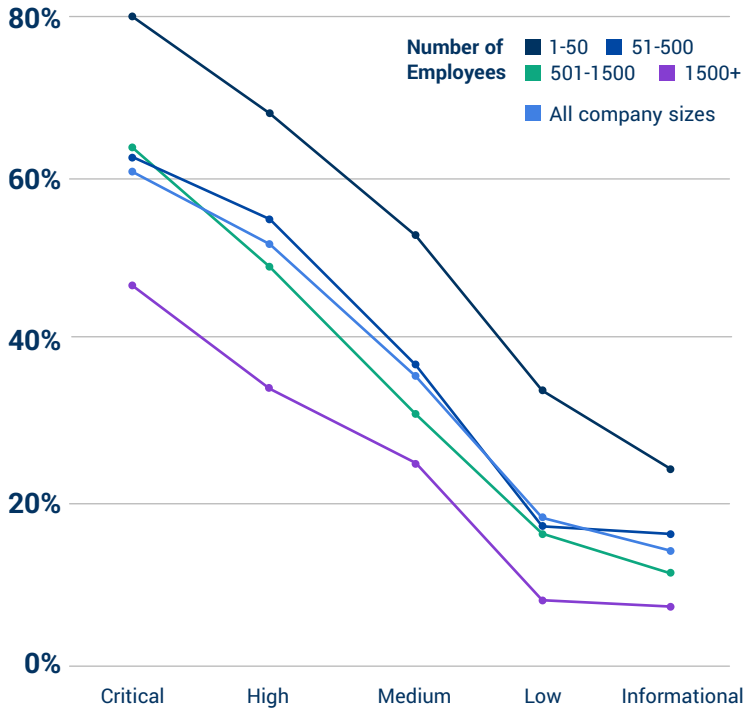
- Teams fix the finding and request a retest to confirm if the fix is working correctly (i.e. validate). Note that we offer retests on discovered findings for free, so there is no financial barrier.
- Teams mark the finding as “Accepted Risk” because its severity level doesn’t meet their remediation threshold, or a compromising control is in place.
- Teams don’t request a retest. The finding could have been remediated, but a retest hasn’t checked whether their fix is working. Alternatively, it’s staying in their backlogs for an indefinite period of time.

At the time of writing this report, customers had remediated, retested, and confirmed as fixed 25% of the findings we discovered in 2022. That number changes depending on a finding’s criticality and the customer’s company size.

For example, smaller companies of up to 50 employees have retested and fixed a sizeably larger portion of their vulnerabilities compared to larger organizations, although that figure does drop considerably with lower-risk findings. This is a trend we observe across the board, which in one part should not come as a surprise — teams have to prioritize, but they do leave themselves vulnerable to chained exploits from lower-risk findings.

What gives us pause is that just 61% of **critical** vulnerabilities in our database, regardless of company size, have been confirmed as fixed. That number drops to as low as 31% for medium-severity findings. This suggests a considerable security gap — despite their pentests, many organizations still remain at risk of a successful attack. In the next section, we dig deeper into what might be holding them back from strengthening their security postures.

Percentage of fixed and retested findings for 2022 per criticality level and company size.



25%

Of 2022 findings confirmed as fixed

39%

Of critical findings potentially untreated

Cobalt

PART 2

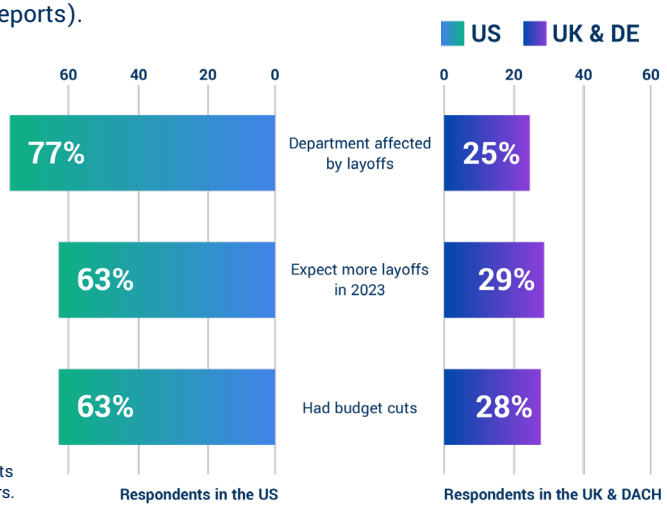
From Micro to Macro

How layoffs and budget cuts are impacting security teams' work.

Layoffs and budget cuts are prevalent in the US, applying more pressure compared to Europe.

Our data shows that, following the pressures of the pandemic-fueled Great Resignation in 2021, security teams now face additional industry headwinds. High employee turnover and scant bandwidth still hamstring productivity, with mounting pressure to restructure and cut costs amidst speculation of a downturn.

To best understand how security teams fare against these larger economic trends, we surveyed 1006 professionals in the field: 501 in the US, and 505 in the UK & Germany. To limit the scope of our research to the US felt shortsighted, and so we chose additional countries in an effort to better represent the global community (and hope to continue the shift in future reports).



To ensure unbiased results, no respondents were Cobalt customers.

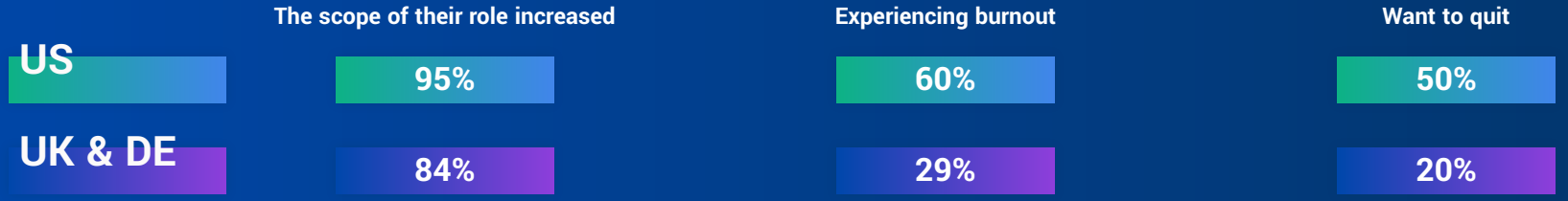
In the US, three-fourths of respondents share that their department had been directly impacted by company layoffs in the last six months. Roughly the same number (72%) said someone from their team had also resigned, and more than half expect further firings. In addition, the majority have been affected by hiring freezes (66%) or recruitment slowdowns (67%).

In the UK and Germany, we see a very different picture. Only one-fourth said their team had been affected by layoffs, less than half (44%) said a security colleague had resigned, and less than a third (29%) expect layoffs in 2023. However, the majority (61%) reported their company has announced a recruitment slowdown for 2023.

In the finance realm, just 28% of UK and German respondents shared their budgets had been cut. That figure was more than double for the US, and we see the same trend when comparing how large the cuts had been on average: 31% for the US, and 16% for the UK and Germany.

The contrast is striking, and it's challenging to pin this to one specific reason. Many factors can be at play, including differences in labor laws, fiscal strategies, and previous hiring decisions. But cybersecurity more often than not works as one large global ecosystem, where one breach can affect many — it's safe to say it's being put under considerable pressure.

Impact on cybersecurity practitioners whose teams have been affected by layoffs and budget cuts.



Cobalt

Many of the affected teams struggle to maintain high security standards.

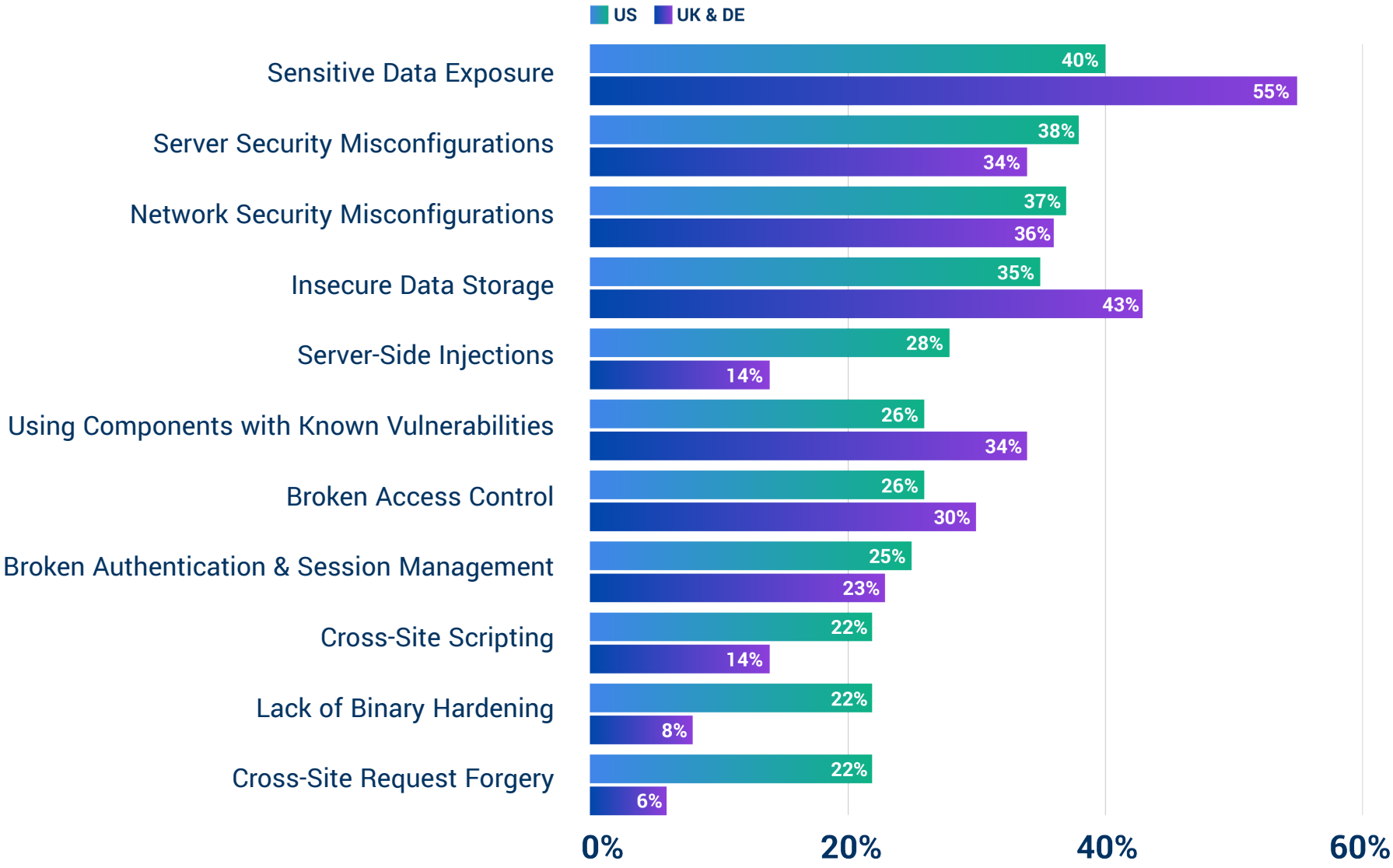
Where the similarities begin is how layoffs and budget cuts are impacting security teams' work. The vast majority of affected teams report their workloads have become unmanageable, and both sides struggle equally with maintaining security at a high enough standard.

Not only that, but a large portion of affected US respondents (73%, 15 points higher than UK & DE) shared they're struggling to monitor and respond to vulnerabilities and incidents. Their top-of-mind concerns are **Sensitive data exposure, Server security misconfigurations,** and **Network security misconfigurations**.

Teams in the UK and Germany have similar concerns, though they ranked **Insecure data storage higher** (see next page).

Cobalt

Which vulnerabilities is your security team most concerned about?



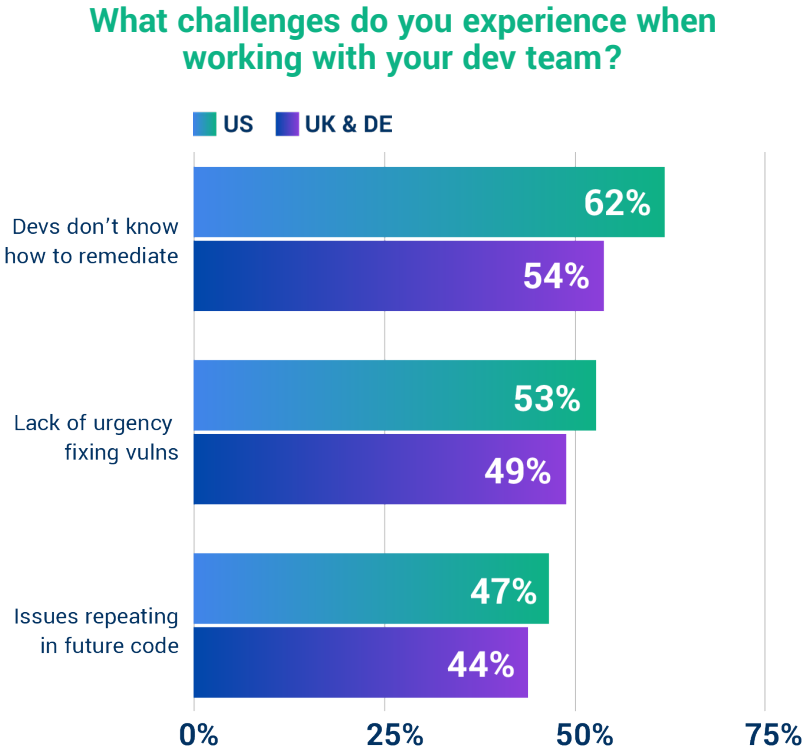
Cobalt

Fewer resources lead to more and more unaddressed vulnerabilities.

In the US, 89% of affected teams struggle to collaborate with their dev counterparts, whereas in the UK and Germany 59% reported this problem — 30 points lower than the US, but still a sizable portion.

Both sides complained equally that their dev teams show a lack of urgency in fixing vulnerabilities. For the US, this led to nearly all (96%) of affected respondents saying critical vulnerabilities get fixed more slowly, and more than three-fourths reported the same problem for high- and medium-severity vulnerabilities. Alarmingly, 76% said their backlog of unaddressed bugs increased in 2022 due to lack of resources, and 82% said they expect this problem to only worsen.

In the UK and Germany, teams were not as pessimistic, but the picture wasn't much improved. 79% shared that their dev team was slower to remediate critical vulnerabilities, and 65% expect the problem to worsen in 2023.



"Fewer resources led to a backlog of unaddressed vulnerabilities in 2022."

76% Agree

65% Agree

US

UK & DE

"I expect this problem to worsen in 2023."

82% Agree

80% Agree

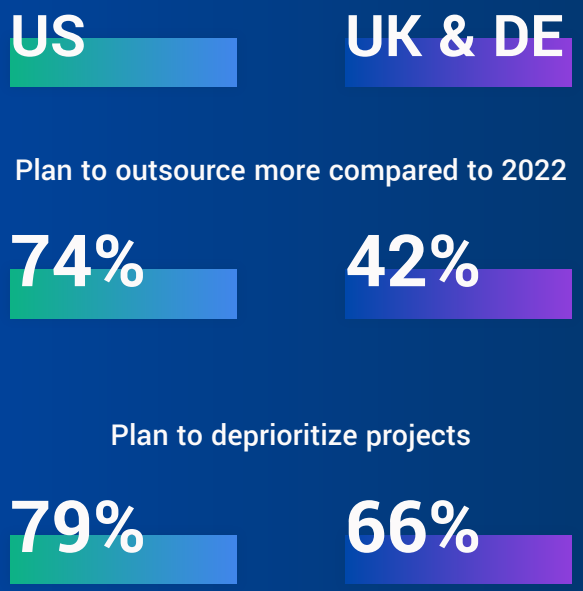
Cobalt

US teams plan to lean much more on third parties compared to their European counterparts.

When it comes to how teams will move forward, US respondents plan to outsource more work compared to 2022. At the top of their outsource list are addressing discovered vulnerabilities, vendor security reviews, and pursuing optional compliance certifications, e.g., SOC 2 or ISO 27001 (see next page).

As far as what they plan to deprioritize: the top projects to go are implementing DevSecOps practices (interestingly, UK and DE respondents plan to continue pursuing this through outsourcing), hiring, and adopting new technology.

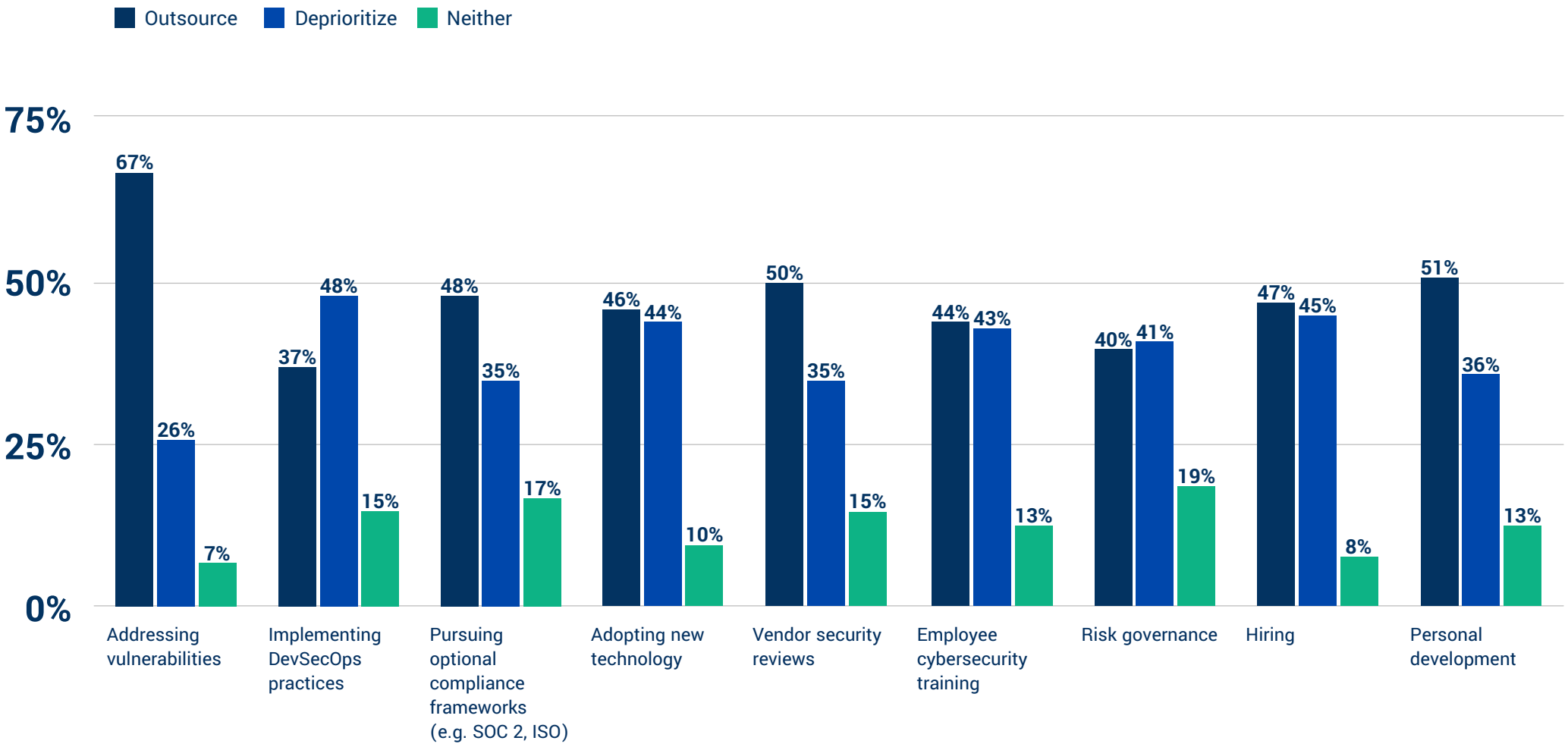
In the UK and Germany, respondents are leaning more towards deprioritizing (66%). Less time and fewer resources will go into adopting new technology, hiring, and personal development.



Deprioritizing business-critical projects can be a dangerous move: on one hand, you're trying to protect your team from burnout, but on the other, you're creating more opportunity for vulnerabilities to materialize or stay unaddressed, compromising the defenses around your organization. It's a tough balance to strike, and sometimes doing it alone is not the answer. A good external team can help balance the scales."

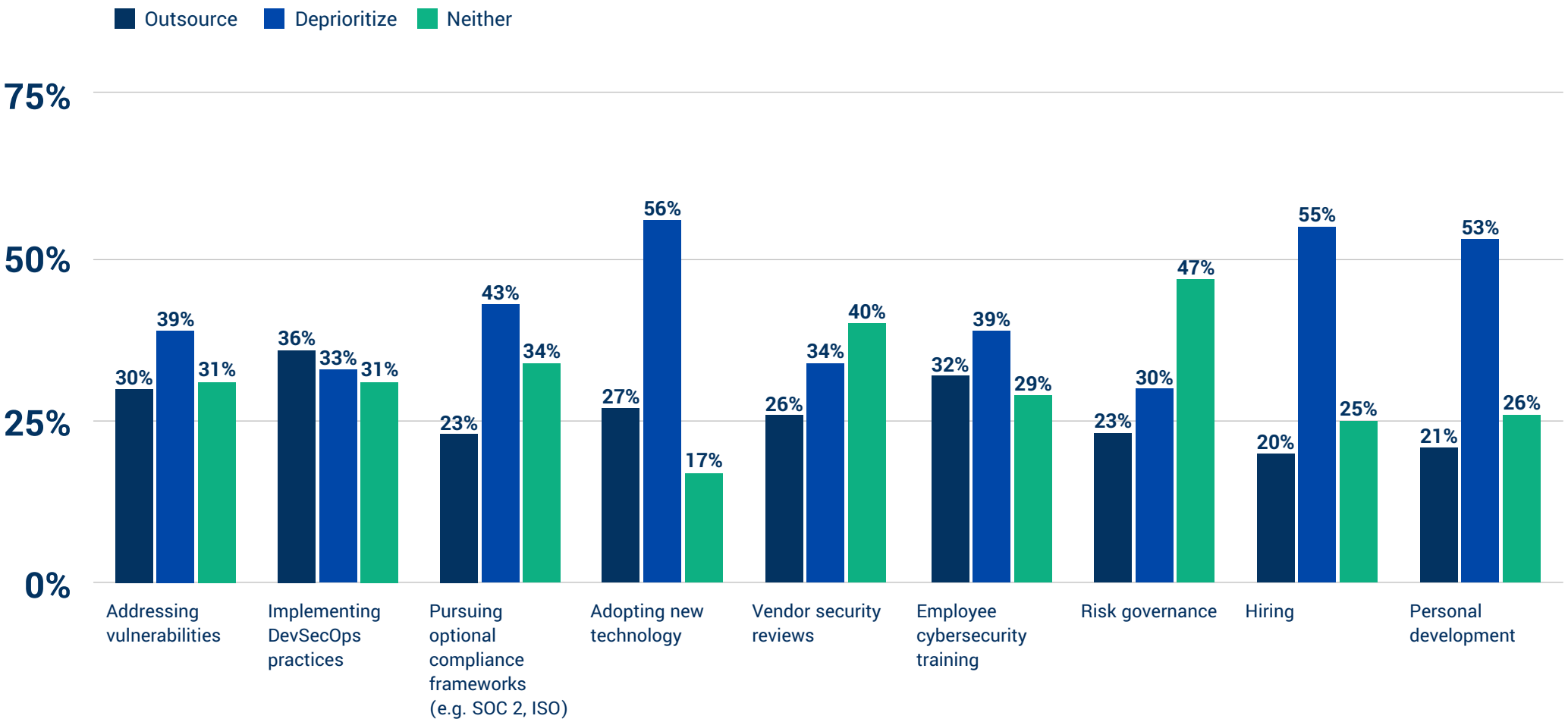
Caroline Wong Chief Strategy Officer at Cobalt

What teams in the US plan to outsource or deprioritize.



Cobalt

What teams in the the UK and Germany plan to outsource or deprioritize.



Cobalt

Teams struggle with preparing for their pentests and experience business disruptions.

Most security teams did between one and three pentests in 2022, but a much more sizable portion in the UK and Germany did more than six pentests.

In the US, compliance was the most common goal (48% selected, see next page), followed by fulfilling customer requests, and testing new features in their application.

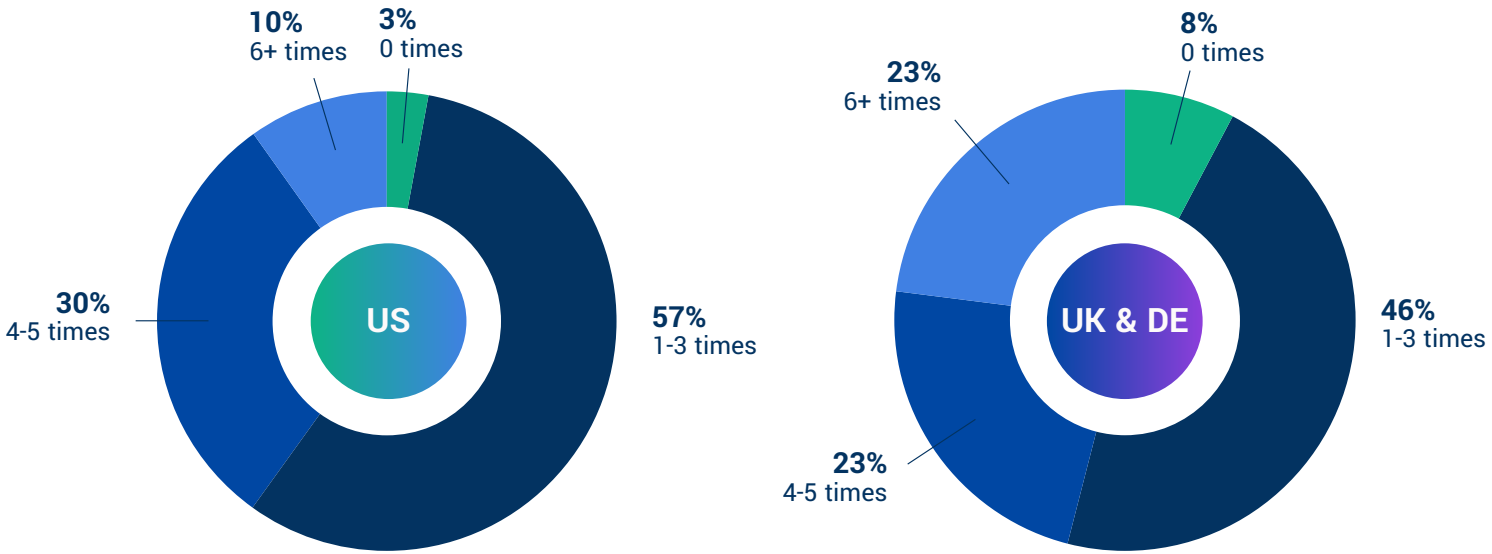
The top objectives in the UK and Germany were checking for specific vulnerabilities (66% selected), fulfilling a compliance requirement, and testing for cloud misconfigurations.

With time and resources in short supply, every pentest should deliver results quickly with no disruption to infrastructure. That, however, is not the case. More than half (62%) of US respondents said engagements with different vendors had disrupted their business operations, and 66% shared they had had to do unexpected clean-up after the test (not counting fixing vulnerabilities the tests had discovered).

In the UK and Germany, fewer complained of these challenges, but where they did struggle is preparing their environment accurately for the test.

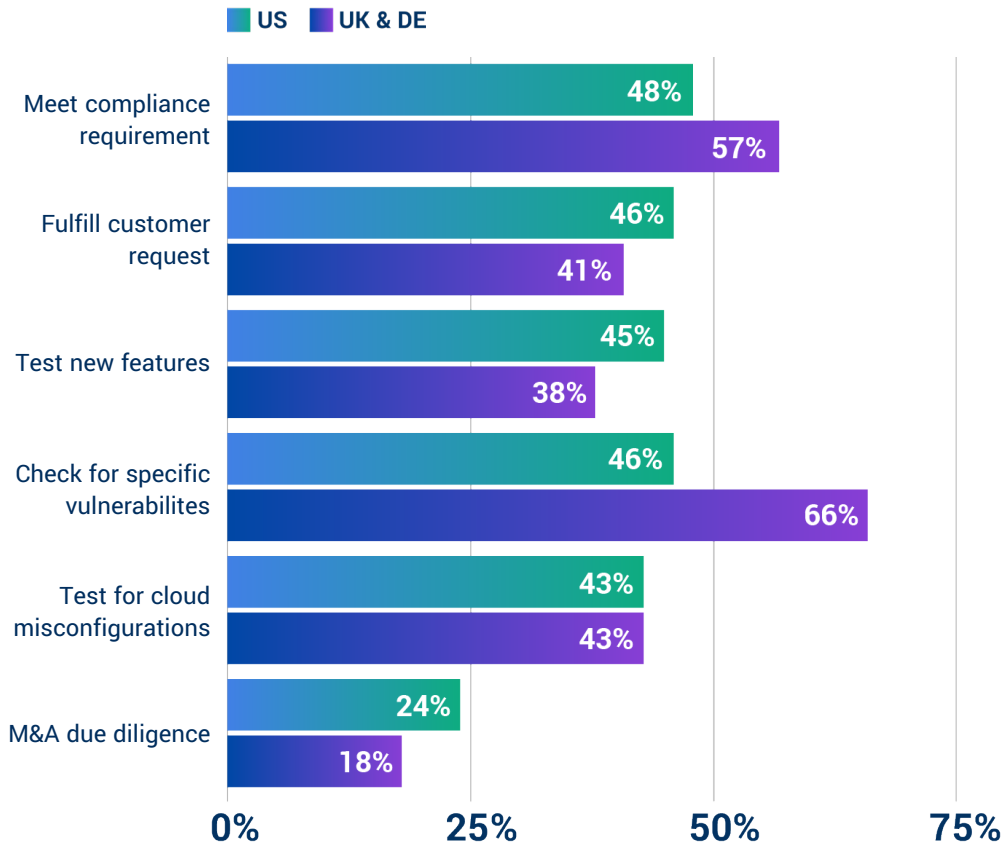
Teams are under pressure to achieve more with less, and an unproductive, disruptive pentest does not help them get closer to their goals. Your pentesting vendor should take charge and ensure tests run smoothly, but that's not to say things are entirely out of your control. In the next part of the report, we share practical steps on how to prepare for each test and extract maximum value, guided by insights from the Cobalt Core — our community of 400+ skilled and vetted pentesting professionals.

How often did you pentest in 2022?

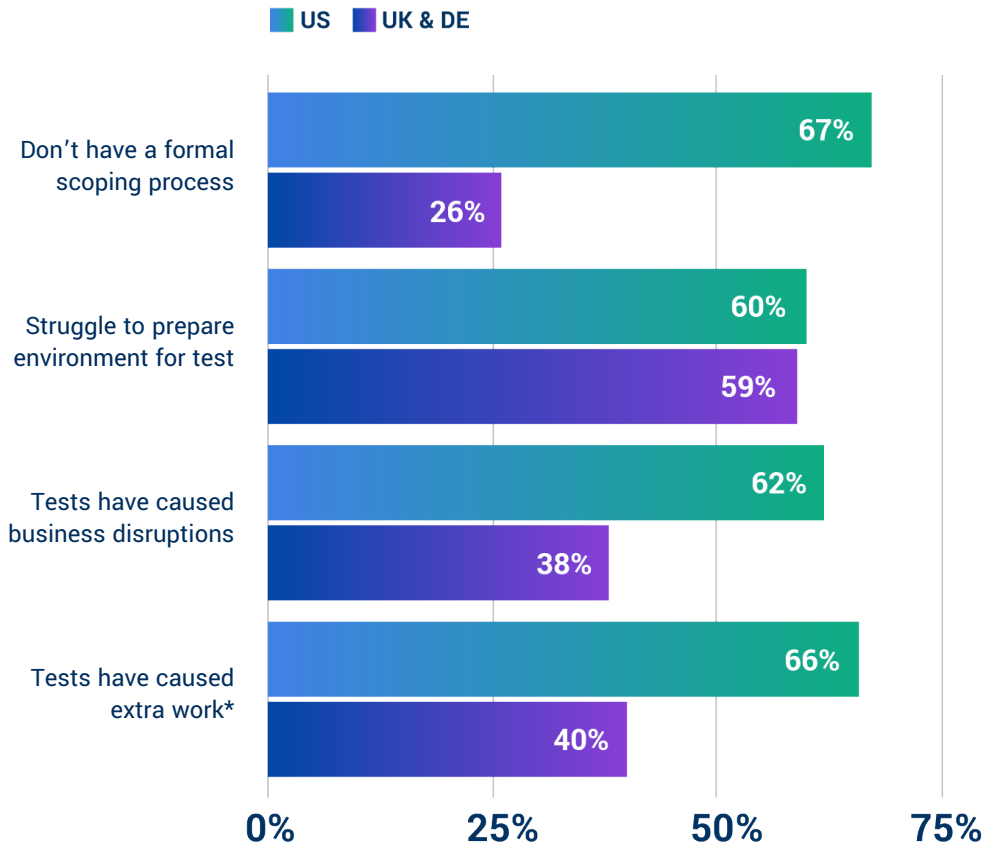


Cobalt

Which objectives does your team need to meet through penetration testing?



Which of the following challenges do you experience while managing pentests?



*not including fixing discovered vulnerabilities, but unexpected “clean-up” tasks after the test

Cobalt

PART 3

Set Up Your Pentests for Success

Recommendations from Cobalt's pentesters on how to prepare and maximize ROI.

Set up the pentest for success with a clear objective and accurate scope.

Out of the 3,100 pentests we did in 2022, the top areas that slowed the process down were:

- Testers lacking credentials or necessary access before the test starts
- Scope misalignment
- No active collaboration throughout the test
- Missing brief/asset information

We'll go over how your team can tackle each of these items, but let's start at the beginning: setting an objective and scoping the test correctly. Most of the time, unclear details in this stage are what leads to misalignments and business disruptions later on.

Start with a clear, achievable objective. Before you kick off your next pentest, align internally on what you want it to achieve, what needs to get tested, and are there areas testers should prioritize. It's important to do as much of this as you can *before* you kick things off with your vendor, because pentests are typically a time-bound exercise; once the clock starts ticking, clearing up details will cost you valuable time and resources.

A clear objective leads to an accurate scope, and an accurate scope means more targeted pentests. One of the first things that should happen when you approach your pentest vendor is to confirm your desired scope. To give pentesters the chance to test in depth, you should provide more than your application's URL or how many static/dynamic pages it has. Consider including more insight into the *complexity* of your asset, answering questions like:

- How many functionalities does your app support?
- What third-party services does your app call?
- How many user roles are there, or how many should the testers focus on?
- Are there any unique setup requirements pentesters should fulfill to follow your internal processes? (e.g. setting up MFA, dummy credentials, signing NDAs, etc.)

Having this information will help your vendor correctly estimate how many testers need to join the project, what skills are required, and how long the engagement should take. If not shared in the preparation stage, this information will still come up — only later, once the pentest has already started and hours go into recalibrating the project instead of analyzing your assets.

> If your internal stakeholders' expectations contradict each other, you may end up starting a white- or gray-box test, only to have to change it to a black-box exercise halfway through. The testers will no longer be in the right mindset and that will hurt results. Take 2-3 days to get everything aligned internally, and you'll have a much more productive pentest."

Tracy Harper

Lead Technical Project Manager at Cobalt

To-do list before the test starts:

1. Align all internal stakeholders on what the goal of your pentest is and what assets should be in scope — then communicate this information to your vendor.
2. Describe the in-scope assets with information on endpoints, URLs, number of static and dynamic pages, etc.
3. Include information on the complexity of your asset, covering the questions we suggest on this page for a more accurate scope — if you want a black-box test, these details don't have to reach the pentesters joining your project, but your vendor should still be aware in order to staff appropriately.

Familiarize the pentesters with how things are supposed to work.

Sometimes your goal will be to simulate an external attack through a black-box pentest, and there's definitely value in that exercise. However, it's important to note that no black-box pentest will perfectly simulate an external attacker. Pentests are time-bound, whereas externals can have unlimited time for reconnaissance. What's more, insider threats can be just as destructive. To capture more scenarios, we recommend a gray- or white-box pentest, where testers have access to documentation outlining setup, business logic, and internal knowledge.

Documentation gets the testers quickly up to speed and can range from diagrams to walkthrough videos to data flow charts — it all depends on how your asset is set up. For example, say you're pentesting for PCI DSS compliance: when testers know how you meant to segment your cardholder data environment from the rest of your systems, they can confirm whether that is in fact working correctly and can withstand attacks.

Documentation doesn't just make testers' lives easier — it also makes your findings more accurate, particularly their severity levels. When testers know the context around your assets and operations, they're able to determine a finding's likelihood and impact much more accurately, in a way that's customized to your circumstances. They can also get creative with your functionalities: instead of following the steps A, B, and C listed in your documentation, they can report if it's possible to jump from A to C, and whether that move can cause issues that expose sensitive information. Ultimately, giving your testers context enables them to deliver the value that makes pentests unique from scanners and other automated tools — you receive results that are specific to your situation and aligned to your business context.

And, you guessed it, you should provide documentation as part of your test prep, not throughout the testing process — otherwise you'll spend 2-3 days meant for testing on gathering paperwork.

> As pentesters, we see a lot of applications, and we have only a little bit of insight before we start on our next project. It really helps us focus when we know the main areas of the application, what exactly are the functionalities, and are users actually able to follow your logic flow without breaking things. This way we can confirm not only where someone external can attack, but also where an internal user might unknowingly create a vulnerability or flaw in your systems."

Goonjeta Malhotra

Security Researcher & Lead Cobalt Pentester

To-do list before the test starts:

1. Decide if you want to have a black-, gray-, or white-box pentest.
2. Share documentation on how your asset(s) are built, how they are meant to function, where data flows, etc.
3. Example documentation includes: walkthrough videos/demos, process diagrams, data flow charts, user role breakdowns, access control matrix.

Prepare a staging environment and your colleagues for the test.

Business disruptions happen most often when tests are taking place in a production environment. While a test on production will give the most accurate picture of your vulnerabilities, we recommend creating an exact mirror image on a staging environment and directing your pentesters there.

“Mirror image” is the important keyword here. If you have even a slightly outdated version of your application on staging, this can hurt your pentests’ results. When you request testers to replicate a discovered issue on production, you take time away from hunting for other issues. Not only that, but mixing environments makes your pentest report much more complex, which might complicate audits or conversations with customers reviewing your security.

In addition to preparing your environment, you should also prepare the credentials that will grant pentesters the access they need to continue with their work once they’re finished reviewing your app from an “unauthenticated” point of view – this is a stage most pentests will start with by default. Having credentials sorted out in advance saves you time during the pentest. This is especially true if the setup isn’t something you directly manage: going back and forth with your engineers can take 2-3 days from your pentest, wasting time and resources.

We understand that credential sharing can make teams nervous, both because they involve a high degree of trust, and because the process can get complicated. We recommend your team creates bogus credentials you can quickly spin up and disable after the test’s end. In addition, pentest vendors should mandate their testers to work via a VPN, so you can whitelist their IP addresses prior to the test’s start and monitor their requests. If a separate team is responsible for security monitoring, make sure they’re aware a test will be taking place so they don’t unknowingly block the testers from moving forward.

> In contrast to bug bounty, pentesting – in particular, PtaaS – encourages collaboration and professionalism, both with other testers as well as clients. I pentest to hone my skills, but also want to get high satisfaction ratings so I can pentest more, and earn more. So delivering on the concept of ‘value’ is extremely important. It’s something I wish more businesses were aware of so they could set engagements up for success at the outset. Our relationship is mutually beneficial.”

Gisela Hinojosa

Senior Security Consultant at Cobalt

To-do list before the test starts:

1. Set up a mirror image of your production environment and back up critical data.
2. Set up and share credentials with the testers.
3. Whitelist pentesters’ IP addresses.
4. Inform colleagues a pentest will take place and which IP addresses will be making requests.

Collaborate with the pentesters for a more productive test and better insights into your vulnerabilities.

You've gone through all the prep steps, provided documentation, set up your environment, and informed internal teams. The test has begun, and you can step back, right? Not quite.

Pentests are becoming more and more of a collaborative process, where the testers communicate directly with customers and share updates as soon as they find issues, especially high-severity ones. At least, this is how it works with Pentest as a Service.

Testers are highly-skilled security experts whose time you're paying for — take advantage of that. To squeeze every bit of value from your pentest, instead of completely stepping away, we recommend actively engaging with the testers, asking them questions around their findings and methodology, and just as importantly, answering their questions too. When testers discover unexpected behaviors, they reach out to confirm if this is an undocumented functionality, or in fact a flaw. If left unanswered, pentesters will continue with their next steps, but the results will likely lack important context. This creates extra work for you at the end of the test — whether to document why you're accepting the risk from a vulnerability your team doesn't consider an issue, or dispute findings altogether. It hurts results and your bandwidth.

Sometimes you might not have the answers and will need time to gather info from other internal teams. We recommend removing the silos between the pentesters and your colleagues, and not just those responsible for security — consider inviting members from the development team, who can answer technical questions and simultaneously learn more about their app's security. Add them to the Slack channel, comment thread, or email chain, whichever you're using with your vendor. This way, people have direct access to each other and can move things forward quickly — otherwise, you risk losing days of testing to internal alignment.

> Testers love customers who are proactive and quick to reply. Their enthusiasm motivates us to cover even more in our limited time frame. The more active the customer, the better the pentest results."

Harsh Bothra Lead Cobalt Pentester

To-do list before the test starts:

1. Establish a point of contact (POC) from your team who can liaison with the testers.
2. That POC should be responsive to the results of a pentest, analyze results, and ask questions if more info is needed.
3. The POC should also be available to help remove blockers slowing down the testers.

Key Takeaways

There's no sugarcoating it — security teams continue to face large-scale challenges in keeping their organizations safe. And yet, it's humbling to observe their resilience over the past 5 years with each State of Pentesting report. Whatever setback teams face, they find a way to adapt and move forward. We hope with this report practitioners can take away practical insights on how to strengthen their security posture and prepare effectively for each upcoming test. To summarize:

1

Server Security Misconfigurations like Lack of Security Headers, Insecure Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Cipher Suites, and Fingerprinting/Banner Disclosure continue to prevail in teams' asset portfolios. Despite their reputation as low-risk issues, we recommend checking for these flaws and proactively addressing them before they enable a more dangerous chain exploit. To tackle the highest severity findings, we recommend reviewing your assets for the possibility of SQL Injections and Remote Code Executions, along with Using Default Credentials, Cross-Site Scripting, and Insecure Direct Object References.

2

A large portion of teams in the US have been affected by layoffs, which in turn have compromised their security. More responsibilities and fewer resources have made workloads difficult to manage, and teams report larger backlogs of unaddressed security issues. While fewer in the UK and Germany said they were affected by layoffs, those who were reported similar struggles — overall, the global software and security ecosystem is at risk of one breach impacting many in a wide-reaching domino effect.

3

More often than not, pentests cause business disruptions. Teams can tackle this problem with a more strategic approach, where thorough preparation and collaborating closely with their pentest vendors can remove errors and significantly raise ROI without draining their budgets. You can find a preparation checklist on the next page.

Pentest Preparation Checklist

Setting the pentest's objective and scope (pg 21)

- [ ] 1) Align all internal stakeholders on what the goal of your pentest is and what assets should be in scope.
- [ ] 2) Describe the in-scope assets with information on endpoints, URLs, number of static and dynamic pages.
- [ ] 3) Include information on the complexity of your asset, covering the questions we suggest on page 21.

Familiarize the pentesters with how things are supposed to work (pg 22)

- [ ] 4) Decide if you want to have a black-, gray-, or white-box pentest.
- [ ] 5) If you want a gray- or white-box pentest, share documentation (walkthrough videos, demos, process diagrams, data flow charts, user role breakdowns, access control matrices) on how your asset(s) are built, how they are meant to function, where data flows, etc.

Prepare a staging environment and your colleagues for the test (pg 23)

- [ ] 6) Set up a mirror image of your production environment and back up critical data.
- [ ] 7) Set up and share credentials with the testers.
- [ ] 8) Whitelist pentesters' IP addresses.
- [ ] 9) Inform affected colleagues a pentest will take place and which IP addresses will be making requests.

Collaborate with the pentesters for a more productive test and better insights into your vulnerabilities (pg 24)

- [ ] 10) Establish a point of contact (POC) from your team who can liaison with the testers.
- [ ] 11) That POC should be responsive to the results of a pentest, analyze results, and ask questions if more info is needed.
- [ ] 12) The POC should also be available to help remove blockers slowing down the testers.

Methodology

Cobalt's State of Pentesting report includes two types of data sets:

1. Anonymized pentest data collected via Cobalt's proprietary Pentest as a Service platform (referred to later as "Cobalt's Pentest Data");

2. Survey responses from security teams, none of which are Cobalt customers (referred to later as "Survey Data")

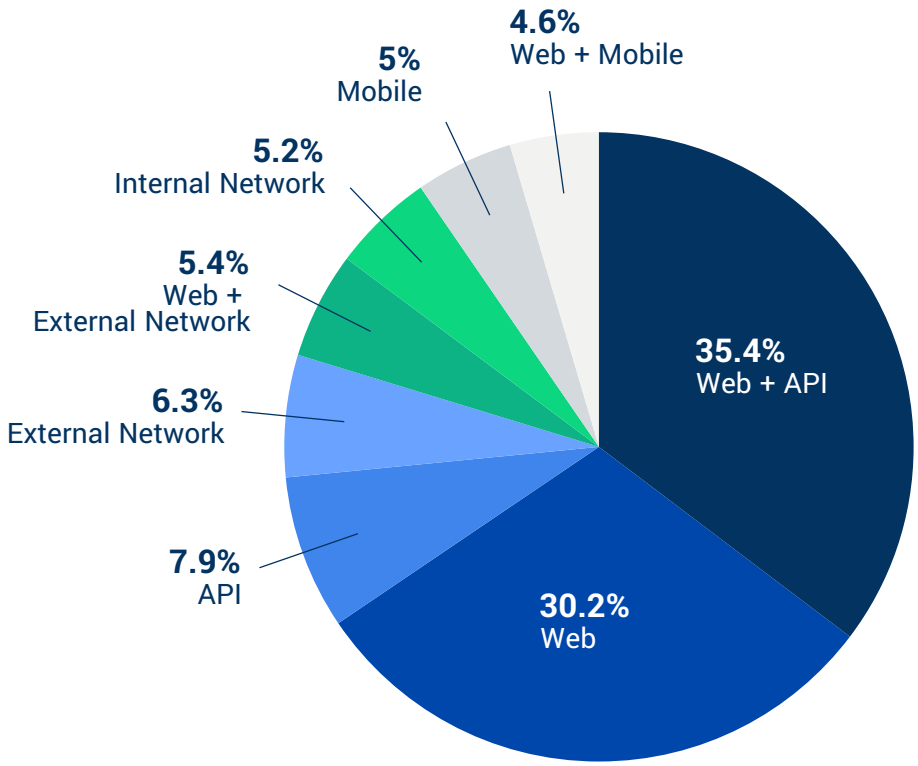
Cobalt's Pentesting Data

Between January 1st 2022 and December 31st 2022, our Penetst as a Service (PtaaS) platform collected data from 3,195 pentests that covered multiple asset types:

- **Web:** An online application. Includes APIs that supply data to the app.
- **API:** Application Programming Interfaces independent of a web app.
- **Mobile:** Any application intended for smartphones or tablets.
- **External Network:** Internet-facing components of a company's network, including external portals and website servers.
- **Internal Network:** Networked devices typically protected by a corporate firewall, including network shares and domain servers.
- **Cloud Configurations*:** Systems on "the Cloud," using services such as Amazon AWS, Microsoft Azure, or Google GCP.

**For top findings from our cloud configurations, we consolidated all the data we have since Cobalt began offering the service, in order to provide more in-depth insights.*

A portion of our pentests covered a combination of assets, such as Web and External Network. The data represents companies of varied sizes, from a variety of industries ranging from SaaS to Insurance and Fintech, and 4 geographic regions: EMEA, APAC, North America and South America.



Cobalt

Survey Data

We distributed an online survey to 1006 cybersecurity professionals across three different countries: the United States (501 participants), the United Kingdom (262 participants) and Germany (243 participants). To ensure an independent view, none of the participants were Cobalt customers. Participants work for companies with 200 or more employees, and come from the following

Industries

US

Information Technology and Services: 41%
Computer Software: 14%
Financial Services: 11%
Marketing & Advertising: 7%
Healthcare: 5%
Internet: 4%
Consumer Services: 4%
Education/eLearning: 4%
Media: 2%
Retail: 2%
Other: 2%
Government Administration: 1%
Insurance: 1%
Agriculture: 1%
Real Estate: 1%

UK & DE

Information Technology and Services: 41%
Computer Software: 16%
Other: 6%
Education/eLearning: 5%
Financial Services: 5%
Government Administration: 5%
Healthcare: 5%
Internet: 5%
Consumer Services: 4%
Marketing & Advertising: 3%
Media: 2%
Insurance: 2%
Real Estate: 1%
Retail: 1%
Agriculture: 0%

Job Titles

US

IT Security Governance: 24%
Data Security Manager: 15%
Manager Offensive Security: 10%
Other: 7%
Cloud Security Manager: 6%
Head of Information Security: 6%
Head of Security: 5%
Product Security Manager: 5%
Security/Risk/Compliance Manager: 5%
Infrastructure Security Manager: 4%
Head of Penetration Testing: 3%
Vulnerability Management: 3%
Head of AppSec: 2%
Director Data & Cloud Security: 1%
AppSec Manager: 1%
SOC Manager: 1%
CIO: 1%
CISO: 1%
CSO: 0%

UK & DE

Other: 26%
Data Security Manager: 16%
IT Security Governance: 13%
Product Security Manager: 8%
Security/Risk/Compliance Manager: 8%
Cloud Security Manager: 6%
Vulnerability Management: 6%
Head of Information Security: 4%
Infrastructure Security Manager: 4%
AppSec Manager: 2%
CSO: 1%
CIO: 1%
Head of Penetration Testing: 1%
Head of Security: 1%
Director Data & Cloud Security: 1%
Manager Offensive Security: 1%
SOC Manager: 1%
Head of AppSec: 0%
CISO: 0%

Cobalt's Take on PtaaS

Cobalt provides manual pentesting delivered through a SaaS platform for security and development teams. Cobalt leads the industry by providing large enterprises with direct tester collaboration during each engagement, integrations into development workflows, and a centralized view of pentest data over time.

Start Testing Faster

Launch pentests in days, not weeks, with our intuitive platform and team of on-demand security experts.

50%

Faster to execute a pentest than traditional consultancies.

Remediate Risk Smarter

Accelerate find-to-fix cycles through technology integrations and real-time collaboration with pentesters.

400+

Highly vetted pentesters around the world.

Make Security Stronger

Mature your security program through a scalable, data-driven approach to pentesting

24 hours

To get a pentest up and running.

> "The main benefits that we get from Cobalt are speed, scalability, and repeatability. We're able to quickly launch and execute pentests; and beyond that, we're able to see individual findings in real time and relay them to the engineering team so they can start triaging immediately."

Eric Galis Chief Information Security Officer at Cengage

Cobalt for End-to-End Security Testing

Cobalt's Pentest as a Service (PtaaS) platform is paired with an exclusive community of testers to deliver the real-time insights you need to remediate risk quickly and innovate securely. The flexible, on-demand consumption model enables security and development teams to proactively meet modern pentesting needs.

"Datto's pentesting program is evolving by using Agile Pentesting, as we're able to schedule more pentests and allow ourselves to only look at the delta between the last pentest that was run and the newer pentest that would then occur. This gives us a better idea of what has already been tested and only focuses on the newer portions instead of always going to the same parts of the product that may not have changed over the course of a year, six months, or three months."

Jeremy Galindo

Offensive Security Manager, Enterprise SaaS Company

Interested in learning more?
Visit us today at www.cobalt.io

Offerings Portfolio

Comprehensive Pentesting

Broad testing scope that encompasses all vuln categories across an entire asset.

- Meet or maintain compliance frameworks, such as SOC 2, ISO 27001, PCI-DSS, CREST, and HIPAA
- Adhere to a customer or third-party attestation request
- Identify and eliminate any risks in an M&A transaction

Agile Pentesting

Targeted testing scope focused on a specific area of an asset, or a specific vuln across an asset.

- Test a new release or code change before it reaches production
- Validate fixes on a single vuln or small subset of vulns across an asset
- Target a single OWASP category for a web/mobile/API asset

Professional Services

Strategic guidance and partnership to take your security program to the next level.

- Code Reviews
- Red Teaming
- Phishing Engagements
- Threat Modeling
- Pentest Program Management
- And more!

Cobalt